Polityka korzystania przez pracowników z narzędzi AI

# §1. Cel Polityki

Celem niniejszej Polityki jest określenie zasad odpowiedzialnego, bezpiecznego i zgodnego z przepisami prawa korzystania z narzędzi opartych na sztucznej inteligencji (AI) przez pracowników i współpracowników organizacji. Polityka dotyczy zarówno systemów wewnętrznych, jak i zewnętrznych, wykorzystywanych w ramach obowiązków służbowych.

# §2. Zakres stosowania

Polityka ma zastosowanie do wszystkich pracowników, współpracowników, zleceniobiorców oraz podwykonawców, którzy korzystają z narzędzi AI w związku z wykonywaniem powierzonych im zadań. Dotyczy to zwłaszcza przypadków, w których przetwarzane są dane osobowe, informacje poufne lub materiały strategiczne.

# §3. Dozwolone zastosowania AI

Dopuszcza się korzystanie z narzędzi AI w celu wsparcia pracy biurowej, analizy danych, przygotowania wstępnych treści marketingowych lub raportów oraz prototypowania rozwiązań – pod warunkiem zachowania zasady minimalizacji danych i przejrzystości źródeł informacji.

# §4. Niedozwolone działania

Zabrania się wprowadzania danych osobowych do publicznych narzędzi AI bez zgody przełożonego, podejmowania decyzji prawnych lub kadrowych wyłącznie na podstawie wyników działania AI, a także generowania treści sprzecznych z przepisami prawa lub interesem organizacji.

# §5. Bezpieczeństwo i ochrona danych

Użytkownicy systemów AI mają obowiązek przekazywać jedynie dane niezbędne do realizacji celu, przestrzegać zasad kontroli dostępu oraz wykorzystywać wyłącznie zatwierdzone narzędzia udostępnione przez organizację.

# §6. Zgłaszanie incydentów

Wszelkie incydenty związane z wykorzystaniem AI, w szczególności naruszenia ochrony danych, należy niezwłocznie zgłaszać do przełożonego, Inspektora Ochrony Danych lub działu IT.

# §7. Nadzór i odpowiedzialność

Za wdrożenie niniejszej Polityki odpowiada Zarząd. Inspektor Ochrony Danych nadzoruje zgodność z RODO, dział IT odpowiada za bezpieczeństwo narzędzi, a pracownicy zobowiązani są do przestrzegania niniejszych zasad.

# §8. Monitorowanie i sankcje

Organizacja przeprowadza audyty wewnętrzne w celu weryfikacji zgodności działań z Polityką. Naruszenie jej postanowień może skutkować sankcjami służbowymi, w tym upomnieniem, ograniczeniem dostępu lub rozwiązaniem umowy.

# §9. Postanowienia końcowe

Polityka obowiązuje od dnia jej zatwierdzenia przez Zarząd. Dokument jest udostępniany wszystkim pracownikom i może być aktualizowany w przypadku zmiany przepisów prawa, technologii lub strategii organizacyjnej.

# Podstawa prawna

• art. 5 ust. 1 lit. c, art. 6, art. 24, art. 25, art. 32, art. 35 – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)

• art. 29 i nast. – projekt rozporządzenia AI Act (UE)

• ISO/IEC 27001 – norma zarządzania bezpieczeństwem informacji