Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

FORUM, Katowice
25 czerwca 2025 r.

ŚLĄSKIE FORUM OCHRONY DANYCH OSOBOWYCH. CYBERBEZPIECZEŃSTWO W PRACY IOD

INFORMACJE O FORUM:

Zapraszamy na kolejne spotkanie Śląskiego Forum Ochrony Danych Osobowych, które zrzesza Inspektorów Ochrony Danych Osobowych w JST lub jednostkach podległych oraz innych pracowników, odpowiedzialnych za wszystkie aspekty związane z ochroną danych osobowych, bezpieczeństwem informacji i przetwarzaniem danych.

Celem działania Śląskiego Forum Ochrony Danych Osobowych jest podnoszenie poziomu wiedzy i doskonalenie umiejętności poprzez działalność szkoleniową, konsultacje, wzajemne wspieranie się członków Forum poprzez wymianę doświadczeń i dobrych praktyk w rozwiązywaniu problemów pojawiających się w codziennej pracy. Aby stać się członkiem Forum należy wypełnić deklarację członkowską do pobrania na stronie www.okst.pl w zakładce Fora i przesłać ją na adres koordynatora barbara.tekien@okst.pl

CELE I KORZYŚCI ZE SZKOLENIA:

- Wzmocnienie kompetencji Inspektorów Ochrony Danych w zakresie praktycznej oceny i weryfikacji technicznych i organizacyjnych środków bezpieczeństwa.
- Przejście od teoretycznej znajomości wymogów art. 32 RODO do umiejętności prowadzenia merytorycznego dialogu z działami IT, oceny ryzyka związanego z nowymi technologiami oraz skutecznego zarządzania incydentem naruszenia ochrony danych z perspektywy cybernetycznej.

PROGRAM:

1. Wstęp i najnowsze trendy w cyberzagrożeniach oraz regulacjach:
   a. Powitanie, przedstawienie celu i zakresu szkolenia.
   b. Najnowsze typy zagrożeń: ransomware 2.0, ataki BEC, zagrożenia AI, deepfake.
   c. Aktualne wymagania regulacyjne wobec IOD w zakresie cyberbezpieczeństwa.
   d. Przegląd aktualnych zmian w prawie: RODO, NIS-2, KSC – co już obowiązuje, co wchodzi w życie.
2. RODO, KSC, NIS-2 – nowe obowiązki dla IOD:
   a. RODO a cyberbezpieczeństwo: jakie wymagania realnie dotyczą IOD? Art. 32 – bezpieczeństwo przetwarzania, ocena ryzyka, DPIA, privacy by design.
   b. KSC (Ustawa o Krajowym Systemie Cyberbezpieczeństwa): Zakres podmiotowy, nowelizacja, zmiana podejścia do zgłaszania incydentów.
      - Rola IOD a współpraca z DPO/CSIRT.
   c. NIS-2 (nowa dyrektywa UE): Podmioty kluczowe i ważne – co się zmienia?
      - Nowe obowiązki raportowania i zarządzania incydentami.
      - Minimalne środki bezpieczeństwa i ich praktyczna implementacja.
      - Przykłady konfliktów i synergii pomiędzy regulacjami (RODO vs. NIS-2/KSC).
3. Mapowanie wymagań prawnych na praktyki IT:
   a. Jak przełożyć prawo na konkretne zabezpieczenia techniczne i organizacyjne:

- Szyfrowanie, kontrola dostępu, rejestrowanie zdarzeń.
- Testy penetracyjne i analiza podatności jako element dokumentacji bezpieczeństwa.

b. Procedury obsługi incydentów zgodne z KSC/NIS-2/RODO – omówienie wzorcowej ścieżki: identyfikacja, klasyfikacja, zgłoszenie do CSIRT, notyfikacja do UODO.
c. Warsztat: Opracowanie scenariusza postępowania dla wybranego incydentu.

4. Współpraca z IT, CSIRT i zarządzanie incydentami – poziom średniozaawansowany:
   a. Kiedy i jak angażować IOD w obsługę incydentu cyberbezpieczeństwa? Współpraca z działem IT, zespołem CSIRT, zewnętrznymi konsultantami.
   b. Praktyczne aspekty komunikacji – minimalizacja ryzyka ujawnienia informacji.
   c. Dokumentowanie działań – jakie elementy są kluczowe pod kątem RODO, NIS-2, KSC.
   d. Warsztat: Symulacja meldunku incydentu cyber (scenariusz przygotowany do wspólnego wypełnienia).
5. Przegląd narzędzi i procedur wspierających IOD:
   a. Audyt cyberbezpieczeństwa – praktyka: Przegląd narzędzi open source i komercyjnych wspierających IOD.
   b. Automatyczne skanery podatności, narzędzia do oceny konfiguracji.
   c. Przykłady raportów i checklist (z elementami wykraczającymi poza podstawy).
   d. Zarządzanie politykami bezpieczeństwa – integracja wymagań RODO, KSC, NIS-2.
   e. Monitoring zgodności – jak systematycznie weryfikować poziom zabezpieczeń.
7. Zmiany i trendy w prawie UE i krajowym – przygotowanie na nowe obowiązki:
   a. Omówienie draftów i planowanych zmian:
   b. Nowelizacja ustawy KSC (aktualny status i zakres zmian).
   c. Projekty implementacji NIS-2 w Polsce – na co muszą być gotowe JST, szkoły, urzędy?
   d. Aktualizacje i wytyczne EROD (Europejskiej Rady Ochrony Danych).
   e. Jak przygotować organizację do zmian: Mapowanie procesów pod kątem nowych wymagań.
   f. Szybkie audyty zgodności z nowymi regulacjami – przykłady działań "last minute".
8. Case study: złożone incydenty – analiza i rekomendacje (30 min)
   a. Omówienie złożonych przypadków naruszeń (np. ransomware, wyciek danych z chmury, błędy konfiguracyjne).
   b. Analiza decyzji UODO i przykładów z praktyki CSIRT GOV.
   c. Dyskusja: co można było zrobić lepiej, rekomendacje na przyszłość.
9. Q&A, podsumowanie. Odpowiedzi na pytania.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Śląskie Forum Ochrony Danych Osobowych. Cyberbezpieczeństwo w pracy IOD

Szkolenie będziemy realizowali **w formie stacjonarnej w siedzibie Ośrodka, Katowice, ul. Moniuszki 7, III piętro**.

25 czerwca 2025 r. **Szkolenie w godzinach: 11:00-15:00**

Cena: członkowie Forum w ramach składki, pozostałe osoby 550 PLN netto/os. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:
udział w profesjonalnym szkoleniu,
dostęp do materiałów w formie elektronicznej,
przerwa kawowa,
certyfikat ukończenia szkolenia.

DANE DO KONTAKTU:
Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
Ośrodek Kształcenia Samorządu Terytorialnego im. Waleriana Pańki
ul. Moniuszki 7, 40-005 Katowice
ul. Piłsudskiego 43, 50-032 Wrocław,
tel. 32 259 86 73, 206 98 43
szkolenia@okst.pl; barbara.tekien@okst.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy (dane do faktury)

Nazwa i adres odbiorcy

NIP **Telefon**

1. **Imię i nazwisko uczestnika,**
   stanowisko,
   E-MAIL i TEL. DO KONTAKTU
2. **Imię i nazwisko uczestnika,**
   stanowisko,
   E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe) TAK ☐ NIE ☐

Członek FORUM TAK ☐ NIE ☐

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora **www.okst.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.okst.pl do 23 czerwca 2025 r.

UWAGA Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej _____