Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

SZKOLENIE ONLINE
29 października 2026 r.

BEZPIECZNE AI W JST – JAK UNIKNĄĆ BŁĘDÓW PRAWNYCH I SKUTECZNIE WYKORZYSTAĆ SZTUCZNĄ INTELIGENCJĘ?

PRAWO, RODO, ODPOWIEDZIALNOŚĆ I ETYKA.

WAŻNE INFORMACJE O SZKOLENIU:

- Szkolenie kompleksowo przedstawia najważniejsze aspekty prawne, organizacyjne, technologiczne i etyczne związane z wykorzystaniem sztucznej inteligencji w jednostkach samorządu terytorialnego. Uczestnicy poznają kluczowe wymagania wynikające z AI Act, RODO oraz prawa autorskiego, a także zasady klasyfikowania systemów AI według poziomu ryzyka i najważniejsze obowiązki związane z ich stosowaniem.
- Istotną część szkolenia stanowią zagadnienia dotyczące ochrony danych osobowych w systemach AI, w tym anonimizacji, pseudonimizacji, danych syntetycznych oraz bezpiecznego testowania rozwiązań w środowiskach typu *proof of concept* (PoC) i sandbox. Omówione zostaną również praktyczne metody ochrony prywatności, w tym zastosowanie nowoczesnych technologii zwiększających bezpieczeństwo danych.
- Program obejmuje także zagadnienia etyki i odpowiedzialności za wykorzystanie AI, ze szczególnym uwzględnieniem przejrzystości działania systemów, nadzoru człowieka, ryzyka dyskryminacji, ochrony prywatności oraz odpowiedzialnego podejmowania decyzji wspieranych przez sztuczną inteligencję.

CELE I KORZYŚCI:

1. Uporządkowanie wiedzy o podstawowych regulacjach dotyczących sztucznej inteligencji, ochrony danych osobowych i praw autorskich.
2. Wyjaśnienie podejścia opartego na ryzyku, stosowanego w AI Act, oraz konsekwencji klasyfikacji systemów AI.
3. Rozwinięcie umiejętności rozpoznawania ryzyk prawnych, etycznych i informacyjnych związanych z wykorzystywaniem AI.
4. Przygotowanie uczestników do bezpiecznej pracy z danymi osobowymi, materiałami tekstowymi, obrazami i nagraniami.
5. Omówienie metod anonimizacji, pseudonimizacji, maskowania oraz technologii zwiększających ochronę prywatności.
6. Pokazanie wpływu jakości danych na rzetelność, przejrzystość i sprawiedliwość działania systemów AI.
7. Wypracowanie praktycznych zasad human-in-the-loop, fact-checkingu i dokumentowania wykorzystania AI w organizacji.

Jeśli chcesz:

- Nauczyć się rozpoznawać podstawowe ryzyka prawne związane z wykorzystaniem AI;
- Umieć ocenić, czy dane mogą być bezpiecznie wykorzystane w narzędziu AI;
- Wiedzieć, jak odróżnić anonimizację od pseudonimizacji;
- Umieć dobrać właściwe metody ochrony danych;
- Wiedzieć jak ocenić jakość danych przed wykorzystaniem ich przez AI;
- Nauczyć się rozpoznać ryzyka etyczne i związane z dyskryminacją;
- Wiedzieć jak określić zakres niezbędnego nadzoru człowieka;
- Umieć przygotować podstawowe założenia bezpiecznego pilotażu AI;
- Wiedzieć jak zadawać właściwe pytania przed zakupem lub wdrożeniem rozwiązania AI w JST.

To szkolenie jest dla Ciebie!

PROGRAM:

I. AI w urzędzie – co wolno, czego nie wolno i za co odpowiadamy?

1. AI w JST – najważniejsze wyzwania prawne związane z wykorzystywaniem sztucznej inteligencji.
2. AI Act, RODO i prawo autorskie – trzy kluczowe obszary, które trzeba uwzględnić przed wdrożeniem rozwiązania AI.

3. AI Act w praktyce – podejście oparte na poziomie ryzyka:
   - systemy minimalnego ryzyka;
   - systemy ograniczonego ryzyka i obowiązki dotyczące transparentności;
   - systemy wysokiego ryzyka – przykłady zastosowań m.in. w edukacji, HR i usługach publicznych;
   - praktyki i systemy zakazane.
   - Co zmienia się dla JST i osób korzystających z narzędzi AI?
   - AI Act w Europie a regulacje i podejścia do AI poza UE.
4. **Prawo autorskie a AI:**
   - skąd pochodzą dane wykorzystywane przez AI?
   - czy można wprowadzać cudze materiały do narzędzi AI?
   - Komu przysługują prawa do treści wygenerowanych przez AI?
   - na co zwracać uwagę w licencjach, regulaminach i warunkach korzystania z aplikacji?
   - Ochrona własności intelektualnej urzędu i twórców.

Warsztat: Uczestnicy klasyfikują przykładowe zastosowania AI w JST według poziomu ryzyka i tworzą listę pytań, które należy zadać przed zakupem lub wdrożeniem narzędzia.

II. RODO w świecie AI – jak chronić dane osobowe i nie narazić urzędu na ryzyko? | ok. 60 min

1. Dlaczego AI wymaga szczególnej ostrożności w zakresie ochrony danych osobowych?
2. Dane osobowe w procesie projektowania, testowania i użytkowania systemów AI.
3. Duże zbiory danych i dane wymagające szczególnej ochrony.
4. Najważniejsze zasady RODO w projektach AI:
   - minimalizacja danych;
   - ograniczenie celu;
   - przejrzystość;
   - rozliczalność;
   - privacy by design i privacy by default.
5. Stanowisko Europejskiej Rady Ochrony Danych dotyczące wykorzystywania danych osobowych do rozwoju i wdrażania modeli AI.
6. Anonimizacja czy pseudonimizacja? – kiedy zastosować które rozwiązanie?
7. Dane syntetyczne jako bezpieczniejsza alternatywa dla danych rzeczywistych.
8. Sandbox i środowiska testowe – jak bezpiecznie prowadzić Proof of Concept?
9. Jak przygotować dane do testowania AI bez niepotrzebnego zwiększania ryzyka?

Warsztat: Uczestnicy analizują scenariusz wdrożenia AI i decydują, jakie dane można wykorzystać, które należy zanonimizować, a które zastąpić danymi syntetycznymi.

III. Etyczna i godna zaufania AI – gdzie kończą się możliwości technologii, a zaczyna odpowiedzialność urzędu?

1. Czym jest etyczna i godna zaufania sztuczna inteligencja?
2. AI a prawa człowieka, prywatność i interes obywatela.
3. Najważniejsze zagrożenia etyczne:
   - *deepfake* i manipulowanie odbiorcami;
   - rozpoznawanie twarzy i ingerencja w prywatność;
   - automatyzacja decyzji i odpowiedzialność człowieka;
   - błędy, uprzedzenia i dyskryminujące wyniki AI.
4. **Europejska Deklaracja Praw i Zasad Cyfrowych.**
5. **7 filarów godnej zaufania AI:**
   - nadzór i kontrola człowieka;
   - bezpieczeństwo i solidność techniczna;
   - ochrona prywatności i właściwe zarządzanie danymi;
   - przejrzystość i wyjaśnialność;
   - odpowiedzialność;
   - różnorodność, niedyskryminacja i sprawiedliwość;
   - dobrostan społeczny i środowiskowy.
6. **Jak dokumentować sposób projektowania, testowania i wykorzystywania AI?**

7. **Jak ustalić, kiedy decyzja może być wspierana przez AI, a kiedy konieczna jest ingerencja człowieka?**

Case study: Analiza sytuacji problemowej z wykorzystaniem AI w organizacji – identyfikacja interesariuszy, możliwych szkód i sposobów ograniczenia ryzyka.

IV. Anonimizacja i pseudonimizacja – jak skutecznie chronić dane przed identyfikacją?

1. Kiedy informacja jest daną osobową?
2. Dane bezpośrednio identyfikujące i informacje, które mogą prowadzić do identyfikacji w połączeniu z innymi danymi.
3. Anonimizacja a pseudonimizacja – kluczowe różnice w praktyce.
4. Dlaczego szyfrowanie danych nie oznacza ich anonimizacji?
5. Metody ograniczania możliwości identyfikacji:
   - maskowanie;
   - generalizacja;
   - dodawanie szumu;
   - pseudonimizacja;
   - dane syntetyczne.
6. Technologie zwiększające ochronę prywatności (Privacy Enhancing Technologies, PETs):
   - prywatność różnicowa;
   - federacyjne uczenie maszynowe;
   - obliczenia homomorficzne;
   - bezpieczne obliczenia wielostronne.
7. Ryzyko ponownej identyfikacji i deanonimizacji.
8. Dlaczego skuteczność anonimizacji należy oceniać w kontekście całego zbioru danych?

Warsztat: Dobór właściwej techniki ochrony danych do czterech scenariuszy: analiza danych mieszkańców, testowanie systemu, wymiana danych między jednostkami oraz trenowanie modelu AI.

V. Machine Learning vs. Generative AI? – jak wybrać właściwą technologię dla JST? | ok. 45 min

1. Czym naprawdę jest uczenie maszynowe i jak „uczy się" model?
2. Główne rodzaje uczenia maszynowego:
   - nadzorowane;
   - nienadzorowane;
   - ze wzmocnieniem.
3. Jakie dane mogą być wykorzystywane przez systemy ML?
4. Dane publiczne, internetowe, finansowe, IoT i inne źródła – korzyści, ograniczenia i ryzyka.
5. Machine Learning vs Generative AI – najważniejsze różnice:
   - cel zastosowania;
   - rodzaj danych;
   - sposób działania;
   - czas i koszt wdrożenia;
   - wymagane kompetencje.
6. Kiedy AI powinna przewidywać lub klasyfikować, a kiedy generować treści lub pracować z dokumentami?
7. Możliwości łączenia ML i GenAI.
8. Przykłady zastosowań AI możliwych do wykorzystania w administracji publicznej.

Warsztat: Dobór ML, GenAI lub rozwiązania hybrydowego do konkretnych problemów i potrzeb organizacji.

VI. Warsztat końcowy – jak bezpiecznie wdrożyć AI w JST? | ok. 45 min

Od pomysłu do bezpiecznego pilotażu - Uczestnicy przechodzą przez kompletny proces przygotowania wdrożenia AI:

1. **Określenie problemu i celu** – co chcemy osiągnąć dzięki AI?
2. **Identyfikacja interesariuszy** – kogo rozwiązanie będzie dotyczyć?
3. **Identyfikacja danych** – jakie dane są potrzebne i skąd pochodzą?
4. **Ocena ryzyka** – jakie mogą wystąpić zagrożenia prawne, organizacyjne i etyczne?
5. **Ochrona danych** – anonimizacja, pseudonimizacja, dane syntetyczne i inne zabezpieczenia.

6. **Ocena jakości danych** – czy dane są kompletne, aktualne i wiarygodne?
7. **Nadzór człowieka** – gdzie i w jaki sposób człowiek powinien kontrolować działanie AI?
8. **Dokumentacja** – co należy udokumentować przed uruchomieniem rozwiązania?
9. **Mierniki i kontrola** – jak sprawdzić, czy AI działa prawidłowo?
10. **Decyzja o pilotażu lub wdrożeniu** – kiedy można bezpiecznie przejść do kolejnego etapu?

Warsztat końcowy: Zespołowe przygotowanie „Mini-karty bezpiecznego wdrożenia AI w JST" dla wybranego zastosowania.

ADRESACI:

Szkolenie skierowane jest do **przedstawicieli i pracowników jednostek samorządu terytorialnego**, którzy wykorzystują lub planują wykorzystanie sztucznej inteligencji w pracy urzędu i jednostek organizacyjnych.
W szczególności zapraszamy:

- **kadrę kierowniczą JST** – wójtów, burmistrzów, prezydentów miast, starostów, sekretarzy oraz dyrektorów i kierowników jednostek;
- **pracowników urzędów gmin, miast i powiatów** odpowiedzialnych za organizację pracy, cyfryzację i wdrażanie nowych technologii;
- **pracowników zajmujących się ochroną danych osobowych, RODO i bezpieczeństwem informacji**;
- **radców prawnych, prawników i osoby odpowiedzialne za zgodność działań urzędu z przepisami prawa**;
- **pracowników działów IT, informatyki i cyberbezpieczeństwa**;
- **koordynatorów i osoby odpowiedzialne za projekty cyfryzacyjne oraz wdrażanie rozwiązań AI**;
- **pracowników merytorycznych**, którzy korzystają lub zamierzają korzystać z narzędzi AI w codziennej pracy;
- **pracowników jednostek organizacyjnych JST**, w tym jednostek oświatowych, pomocy społecznej, kultury i innych podmiotów realizujących zadania publiczne.

PROWADZĄCA:

Audytor wiodący SZBI WG. ISO 27001, Audytor wiodący SZCD WG. ISO 22301, Audytor wewnętrzny ZSZ WG. ISO 9001, 14001 I 45001, SIX SIGMA YELLOW BELT, DPO, wdrożeniowiec systemów klasy ezd, trener i archiwista. partner biznesowy SYGNITY S.A. członek grupy roboczej ds. sztucznej inteligencji przy ministerstwie cyfryzacji, członek ISSA polska (grupa robocza ds. AI), Autor tekstów i porad w portalach Legalis Administracja i Legalis Księgowość Kadry Biznes Wydawnictwa C.H. Beck. Autor książki „Polecenia dla ChatGPT w finansach: praktyczne zastosowanie w biznesie i finansach osobistych" wydanej nakładem wydawnictwa Helion S.A. Prowadzi szkolenia z zakresu cyberbezpieczeństwa, ochrony danych osobowych, bezpieczeństwa informacji, prawa administracyjnego, sztucznej inteligencji, systemów teleinformatycznych oraz elektronicznego zarządzania dokumentacją. Oprócz prowadzenia szkoleń zajmuje się wdrożeniami systemów EZD, prowadzeniem audytów bezpieczeństwa informacji i zarządzania ciągłością działania oraz udzielaniem porad.

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Bezpieczne AI w JST – jak uniknąć błędów prawnych i skutecznie wykorzystać sztuczną inteligencję? Prawo, RODO, odpowiedzialność i etyka.

	Szkolenie będziemy realizowali **w formie webinarium online**.
	29 października 2026 r. **Szkolenie w godzinach 10:00-14:00**
	Cena: 479 PLN netto/os. **Przy zgłoszeniu do 15 października 2026 r. cena wynosi 449 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, Centrum Mazowsze; ul. Jelinka 6, 01-646 Warszawa; tel. 533 849 116; szkolenia@frdl.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.frdl.mazowsze.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Zgłoszenia prosimy przesyłać do 26 października 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.