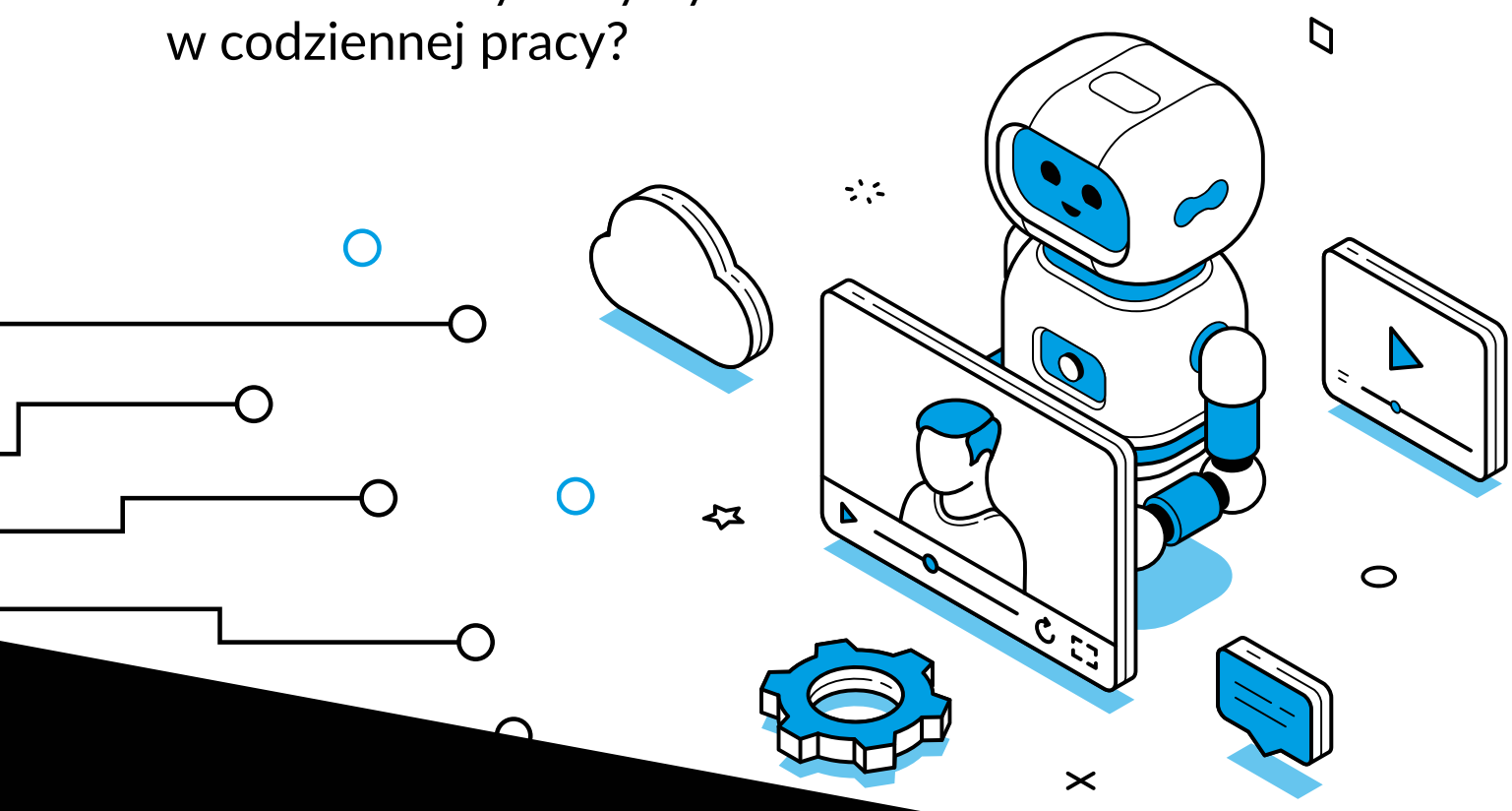
ZASADY KORZYSTANIA ZE SZTUCZNEJ INTELIGENCJI PRZEZ PRACOWNIKÓW

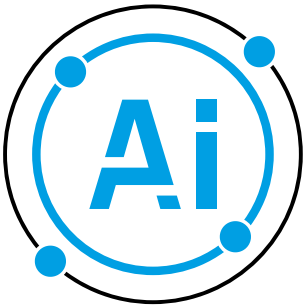
Jak bezpiecznie, odpowiedzialnie i świadomie wykorzystywać AI w codziennej pracy?



www.xemi.pl

- Kilka zasad, dzięki którym unikniesz kłopotów
- Zagrożenia AI - na co zwracać uwagę?

Bez wątpienia sztuczna inteligencja ułatwia codzienną pracę. Warto jednak używać jej z rozsądkiem i odpowiedzialnością. Kluczem jest świadomość, że treści, którymi "karmimy" AI mogą zawierać informacje ważne dla firmy, klientów, kontrahentów czy współpracowników.



Każdy pracownik, który korzysta z narzędzi AI, powinien przestrzegać zasad bezpieczeństwa obowiązujących w organizacji, w której pracuje.

Kilka uniwersalnych zasad, dzięki którym unikniesz kłopotów

Korzystaj tylko z narzędzi zaakceptowanych przez firmę

Po pierwsze sprawdź czy firma ma wewnętrzną politykę korzystania z AI. Pamiętaj, by w celach służbowych nie używać przypadkowych aplikacji AI, dodatków do przeglądarek, generatorów treści, obrazów i transkrypcji, jeśli firma nie dopuściła ich do użytku.

Nie integruj samodzielnie narzędzi AI z pocztą, dyskiem firmowym, komunikatorami, systemami ERP, CRM, HR, WMS i innymi. Każde połączenie powinno zostać wcześniej ocenione pod kątem bezpieczeństwa, ochrony danych i zgodności z politykami obowiązującymi w firmie.

Nie wpisuj poufnych danych do publicznych narzędzi AI

Nie wprowadzaj do AI informacji, które nie powinny trafić poza organizację, w szczególności: danych klientów, kontrahentów i pracowników, numerów PESEL, adresów, numerów telefonów, adresów e-mail, danych finansowych, cen, rabatów, warunków handlowych, treści umów, ofert, reklamacji i korespondencji z klientami, loginów, haseł, kluczy dostępu, strategii, planów rozwoju, dokumentacji wewnętrznej (projektowej, technicznej, serwisowej), kodów źródłowych itp.

Anonimizuj dane przed wprowadzeniem do AI

Jeśli chcesz wykorzystać AI do przygotowania podsumowania, uporządkowania tekstu lub analizy jakiegoś materiału, usuń z niego wszystkie poufne dane tj. dane osobowe, wewnętrzne dane firmowe. Dobrym sposobem jest zamiana rzeczywistych nazw na fikcyjne, np. klient 1, produkt 1, firma X.

Nie wierz w 100% wszystkiemu co generuje AI

Sztuczna inteligencja może się mylić, halucynować, zmyślać i dopowiadać. Może generować przekonujące i profesjonalne odpowiedzi, zawierające nieścisłości lub nieaktualne informacje. Nie mówiąc już o naruszeniu czyichś praw autorskich. Nie kopiuj bez zastanowienia, wszystkiego co produkuje AI, bo możesz wprowadzić odbiorcę w błąd, a nawet obiecać jemu coś, czego nie będziesz mógł dotrzymać.

Należy zweryfikować poprawność wygenerowanych odpowiedzi np. poszukując informacji w niezależnych źródłach i/lub prosząc AI o podanie źródeł, z których czerpała wiedzę. To ważne, zwłaszcza gdy informacje dotyczą prawa, podatków, finansów, danych technicznych, bezpieczeństwa, a Ty na ich podstawie podejmujesz decyzje biznesowe i/lub prowadzisz komunikację z klientami.

Nie podejmuj decyzji wyłącznie na podstawie AI

AI nie powinna być traktowana jak wyrocznia, zwłaszcza w sprawach dotyczących klientów, pracowników, finansów, ocen, wynagrodzeń czy ofert. Jak już wspominaliśmy, AI może się mylić, a jej błędy mogą prowadzić do wielu negatywnych konsekwencji, od wpływu na reputację firmy, aż po poważne skutki prawne. Pamiętaj, aby ostateczna decyzja należała do człowieka.

Ty ponosisz odpowiedzialność za treść

AI nie ponosi odpowiedzialności za końcowy efekt. Za treść, czy materiał opracowany na podstawie odpowiedzi sztucznej inteligencji odpowiada osoba, która ją wykorzystuje. Dlatego nie wysyłaj do klientów, kontrahentów, urzędów, pracowników a nawet przełożonych treści wygenerowanej przez AI bez wcześniejszej weryfikacji i korekty.

Zachowaj ostrożność przy generowaniu grafik, zdjęć i filmów

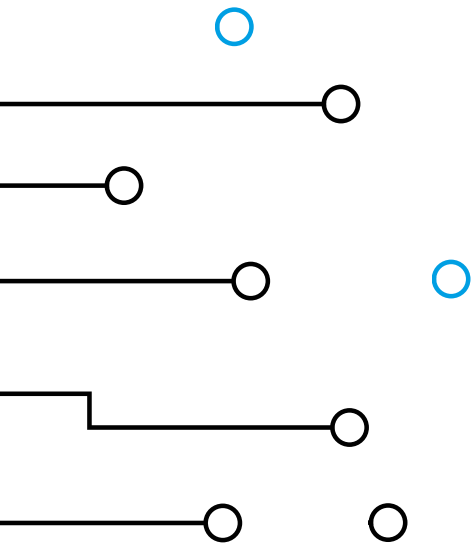
Nie twórz i nie publikuj materiałów wykorzystujących wizerunek, głos lub podobieństwo pracowników, klientów, kontrahentów lub jakichkolwiek osób bez odpowiedniej podstawy i zgody. Nie twórz materiałów, które mogą naruszyć prawa i wolności tych osób. W przypadku gdy masz wątpliwości co do wygenerowanego materiału, skonsultuj go z przełożonym, działem prawnym lub innymi osobami odpowiedzialnymi za komunikację.

Zgłaszaj incydenty i pomyłki

Przypadkowo wpisałeś do AI poufne informacje lub dane osobowe? A może zauważyłeś jakieś podejrzane działanie narzędzia? Nie zwlekaj, nie ukrywaj tego. Koniecznie zgłoś sprawę przełożonemu, działowi IT, inspektorowi ochrony danych lub innej osobie odpowiedzialnej za bezpieczeństwo informacji. Z pewnością w firmie obowiązuje polityka zgłaszania incydentów i naruszeń, więc postępuj zgodnie z jej zasadami.

Korzystaj z AI w sposób uczciwy, przejrzysty i odpowiedzialny

Nie wykorzystuj AI do tworzenia treści obraźliwych, nieetycznych, dyskryminujących, niezgodnych z prawem. Pamiętaj, że za wygenerowane treści odpowiada osoba, która te materiały tworzy, zatwierdza i publikuje.



AI przyspiesza pracę,
ale nie zwalnia z myślenia
i odpowiedzialności.

Zagrożenia AI
na co zwracać uwagę?

Prywatność danych

- wyciek danych osobowych i informacji poufnych do chmury AI
- trening modelu na Twoich dokumentach i materiałach
- nieautoryzowany dostęp do historii chatów
- identyfikacja konkretnych osób na podstawie danych, które wprowadzasz

Dezinformacja

- halucynacje AI wykorzystywane jako fakty
- deepfake - fałszywe obrazy, video i głosy, łudząco podobne do rzeczywistych, wprowadzające odbiorcę w błąd
- manipulacja polityczna i społeczna
- automatyczny SPAM i phishing AI

Ryzyko zawodowe

- nadmierne uzależnienie od AI prowadzące do zaniku umiejętności i kompetencji (deskilling)
- błędne decyzje biznesowe oparte na sztucznej inteligencji
- naruszenie regulacji (RODO, kodeks pracy) oraz wewnętrznej polityki firmy
- odpowiedzialność za błędy AI

Cyberbezpieczeństwo

- AI wykorzystywana do tworzenia ataków malware
- tworzone przez AI ataki phishingowe, trudne do rozpoznania
- kradzież tożsamości (voice cloning), w celu wyłudzenia danych/pieniędzy
- bardziej precyzyjna i wiarygodna manipulacja socjotechniczna dopasowana do konkretnej osoby

Narzędzia AI dają możliwości,
ale bezpieczeństwo zależy od tego, jak z nich korzystamy.