Rada
Unii Europejskiej

Bruksela, 29 marca 2022 r.
(OR. pl)

Międzyinstytucjonalny numer referencyjny:
2022/0084 (COD)

7670/22
ADD 7

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	22 marca 2022 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2022) 65 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW Towarzyszący dokumentowi: Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii

Delegacje otrzymują w załączeniu dokument SWD(2022) 65 final.

Zał.: SWD(2022) 65 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 22.3.2022 r.
SWD(2022) 65 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE SPRAWOZDANIA Z OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii

{COM(2022) 119 final} - {SWD(2022) 66 final}

Streszczenie oceny skutków

Analiza skutków w obszarze bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii

A. Kontekst polityczny

W programie strategicznym Rady Europejskiej na lata 2019–2024 wezwano instytucje do ochrony unijnych sieci informacyjnych i komunikacyjnych oraz procesów decyzyjnych UE przed wszelkiego rodzaju szkodliwymi działaniami, w tym przed zagrożeniami cybernetycznymi i hybrydowymi. W związku z powyższym w grudniu 2019 r. Rada do Spraw Ogólnych stwierdziła, że instytucje i organy UE powinny opracować i wdrożyć kompleksowy zestaw środków w celu zapewnienia bezpieczeństwa informacji.

W lipcu 2020 r. Komisja przyjęła strategię UE w zakresie unii bezpieczeństwa, w której zobowiązała się do uzupełnienia starań podejmowanych przez poszczególne państwa w tym obszarze. W ramach tej strategii Komisja zaproponowała stworzenie minimalnego zestawu przepisów dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa we wszystkich instytucjach i organach Unii.

B. Na czym polega problem?

Najistotniejsze problemy są następujące: i) znaczna różnica między poziomem bezpieczeństwa poszczególnych instytucji i organów Unii w zależności od ich wewnętrznych przepisów dotyczących bezpieczeństwa informacji oraz (ii) brak koordynacji między instytucjami i organami Unii w wykonywaniu ich zadań w zakresie bezpieczeństwa.

Instytucje i organy Unii dysponują obecnie własnymi przepisami dotyczącymi bezpieczeństwa informacji lub w ogóle nie przyjęły takich przepisów. Rozdrobnienie obowiązujących ram prawnych spowodowało, że w poszczególnych instytucjach i organach funkcjonują różne kategorie informacji jawnych, różne oznaczenia i instrukcje postępowania. Jeżeli chodzi o informacje niejawne UE, ograniczona jest nadal interoperacyjność odpowiednich systemów, co uniemożliwia sprawne przekazywanie informacji między instytucjami i organami oraz ich wymianę z państwami członkowskimi.

Taka sytuacja zwiększa ryzyko naruszenia bezpieczeństwa w najsłabszym ogniwie i wykorzystania tego jako punktu wyjścia dla dalszych ataków na inne instytucje lub organy.

C. Co należałoby osiągnąć?

Ogólnym celem inicjatywy jest stworzenie zasad bezpieczeństwa informacji dla wszystkich instytucji i organów Unii, aby zapewnić wzmocnioną i spójną ochronę przed zmieniającymi się zagrożeniami dla posiadanych przez nie informacji.

Ogólny cel przekłada się na cztery cele szczegółowe:

- Ustanowienie zharmonizowanych i obszernych kategorii informacji
- Określenie luk w zakresie bezpieczeństwa i wdrożenie niezbędnych środków
- Ustanowienie uproszczonej współpracy instytucji i organów Unii w zakresie bezpieczeństwa informacji

- Modernizacja polityki bezpieczeństwa informacji z uwzględnieniem transformacji cyfrowej oraz telepracy

D. Jakie są opinie poszczególnych zainteresowanych stron?

Zainteresowane strony, z którymi przeprowadzono konsultacje (instytucje i organy Unii, krajowe organy bezpieczeństwa państw członkowskich i specjaliści analitycy reprezentujący JRC), zgodziły się odnośnie do potrzeby wprowadzenia wspólnych standardów w zakresie bezpieczeństwa informacji dla wszystkich instytucji i organów Unii, ze szczególnym uwzględnieniem następujących kwestii:

- Należy wziąć pod uwagę różnorodność i odmienne otoczenie biznesowe poszczególnych instytucji i organów oraz umożliwić rozwiązania na szczeblu lokalnym.
- Większość instytucji i organów jest wprawdzie gotowa do nawiązania ze swoimi partnerami w krajowych organach współpracy do celów bezpieczeństwa informacji, instytucje i organy nie są jednak skłonne do delegowania swoich uprawnień decyzyjnych.
- Projekt rozporządzenia powinien uwzględniać umowę międzyrządową[1] państw członkowskich w sprawie ochrony informacji niejawnych.

E. Jakie są skutki wniosku?

Korzyści

Dzięki stworzeniu podstawowych zasad bezpieczeństwa informacji we wszystkich instytucjach i organach Unii projekt rozporządzenia przyczyni się do zwiększenia ogólnego poziomu bezpieczeństwa informacji, zmniejszając jednocześnie obecne rozbieżności. Wniosek powinien ponadto pomóc w wyeliminowaniu potencjalnie słabych ogniw, zabezpieczając w tym samym czasie informacje wymieniane w obrębie administracji europejskiej.

Z punktu widzenia efektywności projekt rozporządzenia powinien przynieść korzyści dzięki skoordynowanemu wykonywaniu wspólnych zadań w zakresie bezpieczeństwa informacji (np. poświadczeń, akredytacji systemów teleinformatycznych) oraz dzięki utworzeniu wspólnych organów zarządzających (takich jak międzyinstytucjonalna grupa koordynująca, podgrupy techniczne).

Skutki gospodarcze

Oczekuje się, że w przypadku instytucji i organów Unii wysiłki niezbędne do wdrożenia nowych przepisów zostaną zrekompensowane wzrostem wydajności, natomiast dodatkowe koszty mogą zostać pokryte w ramach istniejących programów poprawy bezpieczeństwa informacji w poszczególnych organizacjach. W perspektywie długoterminowej skorzystają one dzięki spójnemu podejściu do stale zmieniających się zagrożeń dla bezpieczeństwa informacji.

Komisja Europejska powinna zapewnić stały sekretariat międzyinstytucjonalnej grupy koordynującej i przeznaczyć do realizacji tego zadania zasoby ludzkie (jednego urzędnika AD i jednego urzędnika AST).

[1] Umowa między państwami członkowskimi Unii Europejskiej, zebranymi w Radzie, w sprawie ochrony informacji niejawnych wymienianych w interesie Unii Europejskiej, 2011/C202/05

Nie oczekuje się żadnych skutków gospodarczych na szczeblu administracji państw członkowskich i w sektorze prywatnym.
F. Działania następcze
Kiedy nastąpi przegląd przyjętej polityki?
Co pięć lat od daty rozpoczęcia stosowania rozporządzenia przeprowadzana będzie pełna ocena, aby przeanalizować jego skutki oraz proces wdrażania. Komisja będzie przedstawiać sprawozdanie zawierające jej ustalenia i przedkładać je Parlamentowi Europejskiemu i Radzie.