CYFROWA POLSKA

Warszawa, dnia 10 czerwca 2026 r.

Szanowny Pan

Krzysztof Gawkowski

Wiceprezes Rady Ministrów,

Minister Cyfryzacji

Szanowny Panie Premierze,

W kontekście prac nad unijnym akcie o cyberbezpieczeństwie (CSA2), w imieniu Związku Cyfrowa Polska, chciałbym przedłożyć kilka uwag do obecnej propozycji regulacji. Uważamy bowiem, iż jest to wyjątkowa okazja, aby wzmocnić pozycję Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i aby stała się niezależnym i pełnoprawnym organem w zakresie kształtowania polityki, prawodawstwa, wdrażania i egzekwowania prawa UE. Uważamy również za kluczową kwestię harmonizację oraz standaryzację europejskich ram certyfikacji

Obecnie niemal wszystkie przepisy, bezpośrednio lub pośrednio, wpływają na systemy cyfrowe i infrastrukturę cyfrową. Bez dochowania pełnej rozwagi podczas ich tworzenia, takie przepisy mogą nieumyślnie rozszerzyć obszary ataków, stworzyć nowe luki w zabezpieczeniach i podważyć nasze zbiorowe bezpieczeństwo. Cyberbezpieczeństwo musi zatem zostać od podstaw zintegrowane z procesem kształtowania polityki i traktowane na równi z proporcjonalnością, subsydiarnością i prawami podstawowymi podczas oceny projektowania polityki, prawodawstwa i ich wdrażania.

Wzmocnienie ENISA

Kreowanie polityki musi odzwierciedlać tę nową rzeczywistość, jednak UE obecnie nie dysponuje ustrukturyzowanym procesem oceny zagrożeń cyberbezpieczeństwa przed sfinalizowaniem przepisów. Konsultacje z ekspertami często odbywają się doraźnie i zbyt późno - jeśli w ogóle. Zbliżająca się rewizja CSA stanowi okazję do wypełnienia tej luki strukturalnej. Rola doradcza ENISA pozostaje nadal w dużej mierze reaktywna, udzielając porad czy opinii wyłącznie na żądanie. Należy więc rozszerzyć jej kompetencje, aby umożliwić jej niezależne i proaktywne doradzanie decydentom UE. Ponadto ENISA powinna brać udział w procesie decyzyjnym podczas opracowywania, wdrażania i egzekwowania prawodawstwa UE przez

Komisję Europejską. Zalecamy zatem, aby formalnie włączyć ENISA do procesu decyzyjnego, od momentu kreowania nowej regulacji.

Certyfikacja

Europejskie systemy certyfikacji cyberbezpieczeństwa powinny być wiarygodnym narzędziem do wykazania zgodności. Tymczasem znane są przypadki państw, które stanowią swoistą lukę bezpieczeństwa. Certyfikują one bowiem sprzęt i procesy ICT producentów państw trzecich, które w analogicznej procedurze certyfikacyjnej w innych krajach UE, nie miałyby szans tej certyfikacji uzyskać, ze względu na swoje podatności i ryzyka w zakresie cyberbezpieczeństwa. KE musi ustandaryzować oraz zharmonizować procedurę standaryzacji cyberbezpieczeństwa, aby zapewnić zgodność certyfikacji.

Jednocześnie w tym procesie niezwykle ważne jest, aby utrzymać istniejące, uznane, europejskie i międzynarodowe procesy certyfikacji. Nie powielać obowiązków certyfikacji wynikających z różnych regulacji wspólnotowych, a także myśląc o kolejnej certyfikacji, niwelować jedynie uwidocznione luki, a nie obejmować już zagospodarowane obszary.

Certyfikacja powinna odzwierciedlać współczesne realia

Certyfikacja musi odzwierciedlać realia współczesnego rozwoju oprogramowania. Statyczne cykle ponownej certyfikacji mogą prowadzić do złudzenia bezpieczeństwa, w którym certyfikowany produkt staje się nieaktualny, a bezpieczniejsza, poprawiona wersja nie posiada certyfikatu. Certyfikacja powinna ewoluować w kierunku modelu ciągłej zgodności, uwzględniającego aktualizacje, poprawki i zarządzanie lukami w zabezpieczeniach, czyniąc ją zorientowanym na rynek, wiarygodnym wskaźnikiem bezpieczeństwa, a nie barierą dla innowacji.

Konsultacje

Programy nie będą możliwe do wdrożenia bez znaczących konsultacji z interesariuszami. Niestety, organ powołany w tym celu przez CSA, SCCG, nie był skutecznie zaangażowany w ramy i poszczególne programy i został całkowicie usunięty. Proponowane Europejskie Zgromadzenie ds. Certyfikacji Cyberbezpieczeństwa, spotykające się tylko raz w roku, nie nadaje się do tego celu. Ramy certyfikacji powinny obejmować stałą strukturę doradczą z silnym udziałem przemysłu, większą przejrzystość projektów programów i harmonogramów podejmowania decyzji oraz możliwość wydawania niewiążących opinii. Istniejące modele, takie jak Grupa Ekspertów CRA, mogłyby stanowić przykład.

Bezpieczeństwo łańcucha dostaw ICT

Ustanowienie ogólnounijnych ram dla zaufanych kluczowych łańcuchów dostaw ICT, aby skutecznie zarządzać ryzykiem nietechnicznym, jest konieczne, aby zapewnić bezpieczeństwo, odporność i funkcjonowanie rynku wewnętrznego oraz wzmocnić ochronę praw podstawowych.

Związek Cyfrowa Polska
ul. Twarda 2, 00-105 Warszawa
e-Doręczenia:
AE:PL-30344-97239-IDARJ-15
+48 (22) 666 22 46
biuro@cyfrowapolska.org
cyfrowapolska.org
KRS: 0000250359
REGON: 140463214
NIP: 5222802518

Zapewnienie skutecznego, proporcjonalnego i przejrzystego stosowania ram łańcucha dostaw ICT oraz delegowanych uprawnień jest niezbędne. Udział państw członkowskich, właściwych organów krajowych oraz interesariuszy branżowych jest kluczowy w realizacji ram określonych w CSA 2. Kluczowe jest uwzględnienie dowodów opartych na faktach, wpływu ekonomicznego na wdrożenie CSA 2 poprzez akty wdrożeniowe oraz sektorowe zastosowania narzędzi bezpieczeństwa łańcucha dostaw ICT. Szybko ewoluujące cyberzagrożenia uzasadniają odpowiednie środki bezpieczeństwa. Z jednej strony, ryzyka techniczne i nietechniczne są słusznie uwzględniane między innymi przez NIS2, CRA i DORA. Z drugiej strony, makroekonomiczne europejskie podejście do wzmocnienia bezpieczeństwa łańcucha dostaw ICT w sektorach krytycznych uwzględnia rosnącą potrzebę eliminacji luk nietechnicznych związanych z dostawcami o podwyższonym profilu ryzyka.

Dostawcy Wysokiego Ryzyka (DWR)

Polska po wieloletniej debacie i dziesiątkach konsultacji publicznych, opracowała niezwykle precyzyjny model uznawania **produktu ICT, usługi ICT lub procesu ICT** za Dostawcę Wysokiego Ryzyka. Oprócz wieloetapowej procedury uznawania za DWR, przewiduje również dokładnie opisaną procedurę odwoławczą. Za szczególnie istotne uważamy utrzymanie krajowych rozwiązań w tym zakresie, a nawet w ramach możliwości przeniesienia ich na poziom europejski. Szczegółowo opisana procedura zabezpiecza interes państwa, dociera precyzyjnie w konkretne produkty, usługi i procesy ICT, a jednocześnie nie zamyka rynku i nie ogranicza konkurencji dla producentów z państw trzecich.

Proponujemy poniższe zmiany w dokumencie:

	European Commission text	**Amended text**
Section 1 (title)	Support for implementation of Union policy and law	Support for **the drafting and** implementation of union policy and law
	Justification: *Clarify that 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.	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,**

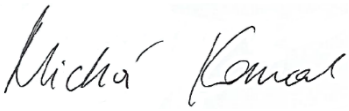
		all Union institutions and bodies on legislative and administrative measures relating to the cybersecurity impact on Union policies, legislation and implementation;
	Justification *This replicates language that already exists in Art. 58 (3c) of Regulation 2018/1725. This ensure that ENISA can independently 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.	(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 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~~
	Explanation:	

	The goal is to make clear that the European Commission should check in with ENISA and rely on its technical expertise in order to cyberproof EU legislation and policy implementation. **Justification** *Clarify that the 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*

Do stanowiska załączam przegląd ogólnoeuropejski, w zakresie zapewnienia zaufanych sieci komunikacji elektronicznej w Unii Europejskiej.

Z poważaniem

Michał Kanownik



Prezes Zarządu

Związek Cyfrowa Polska

Porozmawiajmy o technologii!

Związek Cyfrowa Polska
ul. Twarda 2, 00-105 Warszawa
e-Doręczenia:
AE:PL-30344-97239-IDARJ-15

+48 (22) 666 22 46
biuro@cyfrowapolska.org
cyfrowapolska.org

KRS: 0000250359
REGON: 140463214
NIP: 5222802518