

## **OCHRONA DANYCH OSOBOWYCH W JST: ZARZĄDZANIE, MOŻLIWE RYZYKA, KONTROLE I DOBRE PRAKTYKI**

### **INFORMACJE O SZKOLENIU:**

- W dobie cyfryzacji i rosnącej liczby danych przetwarzanych w sektorze publicznym ochrona danych osobowych stała się jednym z kluczowych wyzwań dla administracji publicznej. Niniejsze szkolenie zostało opracowane z myślą o pracownikach jednostek administracyjnych, którzy w codziennej pracy mają kontakt z różnego rodzaju danymi osobowymi. Głównym celem szkolenia jest przekazanie aktualnej, kompleksowej wiedzy prawnej, a przede wszystkim praktyczne przygotowanie uczestników do bezpiecznego i zgodnego z przepisami zarządzania danymi osobowymi.
- Szkolenie obejmuje kompleksowe ujęcie tematyki ochrony danych osobowych – począwszy od definicji i zasad wynikających z RODO, poprzez procedury reagowania na incydenty, aż po szczegółowe zagadnienia praktyczne, takie jak udostępnianie danych radnym, przetwarzanie danych w czasie pracy zdalnej czy analiza ryzyka. Program zawiera również elementy warsztatowe, przykłady z orzecznictwa oraz dobre praktyki i zalecenia wynikające z raportów NIK i decyzji PUODO.

### **CELE I KORZYŚCI:**

- Rozpoznanie różnic między naruszeniem ochrony danych osobowych a naruszeniem przepisów RODO; zrozumienie zagrożeń wynikających z naruszeń oraz sposobów reagowania.
- Omówienie zasad udostępniania danych pracownikom oraz interesantom, w tym zagadnień związanych z interesem prawnym i zasadami ochrony prywatności.
- Przedstawienie zasad dostępu do informacji publicznej oraz ograniczeń wynikających z ochrony prywatności i tajemnicy przedsiębiorcy.
- Przedstawienie podstaw prawnych oraz ograniczeń przy udostępnianiu danych radnym.
- Wyjaśnienie zasad udzielania informacji przez urzędników podczas rozmów telefonicznych.
- Omówienie procedur uzyskiwania zgody na przetwarzanie danych oraz sytuacji, w których jest to wymagane.
- Zapoznanie uczestników z podstawami prawnymi, które umożliwiają przetwarzanie danych w administracji publicznej.
- Zaprezentowanie przepisów sektorowych (np. KPA) oraz procedur przekazywania podań do właściwych organów.
- Praktyczne omówienie procedur i instrukcji dotyczących realizacji praw osób, których dane są przetwarzane.
- Zwiększenie świadomości pracowników o zagrożeniach związanych z niewłaściwym zarządzaniem uprawnieniami oraz zasady minimalizacji ryzyka.
- Omówienie zagrożeń związanych z wykorzystywaniem służbowej poczty e-mail oraz zasad bezpiecznego przetwarzania danych w tym obszarze.
- Przedstawienie metodologii analizy ryzyka w kontekście ochrony danych oraz bezpieczeństwa informacji.
- Omówienie przykładów zabezpieczeń fizycznych oraz technicznych stosowanych w administracji.
- Analiza zagrożeń związanych z przetwarzaniem danych w trybie mobilnym oraz podczas pracy zdalnej.
- Omówienie dodatkowych szkoleń (cyberbezpieczeństwo, bezpieczeństwo systemów, bezpieczeństwo fizyczne) oraz analiza raportów NIK dotyczących ochrony danych.
- Zapoznanie uczestników z przykładami decyzji PUODO, w tym kar nałożonych na administrację publiczną oraz omówienie ich implikacji.

### **PROGRAM:**

- 1. Wprowadzenie do Ochrony Danych Osobowych:**
  - a. Definicje danych osobowych i kategorii szczególnych.

- b. Podstawowe zasady przetwarzania danych: legalność, celowość, proporcjonalność, minimalizacja danych, prawidłowość, ograniczenie przechowywania i poufność.
  - c. Przegląd regulacji prawnych: RODO, ustawy krajowe dotyczące ochrony danych.
  - d. Zmiany w otoczeniu prawnym.
- 2. Naruszenia Ochrony Danych:**
- a. Różnice między „naruszeniem ochrony danych osobowych” a naruszeniem przepisów RODO.
  - b. Dlaczego naruszenia ochrony danych osobowych są niebezpieczne?
  - c. Przykłady naruszeń w administracji publicznej.
  - d. Procedury zgłaszania naruszeń przez pracowników oraz administratora danych.
  - e. Zasady informowania osób fizycznych o naruszeniach.
  - f. Metody oceny naruszenia – jak rozpoznać incydent oraz procedury reagowania.
  - g. Sposoby minimalizacji skutków naruszeń oraz działania korygujące.
- 3. Udostępnianie Danych Osobowych:**
- a. Wątpliwości związane z udostępnianiem danych – kto i na jakich zasadach może udostępniać dane.
  - b. Interes prawny osoby – kryteria oceny.
  - c. Analiza przypadków udostępniania danych sądom, prokuraturze, policji, komornikowi.
- 4. Dostęp do Informacji Publicznej:**
- a. Prawa do informacji publicznej – podstawy prawne i ograniczenia.
  - b. Przykłady sytuacji, w których informacja powinna zostać ograniczona.
  - c. Zasady skutecznej anonimizacji danych.
  - d. Jak postępować w przypadku błędnie zaadresowanego wniosku o informację publiczną.
- 5. Zasady udostępniania danych radnym:**
- a. Podstawy prawne dotyczące udostępniania danych radnym - czego może żądać radny i na jakich zasadach?
  - b. Ograniczenia przekazywanych informacji – ochrona prywatności osób fizycznych.
  - c. Przykłady praktyczne i analiza przypadków dostępu radnych do danych osobowych.
- 6. Komunikacja Telefoniczna i Przekazywanie Informacji:**
- a. Co może powiedzieć urzędnik podczas udzielania informacji telefonicznie?
  - b. Przykłady „bezpiecznych” i „ryzykownych” informacji.
- 7. Pozyskiwanie zgody w Administracji Publicznej:**
- a. Sytuacje, w których zgoda jest niezbędna.
  - b. Przykłady prawidłowego pozyskiwania zgody.
  - c. Dokumentacja i wymagania formalne.
- 8. Podstawy prawne przetwarzania danych:**
- a. Podstawa prawna przetwarzania danych: umowa, przepis prawa, interes publiczny.
  - b. Obowiązek informacyjny – sposoby spełnienia wymogów, zasady podpisu, przejrzystości i ewentualne zwolnienia.
- 9. Przepisy sektorowe i przekazywanie wniosków:**
- a. Zasady wynikające z KPA w kontekście obowiązków informacyjnych.
  - b. Przekazanie podania do właściwego organu – omówienie sytuacji, gdy wniosek jest błędnie zaadresowany, zgodnie z art. 65 KPA - czy wniosek z innej instytucji należy przekazać czy odesłać?
- 10. Realizacja Praw Podmiotu Danych – Procedury i Instrukcje:**
- a. Procedury zgłaszania wniosków o dostęp do danych, ich sprostowanie, usunięcie czy ograniczenie przetwarzania
  - b. Rola administratora danych i obowiązek informacyjny.
- 11. Bezpieczeństwo Pracowników i Zasady Minimalnych Uprawnień:**
- a. Zagrożenia wynikające z niewystarczającej kontroli uprawnień: błędy ludzkie, brak zasad minimalnych uprawnień, nieodebrane uprawnienia.
  - b. Przykłady problemów związanych z nadmiernymi uprawnieniami.
  - c. Rekomendacje dotyczące audytów i regularnych przeglądów uprawnień.
- 12. Bezpieczeństwo komunikacji elektronicznej:**
- a. Zagrożenia związane z komunikacją e-mailową.
  - b. Sposoby minimalizacji ryzyka, m.in. zasady bezpiecznego przesyłania informacji i szyfrowanie.
  - c. Przykłady dobrych praktyk w administracji publicznej.
- 13. Analiza Ryzyka dla Ochrony Danych i Bezpieczeństwa Informacji:**
- a. Różnice między analizą ryzyka dla ochrony danych a analizą ryzyka dla bezpieczeństwa informacji.
  - b. Metody identyfikacji zagrożeń i oceny ryzyka.
  - c. Przykłady narzędzi i procedur stosowanych w analizie ryzyka.

#### **14. Rejestr czynności przetwarzania:**

- a. Elementy, które powinien zawierać rejestr: opis operacji przetwarzania, kategorie danych, kategorie odbiorców, środki techniczne i organizacyjne.
- b. Kto powinien mieć dostęp do rejestru i zasady jego regularnej aktualizacji.

#### **15. Fizyczne i techniczne zabezpieczenia danych:**

- a. Przykłady zabezpieczeń fizycznych: kontrola dostępu do pomieszczeń, monitoring, systemy alarmowe.
- b. Przykłady zabezpieczeń technicznych: zabezpieczenia sieci, systemy backupu, oprogramowanie antywirusowe.
- c. Znaczenie monitorowania i aktualizacji zabezpieczeń.

#### **16. Rozliczalność zgodnie z RODO:**

- a. Znaczenie rozliczalności w przetwarzaniu danych.
- b. Przykłady dobrych praktyk w dokumentowaniu procesów i audytach wewnętrznych.

#### **17. Przetwarzanie mobilne i praca zdalna:**

- a. Zagrożenia bezpieczeństwa związane z urządzeniami mobilnymi i pracą zdalną.
- b. Środki zapobiegawcze – polityka BYOD, VPN, szkolenia użytkowników.
- c. Przykłady incydentów i procedury reagowania.

#### **18. Szkolenia Komplementarne i Raporty NIK:**

- a. Programy szkoleniowe dla pracowników – tematyką cyberbezpieczeństwa, ochrony danych i bezpieczeństwa fizycznego, bezpiecznego korzystania z stacji roboczych.
- b. Analiza raportów NIK – przykłady, wnioski i rekomendacje wynikające z audytów.

#### **19. Przykładowe Decyzje PUODO:**

- a. Analiza wybranych decyzji PUODO.
- b. Konsekwencje naruszeń ochrony danych i zasady sankcji.
- c. Wnioski i rekomendacje dla administracji publicznej.

#### **20. Podsumowanie i sesja pytań.**

#### **ADRESACI:**

- Osoby funkcyjne w urzędach - dyrektorzy, naczelnicy wydziałów/referatów, osoby odpowiedzialne za bezpieczeństwo systemów informatycznych tzw. ASI, Inspektorzy Ochrony danych, pełnomocnicy SZBI, audytorzy wewnętrzni w urzędach;
- Dyrektorzy/kierownicy jednostek organizacyjnych, IOD w tych jednostkach, IT w tych jednostkach;
- Osoby odpowiedzialne za zarządzanie bezpieczeństwem w jednostkach budżetowych;
- Kierownictwo urzędów: wójtowie, burmistrzowie, starostowie i ich zastępcy.

#### **PROWADZĄCY:**

**Prowadzący I** - nieetatowy współpracownik Wyższej Szkoły Nauk Pedagogicznych w Warszawie, audytor w zakresie realizacji wymagań zgodnych z KRI oraz audytor wiodący ISO 27001, obecnie zatrudniony jako inspektor ochrony danych w jednostkach samorządu terytorialnego, prelegent z wieloletnim doświadczeniem na szkoleniach z zakresu ochrony danych osobowych w jednostkach sektora publicznego. Wykładowca ceniony i polecany przez członków Forum Ochrony Danych działającego przy FRDL.

**Prowadzący II** - 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.

### Ochrona danych osobowych w JST: zarządzanie, możliwe ryzyka, kontrole i dobre praktyki



Szkolenie będziemy realizowali w formie webinarium on line.



**24 czerwca 2025 r.**

**Szkolenie w godzinach 9:00-13:00**



**Cena: 449 PLN netto/os. UWAGA! Przy zgłoszeniu na szkolenie do 3 czerwca 2025 r. cena: 419 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:** Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego, MISTiA  
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 przestać poprzez formularz zgłoszenia  
na [www.mistia.org.pl](http://www.mistia.org.pl) do 18 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 \_\_\_\_\_