

## **OCHRONA DANYCH W ADMINISTRACJI PUBLICZNEJ - NA CO NAPRAWDĘ NALEŻY ZWRÓCIĆ UWAGĘ — BŁĘDY, DECYZJE, SKARGI I WYROKI**

### **WAŻNE INFORMACJE O SZKOLENIU:**

Podczas proponowanego szkolenia szczególnie uwaga zostanie zwrócona na realne problemy występujące w administracji publicznej w tym: BIP, sesje rady, publikacje internetowe, korespondencja, naruszenia, nośniki danych, praca zdalna, monitoring, komunikaty prasowe, dostawcy i rozliczalność.

W 2024 r. do Prezesa UODO wpłynęło 8056 skarg oraz 14 842 zgłoszenia naruszeń ochrony danych osobowych. Wśród problemów wskazano m.in. udostępnianie danych w BIP, wysyłkę e-mail bez UDW, monitoring wizyjny, błędną adresację korespondencji, nieprawidłową anonimizację, zagubienie korespondencji, nieuprawniony dostęp do baz danych i kradzież nośnika danych.

Dodatkowo w planie kontroli sektorowych UODO na 2026 r. znalazły się podmioty prowadzące BIP, w szczególności w zakresie anonimizacji danych oraz udostępniania przebiegu sesji rad gminy.

### **CELE I KORZYŚCI:**

**Po szkoleniu uczestnik powinien umieć:**

- odróżnić jawność informacji publicznej od dowolnego publikowania danych osobowych;
- ocenić, kiedy dokument, nagranie, skan lub załącznik w BIP wymaga anonimizacji;
- rozpoznać naruszenie ochrony danych osobowych i podjąć decyzję: rejestr, zgłoszenie do UODO, zawiadomienie osoby;
- wskazać najczęstsze błędy przy nośnikach danych, pracy zdalnej, migracji danych i ransomware;
- ocenić ryzyka związane z monitoringiem, nagrywaniem dźwięku i publikacją nagrań;
- przygotować bezpieczniejszy komunikat prasowy lub informację publiczną;
- wskazać, jakie dowody powinien posiadać administrator, aby wykazać rozliczalność.

### **PROGRAM:**

#### **1. Ochrona danych w administracji — gdzie realnie powstają problemy”:**

- a. różnica między „mamy podstawę prawną do prowadzenia Obszary” a „możemy ujawnić dane publicznie”;
- b. najczęstsze źródła skarg i naruszeń: BIP, e-mail, korespondencja, monitoring, nośniki, praca zdalna, komunikaty prasowe;
- c. rola IOD: konsultacja przed działaniem, a nie po publikacji lub po incydencie.

#### **2. Jawność działania organu a ochrona danych osobowych:**

- a. ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej a RODO;
- b. BIP, strona internetowa, załączniki, skany, metadane, podpisy, numery PESEL, adresy, dane dzieci, dane o zdrowiu;
- c. nagrania sesji rady gminy, transmisje, YouTube, przechowywanie nagrań;
- d. dane „techniczne” i „publiczne”, które nadal mogą być danymi osobowymi.
- e. Obszary do omówienia:
  - Burmistrz Aleksandrowa Kujawskiego — BIP, YouTube, retencja, powierzenie.
  - NSA 28 lutego 2024 r. oddalił skargę kasacyjną burmistrza i utrzymał decyzję UODO dotyczącą m.in. braku umów powierzenia przy BIP, braku polityk dotyczących danych w BIP, okresów przetwarzania oraz nieprawidłowości przy publikacji nagrań sesji na YouTube.
  - Geoportal i numery ksiąg wieczystych.
  - NSA 28 stycznia 2025 r. potwierdził stanowisko UODO, że numer księgi wieczystej jest daną osobową, a jego publikacja bez podstawy prawnej narusza przepisy o ochronie danych.
  - Nagrania sesji rady gminy.

- UODO wskazuje, że przy nagrywaniu i transmisjach posiedzeń organów JST administratorzy muszą uwzględniać minimalizację, anonimizację i zasady udostępniania nagrań. Wyrok NSA z 13 lipca 2023 r., sygn. III OSK 595/22, dotyczący ujawnienia danych osoby fizycznej w nagraniu z sesji rady.
  - f. Ćwiczenie: Ocena przykładowego dokumentu do publikacji w BIP: co zostawić, co zanonimizować, czego nie publikować, co wymaga decyzji kierownika jednostki lub konsultacji z IOD.
- 3. Naruszenia ochrony danych w urzędzie i jednostce publicznej:**
- a. czym jest naruszenie ochrony danych osobowych;
  - b. naruszenie poufności, integralności i dostępności;
  - c. rejestr naruszeń;
  - d. zgłoszenie do Prezesa UODO w terminie 72 godzin;
  - e. zawiadomienie osób, których dane dotyczą;
  - f. błędy w ocenie ryzyka;
  - g. typowe zdarzenia: błędny adresat, e-mail bez UDW, zagubiona korespondencja, załącznik do niewłaściwej osoby, publikacja niezanonimizowanego dokumentu.
  - h. Obszar do omówienia:
    - Sąd Okręgowy w Krakowie — uszkodzona i niekompletna przesyłka sądowa.
    - Prezes UODO stwierdził naruszenie obowiązków z art. 33 i art. 34 RODO, wskazując na brak zgłoszenia naruszenia oraz brak zawiadomienia osób, których dane dotyczyły. Obszar pokazuje problem oceny ryzyka przy korespondencji zawierającej dane wrażliwe, w tym dane dotyczące zdrowia i dane dzieci.
  - i. Ćwiczenie: Uczestnicy otrzymują trzy krótkie opisy zdarzeń i kwalifikują je jako:
    - tylko wpis do rejestru naruszeń;
    - zgłoszenie do UODO;
    - zgłoszenie do UODO + zawiadomienie osób;
    - brak naruszenia, ale incydent organizacyjny do udokumentowania.
- 4. Bezpieczeństwo techniczne i organizacyjne — nośniki, praca zdalna, ransomware:**
- a. art. 32 RODO w praktyce administracji;
  - b. analiza ryzyka jako dokument roboczy, a nie formalność;
  - c. szyfrowanie laptopów i nośników;
  - d. prywatne pendrive'y, eksporty danych, migracje systemów;
  - e. kopie zapasowe, testy odtworzeniowe, ransomware;
  - f. praca zdalna i urządzenia prywatne;
  - g. dowody zabezpieczeń: polityki, logi, protokoły, testy, potwierdzenia konfiguracji.
  - h. Obszary do omówienia:
    - Kutno — MOPS, MOSiR i zgubiony nieszyfrowany pendrive.
    - UODO nałożył kary na dwie instytucje miejskie oraz spółkę obsługującą zmianę systemu kadrowo-płacowego. Problemem była utrata nieszyfrowanego pendrive'a z danymi ok. 1500 osób oraz brak skutecznej analizy ryzyka przy migracji danych.
    - Sąd Rejonowy w Zgierzu — kurator i niezaszyfrowany pendrive.
    - Obszar dotyczył zgubienia niezaszyfrowanego nośnika z danymi ok. 400 osób, w tym danymi o zdrowiu i wyrokach skazujących. UODO podkreślił, że administrator nie może ograniczyć się do procedur i szkoleń, jeżeli ryzyko wymaga realnych zabezpieczeń technicznych.
    - Sanepid w Policach — prywatny pendrive z danymi 4200 osób.
    - UODO nałożył 20 tys. zł kary za brak odpowiednich zabezpieczeń i analizy ryzyka. Organ wskazał, że samo zakazanie używania nośników nie wystarczy, jeżeli organizacja nie testuje skuteczności tego założenia i nie wdraża realnych kontroli.
    - Rzecznik Finansowy — prywatny komputer i praca zdalna.
    - WSA podtrzymał upomnienie UODO. Problemem był brak analizy ryzyka przy pracy zdalnej i korzystaniu z prywatnych komputerów oraz brak pewności czy dane zostały skutecznie usunięte po zakończeniu pracy.
    - GOPS Aleksandrów — ransomware i utrata dostępności danych.
    - UODO wskazał na niewystarczające zabezpieczenia techniczne i organizacyjne oraz niewłaściwą analizę ryzyka. Nałożono kary na GOPS i Wójta.
  - i. Ćwiczenie: Minimalny zestaw zabezpieczeń dla urzędu/jednostki: laptop, pendrive, praca zdalna, backup, eksport danych do dostawcy, migracja systemu.
- 5. Monitoring, nagrywanie obrazu i dźwięku:**
- a. monitoring wizyjny w jednostkach publicznych;
  - b. różnica między rejestracją obrazu a rejestracją dźwięku;
  - c. cele monitoringu, strefy, oznaczenia, retencja, dostęp do nagrań;
  - d. monitoring w szkołach, OPS/CUS, urzędach, jednostkach pomocniczych;
  - e. udostępnianie nagrań policji, stronie postępowania, osobie zainteresowanej;

- f. ryzyko nagrywania danych szczególnych kategorii.
- g. Obszar do omówienia:
  - Stołeczny Ośrodek dla Osób Nietrzeźwych — nagrywanie dźwięku.
  - WSA w Warszawie oddalił skargę m.st. Warszawy na decyzję UODO. Obszar dotyczyła nagrywania i utrwalania głosu w systemie monitoringu. UODO wskazał, że rejestracja dźwięku wymaga wyraźnej podstawy prawnej i jest znacznie bardziej ingerująca niż sam obraz.

#### **6. Komunikacja publiczna organu — rzecznik, promocja, konferencje, social media:**

- a. komunikat prasowy jako przetwarzanie danych osobowych;
- b. odpowiedzi dla mediów;
- c. konferencje prasowe;
- d. publikacje w mediach społecznościowych;
- e. dane dotyczące zdrowia, życia rodzinnego, sytuacji kryzysowej, przemocy, pomocy społecznej;
- f. zasada minimalizacji w komunikacji publicznej.
- g. Obszary do omówienia:
  - Komendant Główny Policji — konferencja prasowa i dane o zdrowiu.
  - WSA w Warszawie wyrokiem z 28 stycznia 2026 r., sygn. II SA/Wa 890/25, oddalił skargę Komendanta Głównego Policji na decyzję UODO. Decyzja dotyczyła ujawnienia podczas konferencji prasowej danych i informacji o stanie zdrowia kobiety; kara wyniosła 75 tys. zł.
  - Komendant Miejski Policji w Krakowie — komunikat prasowy.
  - UODO nałożył łącznie 78 tys. zł kary za ujawnienie danych kobiety w komunikacie prasowym oraz brak należytego nadzoru nad procesami przetwarzania. Organ podkreślił, że prawo pozyskania danych w ramach czynności służbowych nie oznacza prawa do ich późniejszego publicznego ujawnienia.
- h. Ćwiczenie: Przeredagowanie komunikatu prasowego tak, aby przekazywał informację publiczną, ale nie ujawniał zbędnych danych osobowych.

#### **7. Dostawcy, powierzenie i rozliczalność:**

- a. kiedy potrzebna jest umowa powierzenia;
- b. dostawcy BIP, hosting, transmisje sesji, systemy dziedzinowe, obsługa IT, kadry-płace, SMS, poczta, monitoring;
- c. migracja danych do nowego systemu;
- d. jak sprawdzać procesora przed rozpoczęciem współpracy;
- e. co powinno być dowodem: umowa, zakres przetwarzania, instrukcje, analiza ryzyka, protokół przekazania danych, potwierdzenie usunięcia danych, szyfrowanie nośników, rejestr operacji.
- f. Case powracający: Aleksandrów Kujawski pokazuje problem braku powierzenia przy BIP i usługach technicznych, a Kutno pokazuje ryzyko przy migracji danych kadrowo-płacowych i przekazywaniu danych przez nośniki.
- g. Ćwiczenie: Lista pytań kontrolnych do dostawcy przed przekazaniem danych: kto przetwarza, gdzie, na jakim sprzęcie, w jakim systemie, jak szyfruje, kto usuwa, kto odpowiada za incydent.

#### **8. Podsumowanie praktyczne — lista kontrolna administratora:**

- a. 10 pytań, które urząd powinien zadać przed publikacją danych;
- b. 10 pytań, które należy zadać po incydencie;
- c. 10 dowodów, które administrator powinien mieć „na stole” przy kontroli UODO.

#### **ADRESACI:**

kierownictwo jednostek, sekretarze, pracownicy merytoryczni, osoby prowadzące BIP, biuro rady, promocja/rzecznik prasowy, IOD, ASI/IT, pracownicy OPS/CUS, szkół, jednostek organizacyjnych JST.

#### **PROWADZĄCY:**

**Trener 1** - 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.

**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.

## Ochrona danych w administracji publicznej - na co naprawdę należy zwrócić uwagę — błędy, decyzje, skargi i wyroki



Szkolenie będziemy realizowali w formie **webinarium online**.



**11 czerwca 2026 r.**

**Szkolenie w godzinach 9.00-13.30**



**Cena: 479 zł netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

**CENA zawiera:** udział w profesjonalnym szkoleniu online z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.

**DANE DO KONTAKTU:** Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regułskiego, 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

## DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

(dane do faktury)

**Nazwa i adres nabywcy**

**NIP Nabywcy**

**Nazwa i adres odbiorcy**

**NIP Odbiorcy**

**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

**Faktura zostanie wystawiona jako faktura ustrukturyzowana w Krajowym Systemie e-Faktur (KSeF).**

**Uwagi:** .....

**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) do 8 czerwca 2026 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 faktury w KSeF.**

Podpis osoby upoważnionej \_\_\_\_\_