

PROCEDURA KORZYSTANIA Z NARZĘDZI SZTUCZNEJ INTELIGENCJI PRZEZ PRACOWNIKÓW URZĘDU MIASTA I GMINY KÓRNIK

§ 1. CEL PROCEDURY

Niniejsza procedura określa zasady korzystania z narzędzi opartych na sztucznej inteligencji (AI) do czynności służbowych w sposób etyczny, bezpieczny i zgodny z obowiązującymi przepisami prawa.

§ 2. ZAKRES STOSOWANIA

Procedura dotyczy wszystkich pracowników Urzędu Miasta i Gminy Kórnik niezależnie od formy zatrudnienia, korzystających z narzędzi AI w celach służbowych.

§ 3. DEFINICJE

- 1) AI (sztuczna inteligencja) – narzędzie wykorzystujące algorytmy do przetwarzania danych, analizy tekstu, generowania treści, automatyzacji zadań (np. chatGPT, Copilot, Claude, Gemini itp.);
- 2) dokumenty służbowe – dane, pisma, obrazy, analizy lub inna treść tworzona w ramach obowiązków zawodowych;
- 3) dane syntetyczne – wygenerowane komputerowo dane imitujące cechy rzeczywistych zbiorów, nie zawierające prawdziwych danych osobowych, numerów spraw ani innych informacji poufnych.

§ 4. NARZĘDZIA AI MOGĄ BYĆ WYKORZYSTYWANE POMOCNICZO, np. w celu:

- 1) tworzenie szkiców pism, notatek, raportów, komunikatów;
- 2) wyszukiwania informacji, streszczenie dokumentów, analiza tekstu;
- 3) tworzenie pomysłów, materiałów promocyjnych;
- 4) analizy danych, generowanie tabel, wykresów;
- 5) automatyzacji prostych zadań administracyjnych,

§ 5 NARZĘDZIA AI UTRZYMUJĄCE INFRASTRUKTURĘ INFORMATYCZNĄ

Dopuszczalne jest wykorzystywanie AI w ramach utrzymania infrastruktury teleinformatycznej Urzędu Miasta i Gminy Kórnik przez upoważnionych pracowników Urzędu Miasta i Gminy Kórnik.

§ 6. NIEDOZWOLONE ZASTOSOWANIE AI:

- 1) wprowadzanie danych osobowych w rozumieniu RODO (np. imienia i nazwiska, adresów, wizerunku, numerów telefonów, numerów spraw, numerów ewidencyjnych), danych osobowych szczególnej kategorii (np. danych dotyczących zdrowia, pochodzenia rasowego lub etnicznego, poglądów politycznych) oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
- 2) wprowadzanie danych niejawnych, tajemnic służbowych, informacji finansowych, projektów umów oraz wszelkich danych objętych ochroną prawną;

- 3) wprowadzanie załączników do dokumentacji bez uprzedniej anonimizacji;
- 4) wykorzystywanie AI do podejmowania decyzji administracyjnych bez udziału pracownika;
- 5) tworzenie oficjalnych dokumentów bez weryfikacji przez pracownika;
- 6) podszywanie się pod inne osoby lub instytucje.

§ 7. OCHRONA DANYCH, BEZPIECZEŃSTWO

- 1) pracownik ma obowiązek dbać o bezpieczeństwo informacji przekazywanych do AI;
- 2) zabrania się wprowadzania do narzędzi AI informacji dotyczących osób fizycznych jako elementu zapytania (promptu);
- 3) dopuszczalne jest wyłącznie użycie danych zanonimizowanych lub syntetycznych;
- 4) jeżeli anonimizacja nie jest możliwa – obowiązuje zakaz użycia AI;
- 5) zabrania się z korzystania z publicznych narzędzi AI bez wcześniejszego sprawdzenia ich regulaminu i polityki prywatności;
- 6) w przypadku narzędzi zintegrowanych z systemami w urzędzie, należy stosować się do zaleceń administratora ASI i IOD;
- 7) w przypadku stwierdzenia wprowadzenia danych osobowych do narzędzia AI należy niezwłocznie zgłosić incydent do Inspektora Ochrony Danych, zablokować dostęp do narzędzia do czasu wyjaśnienia oraz zastosować środki przewidziane w procedurach bezpieczeństwa.

§ 8. PRAWA AUTORSKIE I WŁASNOŚĆ INTELEKTUALNA

- 1) treści wygenerowane przy pomocy AI (tekst, grafika, obraz, dane) są traktowane jako współtworzone przez pracownika i narzędzie AI o ile nie jest to zastrzeżone w regulaminie użytkowania AI;
- 2) pracownik ma obowiązek upewnić się, że dane wygenerowane przez AI nie naruszają praw autorskich i pokrewnych (muzyka, obraz, logo) i mogą być używane komercyjnie lub wewnątrz;
- 3) w przypadku wątpliwości co do własności praw autorskich i pokrewnych należy zwrócić się do Sekretarza o zgodę na wykorzystanie AI;
- 4) wszelkie treści stworzone w ramach obowiązków zawodowych (w tym z użyciem AI) stanowią własność pracodawcy;
- 5) w przypadku publikacji treści w całości wygenerowanych przez AI (np. w mediach społecznościowych, promocyjnych itp.) należy dodać adnotację informującą o użyciu AI.

§ 9. ZASADY WERYFIKACJI I ODPOWIEDZIALNOŚCI

- 1) wszystkie treści wygenerowane przez AI muszą być zweryfikowane przez pracownika przed dalszym użyciem, przesłaniem lub opublikowaniem;
- 2) pracownik jest odpowiedzialny za treść każdego dokumentu, decyzji, odpowiedzi czy innego materiału, który powstał przy użyciu AI, również wtedy, gdy powstały one częściowo z wykorzystaniem sztucznej inteligencji;
- 3) pracownik ponosi odpowiedzialność za treści, które przekazuje, niezależnie od tego czy została stworzona przez AI;
- 4) pracownik jest w pełni odpowiedzialny za merytoryczną poprawność, zgodność z prawem i ostateczną treść dokumentu/decyzji;
- 5) treści nie mogą naruszać prawa, zasad etyki ani dobrego imienia urzędu;
- 6) wątpliwości dotyczące zastosowania AI należy zgłaszać do Inspektora Ochrony Danych Osobowych i Sekretarza.

Artykuł 5 unijnego rozporządzenia o sztucznej inteligencji (AI Act) definiuje **praktyki AI o niedopuszczalnym ryzyku**, które są bezwzględnie zakazane na terenie Unii Europejskiej ze względu na ich szkodliwość dla podstawowych praw człowieka i wartości UE.

- 1) **systemy sztucznej inteligencji wykorzystujące techniki podprogowe lub celowo manipulujące lub wprowadzające w błąd** - systemy manipulujące ludzkim zachowaniem w sposób podświadomy, co prowadzi lub może prowadzić do istotnej szkody (fizycznej lub psychicznej);
- 2) **systemy sztucznej inteligencji wykorzystujące słabe punkty osoby lub określonej grupy osób** - systemy manipulujące osobami ze względu na ich wiek, niepełnosprawność lub trudną sytuację społeczno-ekonomiczną, co również powoduje istotną szkodę;
- 3) **systemy oceny społecznej** - systemy klasyfikujące ludzi na podstawie zachowania lub cech osobistych, co prowadzi do niesprawiedliwego traktowania (np. ograniczenia dostępu do usług);
- 4) **systemy sztucznej inteligencji przeznaczone do oceny ryzyka w odniesieniu do prawdopodobieństwa przestępstwa** - systemy oceniające prawdopodobieństwo popełnienia przestępstwa wyłącznie w oparciu o profilowanie osobowości;
- 5) **bazy danych rozpoznawania twarzy** - nieukierunkowane pobieranie obrazów twarzy z internetu lub nagrań CCTV w celu tworzenia baz danych;
- 6) **rozpoznawanie emocji w miejscach pracy i instytucjach edukacyjnych** - systemy wnioskujące o emocjach pracowników lub uczniów (z wyjątkiem celów medycznych lub bezpieczeństwa);
- 7) **systemy kategoryzacji biometrycznej** - systemy wnioskujące o rasie, poglądach politycznych, religii, orientacji seksualnej itp. na podstawie danych biometrycznych;
- 8) **zdalne systemy identyfikacji biometrycznej "w czasie rzeczywistym" w publicznie dostępnych przestrzeniach do celów egzekwowania prawa** - wykorzystywanie takich systemów w przestrzeni publicznej do celów ścigania przestępstw (z wąskimi wyjątkami, np. poszukiwanie zaginionego dziecka, zapobieganie terroryzmowi).

§ 10. ZGODNOŚĆ Z ROZPORZĄDZENIEM UE 2024/1689-AI Act

- 1) wszystkie działania związane z wykorzystaniem AI muszą być zgodne z Rozporządzeniem Parlamentu Europejskiego i rady (UE 2024/1689 z dnia 13 marca 2024 r.;
- 2) zabrania się stosowania SI określonych w art. 5 AI Act jako nieakceptowalne – załącznik do Procedur;
- 3) wszystkie zmiany w procedurze wymagają zatwierdzenia Burmistrza.