Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
11 września 2025 r.

CYBERBEZPIECZEŃSTWO W PRACY INSPEKTORA OCHRONY DANYCH OSOBOWYCH

WAŻNE INFORMACJE O SZKOLENIU:

Zapraszamy na praktyczne szkolenie poświęcone roli Inspektora Ochrony Danych w kontekście rosnących wymagań w zakresie cyberbezpieczeństwa. W trakcie zajęć omówimy aktualne i nadchodzące obowiązki wynikające z przepisów RODO, NIS-2 oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa. Uczestnicy poznają najnowsze typy zagrożeń, takie jak ransomware 2.0, ataki BEC, zagrożenia związane z AI i deepfake, a także dowiedzą się, jak je rozpoznawać, raportować i reagować zgodnie z obowiązującymi regulacjami.

Szkolenie pokaże, jak przełożyć wymagania prawne na realne działania – od szyfrowania i kontroli dostępu po obsługę incydentów i dokumentację działań. Skupiamy się na współpracy IOD z działami IT, zespołami CSIRT i ekspertami ds. bezpieczeństwa. Zajęcia mają charakter praktyczny – uczestnicy wezmą udział w warsztatach, symulacjach incydentów oraz opracują procedury zgodne z przepisami.

Nie zabraknie również przeglądu dostępnych narzędzi wspierających IOD, analizy wytycznych EROD, zapowiadanych zmian w prawie oraz praktycznych wskazówek, jak przygotować organizację na nowe obowiązki.

CELE I KORZYŚCI ZE SZKOLENIA:

- Zdobycie praktycznych umiejętności w zakresie wdrażania i weryfikacji środków cyberbezpieczeństwa wymaganych przez RODO, KSC i NIS-2.
- Wzmocnienie roli IOD jako partnera dla działów IT i zespołów bezpieczeństwa – umiejętność prowadzenia rzeczowej współpracy i komunikacji w sytuacjach incydentalnych.
- Zrozumienie zmian w przepisach prawa i ich wpływu na codzienną pracę IOD – przygotowanie organizacji na nowe obowiązki i wymogi sprawozdawcze.
- Nabycie wiedzy o narzędziach technicznych i procedurach wspierających bezpieczeństwo przetwarzania danych osobowych.
- Praktyczne przećwiczenie procedur zarządzania incydentami – od identyfikacji i analizy ryzyka po zgłoszenie naruszenia do UODO i CSIRT.
- Zdolność do samodzielnego przeprowadzenia wstępnego audytu zgodności i przygotowania rekomendacji w przypadku naruszenia.

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.
   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.

ADRESACI:

Inspektorzy Ochrony Danych Osobowych i wszystkie osoby pełniące obowiązki inspektorów.

PROWADZĄCY:

MBA - CISO, Pełnomocnik Rektora ds. Cyberbezpieczeństwa, Wicedyrektor Centrum Cyberbezpieczeństwa Politechniki Śląskiej, Menedżer Zarządzania Cyberbezpieczeństwem, Architekt: IT/Cyberbezpieczeństwa. Wykładowca: Politechnika Śląska, Akademia WSB, PJATK. (zajęcia na: studiach MBA, podyplomowych CYBER SCIENCE, pierwszy i drugi stopień) Ekspert w systemach IT i OT, członek: PTI, ISSA Polska. Audytor wiodący ISO27001, ISO22301. Posiada certyfikaty PRINCE2, ITIL, AgilePM, CISCO CCNA. Projektuje i wdraża rozwiązania z zakresu Cyberbezpieczeństwa w tym SOC w oparciu o wytyczne NIS2, uKSC, NIST.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Cyberbezpieczeństwo w pracy Inspektora Ochrony Danych Osobowych

Szkolenie będziemy realizowali **w formie webinarium on line**.

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

Cena: 449 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 Centrum Mazowsze ul. Jelinka 6, 01-646 Warszawa tel. 533 849 116, fax: (42) 288 12 86 szkolenia@frdl.org.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.frdl.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.mazowsze.pl do 8 września 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 _____