

Warszawa, dnia 25.09.2024 r.

## Procedura korzystania z narzędzi AI – dlaczego jest niezbędna w nowoczesnej organizacji?

Sztuczna inteligencja (AI) szybko staje się codziennym narzędziem w pracy wielu organizacji. Wykorzystywana jest w różnych branżach i zmienia sposób, w jaki firmy realizują swoje zadania. Narzędzia AI mogą automatyzować procesy, pomagać w analizie danych, wspierać twórczość czy nawet ułatwiać podejmowanie decyzji. Dzięki AI praca staje się szybsza i efektywniejsza – co również dostrzegają sami pracodawcy.

AI wchodzi do mainstreamu – kontrolowane korzystanie jest koniecznością.

AI przestaje być technologią niszową, a jej wpływ na różne branże rośnie z dnia na dzień. Narzędzia takie jak ChatGPT czy MidJourney stały się dostępne dla szerokiego grona odbiorców, a ich zastosowanie w firmach staje się standardem. Oznacza to, że firmy nie mogą już ignorować tego trendu – muszą umożliwić pracownikom korzystanie z AI, ale w sposób kontrolowany.

Jak każda nowa technologia, AI niesie ze sobą pewne ryzyka. W związku z tym wprowadzenie procedur jest naturalną kolejną rzeczą, która pozwala organizacjom korzystać z AI w sposób bezpieczny i odpowiedzialny, jednocześnie minimalizując niebezpieczeństwa wynikające z jej niewłaściwego użycia. Pracownicy powinni mieć swobodę w używaniu narzędzi AI, ale w granicach jasno określonych zasad, które chronią organizację przed niepożądanymi skutkami.

W tym artykule postaram się pokazać, dlaczego procedury są tak ważne i co powinny zawierać, aby zapewnić bezpieczeństwo, zgodność z prawem i efektywność w organizacji jednocześnie nie ograniczając możliwych kreatywnych zastosowań tych technologii w codziennej pracy niezależnie od zajmowanego stanowiska w organizacji, ale zanim, to:

### I. Dlaczego pracownicy powinni wiedzieć, jak korzystać z AI?

Z punktu widzenia każdej firmy, kluczowe jest, aby pracownicy rozumieli, jak mądrze i bezpiecznie korzystać z narzędzi opartych na sztucznej inteligencji. AI potrafi znacząco usprawnić wiele codziennych zadań, takich jak automatyzacja rutynowych procesów, analiza ogromnych ilości danych czy generowanie kreatywnych treści, oszczędzając czas i zwiększając efektywność pracy.

Przykłady branż, w których AI jest szczególnie przydatna, pokazują, jak szerokie może być jej zastosowanie:

- **Agencje reklamowe i marketingowe:** AI może generować teksty reklamowe w kilka sekund, analizować dane z kampanii w czasie rzeczywistym oraz przewidywać, które strategie marketingowe będą najbardziej skuteczne. To nie tylko przyspiesza pracę, ale też pomaga bardziej precyzyjnie docierać do klientów.
- **Branża IT:** W IT narzędzia AI mogą automatyzować procesy pisania i testowania kodu, identyfikować błędy w oprogramowaniu oraz pomagać w analizie danych o

wydajności systemów. Dzięki temu deweloperzy mają więcej czasu na rozwiązywanie bardziej złożonych problemów, a firmy mogą szybciej wprowadzać nowe produkty na rynek.

- **Działy sprzedaży i obsługi klienta:** W sprzedaży i obsłudze klienta sztuczna inteligencja może automatyzować komunikację z klientami, odpowiadać na najczęściej zadawane pytania czy analizować dane o preferencjach klientów, aby oferować im bardziej spersonalizowane produkty i usługi.
- **Służba zdrowia:** Lekarze i pielęgniarki mogą korzystać z AI, aby analizować dane pacjentów, przewidywać ryzyko chorób na podstawie historii medycznej czy wspierać proces diagnostyczny, co może przyczynić się do szybszej i trafniejszej diagnozy.
- **Logistyka:** AI w logistyce może optymalizować trasy dostaw, monitorować stany magazynowe w czasie rzeczywistym oraz przewidywać zapotrzebowanie na towary, co minimalizuje koszty i przyspiesza procesy operacyjne.

#### Dlaczego to ważne?

Znajomość narzędzi AI pozwala pracownikom na bardziej świadome korzystanie z ich potencjału. Bez odpowiedniej wiedzy i procedur, istnieje ryzyko, że będą one używane w sposób nieefektywny lub niebezpieczny. To może prowadzić do różnych problemów, związanych z:

- **Bezpieczeństwem danych:** AI operuje na ogromnych zbiorach danych, a jej skuteczność często zależy od jakości i zakresu przetwarzanych informacji. Jednakże, wprowadzenie do systemów AI poufnych danych, takich jak dane osobowe klientów, dane finansowe czy inne wrażliwe informacje, może prowadzić do poważnych naruszeń bezpieczeństwa. Przykładem zagrożeń może być sytuacja, w której pracownik bez wiedzy na temat zasad ochrony danych osobowych związanych z korzystaniem z AI wprowadza do narzędzia informacje, które nie powinny być udostępniane na zewnątrz. Brak zabezpieczeń w tym względzie lub niewłaściwe użycie może naruszyć prywatność klientów, co nie tylko wpłynie na reputację firmy, ale także grozi karami finansowymi związanymi z naruszeniami w sferze ochrony danych.
- **Odpowiedzialnością prawną:** Korzystanie z AI niesie za sobą poważne implikacje prawne. W przypadku przetwarzania danych osobowych, na przykład w kontekście rekrutacji, oceny wydajności pracowników czy analizowania preferencji klientów, konieczne jest przestrzeganie przepisów o ochronie danych. AI może być stosowana do analizowania dużych ilości informacji, jednak algorytmy mogą nie zawsze działać w pełni transparentnie. Decyzje podejmowane przez AI, jeśli nie są odpowiednio kontrolowane, mogą prowadzić do dyskryminacji lub podejmowania błędnych decyzji, które będą miały negatywne konsekwencje prawne.

Oprócz zagrożeń związanych z ochroną danych osobowych, organizacje muszą również brać pod uwagę kwestie związane z prawem autorskim. AI, szczególnie te narzędzia, które generują treści, takie jak teksty, obrazy, muzyka czy wideo, mogą nieświadomie naruszać prawa autorskie innych podmiotów. Jednym z popularnych

zastosowań AI jest automatyczne generowanie treści – od tekstów reklamowych pod grafiki czy raporty. Choć może to znacznie przyspieszyć pracę i zmniejszyć koszty, istnieje ryzyko, że wygenerowane przez AI treści mogą być oparte na danych, które naruszają właśnie prawa autorskie. Przykładowo, jeśli AI wygeneruje grafikę lub tekst na podstawie istniejących utworów chronionych prawami autorskimi, firma może zostać pociągnięta do odpowiedzialności za plagiat, nawet jeśli nie było to intencją pracownika.

- **Etyka:** Kwestie etyczne związane z AI są szczególnie istotne w kontekście podejmowania decyzji, które bezpośrednio wpływają na ludzi. Algorytmy uczące się z historycznych danych mogą reprodukcować istniejące uprzedzenia, prowadząc do decyzji, które są niesprawiedliwe lub dyskryminujące. W takim przypadku nie tylko reputacja firmy jest zagrożona, ale także jej pozycja prawna i zaufanie ze strony klientów i pracowników.

## II. Kluczowe kwestie dotyczące bezpieczeństwa i odpowiedzialności prawnej

AI to potężne narzędzie, ale jego używanie, jak widać, niesie ze sobą poważne zagrożenia, które muszą być wzięte pod uwagę. Oto kilka kluczowych kwestii, na które należy zwrócić uwagę przy wprowadzaniu procedur korzystania z AI w organizacji:

1. **Ochrona danych osobowych:** Pracownicy muszą być świadomi, że wprowadzanie do narzędzi AI danych osobowych, takich jak imiona, nazwiska, adresy czy numery identyfikacyjne, może prowadzić do naruszenia przepisów o ochronie danych osobowych, takich jak RODO. Firmy muszą zapewnić, że dane osobowe są chronione i przetwarzane zgodnie z prawem.
2. **Poufność informacji:** W sektorach takich jak prawo, finanse czy doradztwo, narzędzia AI mogą mieć dostęp do wrażliwych danych. Ważne jest, aby wprowadzanie tajemnic firmowych lub innych poufnych informacji do systemów AI było surowo ograniczone. Procedury muszą jasno określać, jakie dane mogą być przetwarzane przez AI, a jakie nie.
3. **Prawa autorskie i odpowiedzialność za treści:** Generowanie treści za pomocą AI wiąże się z ryzykiem naruszenia praw autorskich oraz odpowiedzialności za niezgodne z prawem materiały. Przykładowo, treści generowane do kampanii marketingowych muszą być sprawdzane, aby uniknąć przypadkowych naruszeń praw osób trzecich lub wprowadzenia w błąd odbiorców.
4. **Zarządzanie dostępem i bezpieczeństwo IT:** Procedury muszą również obejmować kwestie techniczne, takie jak np.: zapewnienie, że autoryzowani pracownicy mają dostęp do narzędzi AI. Ważne może być, co do zasady, stosowanie bezpiecznych haseł, dwuskładnikowego uwierzytelniania oraz regularne audyty bezpieczeństwa.

### III. Co powinna zawierać procedura korzystania z AI?

Kluczowe punkty, które należy uwzględnić w procedurze:

- 1. Zakres zastosowania AI:** Procedura powinna precyzyjnie określać, w jakich obszarach organizacja dopuszcza użycie narzędzi AI. Należy ustalić, że AI może być wykorzystywane w takich zadaniach jak:
  - Automatyizacja rutynowych procesów;
  - Wsparcie procesów decyzyjnych;
  - Tworzenie i przetwarzanie treści: Takie jak przygotowywanie odpowiedzi na często zadawane pytania czy tworzenie materiałów edukacyjnych.
- 2. Ograniczenia dotyczące wprowadzania danych:** Procedura musi szczegółowo określać, jakie dane mogą być wprowadzane do narzędzi AI, w tym:
  - Zakaz przetwarzania danych osobowych;
  - Ochrona informacji poufnych;
- 3. Weryfikacja treści generowanych przez AI:** Każda treść wygenerowana przez AI powinna być sprawdzana przed jej publicznym użyciem. Proces weryfikacji obejmuje:
  - Kontrolę merytoryczną: Sprawdzenie czy treści są dokładne i zgodne z rzeczywistością.
  - Zgodność z przepisami prawa;
  - Ochronę reputacji organizacji: Weryfikacja czy treści są zgodne z polityką organizacji oraz nie wpływają negatywnie na jej wizerunek
- 4. Zabezpieczenia techniczne:** Procedura powinna obejmować środki bezpieczeństwa, takie jak:
  - Silne hasła i dwuskładnikowe uwierzytelnianie (2FA);
  - Szyfrowanie danych;
  - Monitorowanie dostępu;
- 5. Ochrona praw własności intelektualnej i praw autorskich:** Procedura powinna zawierać wytyczne dotyczące ochrony praw własności intelektualnej:
  - Weryfikacja pod kątem prawa autorskiego: Upewnienie się, że treści generowane przez AI nie naruszają praw autorskich ani innych praw własności intelektualnej.
  - Kontrola wykorzystania materiałów chronionych: Sprawdzenie czy korzystanie z materiałów generowanych przez AI jest zgodne z obowiązującymi licencjami i prawami.
- 6. Sankcje za naruszenie procedur.** Dokument powinien określać konsekwencje za nieprzestrzeganie zasad korzystania z AI, w tym:
  - Sankcje dyscyplinarne: Mogą obejmować ostrzeżenie, zawieszenie w obowiązkach lub rozwiązanie umowy o pracę w przypadku poważnych naruszeń.
  - Odpowiedzialność za naruszenia prawne: Pracownicy mogą ponosić odpowiedzialność za skutki naruszeń przepisów prawa, takich jak ochrona danych osobowych czy prawa autorskie.

7. **Kontrola i nadzór** Procedura powinna przewidywać regularne audyty i aktualizację procedur.
8. **Obowiązki pracowników:** Dokument powinien również określać jak zgłaszać incydenty, zawierać wytyczne dotyczące weryfikacji treści generowanych przez AI.

#### IV. **Najlepszy przykład zastosowania AI = wykorzystanie do stworzenia tego artykułu!!**

Artykuł został opracowany przy wykorzystaniu narzędzia AI, jakim jest ChatGPT. Cały proces polegał na wprowadzeniu szczegółowych instrukcji dotyczących tematów, które miały zostać poruszone, a także kluczowych aspektów, które miały zostać omówione. Narzędzie AI wygenerowało tekst, który następnie został przeanalizowany i dostosowany, wielokrotnie zmieniony, aby spełniać wszystkie powyższe wytyczne. Ponadto, w czasie „tworzenia” narzędzie otrzymywało precyzyjne polecenia co zmienić, uszczegółowić lub na czym jeszcze należy zwrócić uwagę.

To doskonały przykład, jak AI może wspierać procesy kreatywne i generowanie treści, jednocześnie zapewniając, że człowiek nadal ma kontrolę nad ostatecznym wynikiem. Narzędzia AI mogą przyspieszać pracę i ułatwiać realizację zadań, jednak kluczowe jest, aby korzystać z nich w sposób odpowiedzialny i zgodny z obowiązującymi zasadami.

#### V. **Podsumowanie**

Korzystanie z narzędzi AI w organizacji, niezależnie od sektora, przynosi liczne korzyści, ale wymaga wprowadzenia jasnych zasad i procedur. Dzięki temu pracownicy będą mogli czerpać z możliwości, jakie oferuje sztuczna inteligencja, jednocześnie minimalizując ryzyko związane z bezpieczeństwem danych, odpowiedzialnością prawną oraz etyką pracy. Procedura dotycząca korzystania z AI jest niezbędnym krokiem w kierunku nowoczesności i innowacyjności, która pozwala firmom działać efektywniej, zachowując pełną zgodność z przepisami i zasadami etycznymi.

**Paweł Wojciechowski** – radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.