

Pojęcia AI governance po ludzku

19 najważniejszych terminów z AI Act, RODO, norm ISO i bezpieczeństwa — wyjaśnionych prostym językiem, w kolejności alfabetycznej.

A

AI Act

Unijne rozporządzenie regulujące sztuczną inteligencję. Dzieli systemy AI na kategorie ryzyka (od minimalnego do niedopuszczalnego) i nakłada obowiązki zależne od poziomu ryzyka.

AIMS (AI Management System)

System zarządzania sztuczną inteligencją w organizacji, zgodny z normą ISO/IEC 42001. Obejmuje procesy, role i procedury nadzoru nad AI.

AISO

Zwykle skrót od AI Security Officer (osoba odpowiedzialna za bezpieczeństwo systemów AI w organizacji). Znaczenie może się różnić w zależności od firmy.

AISO Retainer

Umowa abonamentowa (retainer), w ramach której firma płaci stałą opłatę za regularny dostęp do usług/doradztwa specjalisty AISO, zamiast płacić za pojedyncze zlecenia.

B

BAA (Business Associate Agreement)

Umowa wymagana w USA (przepisy HIPAA), zawierana gdy firma przetwarza dane medyczne pacjentów w imieniu innej organizacji.

D

DPA (Data Processing Agreement)

Umowa powierzenia przetwarzania danych. Zawierana między administratorem danych a podmiotem, który te dane przetwarza w jego imieniu (np. dostawcą chmury). Wymagana przez RODO.

E

EDPB (European Data Protection Board)

Europejska Rada Ochrony Danych. Organ unijny zrzeszający krajowe organy ochrony danych, wydający wytyczne dotyczące stosowania RODO w całej UE.

G

GPAI (General Purpose AI)

Model sztucznej inteligencji ogólnego przeznaczenia. Termin z unijnego AI Act, oznaczający modele (np. duże modele językowe), które można wykorzystać do wielu różnych zastosowań, a nie tylko jednego konkretnego celu. Dostawcy GPAI mają dodatkowe obowiązki (np. dokumentacja techniczna, transparentność), a modele o szczególnie dużej mocy obliczeniowej podlegają jeszcze surowszym wymogom (tzw. "systemic risk").

I

ISO/IEC 42001

Międzynarodowa norma określająca wymagania dla systemu zarządzania sztuczną inteligencją (AIMS) w organizacji. Pomaga wdrożyć AI w sposób odpowiedzialny i kontrolowany.

ISO27001

Międzynarodowa norma dotycząca systemu zarządzania bezpieczeństwem informacji. Określa, jak firma powinna chronić dane przed wyciekiem, utratą czy nieautoryzowanym dostępem.

K

Kontrole z Aneksu A

Lista konkretnych zabezpieczeń/działań (kontroli) w normie ISO, które organizacja może wdrożyć, żeby spełnić wymagania normy. W ISO/IEC 42001 dotyczy zarządzania ryzykiem AI, przejrzystości i nadzoru nad systemami.

N

NIST AI RMF

Amerykański framework (Ramy Zarządzania Ryzykiem AI) opracowany przez NIST. Pomaga organizacjom identyfikować i zarządzać ryzykiem związanym z systemami AI. Ma charakter dobrowolny, nie jest prawem. Opiera się na 4 filarach:

- **Govern (Zarządzanie)** — Ustanowienie kultury organizacji, zasad nadzoru i polityki odpowiedzialności za AI.
- **Map (Mapowanie)** — Identyfikacja kontekstu, celów oraz potencjalnych ryzyk dla konkretnego systemu AI.
- **Measure (Pomiar)** — Ocena i kwantyfikacja zidentyfikowanych ryzyk za pomocą narzędzi technicznych i jakościowych.
- **Manage (Reagowanie)** — Wdrożenie planów mitygacji, alokacja zasobów i ciągły monitoring po wdrożeniu systemu.

P

Polska ustawa o systemach AI

Planowana polska ustawa wdrażająca unijny AI Act do krajowego porządku prawnego. Ma określać m.in. krajowy organ nadzoru i sankcje za naruszenia.

Prawo autorskie

Zbiór przepisów chroniących twórców utworów (tekstów, kodu, grafik itp.) przed nieuprawnionym kopiowaniem lub wykorzystaniem ich pracy.

R

RFP (Request for Proposal)

Zapytanie ofertowe. Dokument, w którym firma opisuje swoje potrzeby i prosi dostawców o złożenie oferty na usługę lub produkt.

RODO

Ogólne rozporządzenie o ochronie danych osobowych (unijne). Reguluje, jak firmy mogą zbierać, przechowywać i przetwarzać dane osobowe obywateli UE.

S

SIEM (Security Information and Event Management)

System informatyczny zbierający i analizujący logi bezpieczeństwa z całej infrastruktury firmy, żeby wykrywać podejrzaną aktywność i incydenty w czasie rzeczywistym.

SOC2

Amerykański standard audytu bezpieczeństwa dla firm świadczących usługi (np. SaaS). Sprawdza, czy firma odpowiednio chroni dane klientów pod kątem bezpieczeństwa, dostępności i poufności.

T

ToS (Terms of Service)

Regulamin usługi. Dokument określający zasady korzystania z produktu lub usługi, prawa i obowiązki użytkownika oraz dostawcy.