AITRUST · ZASADA, MECHANIZM, PRZYKŁAD DZIAŁANIA I ZAKRES KONTROLI

Mapa polityk i kontroli AiTrust

AiTrust umożliwia przełożenie polityk na mechanizmy techniczne, które w skonfigurowanych procesach kontrolują działania AI, egzekwują określone ograniczenia i rejestrują wyniki kontroli. Przy każdym z sześciu obszarów, które sprawdza też ocena gotowości, widzisz, co ustala polityka bazowa i który mechanizm ją egzekwuje.

Polityki bazowe i bazowa konfiguracja kontroli są minimum organizacyjnym i technicznym na start. Nie oznaczają automatycznie spełnienia wszystkich wymagań prawnych Twojego sektora. Zgodność z AI Act ocenia się dla konkretnego zastosowania.

OBSZAR POLITYKI

AI. Dopuszczalne wykorzystanie AI i rejestr zastosowań

ZASADA POLITYKI BAZOWEJ

Które narzędzia i modele są dozwolone i do czego służą.

MECHANIZM AITRUST

Model przypisany do cyfrowego pracownika AI, działu i etapu. Nowy model przechodzi weryfikację przed użyciem.

DOMYŚLNIE W AITRUST (MODEL DOPASOWANY DO ETAPU PROCESU)

Model jest przypisany do cyfrowego pracownika AI, działu i etapu. Nowy model przechodzi weryfikację przed użyciem.

ORGANIZACJA USTALA

Dla każdego etapu pracy organizacja ustala model, dane, narzędzia i wymagane akceptacje.

Dostawca Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

OBSZAR POLITYKI

Dane. Klasyfikacja danych i ochrona informacji

ZASADA POLITYKI BAZOWEJ

Jakie dane mogą trafić do modelu i w jakiej postaci.

MECHANIZM AITRUST

Kontrola przed wysłaniem do modelu, maskowanie danych w zapytaniach i uprawnienia do dokumentów.

DOMYŚLNIE W AITRUST (MASKOWANIE DANYCH W ZAPYTANIACH)

Model otrzymuje kontekst po sanityzacji wskazanych kategorii danych, a wykryte identyfikatory są zastępowane znacznikami. Wzorce wbudowane działają po stronie serwera, bez AI, i nie maskują imion i nazwisk, adresów ani terminów medycznych.

ORGANIZACJA USTALA

Organizacja ustala własne reguły i zakres wykrywania w konfiguracji. Maskowanie nie jest nieodwracalną anonimizacją.

OBSZAR POLITYKI

Wiedza. Źródła wiedzy i wiarygodność informacji

ZASADA POLITYKI BAZOWEJ

Z jakich źródeł korzysta AI i jak ocenia się odpowiedź.

MECHANIZM AITRUST

Wybrane źródła organizacji i wskazywanie źródeł użytych w odpowiedzi, w zakresie obsługiwanym przez konfigurację.

DOMYŚLNIE W AITRUST (ŹRÓDŁA I SPOSÓB OCENY ODPOWIEDZI)

Polityka bazowa obszaru Wiedza wskazuje źródła organizacji, a odpowiedź może wskazywać użyte źródła w zakresie obsługiwanym przez konfigurację. Przed wyświetleniem odpowiedź przechodzi kontrolę.

ORGANIZACJA USTALA

Organizacja ustala, jakie źródła i jaki sposób oceny wyniku są wymagane w danym procesie.

Dostawca Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

OBSZAR POLITYKI

Decyzje. Walidacja wyników i zasady akceptacji

ZASADA POLITYKI BAZOWEJ

Kiedy wynik AI wymaga przeglądu i zatwierdzenia człowieka.

MECHANIZM AITRUST

Operacje wskazanych klas wymagają decyzji człowieka przed wykonaniem.

DOMYŚLNIE W AITRUST (DECYZJA CZŁOWIEKA W PROCESIE)

W profilu standardowym operacja w strefie C czeka na zatwierdzenie osoby uprawnionej innej niż wnioskujący, a w strefie D wysyłka jest wstrzymana.

ORGANIZACJA USTALA

Organizacja ustala w procesie, gdzie wymagana jest decyzja człowieka, i odróżnia zgodę na działanie od zatwierdzenia treści konkretnej wersji dokumentu.

OBSZAR POLITYKI

Agenci. Uprawnienia i autonomia cyfrowych pracowników AI

ZASADA POLITYKI BAZOWEJ

Z jakich narzędzi korzysta cyfrowy pracownik AI i co może zrobić bez zgody człowieka.

MECHANIZM AITRUST

Paszport agenta z progiem zatwierdzenia, limitami operacji i kosztu oraz grantami do narzędzi. Na jego podstawie działa cyfrowy pracownik AI, a paszport można zawiesić lub odwołać.

DOMYŚLNIE W AITRUST (DZIAŁANIA CYFROWYCH PRACOWNIKÓW AI)

Cyfrowy pracownik AI bez aktywnego paszportu nie użyje narzędzi, a z narzędzia korzysta tylko na podstawie grantu.

ORGANIZACJA USTALA

Organizacja ustala, które działania cyfrowego pracownika AI mogą zostać wykonane samodzielnie, a które wymagają decyzji uprawnionej osoby.

Dostawca Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

OBSZAR POLITYKI

Człowiek. Nadzór, odpowiedzialność i reakcja na incydenty

ZASADA POLITYKI BAZOWEJ

Kto zatwierdza, kto reaguje i jak dokumentuje się decyzje.

MECHANIZM AITRUST

Zapis zdarzeń i decyzji w kontrolowanej ścieżce. Zakres zapisu i czas jego przechowywania ustala organizacja.

DOMYŚLNIE W AITRUST (ZAPIS ZDARZEŃ I DECYZJI)

Przy odpowiedzi powstaje raport wysyłki AI ze strefą, decyzją i liczbą redakcji, a kolejne etapy przebiegu zostawiają zapis.

ORGANIZACJA USTALA

Zakres zapisu zdarzeń i decyzji oraz czas jego przechowywania ustala się dla konfiguracji i objętej nim ścieżki.

Zakres działania każdego mechanizmu ustalasz w konfiguracji dla swoich procesów.

Przykład. Dane klienta w zleceniu dla AI

ELEMENT	W PRZYKŁADZIE
Polityka	Dane kontaktowe klientów nie trafiają do zewnętrznego modelu bez kontroli.
Mechanizm AiTrust	Przed wysłaniem AiTrust pokazuje, co zobaczyłby model. Wykryte identyfikatory są zastąpione znacznikami, a człowiek wybiera, czy anulować, poprawić, czy wysłać ograniczoną wersję.
Dowód	Raport wysyłki AI przy wyniku zapisuje strefę, decyzję i liczbę redakcji.

Przebieg nagrany w AiTrust na danych syntetycznych pokazuje zachowanie interfejsu w tym przykładzie i konfiguracji. Zakres kontroli w innych procesach zależy od wdrożenia.

Zakres kontroli

AiTrust egzekwuje skonfigurowane zasady w procesach i kanałach objętych działaniem jego mechanizmów. Nie blokuje automatycznie pracownika, który korzysta z prywatnego konta w innym narzędziu AI. Do tego służą kontrole na urządzeniach i w sieci organizacji.

Dostawca Polski Instytut AI Sp. z o.o. · ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa · biuro@aiinstytut.pl · +48 22 295 12 14 · KRS 0001201352 · NIP 7011283123 · REGON 543051706

Mapa opisuje mechanizmy produktu i ich ustawienia domyślne. Nie jest certyfikacją ani deklaracją zgodności z AI Act, RODO czy normami ISO. Zgodność ocenia się dla konkretnego zastosowania w organizacji.

Metryka

METRYKA DOKUMENTU

Mapa polityk i kontroli AiTrust

WERSJA I DATA

1.0 · 08.11.2026

WYDAWCA I DOSTAWCA AITRUST

Polski Instytut AI Sp. z o.o., ul. Nowogrodzka 50/54 lok. 515, 00-695 Warszawa

KONTAKT

biuro@aiinstytut.pl · +48 22 295 12 14

DANE REJESTROWE

KRS 0001201352 · NIP 7011283123 · REGON 543051706

ŹRÓDŁO TREŚCI

Strony www.aitrust.pl/polityki-ai i /platforma (odpowiedzi „Domyślnie w AiTrust” i „Organizacja ustala”) w dniu wydania.

CHARAKTER DOKUMENTU

Materiał informacyjny. Nie stanowi porady prawnej. Warunki współpracy określa indywidualna oferta.