LEWIATAN

Warsaw, August 11, 2026
KL/542/WPM/2026

Amendments of the Polish Confederation Lewiatan on Cybersecurity Act 2

Original Text	Proposal from the Confederation Lewiatan
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 standardization, 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 standardization, 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	**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

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

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.	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. **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 ensures 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.

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

Article 5(5) At the Commission's request, ENISA shall provide expertise, technical advice, information or analysis 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.	**Article 5(5)** ~~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 Organization (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 maintenance of a European cybersecurity certification 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 maintenance of a European cybersecurity certification scheme. **2 When developing such technical specifications, ENISA shall** work with the ESOs on these technical specifications. Moreover, any technical specification developed by ENISA should be replaced by ESO based specifications, once these are adopted. Any such

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

	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, specialized service offerings, optimized 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 harmonization principle under Directive (EU) 2022/2555; Any development of extension profiles or/and certification scheme should be, ahead of its development, 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	**Article 99** **Security risk assessments** 1. The Commission or a group of at least ~~three~~ **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

risk assessments shall develop risk scenarios and propose measures to mitigate the identified risks. 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.	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. 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 Assessment taking 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 ICT supply chains, the Commission shall verify the	**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 an 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 serious, continued and structural non-

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 organizations.	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 organizations.~~
Article 103 **Mitigation measures in the ICT supply chain** 6. In exceptional circumstances, which justify an intervention to preserve the proper functioning of	**Article 103** **Mitigation measures in the ICT supply chain** 6. In exceptional circumstances, which justify a~~n~~ timely intervention to preserve the proper functioning of the

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.	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 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	**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 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.

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

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.	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** 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	**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

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.	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).