

Kontrola, audyt AI i kategoryzacja danych w UMiG

Jaki wpływ będzie miała dyrektywa AI Act na korzystanie ze sztucznej inteligencji w urzędach? Jak zapobiegać wyciekom danych wrażliwych do sztucznej inteligencji? Jak stworzyć regulamin weryfikujący naruszenia bezpieczeństwa danych przez narzędzia posługujące się AI?

Wideoszkolenie PCC Poland skierowane do inspektorów ochrony danych osobowych, głównych informatyków oraz informatyków pełniących swoje obowiązki w Urzędach Miast i Gmin.

Jakie kary mogą grozić urzędowi za naruszenie obowiązków wynikających z AI Act i nowych przepisów krajowych po 28 października 2026 r.?

28 października wchodzi 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.:

- Czy korzystanie ze sztucznej inteligencji w urzędach jest zgodne z prawem?
- Jakie są możliwe kary za naruszenie przepisów AI Act w administracji publicznej?
- Jakie kategorie danych nie powinny być umieszczane w sztucznej inteligencji?
- Czym jest Shadow AI i jakie niesie za sobą zagrożenia?
- Jak formułować prompty do bezpiecznego przetwarzania danych przez sztuczną inteligencję?
- Jak postępować, kiedy modele AI przetwarzają dane poza Unię Europejską i czy jest możliwe podpisanie umowy w zakresie takiego przetwarzania danych?
- Jakie grożą konsekwencje za stworzenie wycieku danych osobowych do narzędzia posługującego się sztuczną inteligencją?

Szczegółowy program szkolenia:

1. Ramy prawne i regulacje dotyczące AI Act, RODO oraz przepisów Digital Omnibus

1.1 Relacja RODO i AI Act oraz zasady przetwarzania

- Ingerencja sztucznej inteligencji do danych osobowych - czy jest to dozwolone i jak jest to regulowane w stosunku do przepisów RODO?
- Regulacje RODO a AI Act - jakie są obowiązki administratora danych wobec przetwarzania danych

wedle AI Act? Jakie są różnice między obowiązkami w związku z RODO, a AI Act?

- Jak legalnie zastosować modele sztucznej inteligencji do przetwarzania danych osobowych?
- Czy korzystanie ze sztucznej inteligencji w urzędach jest zgodne z prawem?
- AI Act - Digital Omnibus - uproszczenia przepisów - jak to będzie funkcjonować?
- Jaki wpływ będzie miała dyrektywa AI Act na korzystanie ze sztucznej inteligencji w urzędach?

1.2 Rola administratora, odpowiedzialność i kary

- Kto według przepisów powinien zostać administratorem przetwarzania danych przez sztuczną inteligencję?
- Jakie granice odpowiedzialności prawnej może ponieść administrator przetwarzania danych przez sztuczną inteligencję?
- Jakie są możliwe kary za naruszenie przepisów AI Act w administracji publicznej?
- Jakie grożą konsekwencje za stworzenie wycieku danych osobowych do narzędzia posługującego się sztuczną inteligencją?

1.3 Legalność konkretnych narzędzi i praktyk

- Czy rozporządzenie AI Act wpływa na korzystanie z Chatu GPT w darmowej wersji oraz płatnej i czy obie wersje są legalne?
- Czy samorządy mogą prawnie korzystać z narzędzi AI bez płatnej subskrypcji?
- Czy urzędy mogą zakupić i korzystać z narzędzi sztucznej inteligencji?
- Czy korzystanie ze sztucznej inteligencji do tworzenia i publikowania grafik w urzędzie jest legalne?
- Czy jest podstawa prawna na podważanie pisma od mieszkańców, kiedy istnieje ewidentny ślad użycia sztucznej inteligencji do jego napisania?

2. Ochrona danych osobowych, prywatność i zarządzanie ryzykiem

2.1 Dopuszczalność wprowadzania danych i ich kategorie

- Jakie dane osobowe można wprowadzić do narzędzia posługującego się sztuczną inteligencją?
- Jakich danych osobowych nie wprowadzać do modeli sztucznej inteligencji?
- Jakie kategorie danych nie powinny być umieszczane w sztucznej inteligencji?
- Czy są treści, których prawnie nie można wprowadzać do sztucznej inteligencji w ramach pracy w JST?
- Czy pracownik może wysyłać pliki zawierające dane osobowe do modelu sztucznej inteligencji?
- Czy można przysyłać dokumenty urzędowe do otwartych modeli sztucznej inteligencji?
- Jakie informacje można wprowadzać do sztucznej inteligencji, aby zabezpieczyć dane przed wyciekiem z urzędu?

2.2 Ochrona przed wyciekiem danych i zagrożenia

- Jak powinny być zabezpieczone dane osobowe przed umieszczeniem ich w sztucznej inteligencji?

- Jakie są zagrożenia wpisywania danych osobowych do sztucznej inteligencji?
- Jak zapobiegać wyciekom danych wrażliwych do sztucznej inteligencji?
- Jak zabezpieczyć urząd przed utratą danych przy korzystaniu ze sztucznej inteligencji?
- Jak chronić dane osobowe przed udostępnieniem podczas korzystania ze sztucznej inteligencji?
- Jak chronić dane osobowe i wrażliwe podczas korzystania ze sztucznej inteligencji?
- Czy jest możliwe, aby osoba z zewnątrz była w stanie pozyskać konkretne dane osobowe wcześniej wprowadzone przez pracownika urzędu do sztucznej inteligencji?
- Jak powstrzymać przepływ informacji wprowadzanych do sztucznej inteligencji z organizacji do sfery publicznej?
- Jak powstrzymać wyciek danych z modelu LLM do sfery publicznej przy wprowadzaniu danych do AI?

2.3 Shadow AI i użycie kont prywatnych

- Czym jest Shadow AI i jakie niesie za sobą zagrożenia?
- Jak przeciwdziałać zjawisku Shadow AI?
- Jak usankcjonować używanie sztucznej inteligencji na kontach prywatnych w miejscu pracy?
- Jak zabezpieczyć urząd przed wyciekiem danych przy korzystaniu z prywatnej sztucznej inteligencji?

2.4 Ocena ryzyka i ochrona dóbr osobistych

- Jak poprawnie przeprowadzić ocenę ryzyka używania sztucznej inteligencji przy przetwarzaniu danych w administracji publicznej?
- Jak uchronić się od naruszeń bezpieczeństwa ochrony dóbr osobistych klientów załatwiających sprawy w urzędzie przy procesowaniu ich przez sztuczną inteligencję?

3. Kwestie techniczne, infrastruktura, lokalizacja danych i dostawcy

3.1 Lokalizacja przetwarzania, serwery i transfer danych do krajów trzecich

- Przetwarzanie danych przez narzędzia AI, które korzystają ze swoich zasobów znajdującymi się w krajach trzecich - czy takie przetwarzanie danych przez sztuczną inteligencję jest bezpieczne?
- Gdzie są przechowywane i przetwarzane dane wprowadzane do sztucznej inteligencji?
- Czy serwery, z których korzysta sztuczna inteligencja znajdują się na terenie Unii Europejskiej?
- Jak zagwarantować, że przetwarzane dane pozostaną na terenie Unii Europejskiej?
- Czy sztuczna inteligencja nie przetwarza danych poza urząd?

3.2 Umowy z dostawcami, trenowanie modeli sztucznej inteligencji i specyfika rozwiązań

- Czy da się podpisać umowę o przetwarzanie danych osobowych z producentami modeli sztucznej inteligencji?
- Jak postępować, kiedy modele AI przetwarzają dane poza Unię Europejską i czy jest możliwe podpisanie umowy w zakresie takiego przetwarzania danych?
- Czy dane wysłane do otwartych modeli sztucznej inteligencji mogą zostać wykorzystane do jej

trenowania?

- Jakie zagrożenia niesie używanie modelu OpenAI?
- Do którego momentu jest dozwolona agregacja danych podawanych do Gemini AI (sztuczna inteligencja w wyszukiwarce Google)?

3.3 Architektura techniczna, narzędzia IT i instancje lokalne

- Jak stworzyć lokalne instancje sztucznej inteligencji?
- Jakich narzędzi w dziale IT można użyć, aby chronić dane osobowe przed wyciekiem do sztucznej inteligencji?
- Jak bezpiecznie zaimplementować sztuczną inteligencję w tworzeniu w baz danych?
- Jak połączyć różne modele AI (przykładowo: Chat GPT z Gemini od Google) do sprawniejszego wykonywania zadań?
- Jak są aktualizowane informacje w płatnych wewnętrznych modelach AI?
- W jaki sposób sztuczna inteligencja wykonuje zadane mu polecenia i na jakim algorytmie ona działa?
- Czy sztuczna inteligencja jest w stanie stworzyć alternatywny system przetwarzający dane osobowe?

4. Wdrożenie, polityki wewnętrzne i bezpieczne procedury w urzędzie

4.1 Strategia wdrożenia i zasady dla pracowników

- Jak wdrożyć bezpieczne używanie narzędzi sztucznej inteligencji?
- Jak praktycznie implementować narzędzia sztucznej inteligencji zgodnie z rozporządzeniem AI Act?
- Jak bezpiecznie dobrać narzędzia AI w JST bez ryzyka wycieku danych?
- Jakie są obowiązki administracji publicznej do wprowadzenia w świetle AI Act?

4.2 Tworzenie dokumentów wewnętrznych i polityk bezpieczeństwa

- Jakie elementy powinna zawierać wewnętrzna polityka korzystania z AI w JST?
- Jak dostosować prawnie politykę bezpieczeństwa do sztucznej inteligencji?
- Jak stworzyć regulamin weryfikujący naruszenia bezpieczeństwa danych przez narzędzia posługujące się AI?
- Jak formalnie zabezpieczyć dane wrażliwe przed wyciekiem do sztucznej inteligencji?

4.3 Praktyczne zasady pracy z danymi i bezpieczny prompting

- Jak bezpiecznie korzystać ze sztucznej inteligencji, aby nie spowodować wycieku danych osobowych?
- Jak bezpiecznie przekazywać dane wrażliwe przy używaniu sztucznej inteligencji?
- Jak formułować prompty do bezpiecznego przetwarzania danych przez sztuczną inteligencję?

5. Praktyczne zastosowania AI w administracji publicznej oraz jakość wyników

5.1 Obszary zastosowań w pracy urzędnika

- W jakich obszarach AI może mieć zastosowanie w urzędach?
- W jakim zakresie można korzystać ze sztucznej inteligencji w administracji samorządowej zgodnie z zapisami AI Act?
- Jak można wykorzystywać narzędzia sztucznej inteligencji w codziennej pracy urzędników i jak sprawić, żeby było to robione bezpiecznie?
- W jaki sposób urzędnik może wspomagać się sztuczną inteligencją, aby utworzyć wzorce dokumentów lub regulaminy funkcjonowania dla różnych wydziałów w urzędzie?
- Jak poprawnie używać sztucznej inteligencji do pisania urzędowych maili i jak zweryfikować tą poprawność?
- Jak się ma zastosowanie sztucznej inteligencji do wykonywania zadań przez administrację publiczną do zachowania zasad poufności danych?
- Weryfikacja informacji związanych z rejestrem karnym oraz Niebieskie Karty - jak będzie ona przebiegać w narzędziach korzystających ze sztucznej inteligencji?

5.2 Weryfikacja treści, oznaczanie i jakość danych wejściowych

- Jak zweryfikować czy odpowiedź wygenerowana przez sztuczną inteligencję pokrywa się merytorycznie z prawdą?
- Jak zabezpieczyć się przed wpływem fałszywych informacji tworzonych przez sztuczną inteligencję?
- Jakie treści wygenerowane przez sztuczną inteligencję muszą być oznakowane według AI Act?
- Jak bronić wprowadzone dane przed zniekształceniem oraz spłaszczeniem podczas obróbki przez sztuczną inteligencję?
- Jak tworzyć i interpretować algorytm do odczytywania aktów prawnych i stosowania procedur ochrony danych osobowych przez sztuczną inteligencję?

5.3 Zagrożenia i ryzyka operacyjne

- Jakie są zagrożenia i ryzyka związane z korzystaniem z AI w urzędach?

Prowadzący:

Pracuje jako pomoc administracyjna, gdzie zdobywa doświadczenie w pracy z dokumentacją finansową, danymi oraz systemami informatycznymi wykorzystywanymi w urzędzie. Wspiera również wdrażanie systemu eZDRP, pomagając pracownikom w jego obsłudze od strony merytorycznej.

Przedstawia możliwości wykorzystania narzędzi AI oraz programów wykorzystywanych w pracy urzędu, zwracając uwagę na zasady bezpiecznego korzystania z nich, w szczególności na to, jakie dane mogą być do nich wprowadzane, a jakich nie należy udostępniać.

Wcześniej odbywał praktyki w Zakładzie Ubezpieczeń Społecznych, gdzie miał styczność z ochroną danych w praktyce, między innymi podczas pracy z systemem SAP oraz dokumentacją finansowo-księgową. Podczas studiów rozwijał wiedzę z zakresu podatności aplikacji webowych, bezpieczeństwa modeli językowych (LLM), uczenia maszynowego oraz tworzenia aplikacji i często spotykał się z zagadnieniami

dotyczącymi ochrony danych osobowych i zagrożeń związanych z ich niewłaściwym wykorzystaniem.

Terminy i szkolenia

Data: 16 października 2026 09:00-14:00

Miejsce: Wideoszkolenie

Data: 10 listopada 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