Kontrola, audyt AI oraz kategoryzacja danych w PUP

Jakie są konsekwencje, jeśli do 28.10.2026 r. urząd nie zrobi kategoryzacji danych dopuszczanych do SI? Jak zrobić inwentaryzację i audyt narzędzi AI w PUP oraz co jeśli dane są przetwarzane na serwerach poza UE?

Wideoszkolenie PCC Poland skierowane do **dyrektorów, kierowników oraz pracowników Powiatowych Urzędów Pracy**, odpowiedzialnych za cyfryzację, automatyzację procesów, przygotowanie regulaminów i procedur wewnętrznych oraz bezpieczne wykorzystanie narzędzi AI w codziennej pracy urzędu.

Pracownik kopiuje do AI pismo, dokument lub dane osoby bezrobotnej, poszukującej pracy albo pracodawcy - czy właśnie doszło do naruszenia prawa i przekazania danych poza urząd?
28 października wchodzą w życie kolejne elementy krajowego systemu nadzoru nad AI. Urząd musi wiedzieć, z jakich narzędzi AI faktycznie korzystają jego pracownicy, jakie dane są do nich przekazywane i które zastosowania mogą podlegać dodatkowym obowiązkom. Kolejnym krokiem musi być kategoryzacja danych, np. na dane zielone, żółte i czerwone. Pracownik musi wiedzieć, które informacje może bezpiecznie wykorzystać w zatwierdzonym systemie, które wymagają anonimizacji lub dodatkowej zgody, a których nie wolno przekazywać do narzędzi AI w ogóle. Szczególnie istotne jest także ustalenie, gdzie faktycznie trafiają dane po wpisaniu ich do systemu AI. Sam fakt, że dostawca ma serwery w Europie, nie zawsze oznacza, że każde zapytanie jest przetwarzane wyłącznie w UE. Znaczenie może mieć rodzaj usługi, konfiguracja, region chmurowy, sposób routingu zapytań, miejsce przechowywania logów, kopii zapasowych i danych pomocniczych. W praktyce urząd powinien wiedzieć nie tylko z jakiego narzędzia korzysta, ale również na jakiej infrastrukturze ono działa, gdzie odbywa się przetwarzanie.

W programie m.in.:

- **Pracownik PUP wrzuca pismo do AI. Czy urząd wie, co dzieje się z tymi danymi?**
- Które przepisy AI Act są szczególnie ważne z perspektywy powiatowego urzędu pracy?
- W jaki sposób zapewnić bezpieczeństwo danych urzędowych i informacji chronionych podczas korzystania z narzędzi AI?
- **Jakie dane nie powinny być wprowadzane do narzędzi wykorzystujących AI?**
- Jak weryfikować informacje i odpowiedzi uzyskane od narzędzi AI, aby unikać nieprawidłowości i błędów merytorycznych- biorąc pod uwagę, że narzędzie AI może podać przepisy, które już nie są aktualne?
- W jaki sposób wykorzystać AI przy sporządzaniu pism administracyjnych?
- Jak stworzyć i co powinien zawierać wewnętrzny regulamin określający wdrażanie i korzystanie z AI?
- **Którymi narzędziami może posługiwać się PUP, aby zmaksymalizować bezpieczeństwo korzystania z AI i zminimalizować ryzyko?**

Szczegółowy program szkolenia:

NOWOŚCI

Co zmienia się od 28 października 2026 r.? Nowe obowiązki urzędu w zakresie AI, audytu,

bezpieczeństwa danych i kontroli. Jakie kary grożą za nieprzygotowanie zasad wewnętrznych korzystania z AI? Pracownik PUP wrzuca pismo do AI. Czy urząd wie, co dzieje się z tymi danymi?

- Jak przeprowadzić audyt technologiczny AI w urzędzie i zinwentaryzować wszystkie narzędzia wykorzystujące sztuczną inteligencję, także te używane przez pracowników bez wiedzy przełożonych?
- Jak stworzyć rejestr wykorzystywanych systemów AI i ustalić, jakie dane są w nich przetwarzane, przez kogo, w jakim celu oraz gdzie faktycznie trafiają?
- Jak dokonać praktycznej klasyfikacji danych na zielone, żółte i czerwone oraz ustalić, które informacje można przekazywać do AI, które wymagają anonimizacji, a których nie wolno wprowadzać?
- Jak ocenić ryzyko poszczególnych narzędzi AI i sprawdzić, czy dany system może należeć do kategorii wysokiego ryzyka?
- Jak wybrać i autoryzować narzędzia AI dopuszczone do użytku w urzędzie oraz określić, z jakich innych aplikacji pracownicy nie powinni korzystać?
- Jak ograniczyć Shadow AI, czyli korzystanie przez pracowników z ChatGPT, Gemini, Claude i innych narzędzi bez zgody oraz wiedzy kierownika lub informatyka?
- Co zrobić, gdy pracownik korzysta z AI na prywatnym telefonie lub prywatnym koncie i przekazuje do niego dokumenty albo dane służbowe?
- Jak urząd może kontrolować, jakie dane pracownicy wpisują i wklejają do AI? Czy można zastosować mechanizmy DLP, blokowanie określonych kategorii danych, anonimizację oraz monitoring użycia narzędzi?
- Jak sprawdzić, gdzie znajdują się serwery dostawcy, gdzie odbywa się przetwarzanie danych, czy dane pozostają w UE/EOG oraz czy mogą być przekazywane do państw trzecich?
- Jak przygotować regulamin i politykę bezpiecznego korzystania z AI: katalog dozwolonych narzędzi, zasady korzystania z danych, prywatnych urządzeń, weryfikacji treści oraz zgłaszania incydentów?
- Jakie uprawnienia będzie miała Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI), czego może wymagać podczas kontroli i jaką dokumentację powinien być w stanie przedstawić urząd?
- Co zrobić, jeśli mieszkaniec lub pracownik stwierdzi, że jego prawa zostały naruszone wskutek wykorzystania AI przez urząd?
- Jak postępować w przypadku przekazania do AI danych osobowych, danych wrażliwych lub dokumentów wewnętrznych i kiedy takie zdarzenie może zostać uznane za naruszenie ochrony danych?
- Jak weryfikować treści wygenerowane przez AI, kto odpowiada za ich poprawność oraz kiedy należy poinformować odbiorcę, że przy przygotowaniu treści wykorzystano sztuczną inteligencję?

1. AI Act i prawo w praktyce PUP: Zakres, kluczowe przepisy.

- Jaki zakres obejmuje unijne rozporządzenie AI Act?
- Które przepisy AI Act są szczególnie ważne z perspektywy powiatowego urzędu pracy?
- Na jakich innych ustawach i przepisach opierać się podczas wdrażania AI i tworzenia regulaminów?
- Jakie uprawnienia będzie miała Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI), czego może wymagać podczas kontroli i jaką dokumentację powinien być w stanie przedstawić urząd?
- W jakim zakresie według przepisów można wykorzystywać AI w powiatowych urzędach pracy?
- W jaki sposób pracownicy mogą korzystać z AI, aby działać w ramach obowiązujących przepisów?

- Co zrobić jeśli mieszkaniec lub pracownik stwierdzi, że jego prawa zostały naruszone wskutek wykorzystania AI przez urząd?

2. Ochrona danych, bezpieczeństwo, RODO.

- Jakie ryzyka wiążą się z wdrożeniem AI w urzędzie pracy i w jaki sposób skutecznie je ograniczać?
- W jaki sposób zapewnić bezpieczeństwo danych urzędowych i informacji chronionych podczas korzystania z narzędzi AI?
- Jak postępować zgodnie z przepisami RODO i chronić dane osobowe na etapach wdrażania oraz codziennego używania AI?
- Jak postępować w przypadku przekazania do AI danych osobowych, danych wrażliwych lub dokumentów wewnętrznych i kiedy takie zdarzenie może zostać uznane za naruszenie ochrony danych?
- Jak dokonać praktycznej klasyfikacji danych na zielone, żółte i czerwone oraz ustalić, które informacje można przekazywać do AU, które wymagają anonimizacji, a których nie wolno wprowadzać?
- Jak bezpiecznie korzystać z zewnętrznych, bezpłatnych narzędzi AI (np. ChatGPT), aby nie naruszyć RODO i ochrony danych osobowych?
- Jakie kwestie dotyczące praw autorskich należy uwzględnić przy wprowadzaniu danych do AI oraz korzystaniu z wygenerowanych treści?
- Jakie dane i informacje mogą być wprowadzane do narzędzi wykorzystujących AI?
- W jaki sposób anonimizować dane, aby zachować bezpieczeństwo?
- W jaki sposób chronić dane wrażliwe, korzystając z AI?
- Jakie dane nie powinny być wprowadzane do narzędzi wykorzystujących AI?
- W jaki sposób zagwarantować, że narzędzia AI nie będą przechowywały i potem wykorzystywały wprowadzonych danych, czy istnieje taka możliwość?
- Cyberbezpieczeństwo w chmurze: Jak uniknąć wycieku informacji i zachować procedury sieciowe, gdy dane przetwarzane są na zewnętrznych serwerach?
- Jak sprawdzić gdzie znajdują się serwery dostawcy, gdzie odbywa się przetwarzanie danych, czy dane pozostają w UE/EOG oraz czy mogą być przekazywane do państw trzecich?
- Jak wdrożyć i uruchomić modele AI w sieci lokalnej, aby dane urzędu były bezpieczne?
- Jak urząd może kontrolować, jakie dane pracownicy wpisują i wklejają do AI? Czy można zastosować mechanizmy DLP, blokowanie określonych kategorii danych, anonimizację oraz monitoring użycia narzędzi?
- W jaki sposób legalnie i bezpiecznie korzystać z narzędzi AI w urzędzie, który posiada aktywne blokady sieciowe przed wyciekiem danych?

3. Narzędzia AI i ich wykorzystanie

- Co może zyskać urząd pracy dzięki wprowadzeniu AI? Wady i zalety korzystania ze sztucznej inteligencji.
- Jakie narzędzia AI (w tym bezpłatne) są dostępne i mogą być wykorzystywane przez urzędy pracy? - omówienie.
- Jak ocenić ryzyko poszczególnych narzędzi AI i sprawdzić, czy dany system może należeć do kategorii wysokiego ryzyka?
- Którymi narzędziami może posługiwać się PUP, aby zmaksymalizować bezpieczeństwo korzystania z AI i zminimalizować ryzyko?
- Jak wybrać i autoryzować narzędzia AI dopuszczone do użytku w urzędzie oraz określić, z jakich

innych aplikacji pracownicy nie powinni korzystać?
- Czy istnieją narzędzia AI dedykowane specjalnie do pracy w administracji publicznej?
- Jakie funkcje posiada narzędzie NotebookLM i w jaki sposób można wykorzystać je w codziennej pracy?
- W jakich czynnościach i codziennych obowiązkach wykonywanych przez PUP może pomóc korzystanie z narzędzi AI?
- W jaki sposób wykorzystać AI w wydziale doradztwa zawodowego?
- Jak wykorzystać AI w dziale organizacyjnym i w jaki sposób może ono wspomóc wdrażanie nowych rozwiązań organizacyjnych w urzędzie?
- W jakich czynnościach związanych z obsługą prawną może pomóc AI, np. gdy PUP musi opierać dokumenty na wyrokach sądowych?

4. Tworzenie promptów i weryfikacja odpowiedzi

- Jak tworzyć polecenia i prompty, aby uzyskać oczekiwane efekty?
- W jaki sposób formułować prompty, aby zminimalizować ryzyko błędnych lub nieaktualnych odpowiedzi?
- Jak weryfikować informacje i odpowiedzi uzyskane od narzędzi AI, aby unikać nieprawidłowości i błędów merytorycznych- biorąc pod uwagę, że narzędzie AI może podać przepisy, które już nie są aktualne?
- Jak weryfikować treści wygenerowane przez AI, kto odpowiada za ich poprawność oraz kiedy należy poinformować odbiorcę, że przy przygotowaniu treści wykorzystano sztuczną inteligencję?

5. Praktyczne wykorzystanie

- W jaki sposób zautomatyzować proces tworzenia dokumentów, decyzji oraz analiz przy użyciu AI?
- Jak sztuczna inteligencja może pomóc w automatyzacji pracy z dokumentacją urzędową?
- W jaki sposób wykorzystać AI przy sporządzaniu pism administracyjnych?
- Jak krok po kroku tworzyć pisma za pomocą narzędzi AI?
- Jak przygotowywać regulaminy wewnętrzne z wykorzystaniem AI?
- Jak tworzyć wzory dokumentów z pomocą narzędzi AI?
- W jaki sposób redagować dokumenty i pisma, zwłaszcza gdy trzeba powołać się na podstawy prawne?
- W jaki sposób tworzyć uzasadnienia decyzji z wykorzystaniem AI?
- W jaki sposób sporządzać decyzje wydawane na podstawie Kodeksu postępowania administracyjnego przy użyciu AI?
- W jaki sposób przygotowywać pisma informacyjne o przyznaniu świadczenia z pomocą AI?
- W jaki sposób generować grafiki z wykorzystaniem AI?
- Jak tworzyć plakaty informacyjne za pomocą narzędzia ChatGPT?
- W jaki sposób przygotować prezentację na podstawie posiadanych danych z wykorzystaniem AI?
- W jaki sposób tworzyć materiały wideo przy użyciu narzędzi AI?
- Jak wykorzystać AI do opracowywania analiz na potrzeby realizowanych projektów oraz do tworzenia prostych pism?
- W jaki sposób przeprowadzać i tworzyć analizy statystyczne z wykorzystaniem AI?
- W jaki sposób opracowywać statystyki potrzebne do analizy rynku pracy przy użyciu AI?
- Czy narzędzia AI mogą pomóc w automatyzacji pracy w programie Excel?

6. Wdrożenie AI w urzędzie: Procedury, regulaminy, przygotowanie.

- Jak przygotować urząd do wdrożenia AI pod względem organizacyjnym i formalnym?
- Jak przeprowadzić audyt technologiczny AI w urzędzie i zinwentaryzować wszystkie narzędzia wykorzystujące sztuczną inteligencję, także te używane przez pracowników bez wiedzy przełożonych?
- Jak stworzyć rejestr wykorzystywanych systemów AI i ustalić, jakie dane są w nich przetwarzane, przez kogo, w jakim celu oraz gdzie faktycznie trafiają?
- Jakie kroki należy podjąć przed wprowadzeniem AI do jednostki?
- W jaki sposób przygotować pracowników do wdrożenia AI w codziennej pracy?
- Jak powinno przebiegać i w jaki sposób przeprowadzić wdrożenie AI w urzędzie pracy?
- Czy przed wdrożeniem AI należy stworzyć regulamin oraz procedury dotyczące jej wykorzystania?
- Jak ograniczyć Shadow AI, czyli korzystanie przez pracowników z ChatGPT, Gemini, Claude i innych narzędzi bez zgody oraz wiedzy kierownika lub informatyka?
- Co zrobić, gdy pracownik korzysta z AI na prywatnym telefonie lub prywatnym koncie i przekazuje do niego dokumenty albo dane służbowe?
- W jaki sposób opracować procedury i politykę korzystania z AI zgodnie z przepisami?
- Jak przygotować regulamin i politykę bezpiecznego korzystania z AI: katalog dozwolonych narzędzi, zasady korzystania z danych, prywatnych urządzeń, weryfikacji treści oraz zgłaszania incydentów?
- Jak stworzyć i co powinien zawierać wewnętrzny regulamin określający wdrażanie i korzystanie z AI?
- Jak przygotować regulamin oraz zasady korzystania z AI pod kątem kontroli zarządczej?

Prowadzący:

Prelegent obejmuje stanowisko inspektora na samodzielnym stanowisku ds. informatyczno-statystycznych w Powiatowym Urzędzie Pracy, gdzie od 2019 roku odpowiada za utrzymanie, rozwój i bezpieczeństwo infrastruktury IT oraz przygotowywanie sprawozdań, analiz i informacji dotyczących stanu i struktury bezrobocia. Posiada wykształcenie kierunkowe w obszarze informatyki i cyberbezpieczeństwa – ukończył studia inżynierskie na kierunku informatyka w Wyższej Szkole Informatyki i Zarządzania w Rzeszowie (specjalizacja: technologie mobilne i internetowe) oraz studia podyplomowe na kierunku Cyberbezpieczeństwo systemów informatycznych na tej samej uczelni. Jest Audytorem Wiodącym Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2023-08 (TÜV NORD Polska), a jego rozwój zawodowy obejmuje m.in. kursy CyberOps Associate, Cybersecurity Essentials, Endpoint Security oraz Ethical Hacker (Cisco).

Terminy i szkolenia

Data: 15 grudnia 2026 10:00-15:00
Miejsce: Wideoszkolenie

Prawa autorskie do niniejszego programu przysługują Private Corporate Consulting Sp. z o.o. Udostępnianie, kopiowanie i przerabianie niniejszego programu bez pisemnej zgody Private Corporate Consulting Sp. z o.o., zagrożone jest odpowiedzialnością karną oraz cywilną