IPSOLegal

CHECKLISTA ZGODNOŚCI Z AI ACT

Dostosowanie firmy do przepisów AI Act to proces wymagający kompleksowej analizy ryzyka oraz wdrożenia odpowiednich procedur zgodności. Nowe przepisy nakładają na firmy obowiązki dostosowane do poziomu ryzyka związanego z danym systemem AI, od zakazu stosowania niektórych praktyk po spełnienie określonych wymogów dla systemów wysokiego ryzyka.

ZIDENTYFIKUJ SYSTEMY AI I OKREŚL KLASĘ RYZYKA

Przeanalizuj wszystkie systemy AI używane w Twojej firmie, aby ustalić, które z nich podlegają regulacjom AI Act.

Określ poziom ryzyka każdego systemu AI, biorąc pod uwagę jego wpływ na zdrowie, bezpieczeństwo i prawa użytkowników. Systemy AI są klasyfikowane jako:

- Zakazane: systemy stwarzające niedopuszczalne ryzyko, takie jak manipulacyjne AI czy scoring społeczny.
- Wysokiego ryzyka: systemy wpływające na istotne obszary życia, np. zdrowie, edukację czy egzekwowanie prawa.
- Ograniczonego ryzyka: systemy wymagające pewnych obowiązków w zakresie przejrzystości, np. chatboty.
- Minimalnego ryzyka: systemy niewymagające dodatkowych obowiązków, np. filtry spamu.

PRZEANALIZUJ WPŁYW AI NA UŻYTKOWNIKÓW I PACJENTÓW

Oceń, w jaki sposób każdy system AI oddziałuje na użytkowników końcowych, takich jak klienci czy pracownicy.

Upewnij się, że użytkownicy są świadomi interakcji z systemem AI i rozumieją jego działanie oraz ograniczenia.

Kluczowe pytania to:

- Czy użytkownik jest świadomy korzystania z AI?
- Czy system działa autonomicznie, czy wymaga nadzoru ludzkiego?
- Czy decyzje AI mogą wpływać na proces diagnostyczny?

ZAPEWNIJ PRZEJRZYSTOŚCI SYSTEMÓW AI

- udostępnij jasne informacje o tym, że użytkownik wchodzi w interakcję z systemem AI.
- stwórz dokumentację wyjaśniającą, jak działa system AI, jakie dane przetwarza i w jaki sposób podejmuje decyzje.

Firmy muszą zapewnić użytkownikom możliwość zrozumienia, jak działa AI i na jakiej podstawie podejmuje decyzje. Konieczne jest udostępnienie czytelnej dokumentacji dla profesjonalistów oraz informowanie pacjentów, gdy mają do czynienia z AI, na przykład w przypadku chatbotów zdrowotnych.

STWÓRZ MECHANIZMY NADZORU LUDZKIEGO NAD AI

Systemy AI wysokiego ryzyka nie mogą działać w pełni autonomicznie. AI Act wymaga, aby człowiek miał możliwość interwencji i korygowania decyzji AI. Dlatego:

- wyznacz odpowiedzialne osoby do monitorowania działania systemów AI.
- Zapewnij możliwość interwencji człowieka w przypadku błędnych lub niepożądanych decyzji podejmowanych przez AI.

CHROŃ DANE OSOBOWE I ZADBAJ O CYBERBEZPIECZEŃSTWO

- upewnij się, że systemy AI przetwarzają dane zgodnie z RODO oraz innymi obowiązującymi przepisami o ochronie danych.
- podejmij odpowiednie środki bezpieczeństwa, takie jak anonimizacja, szyfrowanie danych oraz regularne audyty bezpieczeństwa.

AI Act wymaga, aby systemy AI przetwarzające dane osobowe były zgodne z RODO. Firmy muszą zaimplementować mechanizmy anonimizacji i szyfrowania danych oraz monitorować systemy pod kątem wycieków i naruszeń bezpieczeństwa. Użytkownicy są też zobowiązani do oceny skutków dla ochrony danych (DPIA).

PROWADŹ KONIECZNĄ DOKUMENTACJĘ I RAPORTUJ

- sporządź i aktualizuj dokumentację techniczną dla każdego systemu AI, zawierającą informacje o jego działaniu, celach oraz procedurach zgodności.
- monitoruj i raportuj wszelkie incydenty oraz niezgodności związane z działaniem systemów AI do odpowiednich organów nadzoru.

Dokumentacja powinna obejmować opis funkcjonalności, algorytmów, zastosowań systemu oraz raporty zgodności z AI Act, takie jak audyty, testy jakości i oceny ryzyka.

OPRACUJ PLANY AWARYJNE I ZARZĄDZAJ RYZYKIEM

- stwórz procedury postępowania na wypadek awarii systemu AI lub wykrycia jego nieprawidłowego działania.
- regularnie oceniaj ryzyka związane z wykorzystaniem AI i aktualizuj plany awaryjne oraz strategie minimalizacji potencjalnych zagrożeń.

Wdrożenie systemów zarządzania ryzykiem pozwoli na skuteczną interwencję w sytuacjach awaryjnych.