Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

FORUM, Katowice
6 marca 2025 r.

ŚLĄSKIE FORUM OCHRONY DANYCH OSOBOWYCH. NADZÓR IOD NAD SYSTEMEM OCHRONY DANYCH OSOBOWYCH. JAK SKUTECZNIE POPROWADZIĆ AUDYT Z ELEMENTAMI KRAJOWYCH RAM INTEROPERACYJNOŚCI I CYBERBEZPIECZEŃSTWA

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

WAŻNE INFORMACJE O SZKOLENIU:

Podczas zajęć zostaną wskazane i omówione przez ekspertów praktyczne sposoby prowadzenia nadzoru nad obszarem przetwarzania danych. Przedstawione zostaną najczęściej popełniane błędy przy audytach wraz z omówieniem sposobu ich rozwiązania. Uczestnicy szkolenia zdobędą praktyczną wiedzę i umiejętności w zakresie sposobów dobierania obszarów do audytu oraz dowiedzą się, jaki zakres powinien się znaleźć w obszarze audytowym.

CELE I KORZYŚCI:

- Omówienie planów audytu oraz sposobów gromadzenia informacji uwzględniając KRI.
- Nabycie umiejętności prowadzenia nadzoru IOD nad systemem ochrony danych oraz wskazanie najczęściej popełnianych błędów.
- Pozyskanie dokumentacji w zakresie realizowanego audytu.
- Zdobycie praktycznych umiejętności prowadzenia audytu z poprawnym zapisem w dokumentacji poaudytowej, jak również nabycie umiejętności związanych z wyborem obszarów i zakresu audytu.
- Wskazanie podstawowych zakresów audytu zgodności z krajowymi ramami interoperacyjności.
- Omówienie wymagań dla uczestników programu „Cyberbezpieczny samorząd”.

PROGRAM:

1. **Przygotowanie planu audytu:**
   a. Ustalenie obszarów i zakresu audytu.
   b. Informacja dla działów/osób objętych audytem.
   c. Przygotowanie dokumentacji.
2. **Sposób gromadzenia informacji:**
   a. Bezpośrednio od pracowników objętych audytem.
   b. Informacje pozyskane na podstawie obserwacji/wizji lokalnej.
   c. Działania IOD w związku z kontrolami prowadzonymi przez NIK.
3. **Umowy z podmiotami zewnętrznymi w tym umowy powierzenia:** rejestr umów, poprawność zapisów oraz sposób wyboru podmiotu przetwarzającego.
4. **Sprawdzenie regulacji wewnętrznych w zakresie zmieniającego się otoczenia prawnego w tym:** regulaminu pracy, regulaminu ZFŚS, regulaminu monitoringu.

5. **Ocena prowadzenia rekrutacji w oparciu o KP:** zakres gromadzonych danych, obowiązek informacyjny oraz niszczenie CV.
6. **Ocena sposobu realizacji praw osób**, których dane są przetwarzane w jednostce.
7. **Ocena realizacji obowiązku informacyjnego** w oparciu o art. 13 i 14 RODO.
8. **Analiza ryzyka i rejestr czynności przetwarzania uwzględniająca nowe regulacje prawne:**
   a. Ustawa o ochronie sygnalistów.
   b. Ustawa o ochronie małoletnich(tzw. lex Kamilek).
9. **Ocena postępowania z naruszeniem:**
   a. Informowanie ADO, innych osób funkcyjnych.
   b. Podejmowane działania z określeniem czasu.
   c. Analiza naruszenia, w tym również naruszeń związanych z ceberbezpieczeństwem.
   d. Informowanie UODO oraz osób fizycznych, których naruszenie dotyczy.
10. **Audyt obszaru IT, wybrane zagadnienia:**
    a. Kopie bezpieczeństwa.
    b. Inwentaryzacja sprzętu i oprogramowania z elementami par 20.2.2 rozporządzenia KRI.
    c. Zarządzanie uprawnieniami w oparciu o karty uprawnień.
    d. Dokumentacji systemu zarządzania bezpieczeństwem informacji (SZBI).
11. **Realizacja zadań osób funkcyjnych:**
    a. Administrator systemów informatycznych.
    b. Zespół do utrzymania systemu zarządzania bezpieczeństwem informacji (wymóg zgodny z krajowym systemem cyberbezpieczeństwa oraz KRI).
    c. Kierownicy działów.
12. **Cyberbezpieczeństwo i zakres nadzoru IOD:**
    a. Zagrożenia cybernetyczne w samorządzie i jednostkach organizacyjnych.
    b. Ataki socjotechniczne – przykłady skutecznych ataków na samorządy.
    c. Przykładowe złośliwe oprogramowanie i aplikacje.
    d. Podstawowe zasady bezpiecznego funkcjonowania w sieci.
    e. Pozyskiwanie informacji poprzez pracę online.
    f. Gdzie i jak sprawdzić czy nasze hasła są bezpieczne?
13. **Szkolenia pracowników**, plany szkoleń wraz z tematami.
14. **Ochrona danych osobowych a e-doręczenia. Zawiłości po wejściu obowiązku stosowania ustawy.**
15. **Realizacja wymogów rozporządzenia ws. krajowych ram interoperacyjności** (KRI) uwzględniając program „Cyberbezpieczny samorząd”.
16. **Pytania**, dyskusja na każdym etapie szkolenia.

ADRESACI:

Członkowie Forum ODO, inspektorzy ochrony danych osobowych, pracownicy wydziałów kadr, wszystkie osoby odpowiedzialne za prawidłowe wdrożenie ustawy o ochronie sygnalistów.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Śląskie Forum Ochrony Danych Osobowych. Nadzór IOD nad systemem ochrony danych osobowych Jak skutecznie poprowadzić audyt z elementami krajowych ram interoperacyjności i cyberbezpieczeństwa.

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

6 marca 2025 r. **Szkolenie w godzinach: 10:00-13:00**

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 3 marca 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 _____