Rada
Unii Europejskiej

Bruksela, 10 czerwca 2022 r.
(OR. fr)

9719/22

Międzyinstytucjonalny numer referencyjny:
2022/0085(COD)

LIMITE

CYBER 199
TELECOM 257
INST 206
CSC 229
CSCI 75
INF 88
FIN 592
BUDGET 12
CODEC 825
DATAPROTECT 179

NOTA DO PUNKTU I/A

Od:	Prezydencja
Do:	Komitet Stałych Przedstawicieli / Rada
Nr poprz. dok.:	9882/22
Nr dok. Kom.:	7474/22 + ADD 1
Dotyczy:	Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii – Sprawozdanie z postępu prac

Prezydencja przygotowała sprawozdanie z postępu prac nad wnioskiem dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i agencjach Unii, aby przedstawić sprawozdanie z prac przeprowadzonych dotychczas przez organy przygotowawcze Rady oraz ze stanu prac nad analizą wniosku.

Sprawozdanie to zostało przedstawione przez prezydencję Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni na posiedzeniu w dniu 10 czerwca 2022 r.

WPROWADZENIE

1. W dniu 22 marca 2022 r. Komisja przyjęła wniosek dotyczący rozporządzenia ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii Wniosek był jednym ze środków przewidzianych w strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[1], która ma na celu wzmocnienie zbiorowej odporności Unii na cyberzagrożenia. W konkluzjach z dnia 22 marca 2022 r. w sprawie tej strategii[2] Rada podkreśliła, że cyberbezpieczeństwo odgrywa podstawową rolę w funkcjonowaniu administracji publicznej i instytucji publicznych zarówno na poziomie krajowym, jak i UE oraz, ogólnie, naszego społeczeństwa i naszej gospodarki.

2. W konkluzjach z dnia 20 czerwca 2019 r.[3] Rada Europejska zwróciła się do instytucji UE, aby wraz z państwami członkowskimi pracowały nad środkami na rzecz zwiększenia odporności i poprawy kultury bezpieczeństwa UE w obliczu cyberzagrożeń i zagrożeń hybrydowych spoza UE, a także na rzecz skuteczniejszej ochrony unijnych sieci informacyjnych i komunikacyjnych oraz unijnych procesów decyzyjnych przed wszelkiego rodzaju złośliwymi działaniami.

3. Głównym celem wniosku, którego podstawą jest art. 298 TFUE, jest podniesienie poziomu cyberbezpieczeństwa w instytucjach europejskich poprzez ustanowienie wspólnych ram przy zachowaniu autonomii każdej instytucji.

---

1 Dok. 14133/20.
2 Dok. 6722/21.
3 Dok. EUCO 9/19.

4. Głównymi celami wniosku są:

   – wzmocnienie mandatu i finansowania CERT-UE (Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii);

   – utworzenie międzyinstytucjonalnej struktury skupiającej przedstawicieli wszystkich instytucji w celu zapewnienia właściwego wykonania rozporządzenia;

   – nałożenie na instytucje europejskie obowiązku udostępniania CERT-UE (jawnych) informacji informatycznych oraz zgłaszania istotnych zagrożeń, słabych punktów i incydentów; oraz

   – promowanie koordynacji i współpracy w odpowiedzi na poważne incydenty.

AKTUALNA SYTUACJA

5. Horyzontalna Grupa Robocza ds. Cyberprzestrzeni (GHQC) rozpoczęła dyskusje nad wnioskiem na posiedzeniu w dniu 29 września 2022 r., kiedy to Komisja dokonała jego ogólnej prezentacji.

6. GHQC omówiła tekst wniosku dotyczącego rozporządzenia na posiedzeniach w dniach 19 i 26 kwietnia 2022 r.

7. W następstwie dyskusji na forum GHQC państwa członkowskie zostały poproszone o przedstawienie pisemnych uwag do dnia 6 maja 2022 r. Z możliwości przedstawienia swojego stanowiska na piśmie skorzystało 16 państw członkowskich.

8. Państwa członkowskie z zadowoleniem przyjęły wniosek jako odpowiedni i uzupełniający w stosunku do przyszłej dyrektywy NIS 2, a także ogólnie poparły jego główne cele. Państwa członkowskie zaapelowały jednak o zwiększenie ambicji i poruszyły szereg kluczowych kwestii i obaw, które powinny znaleźć odzwierciedlenie w negocjacjach nad wnioskiem, w szczególności brak wzajemności w wymianie informacji między instytucjami a państwami członkowskimi oraz zbyt dobrowolny charakter proponowanych środków. Państwa członkowskie poprosiły również o skreślenie odniesienia do wspólnej jednostki ds. cyberprzestrzeni (której mandat i skład nie zostały jeszcze określone). Ponadto podkreślono potrzebę uwzględnienia we wniosku niektórych przepisów przyszłej dyrektywy NIS 2.

9. Kilka państw członkowskich zwróciło się do Służby Prawnej Rady o przeanalizowanie, czy podstawa prawna jest odpowiednia, i o rozważenie możliwych rozwiązań alternatywnych.

10. W Parlamencie Europejskim na sprawozdawczynię została wyznaczona Henna Virkkunen (EPP) z przedmiotowo właściwej komisji ITRE.

11. W dniu 17 maja 2022 r. opinię wydał Europejski Inspektor Ochrony Danych4.

12. W dniu 23 maja 2022 r. prezydencja zwróciła się do Komitetu ds. Bezpieczeństwa Rady o formalną opinię na temat aspektów wniosku dotyczących bezpieczeństwa informacji.

4 Dok. 9252/22.

13. Na podstawie wkładów państw członkowskich i prac GHQC prezydencja opracuje tekst kompromisowy, który zostanie przeanalizowany podczas posiedzeń GHQC w dniach 21 i 28 czerwca 2022 r.

14. Bazując na postępach poczynionych przez prezydencję francuską, nadchodząca prezydencja czeska planuje kontynuować prace nad tym ważnym dossier z myślą o wypracowaniu podejścia ogólnego.

15. W związku z tym Komitet Stałych Przedstawicieli i Rada są proszone o odnotowanie postępów w analizie proponowanego aktu.