

OCHRONA DANYCH W ADMINISTRACJI I SAMORZĄDZIE – PRAKTYCZNE ZASADY BEZPIECZNEJ PRACY Z INFORMACJĄ

WAŻNE INFORMACJE:

Ochrona danych osobowych i informacji służbowych w administracji to nie teoretyczne paragrafy, lecz codzienna praktyka i unikanie kosztownych pomyłek. Każdego dnia urzędnicy przetwarzają dane mieszkańców, wysyłają setki e-maili, przygotowują dokumenty do BIP, a coraz częściej sięgają także po nowe technologie i narzędzia sztucznej inteligencji (ChatGPT, Copilot, Gemini). Chwila uwagi – wiadomość wysłana do niewłaściwego adresata, niezaanonimizowany załącznik w BIP czy bezrefleksyjne wklejenie dokumentu do darmowego AI – może prowadzić do poważnego naruszenia i kontroli UODO.

Szkolenie zostało zaprojektowane jako praktyczny warsztat bezpiecznej pracy z informacją, pozbawiony trudnego, akademickiego języka. Prowadzący – doświadczony ekspert ds. nowych technologii i cyberbezpieczeństwa Łukasz Bogdali – w przystępny sposób przeanalizuje rzeczywiste przypadki z urzędów i wskaże proste nawyki, które chronią przed wyciekiem danych.

Podczas spotkania przeanalizujemy:

- Pułapki e-mail i dokumentacji papierowej – jak unikać błędów w polach DO/DW/UDW, bezpiecznie przysyłać załączniki oraz przestrzegać zasad czystego biurka i ekranu.
- Publikowanie informacji w BIP i nagrania z sesji – jak prawidłowo anonimizować dokumenty przed publikacją i bezpiecznie udostępniać materiały z posiedzeń organów.
- Sztuczna inteligencja (AI) w urzędzie – jak bezpiecznie i odpowiedzialnie korzystać z narzędzi AI bez ryzyka ujawnienia danych służbowych.
- Reagowanie na naruszenia bez lęku – co zrobić krok po kroku w razie popełnienia błędu, dlaczego nie wolno go ukrywać i jak szybko zminimalizować skutki zdarzenia.

CELE I KORZYŚCI:

- Opanujesz praktyczne zasady ochrony danych i informacji służbowych, co pozwoli Ci bezpiecznie i pewnie realizować codzienne obowiązki urzędnicze.
- Wyeliminujesz najczęstsze błędy w komunikacji e-mailowej i pracy z dokumentami, zapobiegając przypadkowemu wyciekowi danych do nieuprawnionych osób.
- Nauczysz się bezbłędnie anonimizować dokumenty publikowane w Biuletynie Informacji Publicznej oraz na stronach internetowych jednostki.
- Dowiesz się, jak bezpiecznie korzystać z nowych technologii i sztucznej inteligencji (AI) bez złamania przepisów RODO i procedur wewnętrznych.
- Poznasz jasne procedury postępowania w przypadku naruszenia, dzięki czemu w sytuacji kryzysowej zareagujesz szybko, spokojnie i zgodnie z prawem.
- Zbudujesz właściwe nawyki bezpiecznej pracy zdalnej i stacjonarnej (kontrola dostępu, zasada czystego biurka i ekranu, ochrona nośników USB i telefonów).
- Przeanalizujesz realne przykłady i decyzje UODO dotyczące sektorów publicznych, co pozwoli Ci wyciągnąć wnioski z błędów innych i skutecznie zabezpieczyć swoją jednostkę.

PROGRAM:

1. Ochrona danych – co pracownik administracji powinien wiedzieć:

- a. dane osobowe w codziennej pracy – jak je rozpoznawać, przykłady danych przetwarzanych przez urzędy i jednostki organizacyjne,
- b. dane zwykłe oraz szczególne kategorie danych,
- c. czym jest przetwarzanie danych,
- d. podstawowe zasady ochrony danych wynikające z RODO,

- e. minimalizacja danych – dlaczego nie należy gromadzić, wykorzystywać i udostępniać więcej informacji, niż jest to potrzebne,
 - f. administrator, Inspektor Ochrony Danych i pracownik – podstawowy podział odpowiedzialności,
 - g. ochrona danych osobowych a ochrona informacji służbowych.
- 2. Dokumenty i dane w codziennej pracy urzędu:**
- a. bezpieczna praca z dokumentacją papierową i elektroniczną,
 - b. dokumenty pozostawiane na biurku, drukarce i w pomieszczeniach wspólnych,
 - c. kopiowanie, skanowanie, drukowanie i niszczenie dokumentacji,
 - d. zasada czystego biurka i czystego ekranu,
 - e. przenoszenie dokumentów i danych poza miejsce pracy,
 - f. korzystanie z pamięci USB i innych nośników,
 - g. wykonywanie zdjęć dokumentów telefonem,
 - h. udostępnianie dokumentów współpracownikom,
 - i. dostęp do danych zgodnie z zakresem obowiązków i posiadanymi uprawnieniami,
 - j. przykłady najczęstszych błędów pracowników prowadzących do nieuprawnionego ujawnienia informacji.
- 3. Poczta elektroniczna i elektroniczna wymiana informacji:**
- a. dane osobowe przesyłane pocztą elektroniczną,
 - b. wysłanie wiadomości do niewłaściwego odbiorcy,
 - c. pomyłki podczas dołączania załączników,
 - d. pola DO, DW i UDW oraz ryzyko ujawnienia adresów odbiorców,
 - e. sprawdzanie adresata i załączników przed wysłaniem wiadomości,
 - f. bezpieczne przekazywanie dokumentów i plików,
 - g. udostępnianie dokumentów za pomocą linków,
 - h. przysyłanie dokumentów służbowych na prywatne skrzynki pocztowe,
 - i. komunikatory i inne kanały wymiany informacji,
 - j. praktyczne sposoby ograniczania ryzyka przypadkowego ujawnienia danych.
- 4. Dostęp do danych, pliki współdzielone, chmura i praca poza urzędem:**
- a. indywidualne konta użytkowników i odpowiedzialność za dostęp,
 - b. współdzielone foldery i zasoby sieciowe,
 - c. nadawanie dostępu do dokumentów tylko właściwym osobom,
 - d. kontrolowanie uprawnień do udostępnionych plików,
 - e. bezpieczne korzystanie z usług chmurowych,
 - f. pozostawianie aktywnej sesji na komputerze,
 - g. urządzenia mobilne wykorzystywane do pracy,
 - h. praca zdalna i praca poza siedzibą jednostki,
 - i. korzystanie z prywatnego sprzętu do realizacji obowiązków służbowych,
 - j. podstawowe techniczne i organizacyjne zabezpieczenia danych z perspektywy użytkownika.
- 5. Publikowanie informacji – BIP, strony internetowe i nagrania:**
- a. ochrona danych a obowiązek publikowania informacji przez administrację,
 - b. znaczenie minimalizacji danych przed publikacją,
 - c. przygotowanie dokumentów do udostępnienia w Internecie,
 - d. anonimizacja danych w publikowanych dokumentach – praktyczne przykłady,
 - e. sprawdzanie treści dokumentu oraz jego załączników przed publikacją,
 - f. ryzyko związane z publikowaniem skanów dokumentów,
 - g. przypadkowe ujawnienie danych w Biuletynie Informacji Publicznej,
 - h. transmisje i nagrania z posiedzeń organów samorządowych – ryzyko przypadkowego ujawnienia danych,
 - i. przygotowanie dokumentów i informacji wykorzystywanych podczas transmitowanego posiedzenia,
 - j. publikowanie i przechowywanie nagrań,
 - k. aktualne obszary zainteresowania i kontroli UODO dotyczące BIP,
 - l. omówienie rzeczywistych przypadków niewłaściwego opublikowania danych przez podmioty publiczne.
- 6. Naruszenie ochrony danych – co powinien zrobić pracownik:**
- a. czym jest naruszenie ochrony danych,
 - b. przykłady zdarzeń, które mogą prowadzić do naruszenia:
 - o wiadomość wysłana do niewłaściwej osoby,
 - o niewłaściwy załącznik,
 - o zgubienie dokumentacji,
 - o utrata telefonu, laptopa lub nośnika danych,

- pozostawienie dokumentów w miejscu dostępnym dla osób nieuprawnionych,
 - uzyskanie dostępu do konta pracownika przez osobę nieuprawnioną,
 - przypadkowa publikacja danych w Internecie lub BIP,
 - c. pierwsze działania po zauważeniu problemu,
 - d. dlaczego nie należy ukrywać błędu ani zwlekać z jego zgłoszeniem,
 - e. zabezpieczenie informacji dotyczących zdarzenia,
 - f. zgłoszenie zdarzenia zgodnie z procedurami obowiązującymi w jednostce,
 - g. rola przełożonego, administratora systemu i Inspektora Ochrony Danych w dalszej ocenie zdarzenia,
 - h. omówienie rzeczywistych przypadków naruszeń i ich konsekwencji.
- 7. Sztuczna inteligencja i nowe technologie a ochrona danych:**
- a. ChatGPT, Microsoft Copilot, Gemini i inne narzędzia AI jako elementy współczesnego środowiska pracy,
 - b. jakie informacje przekazujemy narzędziom AI podczas wpisywania poleceń i przesyłania plików,
 - c. dlaczego nie należy bezrefleksyjnie przekazywać narzędziom AI danych osobowych i dokumentów służbowych,
 - d. praca z dokumentem zawierającym dane a możliwość jego wcześniejszego zanonimizowania,
 - e. korzystanie z prywatnych kont i ogólnodostępnych usług AI do zadań służbowych,
 - f. narzędzia dopuszczone przez organizację a samodzielnie wybierane usługi internetowe,
 - g. znaczenie wewnętrznych zasad i procedur korzystania z AI,
 - h. przykłady bezpiecznych i ryzykownych zastosowań AI podczas pracy z informacjami,
 - i. nowe technologie a odpowiedzialność użytkownika za przekazywane dane.
- 8. Aktualne przypadki i dobre praktyki w administracji** - W poszczególnych częściach szkolenia omawiane będą aktualne przypadki, decyzje i stanowiska dotyczące ochrony danych, ze szczególnym uwzględnieniem administracji publicznej i samorządu, m.in.:
- a. publikowania niezanonimizowanych dokumentów,
 - b. ujawnienia danych w BIP,
 - c. błędnego przesłania danych,
 - d. niewłaściwego udostępnienia dokumentów,
 - e. utraty danych lub urządzenia,
 - f. ujawnienia informacji osobie nieuprawnionej,
 - g. danych pojawiających się podczas transmisji i w nagraniach,
 - h. wykorzystania sztucznej inteligencji i usług internetowych do pracy z dokumentami.

ADRESACI:

- Szkolenie skierowane jest przede wszystkim do pracowników administracji publicznej i samorządowej, w szczególności urzędów gmin, miast, starostw, jednostek organizacyjnych, ośrodków pomocy społecznej, centrów usług wspólnych oraz innych podmiotów publicznych.
- Jest przeznaczone dla osób, które w codziennej pracy mają kontakt z dokumentami, danymi mieszkańców, pracowników, klientów lub interesantów oraz korzystają z poczty elektronicznej, systemów informatycznych, BIP, usług chmurowych i narzędzi cyfrowych.

Ochrona danych w administracji i samorządzie – praktyczne zasady bezpiecznej pracy z informacją



Szkolenie będziemy realizowali w formie webinarium online.



16 listopada 2026 r.

Szkolenie w godzinach: 9:00 – 13:30



Cena: 479 PLN netto/os. W przypadku zgłoszenia do 27 października cena wynosi 449 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 Regulskiego,
Ośrodek Kształcenia Samorządu Terytorialnego im. W. Pańki
ul. Piłsudskiego 43, 50-032 Wrocław
ul. Moniuszki 7, 40-005 Katowice
71 344 26 90, 722 152 180, 32 206 98 43
szkolenia@okst.pl; milena.dudek@okst.pl

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

(dane do faktury)

Nazwa i adres nabywcy

NIP Nabywcy

Nazwa i adres odbiorcy

NIP 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 ☐

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.okst.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przysyłać do 10 listopada 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 wystawionej i przesłanej FV.

Podpis osoby upoważnionej