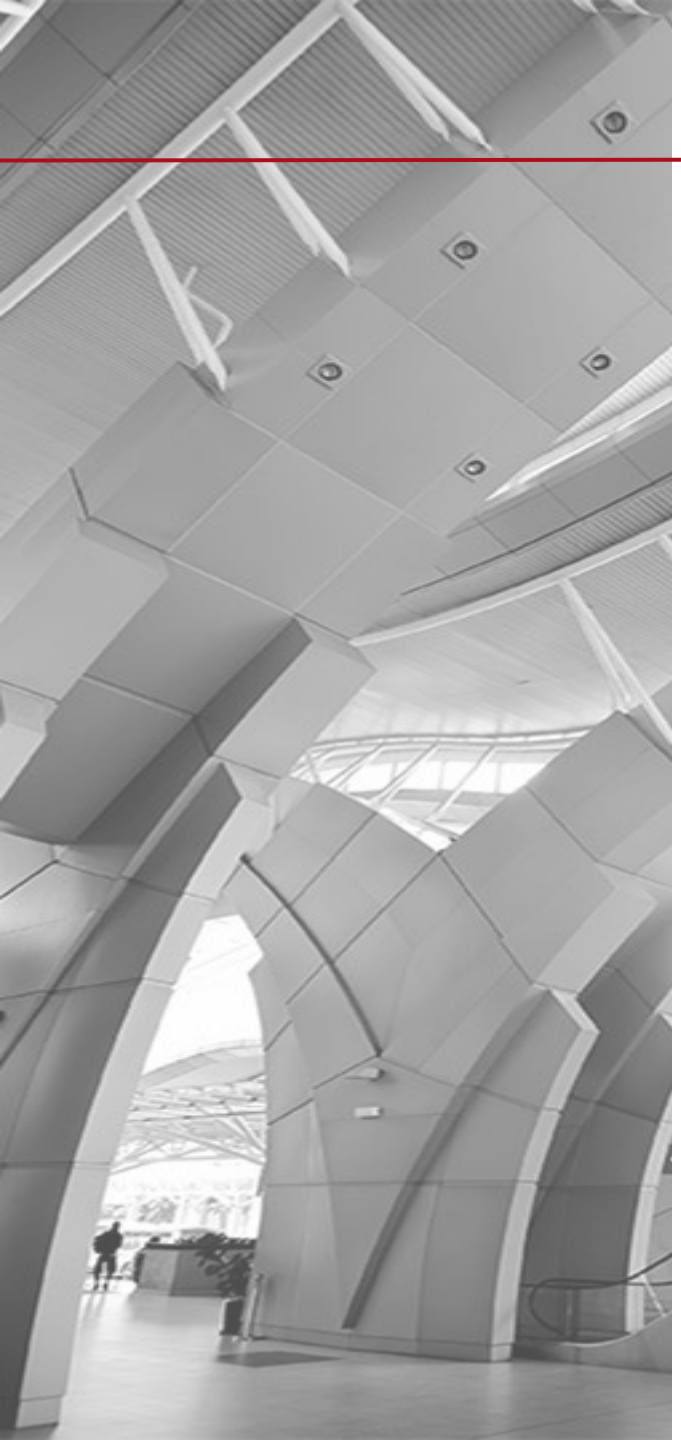
Sztuczna inteligencja w przetwarzaniu danych osobowych

Kompilacja wymogów RODO i AI Act

Ochrona danych osobowych w organizacji



Ochrona danych osobowych – prawo unijne i prawo krajowe

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) – **„RODO”.**
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2024 r. poz. 1513 z późn. zm.).
- Przepisy szczególne, np.:
  - Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124 z późn. zm.).
  - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2023 r. poz. 1465 z późn. zm.).
  - Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (t.j. Dz. U. z 2023 r. poz. 2383 z późn. zm.).
- **Wytyczne Grupy Roboczej art. 29/ EROD** w zakresie m.in.: przejrzystości, zgody, privacy by design i privacy by deflaut, oceny skutków dla ochrony danych osobowych, pojęcia administratora i podmiotu przetwarzającego.

ANDERSEN

RODO - cechy regulacji

Technologiczna neutralność

RODO nie określa sztywnego katalogu technologii/rozwiązań w zakresie ochrony danych osobowych. Administrator może swobodnie dobierać odpowiednie środki ochrony biorąc pod uwagę charakter, zakres, kontekst, cele i ryzyko przetwarzania danych osobowych.

Podejście oparte na ryzyku

Każdy podmiot samodzielnie ocenia ryzyko, jakie może spowodować przetwarzanie danych osobowych dla praw i wolności osób, których te dane dotyczą. Administrator powinien stosować takie środki bezpieczeństwa, które w danych okolicznościach przetwarzania minimalizują związane z nim ryzyko naruszenia praw i wolności.

Rozliczalność

Administrator jest zobowiązany zarówno do przestrzegania przepisów i wdrożenia odpowiednich środków ochrony danych, ale także do odpowiedniego udokumentowania podjętych działań i decyzji w sprawie wyboru określonych rozwiązań oraz do wykazania przestrzegania przepisów w razie kontroli (art. 5 ust. 2 RODO).

Wzmocnienie praw podmiotów danych

Osoby, których dane są przetwarzane mają większy dostęp do informacji w zakresie podejmowanych działań oraz większą kontrolę nad danymi dzięki uprawnieniom przewidzianym w art. 15-18 oraz 20-21.

ANDERSEN

Przedmiot i cele

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodny przepływ danych osobowych.

Wyważenie poszczególnych celów

Brak ograniczeń i zakazów swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.

WAŻNE! Podstawowym celem RODO jest zweryfikowanie jakie negatywne aspekty mogą być związane z przetwarzaniem danych osobowych jednostki, nie sama ochrona danych.

ANDERSEN

Zasięg przedmiotowy

- RODO ma zastosowanie do przetwarzania danych osobowych:
  - w sposób całkowicie lub częściowo **zautomatyzowany;** oraz
  - do przetwarzania **w sposób inny niż zautomatyzowany** danych osobowych **stanowiących część zbioru danych** lub **mających stanowić część zbioru danych**.
- **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- **Wyłączenia**:
  - w ramach działalności nieobjętej zakresem prawa Unii;
  - przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE (wspólna polityka zagraniczna i bezpieczeństwo);
  - przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym;
  - przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Bez znaczenia jest czy przetwarzane są dane publiczne czy niepubliczne. Nie ma też znaczenia czy przetwarzanie jest związane z prowadzeniem działalności gospodarczej lub nie.

Dane osobowe

Dane osobowe - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania **osobie fizycznej** („osobie, której dane dotyczą”)

możliwa do zidentyfikowania osoba fizyczna to osoba, którą można **bezpośrednio** (na podstawie danych, które ADO ma w swoich zasobach) lub **pośrednio** (dla celów identyfikacji ADO musi sięgnąć do zasobów innych podmiotów – jak daleko musi sięgać?) zidentyfikować

w szczególności **na podstawie identyfikatora** takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Pierwsze kroki wdrożenia RODO

Mapowanie procesów biznesowych

- Określona aktywność biznesowa/faktyczna stwarza ramy struktury Rejestru Czynności Przetwarzania (RCP).

Podział na czynności przetwarzania (RCP)

- Obowiązkiem ADO jest prowadzenie rejestru czynności przetwarzania danych osobowych (art. 30 RODO).

Ustalanie kontekstu przetwarzania

- Kontekst wewnętrzny/zewnętrzny.
- Odpowiedź na pytania kto dokonuje przetwarzania, jaki jest przepływ informacji, jakich narzędzi używa ADO, jaki jest łańcuch osób zaangażowanych w proces.

Weryfikacja wewnętrzna i zewnętrzna

- Jakie standardy bezpieczeństwa posiada ADO/podmiot, któremu ADO powierza przetwarzanie danych osobowych.

Przetwarzanie danych osobowych

Przetwarzanie danych osobowych oznacza **operację lub zestaw operacji** wykonywanych **na danych osobowych lub zestawach danych osobowych** w sposób **zautomatyzowany** lub **niezautomatyzowany**, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Operacje zautomatyzowane

Czynności przetwarzania wykonywane są automatycznie, a więc z wykorzystaniem urządzeń pozwalających na ograniczenie udziału człowieka w realizowaniu poszczególnych czynności, a zarazem przyspieszenie i poprawę efektywności procesów dokonywanych na danych (najczęściej komputerów).

Przykład: wykonywanie operacji na danych w bazie danych, tzn. programie komputerowym umożliwiającym dokonywanie różnego rodzaju działań na danych (np. wyszukiwania, sortowania itp.)

Operacje niezautomatyzowane

Przetwarzanie polega na wykonywaniu różnego rodzaju działań na danych metodami tradycyjnymi (ręcznie, manualnie) bez wykorzystywania do tego urządzeń, które ten proces automatyzują.

Przykład: wykonywanie czynności w odniesieniu do danych zapisanych w kartotece (np. wyszukiwanie, poprawianie itp.)

ANDERSEN

Administrator

Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

Obowiązki ADO (art. 24 RODO):

- Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, **administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać**. Środki te są w razie potrzeby poddawane **przeglądom** i **uaktualniane**.
- Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, ww. środki obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

- Środki techniczne
- Audyty wewnętrzne / zewnętrzne
- Polityka ochrony danych osobowych

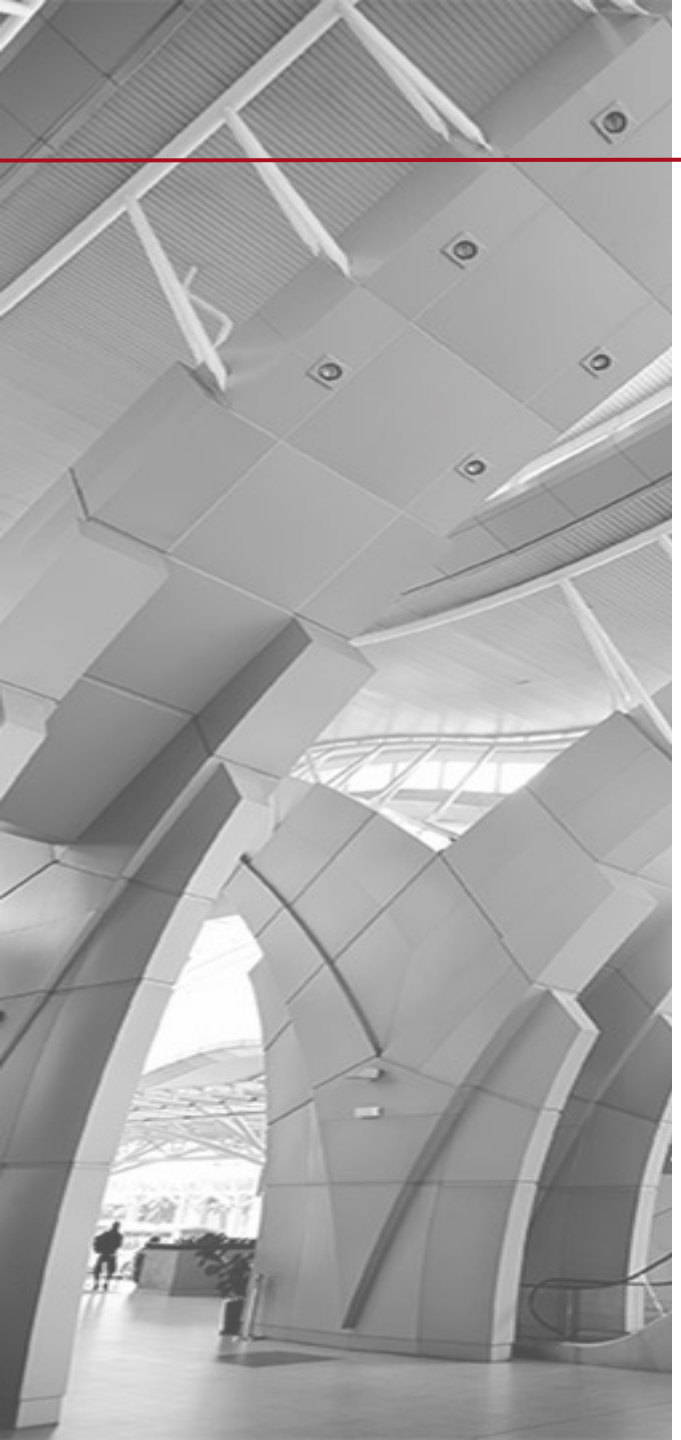
Obowiązki ADO w praktyce:

- Zgodność przetwarzania z zasadami RODO;
- Możliwość wykazania podstawy przetwarzania;
- Zapewnienie realizacji prawa podmiotów danych;
- Obowiązki ADO oparte na ryzyku;
- Powierzenie przetwarzania podmiotom trzecim;
- Transfer do państw trzecich wyłącznie z zachowaniem warunków określonych w RODO.

Ważne: Wszystkie ww. obowiązki mają charakter kontekstowy – muszą być ujęte w ramy tego w jaki sposób działa ADO, w jakich obszarach i w jakim zakresie danych.

ANDERSEN

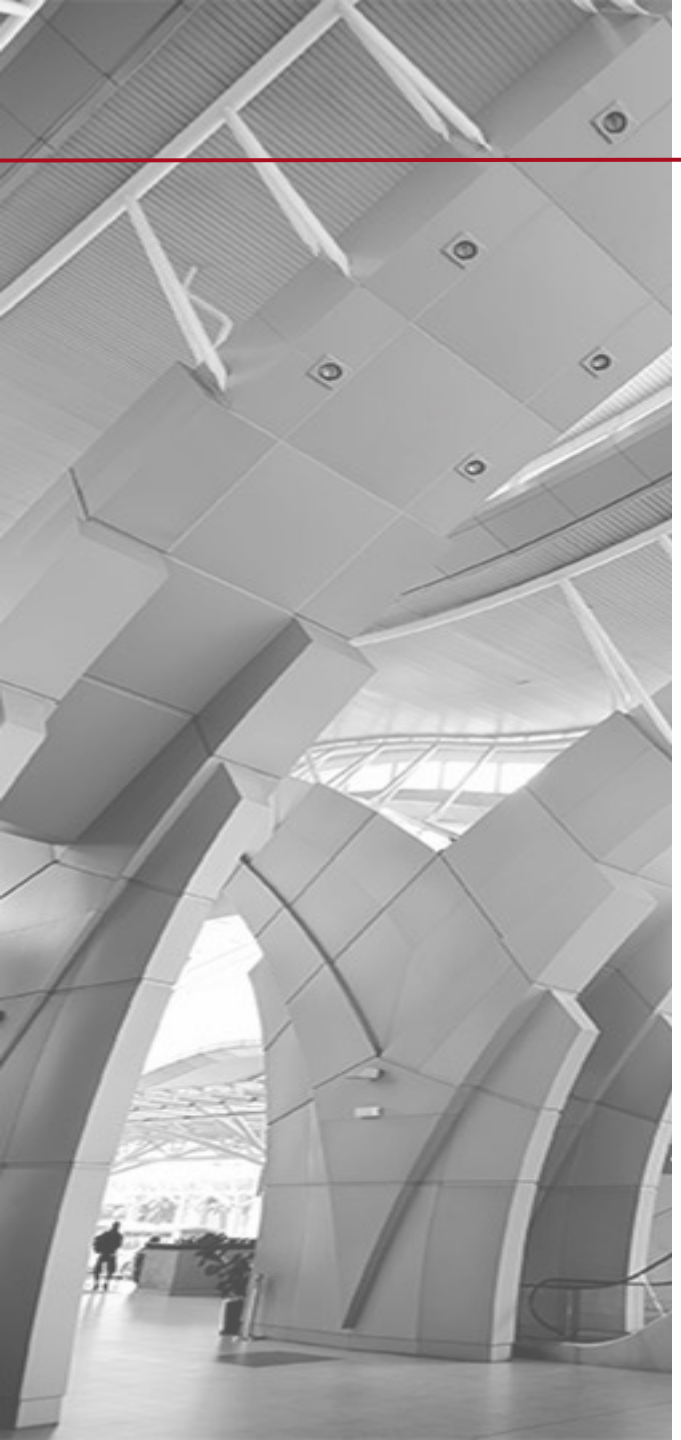
AI ACT



AI Act – ramy prawne 1/2

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 – **„AI Act”**
  - Określa jednolite zasady dotyczące wprowadzania na rynek, udostępniania i stosowania systemów sztucznej inteligencji w Unii Europejskiej.
  - Ma na celu wspieranie innowacji i wdrażania AI, jednocześnie zapewniając jednak wysoki poziom ochrony zdrowia, bezpieczeństwa, praw podstawowych oraz wartości demokratycznych i praworządności.
- **System sztucznej inteligencji** to oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję.
- **Podejście oparte na ryzyku (risk based approach)** - wpływ na bezpieczeństwo i prawa podstawowe użytkownika:
  - AI Act klasyfikuje systemy AI według poziomu ryzyka.
  - Niektóre praktyki AI uznane za nieakceptowalne i zakazane na mocy art. 5.

ANDERSEN



AI Act – ramy prawne 2/2

- **Od kiedy obowiązuje AI Act?**
  - wejście w życie - **1 sierpnia 2024 r.**
  - stosowanie dot. zakazów określonych praktyk (rozdziały I i II) – **2 lutego 2025 r.**
  - stosowanie dot. organów notyfikujących i jednostkach notyfikowanych w kontekście systemów AI wysokiego ryzyka (rozdział III sekcja 4), modeli AI ogólnego przeznaczenia (rozdział V), zarządzania (rozdział VII) kar (rozdział XII) i poufności (art. 78) – **2 sierpnia 2025 r.**
  - stosowanie w odniesieniu do systemów wysokiego ryzyka, określonych w art. 6 ust. 1 i odpowiadających mu obowiązków – **2 sierpnia 2027 r.**
  - zasadnicze stosowanie – **2 sierpnia 2026 r.**

ANDERSEN

Proces klasyfikacji systemów:

Zakres stosowania

Czy system wpływa na prawa, zdrowie lub bezpieczeństwo jednostek?

Konsekwencji użytkowania

Jakie mogą być skutki błędów lub nadużyć systemu?

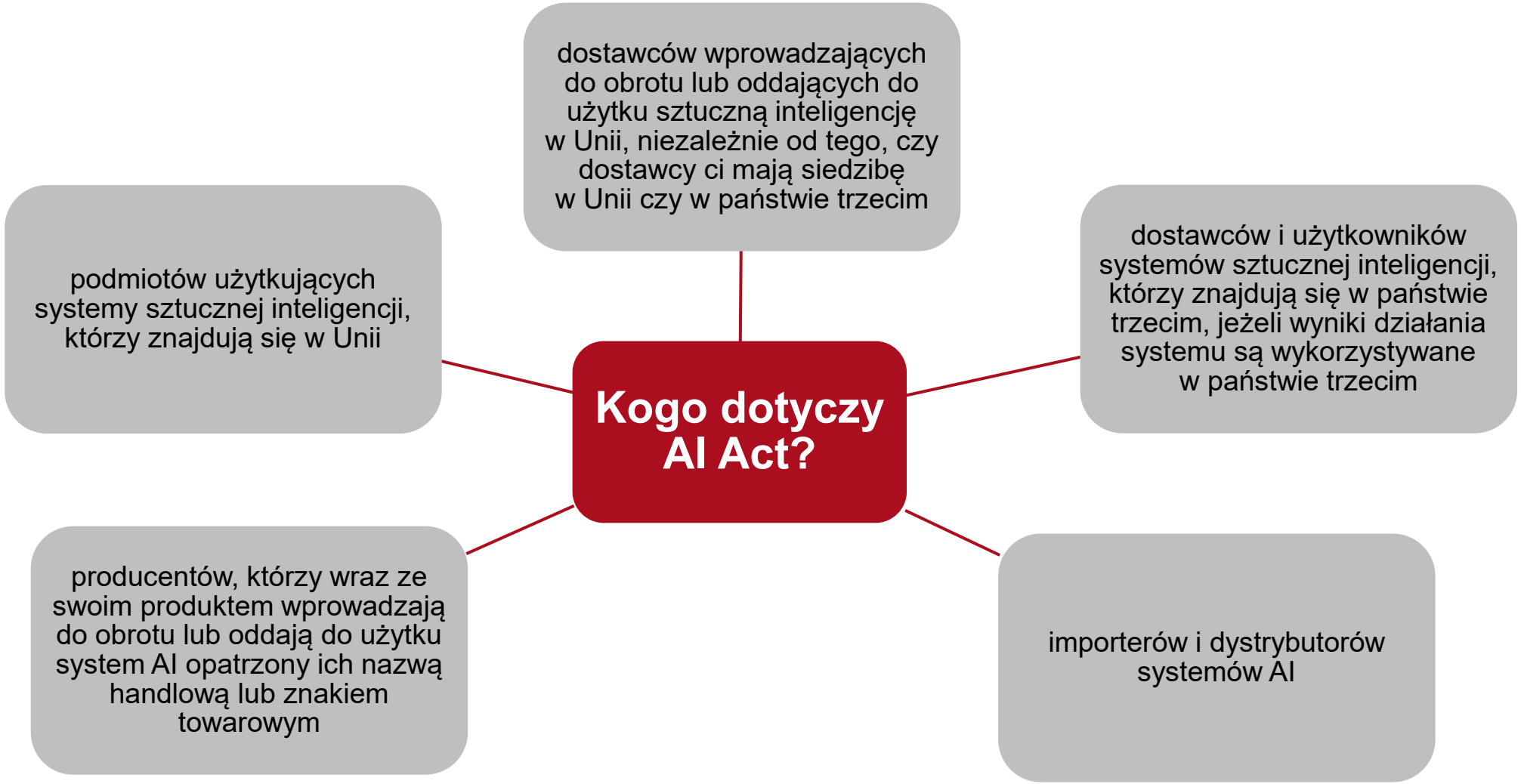
Sektora działania

AI stosowana w sektorach krytycznych, takich jak medycyna, transport czy prawo, zwykle kwalifikuje się jako wysokiego ryzyka.

Stopnia interakcji z człowiekiem

Czy system działa autonomicznie, czy wspiera człowieka?

Podmioty objęte AI Act



Systemy AI

Systemy zabronione (Unacceptable Risk)

- Systemy AI, które są uznane za nieakceptowalne z uwagi na naruszenie praw podstawowych i etyki.
- Systemy wykorzystujące **subliminalne techniki manipulacyjne** do zmiany zachowania w sposób szkodliwy.
- Systemy AI stosujące **ocenę społeczną** obywateli na podstawie ich zachowania lub cech osobistych (np. scoring społeczny przez władze publiczne).
- **Zdalna identyfikacja biometryczna w czasie rzeczywistym** w przestrzeni publicznej, z wyjątkiem niektórych sytuacji, jak poszukiwanie zaginionych dzieci czy zapobieganie terroryzmowi.

Systemy wysokiego ryzyka (High-Risk AI Systems)

- Systemy, które mogą mieć znaczący wpływ na prawa i bezpieczeństwo jednostek. Są dozwolone, ale muszą spełniać rygorystyczne wymogi regulacyjne.
- Obowiązek zgodności z wymaganiami dotyczącymi dokumentacji technicznej, zarządzania ryzykiem, nadzoru oraz monitorowania.
- Obowiązek certyfikacji - wymagana jest ocena zgodności przed wprowadzeniem na rynek.
- np. zatrudnienie i HR: AI używana do selekcji CV, oceny kandydatów czy podejmowania decyzji o zatrudnieniu.

Systemy ograniczonego ryzyka (Limited Risk)

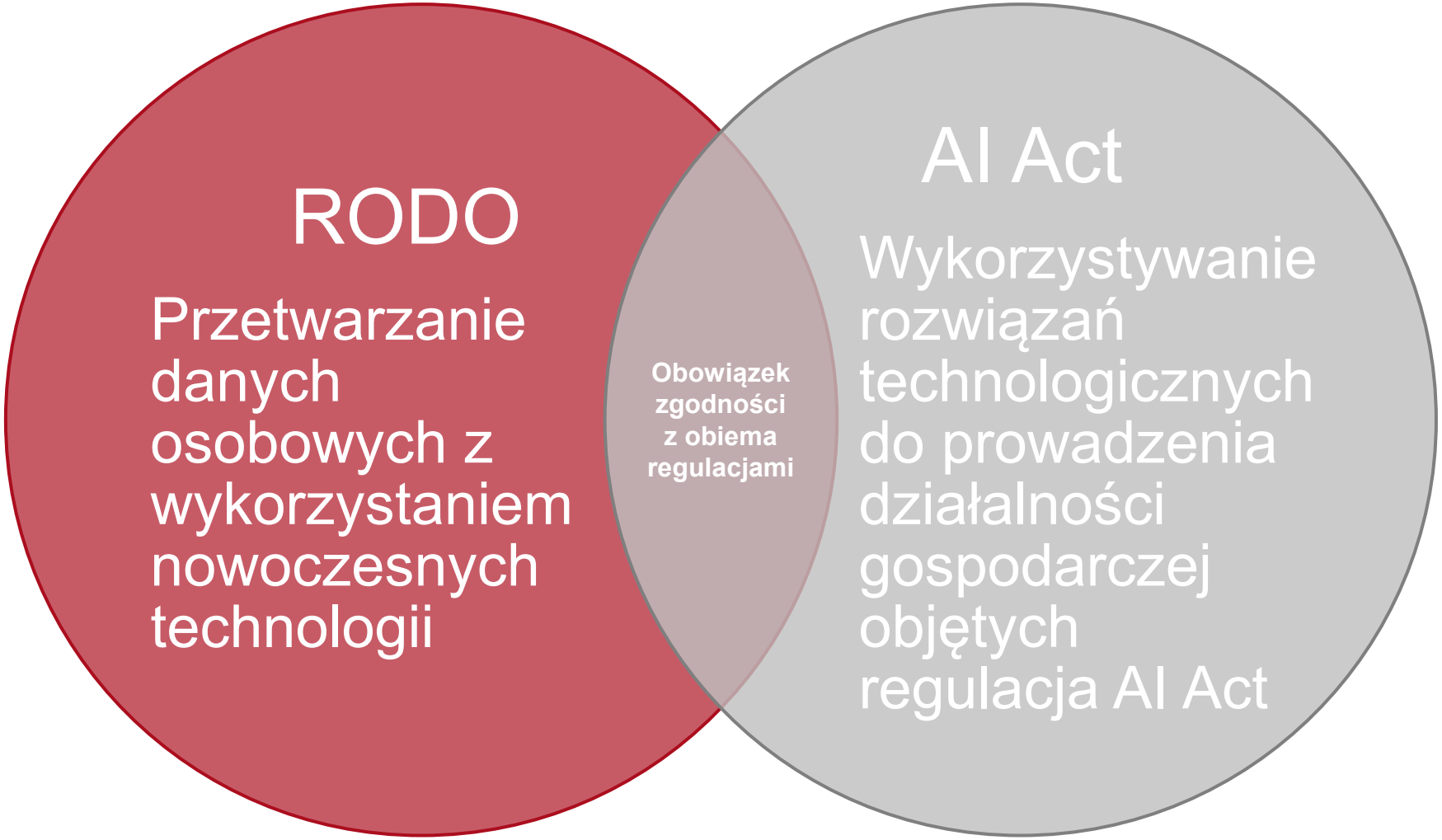
- Systemy, które niosą umiarkowane ryzyko, ale wymagają zapewnienia **transparentności** wobec użytkowników.
- obowiązek informowania użytkownika, że wchodzi w interakcję z systemem AI (np. chatbot musi ujawniać, że jest systemem AI).
- obowiązek oznaczania treści jako wygenerowane przez AI w przypadku systemów generujących treści (np. deepfake).

Systemy minimalnego ryzyka (Minimal Risk)

- Systemy AI, które nie stwarzają istotnego ryzyka dla użytkowników ani społeczeństwa.
- Dla tych systemów nie są nakładane żadne dodatkowe wymogi regulacyjne.

ANDERSEN

AI i RODO



ANDERSEN

Kontakt:

Andersen Tax & Legal Matyka i Wspólnicy Sp.k.

Biuro w Warszawie - ul. Puławska 2, 02-566 Warszawa

Biuro w Poznaniu - ul. Wodna 15/4, 61-782 Poznań

www.pl.andersen.com

Magdalena Kuczyńska
Telefon: + 48 571 270 080
E-mail: magdalena.kuczynska@pl.Andersen.com

Mikołaj Śniatała
Telefon: +48 603 106 949
E-mail: mikolaj.sniatala@pl.Andersen.com

ANDERSEN