

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

### **INFORMACJE O SZKOLENIU:**

Podczas Webinarium zostaną wskazane i omówione przez ekspertów praktyczne sposoby prowadzenia nadzoru nad obszarem przetwarzania danych. Przedstawione zostaną najczęściej popełniane błędy przy audytach wraz z omówieniem sposobów ich rozwiązania. Uczestnicy szkolenia zdobędą 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.

#### **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 14 RODO.
8. 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.
9. 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).
10. 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.
11. Cyberbezpieczeństwo i zakres nadzoru IOD:
  - a. Zagrożenia cybernetyczne w samorządzie i jednostkach organizacyjnych.
  - b. Ataki socjotechniczne – przykłady skutecznych ataków na samorzady.
  - 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?
12. Szkolenia pracowników, plany szkoleń wraz z tematami.
13. Realizacja wymogów rozporządzenia ws. krajowych ram interoperacyjności (KRI) uwzględniając program „Cyberbezpieczny samorząd”.
14. Pytania, dyskusja na każdym etapie szkolenia.

#### **ADRESACI:**

Inspektorzy ochrony danych i ich zastępcy, osoby odpowiedzialne za ochronę danych, kierownicy działów organizacyjnych i IT. Członkowie zespołów ds. utrzymania systemu zarządzania bezpieczeństwem informacji, pełnomocnicy ds. SZBI

#### **PROWADZĄCY:**

**Trener 1** - Inspektor ochrony danych w jednostkach budżetowych, audytor wiodący ISO 27001, nieetatowy współpracownik Instytutu studiów Podyplomowych Wyższej Szkoły Nauk Pedagogicznych w zakresie zajęć o tematyce ochrony danych osobowych w jednostkach publicznych, wieloletni prelegent na kursach i szkoleniach z zakresu ochrony danych osobowych.

**Trener 2** - audytor wewnętrzny bezpieczeństwa informacji normy IOS27001, absolwent studiów podyplomowych na kierunku Inspektor Ochrony Danych. Aktywny członek stowarzyszenia inspektorów ochrony danych (SABI). Posiada doświadczenie w zakresie współpracy z administracją publiczną pełniąc funkcję inspektora ochrony danych oraz obsługując naruszenia ochrony danych. Prowadzi audyty ochrony danych osobowych, audyty bezpieczeństwa systemów informatycznych oraz szkolenia dla pracowników, których tematyka związana jest z danymi osobowymi, prywatnością a także bezpieczeństwem informacji.

## Nadzór IOD nad systemem ochrony danych osobowych. Jak skutecznie poprowadzić audyt z elementami krajowych ram interoperacyjności i cyberbezpieczeństwa



Szkolenie będziemy realizowali w formie webinarium on line.



**25 września 2024 r.**

Szkolenie w godzinach 9:00-14:30



**Cena: 440 PLN netto/os. Przy zgłoszeniu do dnia 2 września 2024 r. obowiązuje cena promocyjna 410 PLN netto/os.**

Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

### CENA zawiera:

udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.

### DANE

### DO

### KONTAKTU:

FRDL Małopolski Instytut Samorządu Terytorialnego i Administracji  
ul. Floriańska 31, 31-019, Kraków  
**Magdalena Stawiarska**, Kierownik zespołu ds. szkoleń  
tel. +48 12 623 72 44, 575 850 930, [szkolenia@mistia.org.pl](mailto:szkolenia@mistia.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

Proszę o przesłanie faktury na adres mailowy: .....

Proszę o przesłanie certyfikatu na adres mailowy: .....

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora [www.mistia.org.pl](http://www.mistia.org.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na [www.mistia.org.pl](http://www.mistia.org.pl) lub mailem na [szkolenia@mistia.org.pl](mailto:szkolenia@mistia.org.pl) do 10 września 2024 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 \_\_\_\_\_