



Rada  
Unii Europejskiej

Bruksela, 20 kwietnia 2023 r.  
(OR. en)

---

---

Międzyinstytucjonalny numer  
referencyjny:  
2023/0109(COD)

---

---

8512/23  
ADD 1

CYBER 92  
TELECOM 108  
CADREFIN 51  
FIN 448  
BUDGET 6  
IND 181  
JAI 471  
MI 314  
DATAPROTECT 110  
RELEX 481  
CODEC 662

#### **PISMO PRZEWODNIE**

---

Od: Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)

Data otrzymania: 19 kwietnia 2023 r.

Do: Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej

---

Nr dok. Kom.: COM(2023) 209 final - Annex

---

Dotyczy: ZAŁĄCZNIK do ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty

---

Delegacje otrzymują w załączeniu dokument COM(2023) 209 final - Annex.

---

Zał.: COM(2023) 209 final - Annex



Strasburg, dnia 18.4.2023 r.  
COM(2023) 209 final

ANNEX

## **ZAŁĄCZNIK**

**do**

**ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY**  
**ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w**  
**zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w**  
**cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i**  
**incydenty**

## ZALACZNIK

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

1) w załączniku I sekcja/rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie” otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

Program ma stymulować wzmocnienie, budowę i nabywanie podstawowych zdolności w celu zabezpieczenia unijnej gospodarki cyfrowej, społeczeństwa i demokracji poprzez wzmocnienie unijnego potencjału przemysłowego i konkurencyjności w dziedzinie cyberbezpieczeństwa, a także zwiększenie zdolności sektora prywatnego i publicznego do ochrony obywateli i przedsiębiorstw przed cyberzagrożeniami, w tym poprzez wspieranie wdrażania dyrektywy (UE) 2016/1148.

Początkowe, a w stosownych przypadkach późniejsze działania w ramach niniejszego celu obejmują:

1. Wspólne inwestycje z państwami członkowskimi w zaawansowane urządzenia, infrastrukturę i know-how w dziedzinie cyberbezpieczeństwa, które są niezbędne do ochrony infrastruktury krytycznej i całego jednolitego rynku cyfrowego. Takie wspólne inwestycje mogą obejmować inwestycje w infrastrukturę kwantową i zasoby danych na potrzeby cyberbezpieczeństwa, orientację sytuacyjną w cyberprzestrzeni, w tym krajowe SOC i transgraniczne SOC tworzące europejską tarczę cyberbezpieczeństwa, a także inne narzędzia, które zostaną udostępnione sektorowi publicznemu i prywatnemu w całej Europie.
2. Zwiększanie istniejących zdolności technologicznych i łączenie w sieć ośrodków kompetencji w państwach członkowskich oraz zapewnienie, aby zdolności te odpowiadały potrzebom sektora publicznego i przemysłu, w tym w odniesieniu do produktów i usług, które wzmacniają cyberbezpieczeństwo i zaufanie w ramach jednolitego rynku cyfrowego.
3. Zapewnienie szerokiego wdrożenia skutecznych, najnowocześniejszych rozwiązań z zakresu cyberbezpieczeństwa i zaufania w państwach członkowskich. Takie wdrożenie obejmuje zwiększenie bezpieczeństwa i ochrony produktów od momentu ich zaprojektowania do komercjalizacji.
4. Zapewnienie wsparcia w celu wyeliminowania luki w umiejętnościach w zakresie cyberbezpieczeństwa poprzez na przykład ujednoczenie programów dotyczących umiejętności w zakresie cyberbezpieczeństwa, dostosowanie ich do konkretnych potrzeb sektorowych oraz ułatwienie dostępu do ukierunkowanych specjalistycznych szkoleń.

5. Promowanie solidarności między państwami członkowskimi w zakresie przygotowania się i reagowania na poważne incydenty w cyberbezpieczeństwie poprzez transgraniczne wdrażanie usług w zakresie cyberbezpieczeństwa, w tym wspieranie udzielania wzajemnej pomocy między organami publicznymi i ustanowienie rezerwy zaufanych dostawców usług w zakresie cyberbezpieczeństwa na poziomie Unii.”;

2) w załączniku II sekcja/rozdział „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie” otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

3.1. Liczba infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień<sup>1</sup>

3.2. Liczba użytkowników i społeczności użytkowników uzyskujących dostęp do europejskiej infrastruktury z zakresu cyberbezpieczeństwa

3.3. Liczba działań wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w ramach mechanizmu cyberkryzysowego”