LEWIATAN

Warszawa, 18 października 2023 r.
KL/398/183/AM/2023

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Minister Cyfryzacji

Szanowny Panie Ministrze,

Kontunuując konstruktywny dialog z Ministerstwem Cyfryzacji w sprawie prac nad projektem rozporządzenia w sprawie odporności cybernetycznej (*Cyber Ressilience Act)* chcielibyśmy podziękować za otwartość z jaką resort podchodzi do dyskusji z biznesem w zakresie dot. istotnych założeń projektu.
W załączeniu przesyłam wypracowany we współpracy z firmami członkowskimi wykaz proponowanych poprawek do projektu rozporządzenia, licząc na kontynuację dyskusji w tej istotnej sprawie.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik: Stanowisko KL – propozycja poprawek do projektu rozporządzenia w sprawie odporności cybernetycznej (*Cyber Ressilience Act*) – wersja na trilogi z dnia 12 września br.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

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

LEWIATAN

Stanowisko KL – propozycja poprawek do projektu rozporządzenia w sprawie odporności cybernetycznej (*Cyber Resilience Act*) – wersja na trilogi z dnia 12 września br.

Motyw 10 – Open Source Software

This Regulation applies only to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. The supply in the course of a commercial activity ~~***might be***~~***is*** *characterized not only by charging a price for a product, but also by charging a price for technical support services* ***for the product*** *when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise,* ~~***by providing a software platform through which the manufacturer monetises other services,***~~ *or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.* ~~***The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity.***~~ ***This Regulation does not apply to the body of free*** *and open-source software****, which*** *is understood as free software that is openly shared and freely accessible, usable,* ***modifiable*** ~~***ed versions***~~ *and redistributable, and which* ***is made available in*** *source code* ***form*** *. Free and open-source software is developed, maintained, and distributed openly, including via online platforms.* ***Any party*** *that facilitates the development and supply of* ***free or open-source*** *software is only considered to be a distributor* ***in relation to a particular item of free or open source software: (1)*** ~~***if***~~ ***where*** *they* ***directly*** ~~***make this software available on the market and hence***~~ *supply it for distribution or use* ***it for a specific purpose*** *on the Union market in the course of a commercial activity****; and (2) to the extent it is used for that purpose.*** *Taking account of the above-mentioned elements determining the commercial nature of an activity*~~***, this Regulation should only apply to***~~ ***in respect of*** *free and open-source software****, this Regulation should only apply to (a) a manufacturer or distributor that has integrated free and open-source software in a product with digital elements*** *that is supplied in the course of a commercial activity, and (b) that product. Products provided as part of the delivery of a service for which a fee is charged solely to recover the actual costs directly related to the operation of that service should, as it is the case of products provided by public administration entities, not be considered on those grounds alone a commercial activity for the purposes of this Regulation.*

Uzasadnienie:

Zalecamy, aby zamiast wyraźnie wykluczać OSS (oprogramowanie oper sosurce) opracowane lub dostarczone poza działalnością komercyjną, motywem powinny być objęci tylko producenci lub dystrybutorzy, którzy udostępniają OSS w ramach działalności komercyjnej (i

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

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

jest on wykorzystywany do tego zamierzonego celu). Daje to pewność, że współtwórcy OSS nie zostaną objęci niniejszym rozporządzeniem (chyba że bezpośrednio dostarczają go do dystrybucji lub wykorzystania w określonym celu w ramach działalności handlowej i jest on ostatecznie wykorzystywany do tego zamierzonego celu).

Art. 6 Critical products with digital elements

Article 6 (1) *Products **with digital elements** which have the core functionality of a category that is listed in Annex III to this Regulation shall **be subject to the conformity assessment procedures referred to in Article 24 (2) and (3). (wersja Rady) The integration or combination of a product of higher class of criticality does not change the level of criticality for the product it is** integrated into. (wersja PE)*

Article 6 (1a) ***The** categories of ~~critical~~ products with digital elements **referred to in paragraph 1 are** divided into class I and class II as set out in Annex III. **The categories of products with digital elements listed in class I of Annex III shall meet all ~~one~~ of the following criterias**:*

(a) ***the product with digital elements performs primarily functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, endpoint security or network protection; and***

(b) ***the product with digital elements performs a primary function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health and safety of a large number of individuals through direct manipulation, such as a central system function, including core network management, configuration control, virtualisation, processing of large amounts of sensitive personal data.***

The categories of products with digital elements listed in class II of Annex III meet both criteria referred to in points (a) and (b) of this paragraph.

Article 6 (2) *The Commission is empowered to adopt delegated acts, **following a public consultation,** in accordance with Article 50 to amend Annex III by including in the list **within each class** of **the** categories of products with digital elements a new category **and specifying its definition**, **moving a category of products from one class to the other** or withdrawing an existing one from that list. When assessing the need to amend the list in Annex III, the Commission shall take into account the **cybersecurity-related functionalities or the function and the level of cybersecurity risk posed by the** products with digital elements **as set out by the criteria referred to in paragraph 1a**.*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

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

Article 6 (3) ***By … [12 months after the date of entry into force of this Regulation], the*** *Commission* ***shall*** *adopt* ***~~an delegated implementing~~*** *act specifying the definitions of the categories* ***of products with digital elements*** *under class I and class II as set out in Annex III* ***and the definitions of the categories of products with digital elements set out in Annex IIIa****.*

That implementing act shall be adopted in accordance with the ~~examination~~ procedure referred to in Article 50 ~~51(2)~~. (wersja Rady)

Article 6 (4) ***Where a new category of critical products with digital elements is added to class I or class II in Annex III by means of a delegated act pursuant to paragraph 2 of this Article, it shall be subject to the relevant conformity assessment procedures referred to in Article 24(2) and (3) within 36 ~~12~~ months of the date of adoption of the related delegated act.(wersja PE)***

Article 50 (4) Before adopting a delegated act, the Commission shall **conduct a public consultation and** consult experts designated by each Member State in accordance with principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

Uzasadnienie:

Potrzebne jest jaśniejsze i bardziej oparte na ryzyku podejście do określania poziomu ryzyka produktu z elementami cyfrowymi, a także większa pewność dla producentów produktów z elementami cyfrowymi co do tego, czy ich produkt jest produktem krytycznym. Na przykład, każdy produkt podłączony do sieci przetwarza dane osobowe, ale nie oznacza to, że produkt ten powinien zostać sklasyfikowany jako produkt krytyczny. Uważamy, że tekst Rady oferuje bardziej precyzyjną metodologię w art. 6. Ponadto ważne jest, aby wyjaśnić, że produkty dodane do załącznika III w drodze aktu delegowanego (zgodnie z art. 6 ust. 4) będą miały taki sam czas jak pozostałe kategorie na dostosowanie procesu produkcji do przepisów CRA - tj. 36 miesięcy.

Art. 10 ust. 6 – Obligations of manufactureres

W paragrafie 6 proponujemy zastąpienie *„for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter”* sformułowaniem “*support period*” zgodnie z propozycją Komisji ITRE:

6. *When placing a product with digital elements on the market, ~~and for the expected product lifetime or for a period of five years from the placing of the product on the market, whichever is shorter~~, manufacturers* ***shall determine the support period during which*** *~~ensure that~~ vulnerabilities of that product are handled effectively and in accordance with the essential requirements set out in Section 2 of Annex I.*

*In doing so, **unless otherwise agreed in a contract,** the manufacturer shall ensure that the support period is proportionate to the expected product lifetime **~~as well as in line with the nature of the product and, users expectations,~~** the availability of the operating environment and, where applicable, the support period of the main components integrated into the product with digital elements **as determined by the manufacturer.***

Pozytywnie oceniamy również pozostałe propozycje Komisji ITRE w tym paragrafie, wskazujące na to, że „suport period" powinien być proporcjonalny, biorąc pod uwagę naturę produktu i oczekiwania konsumentów, jak również na wymóg informowania konsumentów o długości okresu wsparcia.

Uzasadnienie:
Przyjęcie rozwiązania proponowanego przez Komisję ITRE jest bardziej proporcjonalne biorąc pod uwagę zróżnicowany okres użytkowania różnych kategorii urządzeń – w niektórych przypadkach może to być nawet dekada, w innych 2 lata.

Art. 10 ust. 6a – zapewnianie aktualizacji oprogramowania bez opłat (security updates)

*6a. For the purpose of complying with the obligation provided for in the first subparagraph of paragraph 6, where manufacturers have placed subsequent versions of a software product on the market, they may provide security updates only for the software product that they have last placed on the market. They may do so only if the users of the relevant previous product versions have access to the latest product version free of charge and do not incur significant additional costs to adjust the hardware and software environment in which (*wersja Rady)

6a. Where the support period is shorter than five years and the handling of vulnerabilities has ended, manufacturers may provide access to the source code of such a product with digital elements to other undertakings which commit to extending the provision of vulnerability handling services, in particular security updates. Access to such source codes shall be provided only where provided for in a contractual arrangement. Those arrangements shall protect the ownership of the product with digital elements and shall prevent the dissemination of the source code to the public, except where such code has already been provided under a free and opensource licence.(wersja Parlamentu)

Uzasadnienie:
Nie zgadzamy się z zaproponowaną przez Radę kontrowersyjną poprawką (art. 10 ust. 6a), która wymaga od producentów zapewnienia bezpłatnego dostępu do najnowszej wersji oprogramowania, jeśli producent zapewnia aktualizację zabezpieczeń tylko do tej najnowszej wersji. Podczas gdy PE wymaga oddzielenia aktualizacji bezpieczeństwa i funkcjonalności oprogramowania "*tam, gdzie jest to technicznie wykonalne*" (motyw 32a,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

załącznik I sekcja 1(3)(aa)), chcemy uniknąć potencjalnego obowiązkowego oddzielenia aktualizacji. Nie zgadzamy się również z obowiązkowym udostępnianiem kodu źródłowego po zakończeniu okresu wsparcia, czego domaga się Parlament.

Perspektywa B2B musi być dalej rozważana podczas rozmów trójstronnych, aby zapewnić zgodność przepisów z produktami niekonsumenckimi - dlatego zgadzamy się z proponowanym przez Radę motywem 11a.

Art. 11 - Reporting obligations of manufacturers

Article 3 (39) *'actively exploited vulnerability' means a vulnerability for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner*

Recital (19) … ***Vulnerabilities subject to mandatory reporting concern instances where an actor successfully ~~is~~ executes~~ing~~ malicious code by exploiting weaknesses on a product with digital elements which and ~~in order to~~ generates severe security breach, for example by exploiting weaknesses in identification and authentication functions. Vulnerabilities that are discovered with no malicious intent for purposes of good faith testing, investigation, correction or disclosure to promote the security or safety of the system owner and its users should not be subject to mandatory notifications. A significant incident having an impact on the security of the product with digital elements concerns a cybersecurity incident that can severely affect the development, production and maintenance processes of the manufacturer and that in turn can significantly impact the security of its products. This could be the case, for example, where an attacker has successfully compromised the release channel via which the manufacturer releases security updates to users.***

Article 11 (1) *The manufacturers shall* , ~~without undue delay and in any event within 24 hours of becoming aware of it,~~ *notify any actively exploited vulnerabilities contained in the product with digital elements* **that poses a significant cybersecurity risk**, ~~The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken. ENISA shall, without undue delay, unless for justified cybersecurity riskrelated grounds, forward the notification~~ that they become aware of to the ~~CSIRT~~CSIRTs designated ~~for the purposes of coordinated vulnerability disclosure in accordance withas~~ coordinators pursuant to Article ~~[Article X]~~12(1) of Directive ~~[Directive XXX/XXXX (NIS2 (EU)] of Member States. (~~wersja Rady)

Article 11 (1a) *For the purpose of the notification referred to in paragraph 1, the manufacturers shall submit:*

a) without undue delay and in any event within ***72*** *hours of* ***confirming the vulnerability*** ~~*becoming aware*~~ *of* ***and issuing a mitigation measure to*** *the actively exploited vulnerability****,*** ~~***an early warning which shall provide general information,***~~ ***a notification,*** *as available, about the product with digital elements concerned, the nature of the exploit and of the respective vulnerability****.*** *The* ***notification*** ~~***early warning***~~ *shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available. Where applicable, the* ***notification*** ~~***early warning***~~ *shall also indicate any corrective or mitigating measures taken, corrective or mitigating measures that users can take, and include an indication of how sensitive the manufacturer deems the notified information to be.*

~~***(b)Without undue delay and in any event within 72 hours of becoming aware of the actively exploited vulnerability, a notification updating the information referred to in point (a). Where applicable, the notification shall indicate any available information about the actively exploited vulnerability, the status of remediation and any corrective or mitigating measures taken***~~

(wersja Rady)

Article 11 *(1b) After a security update is made available or another form of corrective or mitigating measures is put in place* ***and upon manufacturer's consent****, ENISA shall add the notified vulnerability pursuant to paragraph 1 to the European vulnerability database referred to in Article 12 of Directive (EU) 2022/2555.* (wersja PE)

Article 11 (2) *The manufacturers shall notify any significant incident having an impact on the security of the product with digital elements that they become aware of to the CSIRTs designated as coordinators pursuant to Article 12(1) of Directive (EU) 2022/2555, in accordance with paragraph 2b of this Article. (*wersja Rady)

Article 11 (2a) *An incident shall be considered to be significant as referred to in paragraph 2, where where it has caused or is capable of causing severe operational disruption of the production environment or the primary function of the product which would compromise the security level of a product, as determined by the manufacturer.(wersja PE)*

Article 11 (2a) *For the purpose of the notification referred to in paragraph 2, the manufacturers shall submit:*

(a) Without undue delay and in any event within 24 hours of ~~*becoming aware of*~~ *confirming the incident, an early warning which shall provide general information, as available, about the nature of the incident and shall indicate whether the incident is suspected of being caused by unlawful or malicious acts or could have a cross- border impact. The early warning shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available. Where applicable, the early warning shall also*

indicate any corrective or mitigating measures taken, corrective or mitigating measures that users can take, and include an indication of how sensitive the manufacturer deems the notified information to be.

(b)Without undue delay and in any event within 72 hours of becoming aware of the incident, an incident notification which shall include information on the severity and impact of the incident, and, where applicable, update the information referred to in point (a). The notification shall also include, if available, information on the indicators of compromise. (wersja Rady)

Article 11(2aaa) In duly justified cases and in agreement with the CSIRTs referred to in paragraphs 1 and 2, manufacturers can deviate from the deadlines laid down in paragraphs 1a and 2a. In particular, a deviation from the deadlines provided for in paragraph 2a can be justified in cases where there is an ongoing process of developing a mitigation measure.

Article 11 (2ab) *Where a third party other than the manufacturer notifies an actively exploited vulnerability or an incident having an impact on the security of a product with digital elements under the scope of this Regulation to a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555, that CSIRT shall without undue delay inform the manufacturer. (wersja Rady)*

Uzasadnienie:

Ad. ust. 1 - Konieczność zgłaszania "każdej aktywnie wykorzystywanej podatności" prowadziłaby de facto do zgłaszania nawet niezałatanych luk (unpatched vulnerabilities), które mogłyby stwarzać dodatkowe lub nowe zagrożenia dla cyberbezpieczeństwa. Ponadto różne podatności mają różne poziomy ryzyka. W związku z tym zgłaszanie podatności powinno być ograniczone do tych, które wiążą się ze znacznym ryzykiem dla cyberprzestrzeni, które zostało zdefiniowane w art. 3 pkt 36 jako "ryzyko w cyberprzestrzeni, w przypadku którego, na podstawie jego charakterystyki technicznej, można założyć wysokie prawdopodobieństwo wystąpienia incydentu, który mógłby doprowadzić do poważnych negatywnych skutków, w tym przez spowodowanie znacznej straty materialnej lub niematerialnej lub znacznego zakłócenia".

Uwagi ogólne do całości:

Oba teksty (PE, Rady) nadal wymagają od producentów zgłaszania niezałatanych luk w zabezpieczeniach, co uważamy za kwestię bezpieczeństwa. Wcześniej w czerwcu wydano wspólne oświadczenie branżowe, w którym wezwano decydentów do usunięcia tego wymogu. Zgłaszanie niezałatanych luk stworzyłoby zagrożenia dla bezpieczeństwa, a nie korzyści. Co więcej, proces raportowania musi unikać niepotrzebnych obciążeń związanych ze zgodnością (na przykład EP wymaga nadmiernego 3-etapowego raportowania luk i incydentów). Nie zgadzamy się z przyjętą przez Radę definicją podatności, która obecnie

obejmuje "próby" naruszenia (motyw 19a, art. 3(39)). Wreszcie, poprawka Rady do art. 11(4) jest problematyczna, ponieważ daje CSIRT uprawnienia do udostępniania informacji o podatnościach i incydentach bez zgody producenta, gdy producent nie poinformuje użytkowników "w odpowiednim czasie". Udostępnianie takich informacji bez zgody producenta jest poważną kwestią bezpieczeństwa, która podważy zaufanie i zniechęci producentów do zgłaszania luk w zabezpieczeniach.

Załącznik 1 sekcja 1

Section 1 (1) *Products with digital elements shall be designed, developed and produced in such a way that they* ***enable*** ~~*ensure*~~ *an appropriate level of cybersecurity based on the risks;*

Section 1(2) ~~*Products with digital elements shall be delivered without any known exploitable vulnerabilities;*~~

Section 1 (3) *On the basis of the* ***cybersecurity*** *risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall*

(aa) be placed on the market without any known critical or high severity ~~***exploitable***~~ ***vulnerabilities listed in the ENISA known exploited vulnerabilities catalogue;***

(a) be ***placed on the market*** ~~*delivered*~~ *with a secure by default configuration,* ***unless otherwise agreed between the parties in a business-to-business context,*** *including the possibility to reset the product to its original state* ~~**while retaining all installed security updates;**~~

(b) unless otherwise agreed between the parties in a business-to-business context, ensure automatic security updates **with a clear and easy-to-use opt-out mechanism** and the notification of available updates to users;

[…]

(l) ensure that vulnerabilities can be addressed through security updates, including, where applicable ***and unless otherwise agreed between the parties in a business-to-business context,*** *through automatic updates and the notification of available updates to users.*

Section 2 (4) once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and **clear and user friendly** information helping users to remediate the vulnerabilities; **Where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;**

Section 2 (7) *provide for mechanisms to securely distribute* ***security*** *updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner;*

Section 2 (8) *ensure that,* ***unless otherwise agreed between the parties in a business-to-business context****, where security patches or updates are available to address identified security issues, they are disseminated without delay and, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken;*
Section 2 (9) ***where possible and applicable, notify the user of the end of the support period****.*

Uzasadnienie:

W sekcji 1 załącznika I oba teksty (Rada, Parlament) nadal zawierają wymóg wprowadzania na rynek produktów bez znanych luk, które można wykorzystać (*known exploitable vulnerabilities).* Dostarczanie produktów bez luk, które można wykorzystać, jest wymaganiem niemożliwym do osiągnięcia. Na bezpieczeństwo produktu może mieć wpływ wiele czynników, które wpływają na to, czy podatność może zostać faktycznie wykorzystana, czy też nie. Co więcej, taki wymóg zniechęcałby producentów do przeprowadzania znaczących testów bezpieczeństwa (w ten sposób potencjalne luki pozostawałyby "nieznane"). Wreszcie, niektóre luki nie są w rzeczywistości możliwe do wykorzystania w kontekście danego produktu.

Ponadto obowiązek automatycznego lub bezpłatnego dostarczania aktualizacji zabezpieczeń nie odzwierciedlałby realiów ekosystemu B2B. W przeciwieństwie do środowisk B2C, w których aktualizację urządzenia konsumenckiego można przeprowadzić w ciągu kilku minut, akceptując powiadomienie push, aktualizacja i łatanie całych systemów B2B jest złożonym procesem wymagającym znacznych zasobów, wiedzy specjalistycznej i różnych zainteresowanych stron (w tym różnych operatorów). Te usługi związane ze wsparciem są dostępne dla klientów za opłatą, naliczaną na podstawie umowy i nie mogą być zautomatyzowane.

Załącznik V

Annex V. *The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:*

2. a description of the design, development and production of the product and vulnerability handling processes, including: (a) ***~~complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing~~***

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

VIDE: [Article 10(8) *[…]* ***Market surveillance authorities shall ensure the confidentiality and appropriate protection of the information in the technical documentation provided by manufacturers in accordance with Article 52.]***

Uzasadnienie:

Z jednej strony CRA nie powinien wymagać od producentów umieszczania w dokumentacji technicznej nadmiernej ilości informacji na temat pełnego projektu produktu (design). Z drugiej strony, w ostatecznym tekście należy wyjaśnić, że dokumentacja techniczna może być udostępniana wyłącznie organom nadzoru rynku i nie powinna być podawana do wiadomości publicznej. Takie wymogi sprawiłyby, że produkty byłyby mniej bezpieczne, zarówno z perspektywy własności intelektualnej, jak i cyberbezpieczeństwa. Co więcej, szczegółowe oceny ryzyka nie powinny być w pełni uwzględniane w dokumentacji technicznej, ponieważ zwiększa to również ryzyko cyberbezpieczeństwa z potencjalną procedurą dostarczania pełnych informacji odpowiednim organom na żądanie.

KL/398/183/AM/2023

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

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