

LATO Z RODO

Korzystasz z ChatGPT, Copilota lub innych narzędzi AI w firmie? – zachowaj ostrożność. To potężne wsparcie, ale też poważne ryzyko dla organizacji. Pamiętaj: Twoja ostrożność w korzystaniu z AI, to najlepsza ochrona danych i interesów firmy.

*Agnieszka Rzycka-Osiej
Inspektor Ochrony Danych*



LATO Z RODO

Korzystasz z ChatGPT, Copilota lub innych narzędzi AI w firmie? – zachowaj ostrożność.

To potężne wsparcie, ale też poważne ryzyko dla organizacji:

1. Ujawnienie tajemnicy przedsiębiorstwa

Wprowadzenie do AI informacji poufnych (np. strategii, kodów, umów) może skutkować ich utratą i wykorzystaniem przez osoby trzecie.

2. Naruszenie ochrony danych osobowych

AI nie może być wykorzystywane do przetwarzania danych osobowych bez odpowiednich podstaw prawnych i zabezpieczeń.

3. Problemy z prawami autorskimi

Treści generowane przez AI mogą naruszać cudze prawa, a użycie materiałów firmowych do „trenowania” modeli może być ryzykowne.

4. Zaufanie do odpowiedzi AI

AI może się mylić – generować fałszywe, nieaktualne lub zmanipulowane informacje. To Ty odpowiadasz za ich wykorzystanie.

Jak bezpiecznie korzystać z AI w firmie?

1. Nie wprowadzaj danych osobowych

Nie podawaj imion, nazwisk, numerów PESEL, adresów, danych klientów ani pracowników.

2. Nie ujawniaj informacji poufnych

Treści firmowe, dokumenty wewnętrzne, plany strategiczne – powinny być szczególnie chronione.

3. Sprawdzaj zgodność z procedurami firmowymi

Korzystaj z narzędzi tylko wtedy, gdy są zatwierdzone przez firmę i zgodne z polityką bezpieczeństwa.

4. Weryfikuj wyniki AI

Traktuj odpowiedzi AI jako pomoc, nie źródło prawdy ostatecznej.

5. Zgłaszaj wątpliwości

Jeśli nie wiesz, czy możesz użyć AI w danej sytuacji – skontaktuj się z Inspektorem Ochrony Danych lub działem IT.

Pamiętaj: Twoja ostrożność w korzystaniu z AI to najlepsza ochrona danych i interesów firmy.