LEWIATAN

Warszawa, 27 kwietnia 2026 r.
KL/294/78/ET/2026

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w nawiązaniu do przekazanego stanowiska Konfederacji Lewiatan z dnia 17 kwietnia br. w sprawie unijnego aktu o cyberbezpieczeństwie, w załączeniu przekazujemy uzupełnienie postulatów.

Z poważaniem

Marek Górski
Prezydent Konfederacji Lewiatan

Załącznik: Uzupełnienie stanowiska Konfederacji Lewiatan w sprawie aktu o cyberbezpieczeństwie

Do wiadomości:

1) Pan Łukasz Wojewoda, Dyrektor, Departament Cyberbezpieczeństwa, Ministerstwo Cyfryzacji
2) Pan Marcin Domagała, Naczelnik, Wydział Współpracy Międzynarodowej w obszarze cyberbezpieczeństwa, Departament Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

Uzupełnienie stanowiska Konfederacji Lewiatan z dnia 17 kwietnia br. w sprawie aktu o cyberbezpieczeństwie

I. General remarks

1. Title II. Mandate of ENISA

We support strengthening ENISA's mandate as an independent, technical, and advisory body while providing supplementary resources for its ever evolving mission.

The Cybersecurity Act should take a bolder stance by formally integrating ENISA into the decision making process. The EU should look for an inspiration on how to do it within its own governance framework. The European Data Protection Supervisor (EDPS) – for instance- is empowered to issue opinions on its own initiative regarding any legislative proposal with data protection implications. While its opinions are non-binding, they carry significant institutional weight and ensure that data protection is not an afterthought, but a core consideration from the outset. Granting ENISA with a similar mandate would enable the agency to review legislative initiatives and issue reasoned technical opinions without a formal request from the Commission. Although EU lawmakers would retain full political discretion their decisions would be informed by independent expert analysis of cybersecurity impacts.

To further expand on the above however, we believe there is a need in this mandate revision to introduce a "secure-by-design" approach to policymaking by institutionalizing Security Impact Assessment (SIA) as a part of ENISA's technical advisory role.

The Security Impact Assessment (SIA) is a structured process that identifies, analyses, and evaluates the security implications of a proposed tech policy or legal instrument before its implementation, as well as, as appropriate, provides continuous security oversight during the implementation phase of policies and interventions.

We strongly believe that ENISA is uniquely positioned to provide this technical/advisory expertise in a form of the SIA necessary to translate legislative intent into secure operational reality. It is also in line with ENISA's mandate to raise the common level of security.

We believe that "secure-by-design" is a prerequisite for Europe's resilience and defence. Just as technology itself should undergo rigorous threat modeling from the design phase onward

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

and this notion has been strongly integrated into EU's cybersecurity legislation (e.g., CRA), we need to advocate a mindset in public policy that takes security into account at every step in the legislative or regulatory process. Societies and Europe's resilience at large will benefit from a more balanced approach to regulation which ensures security risks are evaluated alongside other imperatives like economics, sustainability and fundamental values.

2. Title III. European Cybersecurity Certification Framework

We welcome the revision of the European Cybersecurity Certification Framework (ECCF). The revised framework introduces several structural improvements that provide much-needed predictability, agility, and international alignment.

Most importantly, we strongly welcome the clear delineation established in the text, which clarifies that the ECCF remains strictly focused on mitigating technical risks related to ICT products, services, and processes. Consequently, non-technical risks are appropriately left to the separate, dedicated Supply Chain Framework. Maintaining this structural separation is absolutely vital for preserving the objective, technical integrity of the European cybersecurity certification process.

We also support the established transition mechanism, which guarantees that existing certificates issued under national schemes (such as SecNumCloud) "shall remain valid until their expiry date". This "grandfathering" clause is vital for protecting past investments and ensuring legal certainty for vendors. To further smooth this transition, we recommend that the date for phasing out national schemes like SecNumCloud be conditional on the readiness of the European ecosystem and with clarity on dates.

Lastly, while we strongly support the Commission's stated ambition to enhance transparency and stakeholder engagement throughout the planning, development, adoption, and maintenance stages of certification schemes, the practical mechanisms proposed in the revised framework fail to deliver on this objective. Specifically, the proposal appears to replace the standing Stakeholder Cybersecurity Certification Group (SCCG) with a "European Cybersecurity Certification Assembly". The Assembly is mandated to meet only "at least once a year" with a loose mandate to "discuss strategic priorities". Moving from a permanent industry stakeholder expert group to an annual, large-scale assembly significantly reduces the industry's ability to provide continuous, detailed, and structural input into the planning of new schemes and the overall governance of the framework. This appears as a dilution of already scarce industry input and needs to be seriously reconsidered.

LEWIATAN

3. Title IV. ICT Supply Chain Framework

We understand the necessity to reinforce the security of Europe's ICT supply chain. However, the proposed in CSA2 ICT supply chain framework lacks significant procedural clarity and legal certainty in various areas – proposal in this area would impose unprecedented financial, operational and investment impacts on the European telecommunications sector, without sufficient justification or proportionate risk assessment.

The proposal significantly departs from existing Member State frameworks that have already guided long term investment decisions and ensured legal certainty. Instead of regulatory simplification, CSA2 introduces additional non technical, sector specific obligations for telecoms, further increasing regulatory complexity and undermining planning stability.

Critically, the impact assessment underpinning the proposal is not sound. It relies heavily on the 5G Cybersecurity Toolbox, despite fixed and satellite networks being outside its original scope. The proposals do not reflect real world deployment experience and depart from the risk based, horizontal approach embedded in NIS2 Directive. Telecom operators are uniquely singled out for fast tracked and immediate removal obligations, without adequate justification.

The proposal also fails to properly recognize alternative risk mitigation measures such as multi vendor and diversification strategies, despite these being explicitly endorsed by the 5G Toolbox and EU competition principles. Horizontal vendor exclusion risks undermining diversification objectives and may inadvertently increase systemic risk. Moreover, the envisaged full removal across both fixed and mobile networks goes far beyond what is necessary and proportionate, particularly compared with targeted measures focusing on genuinely critical network elements.

Large scale 'rip and replace' exercises of this nature will inevitably disrupt service quality, network resilience and operational stability, while severely constraining operators' ability to invest in future technologies. The impacts on innovation, 6G readiness, resilience and customer outcomes are significantly underestimated.

At a time when Europe must accelerate digital infrastructure deployment to remain globally competitive, forcing operators to divert scarce capital and skills to large scale replacements would be economically and strategically counterproductive. The proposed timelines also contradict realistic investment and deployment cycles of at least ten years, undermining

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

legal certainty and potentially overriding national security decisions already being implemented by Member States.

Overall, the CSA2 supply chain approach risks placing Europe at a lasting competitive disadvantage by diverting resources away from innovation, delaying new network roll outs and weakening the continent's ability to keep pace with global technological progress.

We strongly believe that predictability, proportionality and legal certainty are of utmost importance for the mechanism to deliver on its intended goals without negatively impacting Europe's competitiveness and security.

Therefore we are keen to share our thoughts and ideas on several issues to improve the current draft framework. Notably, however, many more elements in the draft text should be revised for legal clarity and certainty of the process.

The framework also allows the Commission to impose severe measures (like blanket bans) without mapping them to specific risk levels (Article 103). We therefore ask to introduce a "Severity Matrix" that legally restricts high-impact prohibitions strictly to critical risk scenarios, using lighter measures (like audits) for lower risks.

The emergency procedure in the same Article allows the Commission to bypass formal risk assessments based on vague criteria like "sufficient reason to consider" and undefined "exceptional circumstances," applying severe, permanent sanctions across the EU if just meaningful group of Member States are affected. These shortcomings could be addressed by replacing "sufficient reason" with "substantiated evidence", explicitly defining "exceptional circumstances" (e.g., imminent threat to essential services or large-scale exploitation), increasing the threshold to a "significant number of Member States" and explicitly stating that any emergency measures and resulting sanctions are strictly provisional until a full risk assessment is completed.

Finally, failing to provide requested information, which might be due to conflicting domestic laws in the supplier's home country, trade secrets, or simple administrative failure, automatically results in a high-risk designation, reversing the burden of proof (Article 104). It should rather be clarified that failure to provide information can trigger a detailed investigation or be used as one factor among others, but cannot serve as the sole basis for a high-risk designation and the Commission must still affirmatively prove control.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

Designating key ICT assets is one of the most important elements of supply chain procedures. Article 102(2c) appropriately emphasizes the need to examine whether there is a dependency on a limited number of suppliers of these assets. Similarly, in the case of issuing regulations containing mitigating measures (Article 103), the Commission should investigate the availability of alternative suppliers to high-risk ones.

However, Articles 110 and 110 introduce exceptions to these general principles, which we consider unjustified. The CSA2 draft explicitly provides both a list of key resources and mitigating measures within its text. Consequently, for the electronic communication sector, this approach abandons the assessment of critical elements that determine the actual feasibility of decisions related to so-called HRV.

Appropriate analysis of the availability of alternative solutions should be conducted each time and, equally importantly, within a timeframe that is coordinated with the process of determining whether the resources are key and whether the supplier is classified as high-risk. Therefore, the same principles should be applied to the scope covered by Articles 110-111 as are applied to other sectors. This analysis should also consider the necessity of implementing multi-vendor strategies under conditions that ensure market competition.

Preliminary and timely assessment of this area is therefore essential to ensure that entities affected by the designation of high-risk suppliers (HRV) will be able to implement these decisions under the new market conditions across the entire EU, including maintaining pricing, deadlines and quality standards. This is particularly important since these entities—rather than the suppliers—will bear the risk of financial penalties related to deadline breaches.

We also note that the 36-month withdrawal period specified in Article 110(3) is shorter than the four-year period deemed appropriate under regulations adopted in Poland. In cases where equipment needs to be replaced across the entire EU rather than in a single country, the risk of negative impacts on contracting possibilities justifies the introduction of longer deadlines, or the possibility to extend them upon a justified request, or alternatively, the implementation of a review mechanism for the already established deadline. These concerns also support the idea of avoiding rigid deadlines within the regulation itself. More flexible measures may be necessary to address these issues.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

4. The multiple of implementing acts hinders legal certainty for companies

CSA2 empowers Commission to issue vast list of implementing acts. None of those were yet drafted, consulted or assessed in terms of costs and impact on the market. This makes it impossible for any stakeholders (incl. businesses and capitals) to assess the final scope of CSA2 which will be largely decided in those implementing regulations.

• Art. 47(5) - detailed rules relating to determining the fees to be levied by ENISA

• Art. 74(9) - implementing acts providing for a European cybersecurity certification scheme for ICT products, ICT services, ICT processes

• Art. 81(5) - implementing acts laying down common principles and model provisions for elements set out in paragraphs 1, 2 and 3 across European cybersecurity certification schemes

• Art. 85(5) - implementing acts specifying procedures for prior approval or general delegation models

• Art. 89(6) - implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to peer review

• Art. 92(8) - implementing acts to lay down the procedures, including on cross-border cooperation, for authorisation of conformity assessment bodies

• Art. 93(3) - implementing acts to lay down the circumstances, formats and procedures for notifications (…) of the conformity assessment bodies that have been accredited and, where applicable, authorised

• Art. 100(2) - by means of an implementing act, designate that third country as a country posing cybersecurity concerns to ICT supply chains

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

• Art. 102(1) - implementing acts identifying key ICT assets used for the manufacturing of products or the provision of services by entities of the type referred to in Annexes I and II to Directive (EU) 2022/2555.

• Art. 103(1) - implementing acts establishing, where necessary to ensure high level of cybersecurity, cyber resilience and trust within the Union, that specific type of entities referred to in Annex I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate in any form ICT components or components that include ICT components from high-risk suppliers

• Art. 103(2) - implementing acts establishing, where necessary to ensure a high level of cybersecurity, cyber resilience and trust within the Union, that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be subject to one or several of the following mitigating measures in relation to their ICT supply chain and in particular to key ICT assets

• Art. 103(7) - implementing acts to establish that specific type of entities referred to in Annexes I and II to Directive (EU) 2022/2555 shall be prohibited to use, install or integrate ICT components or components that include ICT components from an entity referred to in paragraph 6.

• Art. 104(1) - implementing acts, the Commission shall establish lists of high-risk suppliers relevant for the prohibitions laid down in the implementing acts adopted in accordance with Article 103(1), Article 103(7) or the prohibition referred to in Article 111(1)

• Art. 105(3) - implementing acts to further specify the conditions related to the reasoned request of an entity established in or controlled by entities from a third country posing cybersecurity concerns to the Commission to be exempted

• Art. 109(4) - implementing acts laying down detailed rules relating to the fees, specifying the amount of the fees and the way in which they are to be paid

• Art. 110(4) - implementing acts in accordance with Article 118(2) to specify the time periods for the phasing out the ICT components or components that include ICT components provided by high-risk suppliers with regard to fixed and satellite electronic communications networks

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

In the case of such far-reaching regulations, particular care must be taken to ensure appropriate consultation mechanisms for all stakeholders (public and private) regarding the proposed provisions, together with adequate timelines for assessments and the submission of positions.

5. Directive on simplification measures and alignment with the Cybersecurity Act

We welcome the targeted amendments to the NIS 2 Directive, together with the earlier Digital Omnibus package. The stated ambition to reduce market fragmentation, lower compliance costs, and build a more resilient and cohesive digital single market is one we strongly share.

However, while the intent is clear, we believe the current proposals still miss a critical opportunity to deliver the deep, structural cyber simplification that the European industry urgently needs. For example, the targeted amendments to NIS 2 fail to meaningfully address long-standing industry concerns regarding complex and overlapping reporting requirements. To truly unlock resources for operational cybersecurity rather than administrative paperwork, more must be done.

DORA was just implemented. The NIS2 and CER directives are still being implemented in most countries. At the turn of 2025/2026, a number of new initiatives related to security have already appeared: changes to NIS2 regarding reporting, new CSA2, the announced certification schemes for managed cybersecurity services, a targeted amendment to NIS2, the DNA (resilience measures for electronic communications), and a series of “soft-law” documents concerning drone security, submarine cables, and the ICT supply chain. Some of these already signal further thematic clarifications to be included in implementing acts, plans, or recommendations. Many of those (as CSA2 in particular) give EC power to issue new implementing or delegated acts in the future. CRA (and previous RED2 and more general GPSR) is just behind the corner. On top of that national cybersecurity strategies adopted under NIS2 are also signaling further changes in the regulatory environment at the national level.

From the perspective of the entities targeted, even monitoring, analyzing and addressing cybersecurity requirements - or simply monitoring how they change - is becoming an increasingly significant burden, requiring the allocation and maintenance of dedicated resources. In this context, it becomes increasingly challenging - and therefore more costly - to clearly and precisely define a stable set of requirements and to demonstrate compliance

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

with them. This is why we call for in-depth analysis of security related legislation focused on the possibility to introduce real simplification, especially for the digital sector which is covered directly or indirectly (supply chain) by all those legislative initiatives.

In addition, the CSA proposal correctly notes that European cybersecurity certification should generally remain voluntary. It is imperative that it stays that way and we strongly caution against any move to make "cyber posture" certification mandatory under the NIS 2 regime.

For entities operating across multiple Member States, navigating disjointed national supervisory approaches and duplicative security audits drains critical resources that should be spent on operational resilience. We therefore strongly advocate for the establishment of a "single audit" principle across the internal market.

We also welcome the introduction of the maximum harmonisation principle to the NIS2 Directive. For entities operating cross-border, the assurance that compliance with Union-level implementing acts fully satisfies national requirements, without the risk of additional, fragmented "gold-plating" by Member States, is vital. To fully realize the benefits of the maximum harmonisation principle, we call for its explicit extension to Electronic Communication Services (ECSs). We also advocate for the inclusion of ECS in a true "one-stop-shop" reporting mechanism.

New article 37a on ENISA's role in mutual assistance obliges ENISA to conduct comprehensive analysis of cross-border cybersecurity risks relating to essential and important entities. Article 37a(4) mandates Member States to provide ENISA with list of cybersecurity-risk management measures taken by the essential or important entity in accordance with Article 21, a list of supervisory or enforcement actions carried out, as well as the relevant documentation including evidence of implementation of cybersecurity policies, such as the results of security audits, that the competent authorities. In this way, ENISA could effectively build profiles of specific essential and important entities that provide services across more than one Member State - or that provide services in one or more Member States while having their network and information systems located in one or more other Member States. In this regard, we emphasize, on one hand, the necessity of maintaining the highest level of confidentiality for such data sets. On the other hand, we urge that the execution of these tasks should not entail the introduction of additional reporting obligations for the essential and important entities.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

II. Specific amendments

Original Text	Lewiatan's Proposal
Mot. (9) The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support Member States in the consistent implementation of Union policy and legislation regarding cybersecurity and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States.	**Mot. (9)** The mission of ENISA should be to support Member States and Union entities to achieve a high level of cybersecurity, resilience and trust in the Union. To that end, ENISA should act as a reference point for advice and expertise on cybersecurity, and its work should primarily revolve around four key areas of cybersecurity at Union level. First, ENISA should support **the Union and** Member States in the consistent **elaboration** ~~implementation~~ of Union **policies and drafting of legislation, as well as their implementation** ~~policy and legislation regarding cybersecurity~~ and assist Member States through capacity-building activities to continuously improve their capacities in terms of preparedness, resilience and response. Second, ENISA should contribute to operational cooperation at Union level, amongst Member States, and to enhanced shared situational awareness of cyber threats and incidents among Member States and Union entities. The third key area should be cybersecurity certification and standardisation, while the fourth should be the implementation of the Cybersecurity Skills Academy, which should contribute to the development of a thriving European cybersecurity workforce with skills that should be portable across Member States. **Justification** ENISA can support both EU Member States and EU institutions.
Mot. (15) ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.	**Mot. (15)** ENISA acts as a reference point for advice and expertise on cybersecurity. Therefore, at the Commission's request **or at its own initiative**, ENISA should assist it by means of expertise, technical advice, information, analyses, including feasibility studies, opinions and preparatory work regarding any specific matter in the field of cybersecurity with a view to informing the Commission's policymaking **and legislative proposals** and facilitating the Commission's monitoring of the implementation of Union legislation regarding cybersecurity.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

	Justification Our proposition ensure that ENISA can independently issue opinions on the cyber-security impact of Union legislation.
Section 1 (title) Support for implementation of Union policy and law	**Section 1 (title)** Support for **the drafting and** implementation of union policy and law **Justification** ENISA should not only be consulted for the implementation of EU policy, but also in its making.
Article 4(3) ENISA shall provide its expertise and assist the Commission in developing Union policies and legislation related to cybersecurity.	**Article 4(3)** ENISA shall ~~provide its expertise and assist the Commission in developing Union policies and legislation related to cybersecurity.~~ **advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the cybersecurity impact on Union policies, legislation and implementation;** **Justification** Our proposition replicates language that already exists in Art. 58 (3c) of Regulation 2018/1725. This ensure that ENISA can independently issue opinions on the cyber-security impact of Union legislation
Article 5(h) (h) at the request of the European Data Protection Board, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy.	**Article 5(h)** (h) ~~**at the request of the European Data Protection Board**~~, providing advice on the implementation of specific cybersecurity aspects of Union policy and law related to data protection and privacy. Justification: **ENISA should independently be able to provide advice on cybersecurity matters.**
Article 5(5) **At the Commission's request, ENISA shall provide expertise, technical advice, information or analysis**	**Article 5(5)**

or carry out preparatory work on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation	~~At the Commission's request,~~ **The Commission shall consult with** ENISA ~~shall~~ **to** provide expertise, technical advice, information or analysis or carry out preparatory work **when developing Union policies, legislation and implementation.** ~~on specific cybersecurity matters with a view to informing the Commission's policymaking and monitoring of the implementation of Union legislation~~ **Justification** **European Commission should consult with ENISA and rely on its technical expertise. This replicates the requirement for the European Commission with the EDPS set in Art. 42 (1) of Regulation 2018/1725.**
Article 74 ***Preparation and adoption of European cybersecurity certification schemes*** 1. No later than 12 months after receiving a request from the Commission pursuant to Article 73, unless otherwise specified in the request, ENISA shall prepare a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81.	***Article 74*** ***Preparation and adoption of European cybersecurity certification schemes*** 1. No later than 18 months after receiving a request from the Commission pursuant to Article 73, and without prejudice to underlying work of European Standardization Organisation (ESO), unless otherwise specified in the request, ENISA shall prepare a candidate European cybersecurity certification scheme that meets the requirements set out in Articles 80 and 81. ENISA shall provide for sufficient deadline to the (ESO) in order to provide for their effective contribution to the candidate scheme.
	Article 77 **Technical specifications in European cybersecurity certification schemes** **1. ENISA may develop technical specifications in view of a future European Cybersecurity certification scheme or in support of the maintanance of a European cybersecurity certification scheme.** **2 (NEW) when developing such technical specifications, ENISA shall** work with the ESOs on these technical specifications. Moreover, any technical specification developed y ENISA should be replaced by ESO based specifications, once these are adopted.

	Any such development should be subject to analysis of necessity, duly justified and proportionate.
Article 81 ***Elements of European cybersecurity certification schemes*** 3. A European cybersecurity certification scheme shall, where appropriate, also include the following: ... (c) Extension profiles to set out additional security requirements, including, where applicable, security requirements set out in national provisions transposing Union law;	***Article 81*** ***Elements of European cybersecurity certification schemes*** 3. A European cybersecurity certification scheme shall, where appropriate, also include the following: ... (c) extension profiles to set out additional or specific requirements for defined use cases, including, where appropriate, additional capabilities such as enhanced product features, specialised service offerings, optimised processes or advanced security measures. Extension profiles shall describe their scope and purpose in detail, including the security threats addressed, and may demonstrate compliance with specific standards and regulatory requirements, including, where applicable, cybersecurity risk-management measures laid down by a Member State in accordance with the minimum harmonisation principle under Directive (EU) 2022/2555; Any development of extension profiles or/and certification scheme should be, ahead of its development, be subject to analysis of its necessity and justified objective/purpose. ~~including, where applicable, security requirements set out in national provisions transposing Union law~~
Article 99 ***Security risk assessments*** 1. The Commission or a group of at least three Member States may request the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') to conduct the Union-level coordinated security risk assessments in accordance with Article 22 of that Directive. Where a security risk assessment is conducted following such request, it shall include in particular the proposed identification of the key ICT assets of the respective ICT supply chain as well as the main threat actors, risks and vulnerabilities affecting those assets. The Union-level coordinated security risk assessments shall develop risk scenarios and propose measures to mitigate the identified risks.	***Article 99*** ***Security risk assessments*** 1. The Commission or a group of at least seven Member States, and upon a positive and publicly available opinion made by the Management Board of ENISA, may request the Cooperation Group established by Article 14 of Directive (EU) 2022/2555 ('NIS Cooperation Group') to conduct the Union-level coordinated security risk assessments in accordance with Article 22 of that Directive. The risk assessment made by the NIS2 Cooperation Group must be published on its website as NIS2 Cooperation Group opinion. Where a security risk assessment is conducted following such request, it shall include in particular the proposed identification of the key ICT assets of the respective ICT supply chain as well as the main threat

2. The Union-level coordinated security risk assessments shall be completed within six months from the request referred to in paragraph 1. Upon request of the Commission, the NIS Cooperation Group may agree to a shorter period. 3. Where the Commission has sufficient reason to believe that there is a significant cyber threat for the security of the Union in relation to an ICT supply chain and that action is required to preserve the proper functioning of the internal market, the Commission shall without delay: (a) consult the Member States on the need to take one or several of the mitigating measures referred to in Article 103; and (b) conduct a security risk assessment, taking into account the consultation of the Member States. The security risk assessment shall include the proposed identification of the key ICT assets as well as the main threat actors, risks and vulnerabilities affecting those assets. The security risk assessment shall develop risk scenarios and propose measures to mitigate the identified risks.	actors, risks and vulnerabilities affecting those assets. The Union-level coordinated security risk assessments shall develop risk scenarios and propose measures to mitigate the identified risks. It should further include draft Impact Assessment evaluating economic, security and supply chain impact of the given measures. 2. The Union-level coordinated security risk assessments shall be completed within six months from the request referred to in paragraph 1. Upon request of the Commission, the NIS Cooperation Group may agree to a shorter period. 3. In exceptional circumstances justifying an immediate intervention, where the Commission has duly justified, sufficient and ~~sufficient reason to believe~~ concrete evidence to demonstrate that there is a significant cyber threat for the security of the Union in relation to an ICT supply chain and that action is required to preserve the proper functioning of the internal market, and where the procedure referred to in paragraph 1 cannot be completed within a reasonable period, the Commission shall without delay: (a) consult the Member States on the need to take one or several of the mitigating measures referred to in Article 103; and (b) conduct a security risk assessment and Impact Assessmenttaking into account the consultation of the Member States. The security risk assessment shall be completed within 6 months of its initiation and include the proposed identification of the key ICT assets as well as the main threat actors, risks and vulnerabilities affecting those assets. The security risk assessment shall develop risk scenarios and propose measures to mitigate the identified risks.
Article 100 ***Designation of third countries posing cybersecurity concerns*** 1. Where, as a result of the security risk assessment referred to in Article 99, or based on other sources, such as a public statement on behalf of the Union or a Member State, it appears that a third country poses a serious and structural non-technical risk to	***Article 100*** ***Designation of third countries posing cybersecurity concerns*** 1. Where, as a result of the security risk assessment referred to in Article 99, or based on other verifiable and official sources, such as a official public statement on behalf of the Union or a group of at least seven Member States, it appears that a third country poses a

ICT supply chains, the Commission shall verify the risk posed by that country, taking into account the following elements: (a) the existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited; (b) existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited; (c) the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns, including about existing practices referred to in point (b); (d) substantiated information about one or more incidents of threat actors controlled from that country and operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors; (e) Relevant information stemming from Union-level coordinated security risk assessments or reports by Member States or international organisations.	serious, continuedand structural non-technical risk to ICT supply chains, the Commission shall verify the risk posed by that country, ~~taking into account the following elements~~ and shall designate a third country followed by justification and impact assessment, only where at least three of the following criteria are met: (a) the existence of laws in the third country which require entities under their jurisdiction to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being disclosed publicly through a Coordinated Vulnerability Disclosure (CVD) and without prejudice to CRA ; (b) existing practices in the third country, demonstrated by independent sources, that require entities under the jurisdiction of the third country to report information on software or hardware vulnerabilities to authorities of that third country prior to those vulnerabilities being known to have been exploited; (c) the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns, including about existing practices referred to in point (b); (d) substantiated information about one or more incidents of state sponsored actors controlled from that country and operating out of the territory of that country carrying out malicious cyber activities or campaigns,(as referenced in point c) and the lack of ability or willingness of the third country to cooperate with the Commission or Member States to address the risk stemming from the operation of such threat actors; ~~(e) Relevant information stemming from Union-level coordinated security risk assessments or reports by Member States or international organisations.~~
Article 103 ***Mitigation measures in the ICT supply chain***	***Article 103*** ***Mitigation measures in the ICT supply chain***

6. In exceptional circumstances, which justify an intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the use, installation or integration of ICT components or components that include ICT components from a specific entity established in or controlled by a third country or entities from a third country, or a national from a third country represent a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States, the Commission shall without delay consult the Member States on the need to take measures at Union level.	6. In exceptional circumstances, which justify a~~n~~ timely intervention to preserve the proper functioning of the internal market and where the Commission has sufficient and demonstratable and duly justified reason and evidence to consider that the use, installation or integration of ICT components or components that include ICT components from a specific entity established in or controlled by a third country or entities from a third country, or a national from a third country represent a significant non-technical cybersecurity risk for the economic or societal activities of at least three Member States, the Commission shall without delay consult the Member States on the need to take measures at Union level.
Article 104 ***Identification of high-risk suppliers*** 2. For that purpose, the Commission shall map the suppliers providing ICT components and components that include ICT components relevant for the prohibition referred to in paragraph 1. On this basis, the Commission shall do an initial assessment to identify which of the mapped suppliers are potentially established in a third country designated in accordance with Article 100 or controlled by such third country, by an entity established in such third country or by a national of such third country. The Commission shall also do an initial mapping on suppliers potentially controlled by the entity referred to in Article 103(6). 3. The Commission shall assess the place of establishment as well as the ownership and control structure of the suppliers initially identified in accordance with the second subparagraph of paragraph 2. 4. For the purpose of the assessment referred to in paragraph 3, the Commission shall be entitled to request the necessary information from the suppliers. In case the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is established in a third country designated in accordance with Article 100 or controlled by such	***Article 104*** ***Identification of high-risk suppliers*** 2. For that purpose, the Commission shall map the suppliers providing ICT components and components that include ICT components relevant for the prohibition referred to in paragraph 1. On this basis, the Commission shall do an initial assessment to identify which of the mapped suppliers are potentially established in a third country designated in accordance with Article 100 (the jurisdiction of the supplier's headquarters) or demonstrably controlled by such third country, through formal legal or financial state mechanisms, by an entity established in such third country ~~or by a national of such third country~~. The Commission shall also do an initial mapping on suppliers potentially controlled by the entity referred to in Article 103(6). 3. The Commission shall assess the place of establishment as well as the ownership and control structure of the suppliers initially identified in accordance with the second subparagraph of paragraph 2. In conducting this assessment, the Commission shall take into account legal, technical, and organizational measures implemented by the supplier that

third country, by entities from that third country or by nationals of such third country. Where the Commission is carrying out an assessment for the purpose of Article 103(7) and the supplier does not provide the necessary information within the established deadline, the Commission may conclude that the supplier is controlled by an entity designated in line with that Article. The competent authorities referred to in Article 112 shall also share relevant information with the Commission upon request.	demonstrably reduce or eliminate the risks associated with the supplier's place of establishment, ownership, or control structure. It shall also take into account if the supplier acts repeatedly against the cybersecurity interests of the Union. 4. For the purpose of the assessment referred to in paragraph 3, the Commission shall be entitled to request the necessary information from the suppliers. In case the supplier does not provide the necessary information within the established deadline, the Commission may take this failure into account as one factor among others and may initiate a detailed investigation. However, the failure to provide information shall not constitute the sole basis to conclude that the supplier is established in a third country designated in accordance with Article 100 or controlled by such third country, by entities from that third country or by nationals of such third country. Where the Commission is carrying out an assessment for the purpose of Article 103(7) and the supplier does not provide the necessary information within the established deadline, the Commission may similarly initiate a detailed investigation, but shall not solely rely on this failure to conclude that the supplier is controlled by an entity designated in line with that Article. In all cases, the Commission's conclusions regarding establishment or control shall be affirmatively proven and based on objective facts and duly justified and proportionate The competent authorities referred to in Article 112 shall also share relevant information with the Commission upon request. 5. An entity from third country that has been identified as a high-risk supplier shall have the right to judicial review.
Article 105 ***Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns***	***Article 105*** ***Exemption for entities established in or controlled by entities from a third country posing cybersecurity concerns***

4. The Commission shall assess the request referred to in paragraph 1 through a fair and transparent process, taking into account: (a) the circumstances and additional elements referred to in Article 100(1) and (2) in relation to the designated country posing cybersecurity concerns to ICT supply chains where the entity is established or from where it is controlled; (b) the effectiveness of the mitigating measures referred to in paragraph 2 point (c) whether the exemption for the entity established in or controlled by entities from a third country posing cybersecurity concerns to ICT supply chains would not be detrimental to the Union's interest.	4. The Commission shall assess the request referred to in paragraph 1 through a fair and transparent process, taking into account: (a) the circumstances and additional elements referred to in Article 100(1) and (2) in relation to the designated country posing cybersecurity concerns to ICT supply chains where the entity is established or from where it is controlled; (b) the effectiveness of the mitigating measures referred to in paragraph 2 point (c) whether the exemption for the entity established in or controlled by entities from a third country posing cybersecurity concerns to ICT supply chains would not be detrimental to the Union's interest and effective functioning of the Internal Market and/or effect negatively supply chain of two or more EU countries. The assessment under point (c) shall be based strictly on verifiable, technical cybersecurity evidence. An exemption shall not be denied under point (c) if the entity has successfully demonstrated the effectiveness of its mitigating measures under point (b).

III. Final conclusion

While the proposed Cybersecurity Act 2 and the targeted amendments to the NIS 2 Directive set a strong trajectory for Europe's cyber resilience, their ultimate success hinges on delivering true simplification, predictability, and legal certainty.

By ensuring that cybersecurity certification remains a strictly voluntary and technical tool, establishing a proportionate and evidence-based approach to ICT supply chain security, and empowering ENISA to champion a "secure-by-design" approach to policy-making, co-legislators can avoid unnecessary administrative burdens and market distortions. We stand ready to collaborate with European policymakers to refine these proposals, ensuring that the final framework not only protects our critical infrastructure but also empowers a highly competitive, innovative, and deeply cohesive European digital single market.

KL/294/78/ET/2026