Warszawa, dn. 23.06.2026 r.

Shadow AI w firmie. Dlaczego warto wdrożyć politykę korzystania z AI?

Sztuczna inteligencja (w Polsce zamiennie używamy także skrótów AI albo SI) za sprawą modeli udostępnionych w sieci dla szerokiego grona odbiorców stała się nieoderwaną częścią pracy wielu firm. Narzędzia takie jak ChatGPT, Copilot czy Gemini już na dobre wniknęły do naszej codzienności. Choć AI rozwija się od kilkudziesięciu lat, dopiero kilka lat temu duże modele językowe, czyli tzw. generatywna sztuczna inteligencja stały się powszechnie dostępne.
Sztuczna inteligencja pomaga dzisiaj szybciej i sprawniej realizować część zadań. Jest wykorzystywana do przygotowania dokumentów, analizy informacji, tłumaczenia tekstów czy wyciągania najważniejszych wniosków. A jest to tylko ułamek czynności, które można wykonywać z pomocą AI.
W wielu firmach wykorzystanie AI rozwija się jednak szybciej niż wewnętrzne procedury. Pracownicy zaczynają korzystać z dostępnych narzędzi samodzielnie. Może to się dziać niezależnie od firmy. Takie zjawisko określa się mianem Shadow AI.

Czym jest Shadow AI?

Shadow AI to korzystanie z narzędzi opartych na sztucznej inteligencji bez zgody lub wiedzy firmy. Przykładem może być pracownik, który wkleja fragment dokumentu do ChataGPT, aby przygotować jego streszczenie albo raport dla klienta.
Jeżeli firma nie zapewnia oficjalnych narzędzi, pracownicy w łatwy sposób mogą sięgać po te dostępne w sieci. W ten sposób dużo szybciej mogą wykonać zlecone zadanie. Dla pracownika jest to po prostu kolejne narzędzie wspierające codzienną pracę, ale dla pracodawcy może się stać źródłem potencjalnych ryzyk.

Jakie ryzyka wiążą się z Shadow AI?

Najważniejszym ryzykiem jest utrata kontroli nad informacjami wprowadzanymi do modeli AI. Tak naprawdę nie wiemy jak wprowadzone dane są przechowywane i wykorzystywane oraz czy mogą zostać przypadkiem ujawnione podczas korzystania z modelu przez inne osoby. Przykładowo do modelu AI mogą trafić dane klientów lub informacje dotyczące planów biznesowych firmy. Nawet jeśli pracownik działa w dobrej wierze, może nieświadomie naruszyć wewnętrzne zasady ochrony danych.
Sztuczna inteligencja nie zawsze podaje poprawne informacje. Dlatego każdą odpowiedź wygenerowaną przez AI warto sprawdzić przed wykorzystaniem jej w pracy. W przeciwnym razie można oprzeć swoje działania na błędnych danych.
Problemem może być także brak wiedzy o tym, jakie narzędzia są używane w firmie. Jeżeli firma nie monitoruje wykorzystania AI, trudno jest ocenić poziom ryzyka i wprowadzić odpowiednie zabezpieczenia.

Jak zaopiekować pojawiające się wątpliwości?

Pierwsze co przychodzi do głowy (zapewne nie tylko mi) to próba całkowitego ograniczenia korzystania z AI do celów pracowniczych. Trudno mi sobie wyobrazić, żeby taki pomysł przyniósł oczekiwane rezultaty. Pracownicy mogą korzystać z prywatnych urządzeń, a generatywnych modeli AI wciąż wyrasta jak grzybów po deszczu. W rezultacie wykorzystanie AI nie znika, lecz staje się mniej widoczne dla firmy.

Znacznie skuteczniejsze jest stworzenie jasnych zasad korzystania z AI oraz zapewnienie pracownikom bezpiecznych narzędzi do wykonywania obowiązków. Dzięki temu organizacja zachowuje kontrolę nad procesem, a jednocześnie może korzystać z możliwości oferowanych przez nowe technologie.

Co z tą polityką?

Polityka AI powinna przede wszystkim określać, jakie narzędzia są dopuszczone do wykorzystania. Dzięki temu pracownicy wiedzą z których rozwiązań mogą korzystać podczas wykonywania obowiązków służbowych.

W dokumencie warto również wskazać, jakie dane nie powinny być wprowadzane do systemów AI. Dotyczy to w szczególności danych osobowych oraz danych kontrahentów. Przy czym należy pamiętać, że kontekst też ma bardzo duże znaczenia. Jeśli do modelu językowego wprowadzimy informację, że klientem jest „największa sieć mały sklepów z płazem w nazwie", to nietrudno domyślić się, o którą franczyzę chodzi.

Istotnym elementem jest także obowiązek weryfikacji wyników generowanych przez sztuczną inteligencję. Ostateczna odpowiedzialność za wykorzystanie informacji w procesach biznesowych powinna zawsze pozostawać po stronie człowieka. Dobrą praktyką jest również określenie procedury zgłaszania nowych narzędzi AI. Dzięki temu pracownicy mogą proponować rozwiązania wspierające ich pracę, a organizacja ma możliwość wcześniejszej oceny ryzyka.

Korzyści z wdrożenia polityki korzystania z AI

Wdrożenie polityki korzystania z AI przynosi korzyści zarówno organizacji, jak i pracownikom. Przede wszystkim zwiększa kontrolę nad wykorzystywanymi narzędziami. Firma wie, jakie rozwiązania są stosowane oraz jakie dane są przetwarzane.

Polityka pomaga również spełniać wymagania związane z bezpieczeństwem informacji i ochroną danych. Ma to szczególne znaczenie dla firm współpracujących z klientami, którzy oczekują odpowiedniego poziomu ochrony danych osobowych.

Zatem pierwszym krokiem powinno być zrozumienie, w jaki sposób pracownicy już teraz korzystają z narzędzi AI. Następnie warto przeprowadzić ocenę ryzyka oraz określić, które narzędzia i modele mogą być wykorzystywane w działalności firmy. Kolejnym etapem jest przygotowanie polityki AI dostosowanej do specyfiki firmy.

Oczywiście samo opracowanie dokumentu nie jest wystarczające. Ważne są również szkolenia oraz regularne przypominanie zasad bezpiecznego korzystania z nowych technologii.

Dlaczego to jest ważne już dzisiaj?

11 czerwca 2026 r. Sejm przyjął ustawę o systemach sztucznej inteligencji (nr druku: 2443), której celem jest dostosowanie polskiego porządku prawnego do wymogów unijnego AI Act. Choć zdecydowana większość przepisów AI Act dotyczy modeli wysokiego ryzyka (a takimi nie są ogólnodostępne modele generatywne) nowe regulacje stanowią wyraźny sygnał, że wykorzystywanie sztucznej inteligencji staje się obszarem podlegającym coraz większym wymaganiom prawnym.

Mateusz Wrotny – młodszy specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.