

Tajemnica przedsiębiorstwa w erze AI – dlaczego firma potrzebuje regulacji korzystania z narzędzi AI przez pracowników

Wprowadzenie

Przedsiębiorca, który pozwala pracownikom korzystać z narzędzi sztucznej inteligencji bez jasno określonych zasad, naraża się nie tylko na wyciek informacji, lecz także na osłabienie ich ochrony prawnej jako tajemnicy przedsiębiorstwa. Sam poufny lub gospodarczo wartościowy charakter informacji nie wystarcza bowiem do objęcia jej ochroną. Przedsiębiorca musi również wykazać, że podjął odpowiednie działania w celu zachowania jej poufności.

Generatywna AI stała się codziennym narzędziem pracy. Pracownicy wykorzystują ją do streszczania umów, poprawiania kodu, tłumaczenia ofert, przygotowywania prezentacji czy analizowania arkuszy zawierających dane sprzedażowe. Najczęściej robią to w dobrej wierze – chcąc wykonywać swoje obowiązki szybciej i efektywniej. Problem zaczyna się wtedy, gdy do zewnętrznego narzędzia trafiają informacje firmowe bez uprzedniej oceny zasad ich przetwarzania, retencji, wykorzystania przez dostawcę czy lokalizacji infrastruktury.

W 2026 r. wewnętrzne zasady korzystania z AI, połączone z rzeczywistym uświadamianiem pracowników, trudno już traktować jako rozwiązanie wyłącznie fakultatywne. Z perspektywy ochrony tajemnicy przedsiębiorstwa mogą one stanowić istotny element działań podejmowanych w celu utrzymania informacji w poufności – a więc jednej z przesłanek, od których zależy możliwość skorzystania z ochrony przewidzianej w ustawie o zwalczaniu nieuczciwej konkurencji.

Tajemnica przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji

Podstawą ochrony jest art. 11 ustawy z 16 kwietnia 1993 r. - o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2026r., poz. 85 ze zm.; „UZNK”). Zgodnie z art. 11 ust. 2 UZNK tajemnicą przedsiębiorstwa są informacje techniczne, technologiczne, organizacyjne lub inne informacje posiadające wartość gospodarczą, które spełniają łącznie trzy przesłanki:

1. Jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są dla takich osób łatwo dostępne.
2. Mają wartość gospodarczą — także potencjalną — wynikającą właśnie z ich poufnego charakteru.
3. Uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności.

W kontekście AI kluczowa jest przesłanka trzecia. Ochrona nie powstaje z mocy samego faktu, że informacja jest cenna. Przedsiębiorca musi wykazać, że realnie zabezpieczał poufność — organizacyjnie, technicznie i prawnie. W sporze to na nim spoczywa ciężar dowodu, a sądy oceniają adekwatność działań do rodzaju informacji, skali działalności i znanych zagrożeń.

To ostatnie ma znaczenie praktyczne. Ryzyko wycieku danych przez narzędzia generatywnej AI jest dziś powszechnie znane i szeroko opisywane. Trudno więc będzie przekonać sąd, że firma działała z należyłą starannością, jeśli tolerowała niekontrolowane wklejanie poufnych dokumentów do publicznych chatbotów, nie wydając w tej sprawie żadnych zasad.

Jak narzędzia AI zagrażają poufności

Największe ryzyko nie wynika ze spektakularnych scenariuszy technologicznych, lecz z codziennych i pozornie niewinnych czynności pracowników. W praktyce warto zwrócić uwagę przede wszystkim na kilka sytuacji.

Dane wejściowe przekazywane dostawcy. Treść wpisana w prompt lub dokument przesłany do usługi może zostać przekazany do infrastruktury dostawcy. To, co dzieje się z danymi dalej, zależy od konkretnego produktu, wersji usługi, umowy, ustawień oraz polityki prywatności.

Wykorzystywanie danych do ulepszania modeli. W części usług – zwłaszcza konsumenckich – treści użytkowników mogą, zależnie od obowiązujących warunków i ustawień, być wykorzystywane do rozwoju lub ulepszania modeli. Nie należy jednak zakładać, że wszystkie narzędzia AI działają pod tym względem identycznie. Dlatego przed dopuszczeniem konkretnej usługi konieczna jest analiza jej rzeczywistych warunków.

Retencja i dostęp do danych. Nawet jeżeli dane nie są wykorzystywane do trenowania modeli, mogą być przechowywane przez określony czas, np. ze względów bezpieczeństwa lub w celu wykrywania nadużyć. Znaczenie ma również to, kto i w jakich okolicznościach może uzyskać do nich dostęp.

Shadow AI. Szczególne ryzyko powstaje wtedy, gdy pracownicy wykorzystują do celów służbowych prywatne konta lub narzędzia, o których nie wie dział IT. Organizacja traci wówczas kontrolę nad ustawieniami, historią rozmów, zakresem udostępnianych informacji oraz dostępem do nich po zakończeniu współpracy z daną osobą.

Wtyczki, integracje i agenci AI. Narzędzia z dostępem do poczty elektronicznej, dysku, CRM, komunikatorów czy repozytoriów kodu mogą samodzielnie pobierać informacje z wielu źródeł. Nadanie zbyt szerokich uprawnień może więc stworzyć dostęp do znacznie większego zbioru danych, niż użytkownik pierwotnie zamierzał udostępnić.

Treści generowane przez AI. Ryzyko nie kończy się na danych wejściowych. Wygenerowana odpowiedź może zawierać informacje pochodzące z materiałów poufnych, a następnie trafić np. do klienta, prezentacji, raportu czy publicznego dokumentu.

Głośnym przykładem było ujawnienie w 2023 r. fragmentów kodu źródłowego i notatek wewnętrznych przez inżynierów dużego koncernu elektronicznego, którzy korzystali z publicznego chatbota do poprawiania kodu. Firma zareagowała czasowym zakazem używania takich narzędzi. Przypadek ten pokazuje, że organizacja powinna ustalić zasady korzystania z AI zanim dojdzie do incydentu, a nie dopiero w reakcji na niego.

Warto również pamiętać, że tajemnica przedsiębiorstwa rzadko występuje w izolacji. Ten sam prompt może zawierać dane osobowe, informacje chronione umową o zachowaniu poufności, tajemnicą zawodową albo – w określonych przypadkach – informacje poufne podlegające szczególnym regulacjom. Jedna nieostrożna czynność może więc uruchomić konsekwencje na gruncie kilku różnych reżimów prawnych.

Brak regulacji oznacza ryzyko utraty ochrony

Brak zasad korzystania z AI stwarza dwa rodzaje ryzyka. Po pierwsze, zwiększa prawdopodobieństwo niekontrolowanego ujawnienia informacji. Po drugie, może utrudnić przedsiębiorcy wykazanie, że dochował należytej staranności w celu zachowania ich poufności.

Jeżeli pracownik przekazał chronione know-how do niezatwierdzonego zewnętrznego narzędzia AI, a przedsiębiorca nie określił wcześniej żadnych zasad dotyczących takiego wykorzystania danych, w ewentualnym sporze może pojawić się argument, że zastosowane środki ochrony informacji były niewystarczające. Nie oznacza to automatycznej utraty statusu tajemnicy przedsiębiorstwa – ocena zależy od całokształtu zastosowanych zabezpieczeń i konkretnych okoliczności – ale brak regulacji dotyczących znanego kanału ryzyka może istotnie osłabić pozycję dowodową przedsiębiorcy.

Ma to znaczenie także dla możliwości dochodzenia roszczeń związanych z naruszeniem tajemnicy przedsiębiorstwa, w tym roszczeń przewidzianych w art. 18 UZNK oraz – gdy spełnione są ustawowe przesłanki – odpowiedzialności karnej określonej w art. 23 UZNK.

Jasne zasady są istotne również z perspektywy odpowiedzialności pracownika. Jeżeli organizacja nie określiła, które narzędzia są dozwolone, jakiego rodzaju informacje mogą być w nich przetwarzane oraz jakie obowiązki ma użytkownik, trudniejsze może być wykazanie, że konkretne zachowanie stanowiło zawinione naruszenie obowiązków pracowniczych.

Do tego dochodzą konsekwencje wynikające z innych regulacji i zobowiązań, takich jak naruszenie umów o zachowaniu poufności, obowiązków związanych z ochroną danych osobowych czy nawet straty reputacyjne. W sektorach regulowanych mogą ponadto znaleźć zastosowanie szczególne wymagania dotyczące bezpieczeństwa ICT, outsourcingu oraz zarządzania dostawcami.

Co powinny zawierać regulacje wewnętrzne

System zarządzania korzystaniem z AI może opierać się na trzech powiązanych elementach: polityce AI na poziomie organizacji, zasadach korzystania z narzędzi AI skierowanych do pracowników i współpracowników oraz rejestrze zatwierdzonych narzędzi. Dokumenty te pełnią odmienne funkcje i nie powinny być prostymi kopiami tej samej regulacji.

Polityka AI wyznacza ramy organizacyjne: cele korzystania z AI, role i odpowiedzialności, sposób oceny ryzyka nowych narzędzi oraz powiązanie zasad AI z bezpieczeństwem informacji, ochroną danych osobowych i compliance.

Regulamin lub instrukcja dla użytkowników powinny mieć przede wszystkim charakter praktyczny. Pracownik przed użyciem AI powinien móc szybko ustalić:

- z jakich narzędzi wolno korzystać i na jakich kontach;
- jakich kategorii informacji nie wolno wprowadzać do zewnętrznych systemów AI;
- jakie informacje mogą być przetwarzane wyłącznie w zatwierdzonych rozwiązaniach;
- kiedy i w jaki sposób należy anonimizować lub pseudonimizować dane;
- jak weryfikować rezultaty pracy AI;
- jakie zasady obowiązują przy korzystaniu z integracji, wtyczek i agentów;
- komu i w jakim trybie zgłaszać przypadkowe przekazanie informacji do niewłaściwego narzędzia.

Rejestr narzędzi AI powinien natomiast dokumentować, które rozwiązania zostały ocenione i dopuszczone do używania, w jakiej wersji lub planie, z jakimi ustawieniami oraz do przetwarzania jakich kategorii informacji. W zależności od przypadku warto odnotować również podstawę kontraktową korzystania z usługi, zasady retencji, lokalizację przetwarzania czy kwestie związane z przetwarzaniem danych osobowych.

Rejestr pełni nie tylko funkcję operacyjną. Może być również dowodem, że przedsiębiorca świadomie identyfikował ryzyko związane z AI i podejmował działania mające mu przeciwdziałać.

Fundamentem całego systemu pozostaje jednak klasyfikacja informacji. Sam zakaz wprowadzania do AI „informacji poufnych” będzie mało skuteczny, jeśli pracownik nie wie, co organizacja rozumie przez to pojęcie. W praktyce sprawdza się prosty, trzy- lub czterostopniowy podział – np. na informacje publiczne, wewnętrzne, poufne i ściśle poufne – uzupełniony przykładami charakterystycznymi dla poszczególnych działów.

Regulacje muszą również odpowiadać rzeczywistej praktyce. Jeżeli organizacja formalnie zakazuje korzystania z AI, ale w rzeczywistości toleruje jego powszechne używanie, skuteczność takiego zakazu – także jako dowodu należytej staranności – może być ograniczona. Z perspektywy zarządzania ryzykiem bardziej efektywne bywa zapewnienie pracownikom zatwierdzonego rozwiązania i ustalenie jasnych zasad jego używania niż utrzymywanie zakazu, który sprzyja rozwojowi shadow AI.

Uświadamianie pracowników – od dokumentu do nawyku

Sam regulamin nie będzie skuteczny jeżeli pracownicy nie znają jego treści albo nie rozumieją, jak stosować go w codziennej pracy. Z perspektywy ochrony tajemnicy przedsiębiorstwa istotne jest nie tylko przyjęcie dokumentu, lecz również możliwość wykazania, że zasady zostały skutecznie zakomunikowane i są rzeczywiście stosowane.

Z perspektywy organizacji oznacza to, że szkolenia, instrukcje oraz inne działania uświadamiające pozostają istotnym elementem zarządzania AI, choć przepisy nie wymagają konkretnego certyfikatu ani jednego, narzuconego modelu szkolenia. Skuteczny program może obejmować:

- szkolenie wprowadzające dla nowych pracowników oraz szkolenie dla obecnego zespołu, wykorzystujące przykłady odpowiadające rzeczywistym zadaniom danego działu;
- udokumentowanie zapoznania się z obowiązującymi zasadami;
- krótkie szkolenia lub przypomnienia po zmianie narzędzi, zasad albo po wystąpieniu istotnego incydentu;
- prostą checklistę „przed wpisaniem promptu”, pomagającą ustalić m.in., czy narzędzie jest zatwierdzone, czy użytkownik korzysta z właściwego konta oraz czy przekazywane informacje mogą zostać w nim przetworzone;
- łatwo dostępny kanał zgłaszania pomyłek i incydentów.

Celem takich działań nie powinno być odstraszenie pracowników od AI. Chodzi o wyrobienie nawyku świadomego korzystania z technologii – podobnie jak wcześniej organizacje uczyły zasad bezpiecznego korzystania z poczty elektronicznej, chmury czy urządzeń mobilnych.

Aspekty prawa pracy, a współpraca B2B

Zgodnie z art. 100 § 2 pkt 4 Kodeksu pracy pracownik ma obowiązek dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę. Ogólny obowiązek ustawowy nie odpowiada jednak na praktyczne pytania dotyczące korzystania z AI. Wewnętrzne zasady mogą go konkretyzować, wskazując pracownikowi, jak powinien postępować z określonymi informacjami i narzędziami.

Sposób wprowadzenia takich zasad powinien być dostosowany do struktury organizacji oraz charakteru regulowanych obowiązków. Mogą one funkcjonować jako odrębna polityka, instrukcja lub zarządzenie, a tam, gdzie ich treść ingeruje w materię regulaminu pracy, należy uwzględnić wymagania wynikające z art. 104 i nast. Kodeksu pracy.

Jasne i prawidłowo zakomunikowane zasady mają znaczenie także w przypadku wyciągania konsekwencji wobec pracownika. W zależności od okoliczności mogą wchodzić w grę kary porządkowe, odpowiedzialność materialna, a w najpoważniejszych przypadkach również rozwiązanie umowy o pracę bez wypowiedzenia. Każdy taki przypadek wymaga jednak indywidualnej oceny, w szczególności pod kątem winy pracownika, rodzaju naruszonego obowiązku i skutków zdarzenia.

Odrębnego podejścia wymagają zleceniobiorcy, osoby samozatrudnione i inni współpracownicy B2B, do których przepisy Kodeksu pracy nie znajdują zastosowania. Ich obowiązki dotyczące korzystania z AI powinny wynikać przede wszystkim z umowy. W praktyce warto rozważyć wprowadzenie do umów współpracy oraz umów o zachowaniu poufności zobowiązania do przestrzegania obowiązującej polityki AI, zasad zgłaszania incydentów oraz – tam, gdzie jest to uzasadnione – odpowiednio skonstruowanej odpowiedzialności kontraktowej.

Ma to szczególne znaczenie w relacjach z podwykonawcami IT, agencjami marketingowymi, konsultantami i innymi podmiotami, które wykonując usługi na rzecz przedsiębiorcy, mogą przetwarzać jego dane we własnych narzędziach AI.

Checklista wdrożeniowa dla przedsiębiorcy

Przejście od niekontrolowanego korzystania z AI do uporządkowanego systemu zarządzania nie musi być wielomiesięcznym projektem. Punktem wyjścia może być następująca sekwencja działań:

1. **Zinwentaryzuj rzeczywiste wykorzystanie AI.** Ustal, z jakich narzędzi pracownicy i współpracownicy faktycznie korzystają do celów służbowych – również za pośrednictwem prywatnych kont.
2. **Zidentyfikuj chronione informacje.** Określ, które informacje mają znaczenie gospodarcze i wymagają zachowania poufności, a następnie wprowadź zrozumiałą klasyfikację informacji.
3. **Oceń używane narzędzia.** Przeanalizuj m.in. warunki świadczenia usług, wykorzystanie danych przez dostawcę, retencję, lokalizację przetwarzania, mechanizmy bezpieczeństwa oraz dostępność planów przeznaczonych dla organizacji.
4. **Zapewnij zatwierdzone narzędzie.** Jeżeli AI ma być wykorzystywana w pracy, zapewnij pracownikom rozwiązanie odpowiednie do rodzaju przetwarzanych informacji i skonfiguruj je zgodnie z wymaganiami organizacji.
5. **Przyjmij wewnętrzne zasady.** Opracuj politykę AI, instrukcję lub regulamin dla użytkowników oraz rejestr dopuszczonych narzędzi.
6. **Uwzględnij współpracowników i podwykonawców.** Dostosuj umowy B2B, NDA i umowy z dostawcami, jeżeli osoby trzecie mogą korzystać z AI przy przetwarzaniu informacji przedsiębiorcy.
7. **Przeszkol użytkowników.** Wyjaśnij zasady na konkretnych przykładach i udokumentuj działania szkoleniowe.
8. **Przygotuj procedurę incydentową.** Pracownik powinien wiedzieć, co zrobić natychmiast po przypadkowym przekazaniu danych do niewłaściwego narzędzia i komu zgłosić zdarzenie.
9. **Regularnie aktualizuj system.** Przeglądaj listę narzędzi i zasady po istotnych zmianach technologicznych, organizacyjnych lub prawnych i dokumentuj przeprowadzone przeglądy.

Podsumowanie

Sztuczna inteligencja nie zmieniła prawnej definicji tajemnicy przedsiębiorstwa. Zmieniła natomiast środowisko, w którym przedsiębiorcy muszą tę tajemnicę chronić. Powstał kolejny – wyjątkowo łatwy w użyciu – kanał, którym poufne informacje mogą opuścić organizację, często bez złej woli pracownika i bez świadomości, że właśnie doszło do ich przekazania zewnętrznemu podmiotowi.

Dlatego zarządzanie korzystaniem z AI staje się elementem szerszego systemu ochrony informacji. Polityka AI, praktyczne zasady dla pracowników, rejestr zatwierdzonych narzędzi, klasyfikacja informacji, odpowiednie rozwiązania techniczne i udokumentowane działania szkoleniowe tworzą razem system, który zarówno ogranicza ryzyko incydentu, jak i pomaga przedsiębiorcy wykazać, że rzeczywiście podejmował działania w celu utrzymania swoich informacji w poufności.

Najważniejsza zmiana nie polega więc na zakazaniu AI. Polega na przejściu od niekontrolowanego korzystania z niej do korzystania świadomego i zarządzanego. W realiach 2026 r. to nie tylko kwestia cyberbezpieczeństwa czy compliance, lecz także istotny element skutecznej ochrony know-how i innych kluczowych aktywów informacyjnych przedsiębiorstwa.