

10 zasad stosowania AI przez pracowników

AI nie można pozostawić „samopas”. Rodzi ona fundamentalne wyzwania dot. bezpieczeństwa danych, czy ochrony własności intelektualnej i innych dóbr prawnie chronionych.

W poradniku zebraliśmy doświadczenia i spisaliśmy 10 zasad, które warto stosować.



Sławomir Paruch

radca prawny, partner

slawomir.paruch@pcslegal.pl



Klaudia Majkutewicz-Jędrzejak

prawnik

klaudia.majkutewicz-jedrzejak@pcslegal.pl



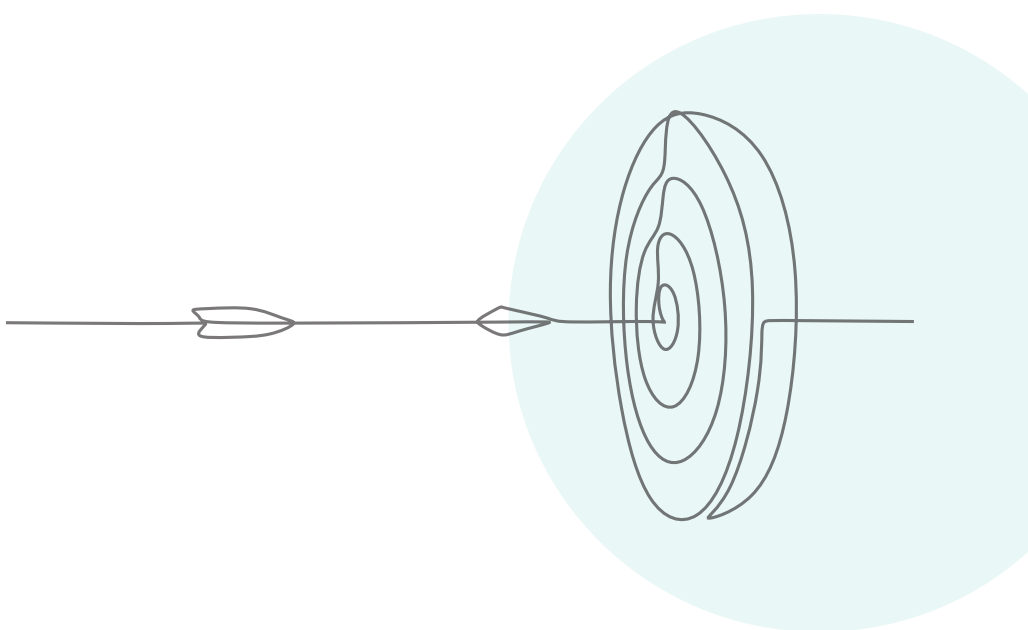
Informuj pracowników, czy i w jakim zakresie mogą korzystać z AI

Pracownicy powinni znać zasady co do możliwości i ograniczeń korzystania z narzędzi sztucznej inteligencji. Określenie zakresu, w jakim AI jest dopuszczalne, pozwala uniknąć przypadkowego naruszenia polityki firmy lub przepisów dotyczących ochrony danych. Należy jasno wskazać, do jakich zadań AI może być wykorzystywana, a kiedy korzystanie z niej jest dozwolone. Pracownicy powinni mieć także świadomość odpowiedzialności związanej z przetwarzaniem danych.



Ogranicz liczbę narzędzi AI do tych przydatnych

Wybór tylko najważniejszych i sprawdzonych aplikacji pozwala na lepsze monitorowanie ich użycia oraz kontrolowanie dostępu do danych wrażliwych. Możliwie ułatwia także zarządzanie danymi - przy ograniczeniu liczby narzędzi znacznie łatwiej skupić się na ich efektywnym wdrażaniu oraz szkoleniu pracowników. Dzięki temu procesy w organizacji stają się bardziej przejrzyste i łatwiejsze do nadzorowania, a ryzyko związane z nieautoryzowanym dostępem do informacji możliwe ograniczone.



3 **Określ katalog informacji, które są ściśle poufne i nie mogą być przesyłane AI**

Kluczowe jest sprecyzowanie, które dane w organizacji mają charakter poufny i wrażliwy. Pracownicy powinni znać i rozumieć, jakie informacje nie mogą być udostępniane narzędziom AI, aby uniknąć przypadkowego wycieku danych. Wprowadzenie wytycznych minimalizuje ryzyko nieautoryzowanego ujawnienia informacji, które mogłyby narazić spółkę na negatywne konsekwencje. Tworzenie katalogu danych poufnych przyda się także przy wprowadzaniu zabezpieczeń technicznych ograniczających dostęp AI do wewnętrznych baz danych.



4 Weryfikuj źródła, z których pozyskiwane są informacje dostarczane przez AI

Przed użyciem danych uzyskanych z pomocą AI w decyzjach biznesowych, warto sprawdzić ich pochodzenie.

Niezweryfikowane informacje mogą prowadzić do błędnych konkluzji, co może się odbić negatywnie na spółce.

Wprowadzenie polityki weryfikacji źródeł zmniejsza ryzyko operowania z użyciem informacji fałszywych lub niepełnych.



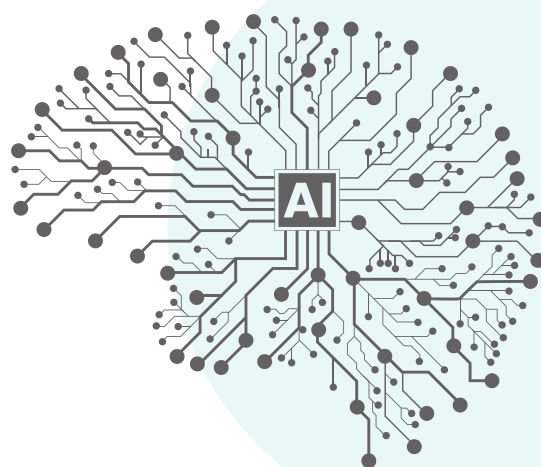
5 Dokładnie sprawdzaj cytaty i sentencje przytaczane przez sztuczną inteligencję

Treści generowane przez AI mogą zawierać informacje nieprecyzyjne lub nieprawdziwe - cytaty sugerowane przez sztuczną inteligencję mogą być źle zinterpretowane lub wyrwane z kontekstu. Użytkownicy AI powinni odpowiedzialnie sprawdzać wyniki wyszukiwania, by maksymalnie zminimalizować ewentualne ryzyko błędu.



6 Informuj klientów, jakie usługi są wytworem AI, a które są „made by human”

Przejrzystość w zakresie użycia sztucznej inteligencji w produktach i usługach zwiększa zaufanie klientów, dlatego powinni oni wiedzieć, czy mają do czynienia z usługą świadczoną przez ludzi, czy wspieraną przez technologię. Takie rozróżnienie pomaga w odpowiednim zarządzaniu oczekiwaniami (szczególnie w sytuacjach, gdzie interakcja międzyludzka jest kluczowa). Transparentność to podstawa budowania pozytywnego wizerunku spółki na rynku.



7 | **Stwórz politykę bezpiecznego korzystania z możliwości, jakie daje AI**

Zasady bezpiecznego korzystania z AI powinny być szczegółowo opisane i dostosowane do specyfiki działalności firmy. Taka polityka pomoże pracownikom zrozumieć potencjalne ryzyka i sposoby ich minimalizacji, zapewniając bezpieczeństwo danych oraz ciągłość procesów. Przemyślane zasady bezpieczeństwa mogą obejmować między innymi kontrolę dostępu do narzędzi AI, procedury postępowania w razie naruszenia danych oraz wytyczne dotyczące ochrony informacji poufnych.



Zaplanuj szkolenia dla pracowników, by podnieść poziom świadomości w zakresie ryzyka związanego z upublicznieniem danych szczególnie wrażliwych

Edukacja pracowników w zakresie ochrony danych to kluczowy element strategii zarządzania ryzykiem w organizacji. Szkolenia mają na celu pomóc zrozumieć, jakie konsekwencje mogą mieć nieświadome działania prowadzące do ujawnienia danych.

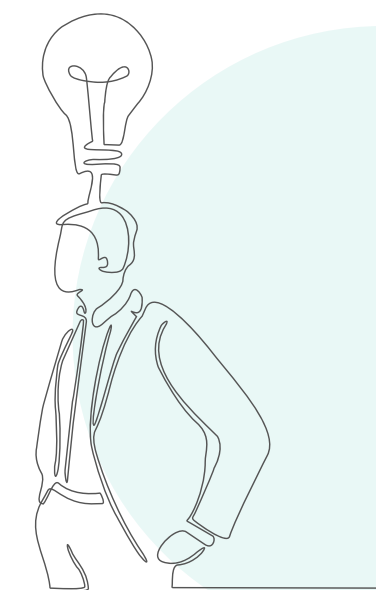
Pracownicy powinni wiedzieć, jakie informacje są szczególnie wrażliwe oraz jakich praktyk należy unikać, by je chronić.

Regularne poszerzanie wiedzy pozwala również pozostać na bieżąco z nowymi zagrożeniami oraz najlepszymi praktykami rynkowymi w obrębie ochrony danych.



Bądź elastyczny w zakresie zmian i na bieżąco wprowadzaj i aktualizuj regulaminy i polityki obowiązujące w firmie

Chcąc być na bieżąco trzeba być elastycznym - regularne przeglądy i aktualizacje polityk zapewniają, że firma pozostaje zgodna z najnowszymi standardami i obowiązującym prawem. Proaktywne dostosowanie regulaminów do zmieniających się warunków rynkowych i technologicznych zwiększa także poziom bezpieczeństwa spółki.



Sprawdzaj, w jakim zakresie i na jakich zasadach kontrahenci świadczący usługi wykorzystują AI, w tym Twoje dane

Współpracując z zewnętrznymi podmiotami należy mieć pełną świadomość w zakresie bezpieczeństwa i polityki prywatności stosowanej przez kontrahentów - zwłaszcza w przypadku wykorzystania AI. Bycie transparentnym pozwala także na ocenę potencjalnych ryzyk związanych z daną współpracą.



O kancelarii

PCS Paruch Chruściel Schiffter Stępień Kanclerz specjalizuje się we wszystkich kwestiach prawa HR dot. zatrudnienia, w tym zatrudnienia i zwolnień, *global mobility & immigration*, wynagrodzeń i premii, compliance, ZFŚS, ZUS, sporów sądowych, restrukturyzacji, zasad motywacyjnych i lojalnościowych, czasu pracy, programów emerytalnych, PPK, PPE, danych osobowych.

Zespół PCS tworzy obecnie grono 130 doświadczonych prawników, konsultantów oraz wsparcia administracyjnego. Pracujemy w 6 biurach: Warszawa, Kraków, Katowice, Poznań, Wrocław oraz Gdańsk.

PCS Paruch Chruściel Schiffter Stępień Kanclerz niezależny lider w branży HR legal w Polsce oraz na świecie, w szczególności w regionie CEE. Dostarczamy Klientom pragmatyczne rozwiązania na miarę ich potrzeb.



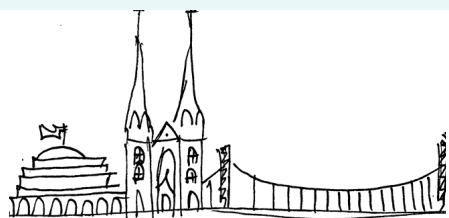
WARSZAWA, 00-073
pl. Piłsudskiego 2
T: +48 22 551 50 01



KATOWICE, 40-043
Podchorążych 1
T: +48 604 906 364



POZNAŃ, 60-234
Niegolewskich 12/8
T: +48 502 411 397



WROCŁAW, 50-069
Ofiar Oświęcimskich 17
T: +48 510 043 397



KRAKÓW, 31-547
Mosiężnicza 3
T: +48 665 250 666



GDAŃSK, 80-822
Żabi Kruk 16 lok. 1/10a
T: +48 502 487 699