Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

FORUM, Katowice
23 czerwca 2026 r.

ŚLĄSKIE FORUM OCHRONY DANYCH OSOBOWYCH. CYBERBEZPIECZEŃSTWO I OCHRONA DANYCH OSOBOWYCH W ADMINISTRACJI PUBLICZNEJ — OBOWIĄZKI, RYZYKA, INCYDENTY I PRAKTYCZNE PROCEDURY

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:

Zapraszamy na zajęcia, podczas których uczestnicy nabędą praktycznych umiejętności w zakresie ochrony danych osobowych i cyberbezpieczeństwa w jednostkach publicznych, czyli nauczą się skutecznie zapobiegać, wykrywać i reagować na incydenty oraz wykazywać należytą staranność wynikającą z RODO i SZBI.

CELE I KORZYŚCI:

Po szkoleniu uczestnicy będą potrafili):

- Wyjaśnić powiązania między RODO, SZBI (ISMS) i cyberbezpieczeństwem oraz wskazać, dlaczego ochrona danych to odpowiedzialność całej organizacji, nie tylko IT.
- Rozpoznać najczęstsze zagrożenia dla jednostek publicznych (phishing, ransomware, błędy pracowników, utrata dostępu do systemów i poczty) oraz typowe scenariusze incydentów.
- Opisać role i obowiązki administratora danych, IOD (DPO), kierownictwa, działu IT i pracowników w zakresie bezpieczeństwa informacji.
- Postępować zgodnie z procedurą zgłaszania incydentów — właściwie klasyfikować, eskalować i dokumentować zdarzenia i potencjalne naruszenia ochrony danych.
- Przeprowadzić prostą, praktyczną ocenę ryzyka dla procesów i zasobów przetwarzających dane osobowe oraz sporządzić rejestr ryzyk z planem działań ograniczających.
- Przygotować i wdrażać kluczowe procedury praktyczne: procedurę incydentową, procedurę nadawania i odbierania uprawnień, procedurę kopii zapasowych i odtwarzania oraz zasady bezpieczeństwa dostawców.
- Skutecznie reagować w konkretnych sytuacjach (błędny adresat wiadomości, phishing, zainfekowana stacja robocza, utrata dostępu do poczty, ransomware) i ograniczać skutki incydentów.
- Zaplanować działania zapewniające ciągłość działania i odporność organizacji oraz zrozumieć, dlaczego backup to nie to samo co plan ciągłości działania.
- Dokumentować wdrożone środki i działania dowodzące należytej staranności przed organami nadzorczymi i audytami.
- Budować kulturę zgłaszania incydentów w organizacji oraz zwiększyć zaangażowanie pracowników w zakresie bezpieczeństwa informacji.

PROGRAM:

1. **Wprowadzenie: cyberbezpieczeństwo jako element ochrony danych osobowych:**
   - dlaczego cyberbezpieczeństwo nie jest wyłącznie zadaniem IT?
   - dane osobowe jako kluczowy zasób organizacji,
   - najczęstsze zagrożenia dla jednostek publicznych: phishing, ransomware, błędy pracowników, utrata dostępu do systemów i poczty,
   - skutki incydentów dla administratora, IOD, pracowników i osób, których dane dotyczą.
2. **RODO, SZBI i cyberbezpieczeństwo — wspólna odpowiedzialność organizacyjna:**
   - rola administratora, IOD, kadry kierowniczej, IT i pracowników,
   - bezpieczeństwo informacji jako element rozliczalności,
   - dokumentowanie działań i wykazywanie należytej staranności,
   - jak uniknąć sytuacji, w której procedury istnieją wyłącznie „na papierze".
3. **Incydenty cyberbezpieczeństwa a naruszenia ochrony danych osobowych:**
   - kiedy zdarzenie techniczne może stać się naruszeniem ochrony danych?
   - procedura zgłaszania incydentów przez pracowników,
   - klasyfikacja, eskalacja i dokumentowanie zdarzeń,
   - współpraca IOD z IT, kierownictwem i osobami odpowiedzialnymi za organizację pracy,
   - praktyczne przykłady: błędny adresat wiadomości, phishing, zainfekowana stacja robocza, utrata dostępu do poczty, ransomware.
4. **Zarządzanie ryzykiem z perspektywy ochrony danych osobowych:**
   - identyfikacja zasobów, procesów i systemów przetwarzających dane osobowe,
   - właściciel procesu i właściciel zasobu,
   - prosta, praktyczna ocena ryzyka,
   - rejestr ryzyk i plan działań ograniczających ryzyko,
   - powiązanie ryzyka cyberbezpieczeństwa z analizą ryzyka RODO.
5. **Procedury i dokumentacja, które powinny działać w praktyce:**
   - polityka bezpieczeństwa informacji / SZBI,
   - procedura incydentowa,
   - procedura naruszeń ochrony danych osobowych,
   - procedura nadawania, zmiany i odbierania uprawnień,
   - procedura kopii zapasowych i odtwarzania,
   - bezpieczeństwo dostawców i umów,
   - szkolenia pracowników i budowanie kultury zgłaszania incydentów.
6. **Ciągłość działania i odporność organizacji:**
   - dlaczego backup nie zastępuje planu ciągłości działania,
   - dostępność systemów a bezpieczeństwo danych osobowych,
   - komunikacja kryzysowa, ścieżki decyzyjne i zastępstwa,
   - testowanie procedur i dokumentowanie wyników.
7. **Podsumowanie i checklista dla uczestników:**
   - najczęstsze braki w jednostkach publicznych,
   - 10 pytań kontrolnych dla administratora, IOD i kierownictwa,
   - rekomendowany plan działań po szkoleniu.

ADRESACI:

Członkowie Forum ODO, inspektorzy ochrony danych osobowych, pracownicy odpowiedzialni za cyberbezpieczeństwo i ochronę danych osobowych w praktyce, odpowiedzialnych za bezpieczeństwo informacji w jednostkach administracji publicznej.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Śląskie Forum Ochrony Danych Osobowych. Cyberbezpieczeństwo i ochrona danych osobowych w administracji publicznej — obowiązki, ryzyka, incydenty i praktyczne procedury

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

23 czerwca 2026 r. **Szkolenie w godzinach: 9:00-14:00**

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

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

Zgłoszenia prosimy przesyłać do 18 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 _____