

7.10.2025



Fundusze Europejskie

# K O N F E R E N C J A

## Cyberbezpieczeństwo w zamówieniach publicznych

Warszawa, 12 września 2025 r.



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską





Ministerstwo  
Cyfryzacji

7.10.2025

Fundusze Europejskie

# Cyberbezpieczeństwo w zamówieniach publicznych – realizowane i planowane działania Ministerstwa Cyfryzacji

**Łukasz Wojtachnio**

**Ministerstwo Cyfryzacji**



Fundusze  
Europejskie



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



## **Dlaczego cyberbezpieczeństwo jest tak ważne?**

- Rosnąca cyfryzacja administracji i usług publicznych
- Wzrost skali cyberataków na sektor publiczny
- Ochrona danych obywateli i informacji strategicznych
- Zapewnienie ciągłości funkcjonowania usług publicznych
- Spełnienie wymogów prawnych (RODO, NIS2, KSC )

# Cyberbezpieczeństwo od czego zacząć?

- Analiza ryzyka przed wszczęciem postępowania
- Analiza wymogów wynikających z aktów prawnych oraz soft law
- Analiza łańcucha dostaw
- Współpraca z ekspertami ds. cyberbezpieczeństwa przy tworzeniu OPZ
- Szkolenia dla osób odpowiedzialnych za zamówienia

# Rekomendacje Ministra Cyfryzacji

- Wydawane przez Ministra Cyfryzacji po uzyskaniu opinii Kolegium
- Dotyczą stosowania urządzeń informatycznych lub oprogramowania w zakresie ich wpływu na bezpieczeństwo (art. 33 KSC)
- Mają charakter pozytywny – rekomendują dane oprogramowanie lub uznają je za niepożądane
- Są dobrowolne adresowane do podmiotów KSC, nie dotyczą podmiotów prywatnych
- Podstawa odrzucenia oferty (art. 226 Pzp)

# Narodowe Standardy Cyberbezpieczeństwa

- Wydane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa
- Opracowane na podstawie standardów NIST
- Merytoryczne wsparcie dla zamawiającego
- Na standardy składają się m. in.:
  - Standardy kategoryzacji bezpieczeństwa (NSC 199);
  - Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200);
  - Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53)

# Projekt Strategii Cyberbezpieczeństwa RP na lata 2025-2029

- Przyjmowana w drodze uchwały RM. Obecnie po uzgodnieniach
  
- Projekt Strategii zakłada:
  - wyłączenie stosowania PZP lub wprowadzenie odrębnego trybu w zakresie zakupu pilnych usług i produktów związanych z cyberbezpieczeństwem
  - uwzględnianie certyfikatów cyberbezpieczeństwa wydawanych na podstawie europejskich programów certyfikacji cyberbezpieczeństwa

# Przegląd dyrektyw z zakresu zamówień publicznych

- umożliwienie wyłączenia zakupów związanych z cyberbezpieczeństwem spod wymogów zamówień publicznych, podobnie jak ma to zastosowanie do zamówień obejmujących aspekty obronności lub bezpieczeństwa;
- transparentne rozdzielanie zamówień z zakresu cyberbezpieczeństwa od zamówień IT;
- wprowadzenie mechanizmu uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług ICT oraz specyfikacji tych wymogów;
- wprowadzenie mechanizmu umożliwiającego wyłączenie pilnych zakupów związanych z cyberbezpieczeństwem spod wymogów prawa zamówień publicznych, co pozwoli uniknąć długotrwałych postępowań przetargowych negatywnie oddziałujących na cyberbezpieczeństwa państwa.

# Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa

■ Weszła w życie 28 sierpnia – Dz. U. poz. 1017

■ Służy stosowaniu Aktu o cyberbezpieczeństwie

■ Podstawowe założenia:

- Certyfikacja cyberbezpieczeństwa jest dobrowolna;
- Obok europejskich programów certyfikacji cyberbezpieczeństwa zostaną wprowadzone krajowe schematy certyfikacji cyberbezpieczeństwa;
- Minister Cyfryzacji jest Krajowym Organem ds. Certyfikacji Cyberbezpieczeństwa
- Minister Cyfryzacji jest organem nadzorczym nad procesem certyfikacji ze wsparciem PCA;
- Certyfikacja będzie prowadzona na podstawie umowy zawieranej z jednostką certyfikującą;

# Podmioty KSCC

- Minister Cyfryzacji
- PCA
- Jednostki oceniające zgodność
- Dostawcy produktów ICT, usług ICT, procesów ICT lub usługi zarządzane w zakresie bezpieczeństwa
- Osoby fizyczne, które poddadzą swoją wiedzę ocenie zgodności
- Podmioty, które poddadzą wykorzystywane systemy zarządzania cyberbezpieczeństwem ocenie zgodności

# Przedmiot certyfikacji

## W ramach europejskich programów certyfikacji cyberbezpieczeństwa

- ✓ Produkty ICT
- ✓ Usługi ICT
- ✓ Procesy ICT
- ✓ Usługi zarządzane w zakresie bezpieczeństwa

## W ramach krajowych schematów certyfikacji cyberbezpieczeństwa

- ✓ Produkty ICT
- ✓ Usługi ICT
- ✓ Procesy ICT
- ✓ Usługi zarządzane w zakresie bezpieczeństwa
- ✓ Systemy zarządzania cyberbezpieczeństwem
- ✓ Osoby

# Zadania Ministra Cyfryzacji

- Sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa
- Wyrażanie zgody na wydanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”
- Prowadzenie postępowań w sprawie zezwoleń na wykonywanie określonych działań, w przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa tego wymaga
- Przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa

# Krajowy organ ds. certyfikacji cyberbezpieczeństwa



■ strona internetowa: <https://www.gov.pl/web/ncca-pl>



Ministerstwo  
Cyfryzacji



- Partnerstwo publiczno-prywatne realizowane na rzecz krajowego systemu cyberbezpieczeństwa (2019)
- Budowanie zaufanych relacji z partnerami technologicznymi z państw:
  - Unii Europejskiej
  - NATO
  - Państw partnerskich NATO

### **Założenia Programu PWCyber:**

- Dobrowolne i aktywne uczestnictwo w Programie,
- Format partnerstwa - porozumienie jednakowe dla wszystkich podmiotów,
- Brak zobowiązań finansowych,
- Klauzula zachowania poufności wskazanych informacji (NDA),
- Możliwość przystąpienia innych podmiotów – za zgodą obu stron



Ministerstwo  
Cyfryzacji

---



### **Obszary współpracy PW Cyber, w szczególności:**

- Podnoszenie kompetencji podmiotów KSC,
- Identyfikacja i wymiana informacji o podatnościach i zagrożeniach,
- Rekomendacje w zakresie m.in. konfiguracji urządzeń i oprogramowania,
- Promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa



Ministerstwo  
Cyfryzacji

---



■ W ramach PW Cyber działa grupa robocza ds. zamówień publicznych

■ Cele:

- Identyfikacja obszarów istotnych dla zamówień z związanych z cyberbezpieczeństwem,
- Przygotowanie propozycji rozwiązań,
- Wzmocnienie pozycji MŚP



Ministerstwo  
Cyfryzacji



## **Zidentyfikowane obszary istotne dla zamówień z związanych z cyberbezpieczeństwem:**

- podział zamówień,
- zamówienia przedkomercyjne oraz inwestowanie w innowacje,
- kryteria pozacenowe – ograniczenie kryterium ceny
- wstępne konsultacje rynkowe, dialog techniczny
- ujednolicenie wzorów umów, SWZ



# Ministerstwo Cyfryzacji

---

---