WARMIŃSKI WSPÓLNICY

Generatywne systemy AI w organizacji - jak z nich korzystać zgodnie z RODO?

dr Iga Małobęcka-Szwast, LL.M.

radczyni prawna

Plan prezentacji

Czym jest generatywna sztuczna inteligencja (GenAI)?

Jakie zagrożenia z perspektywy ochrony danych osobowych mogą wiązać się z wykorzystaniem generatywnej AI w organizacji?

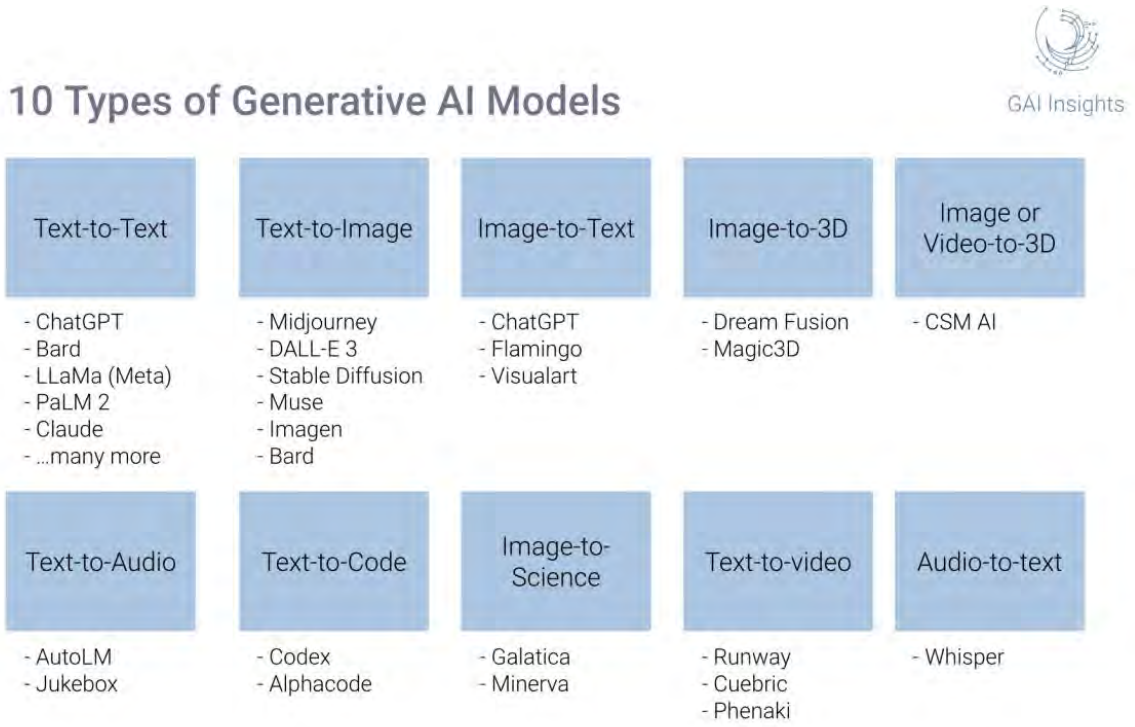
Jak zapobiegać takim zagrożeniom?

Co powinna zawierać polityka stosowania generatywnej AI w organizacji i czy warto ją mieć?

Jaka jest relacja między RODO a AI Act i czemu powinniśmy to wiedzieć?

Czym jest generatywna sztuczna inteligencja (GenAI)?

- **Generatywna sztuczna inteligencja (GenAI) – modele SI zaprojektowane do generowania nowych treści w postaci tekstu pisanego, dźwięku, obrazów lub filmów (...) na podstawie promptu dostarczonego przez użytkownika.**
- **Jakie to narzędzia?**
- **ChatGPT, Bard, Claude, GitHub Copilot, DALL-E, DeepL, Google Translate, Synthesia**
- **Gdzie możemy ją zastosować?**
- **Np. kontakt z klientami (wsparcie obsługi klienta); analiza i zarządzanie dokumentami; generowanie dokumentów/podsumowań/odpowiedzi itp.; zarządzanie wiedzą; tłumaczenia; podejmowanie decyzji/wspieranie procesu rekrutacyjnego (...).**



Zagrożenia związane z wykorzystaniem GenAI z perspektywy RODO

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

Microsoft's AI Data Leak Isn't the Last One We'll See

SEPTEMBER 29, 2023 | INFORMATION MANAGEMENT

NEWS

Questions raised as Amazon Q reportedly starts to hallucinate and leak confidential data

Generative AI data leaks are a serious problem, experts say

Source code, meeting notes, and even senior management comms are all being pasted into ChatGPT prompts.

Zagrożenia związane z wykorzystaniem GenAI z perspektywy RODO

Ujawnienie danych nieuprawnionej osobie trzeciej (naruszenie ochrony danych – naruszenie poufności)

Naruszenie zasady legalności - przetwarzanie danych bez podstawy prawnej (wpisanie promptów zawierających dane osobowe; przetwarzanie danych wyjściowych) → ZGODA/prawnie uzasadniony interes?

Halucynacje – zasada prawidłowości (art. 5 ust. 1 lit. e RODO)

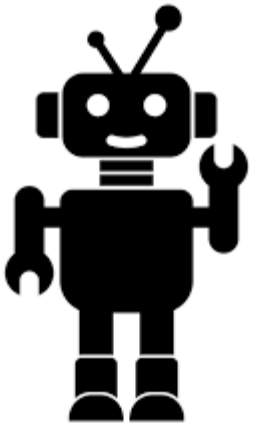
Naruszenie pozostałych zasad przetwarzania danych (zasada ograniczenia celu, minimalizacji...)

Naruszenie przepisów dot. obowiązku przeprowadzenia DPIA (w szczególności zob. art. 35 ust. 3 lit. a RODO)

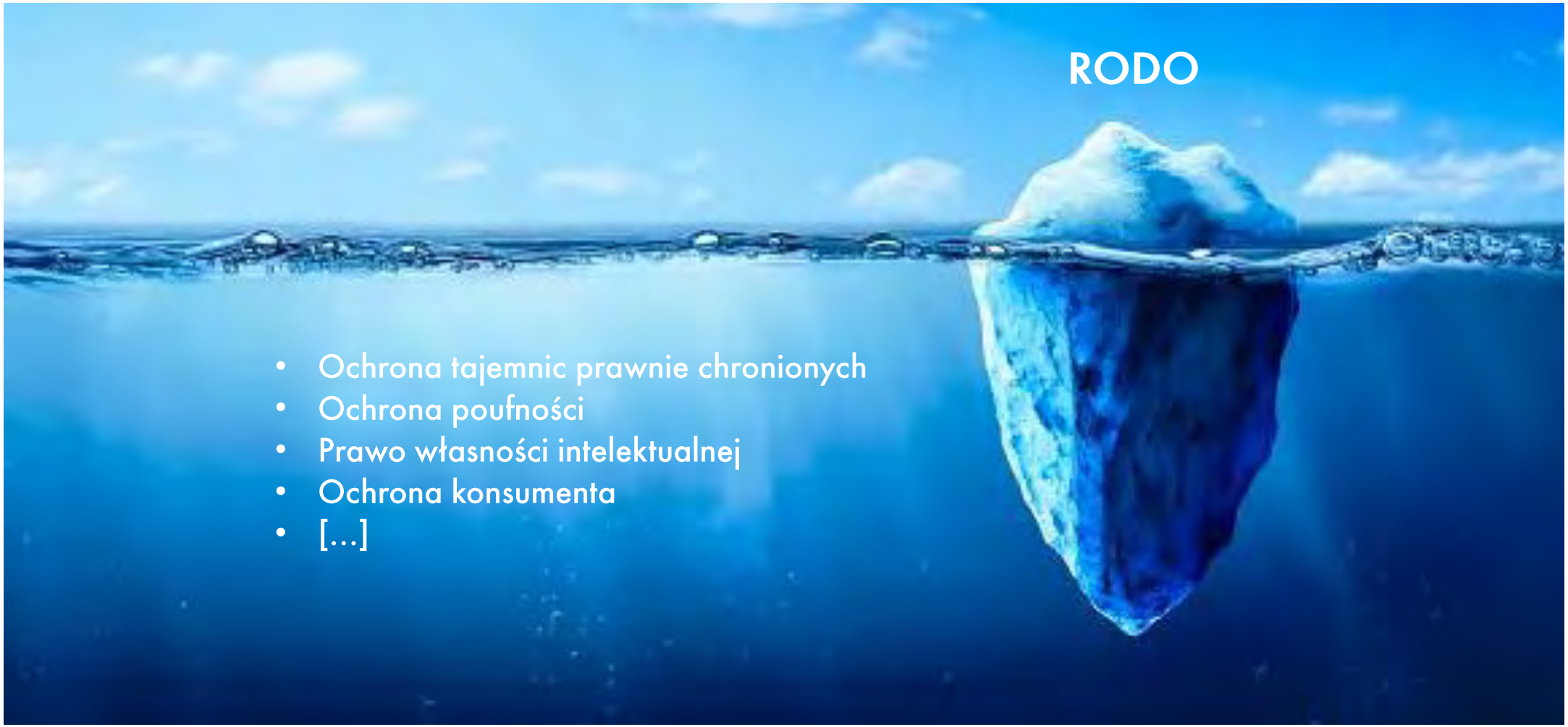
Naruszenie obowiązku informacyjnego (np. wykorzystanie danych w innych celach; przekazanie do innych odbiorców – dostawca narzędzia GenAI)

Naruszenie przepisów dot. transferu danych do państwa trzeciego

Naruszenie innych praw podmiotów danych (np. art. 22 RODO)



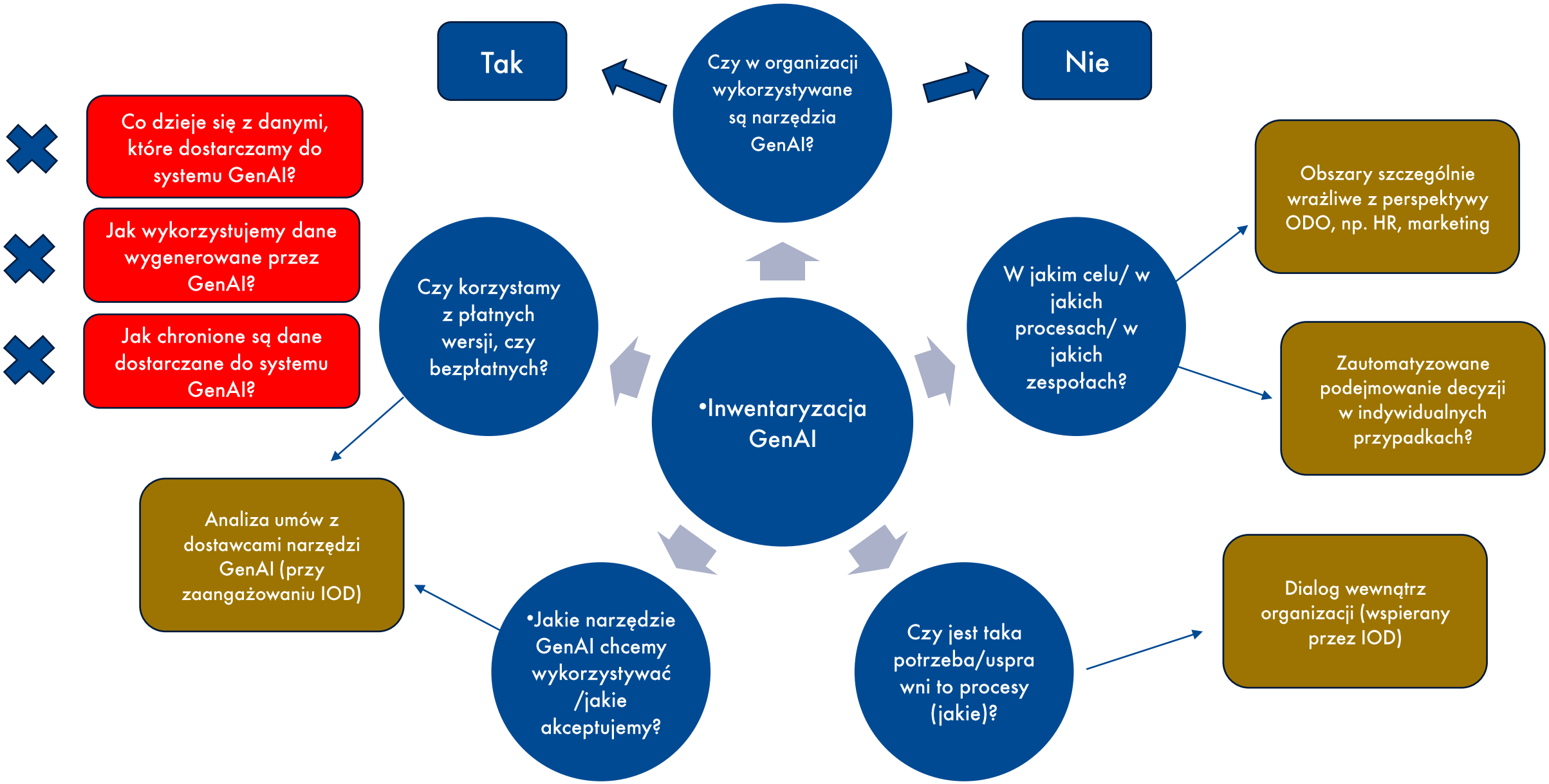
GenAI: RODO to wierzchołek góry lodowej



Jak zapobiegać takim zagrożeniom?

- Przegląd („inwentaryzacja”) narzędzi wykorzystywanych w organizacji
- Jeżeli organizacja chce dopuścić korzystanie z określonego narzędzia GenAI sprawdź umowy/regulaminy/polityki prywatności znajdujące zastosowanie do takich narzędzi (jak wykorzystywane są dane, które wprowadzane są do systemu – input data; jakie zabezpieczenia są stosowane)
- **Polityka wykorzystywania GenAI w organizacji** (jakie narzędzia są dozwolone, jakie nie; blokowanie korzystania z niektórych narzędzi; ścieżka wsparcia w razie wątpliwości)
- **„DPO in the loop”** - IOD powinien pełnić aktywną rolę w opracowywaniu polityki GenAI, ale też być punktem kontaktowym w ramach organizacji dla pracowników w sprawach na styku RODO i GenAI
- **Szkolenia z wykorzystania GenAI** dostosowane do organizacji (jak korzystać z GenAI zgodnie z RODO i innymi regulacjami, w tym tajemnicami itd.)
- **Monitorowanie zmian w tym obszarze** – śledź wytyczne organów nadzorczych, organów właściwych dla danego sektora (np. KNF)

„Inwentaryzacja" wykorzystywania GenAI w organizacji



Perspektywy: czy rzeczywiście nie chcemy GenAI w organizacji?

The World Ahead | Business in 2024

Generative AI will go mainstream in 2024

Data-savvy firms will benefit first

The Economist

Polityka stosowania generatywnej AI w organizacji

Jak zamierzasz zapewnić zgodność z RODO:

(i) podstawy prawne przetwarzania (zgoda);

(ii) transparentność w informowaniu o wykorzystaniu danych;

(iii) privacy-by-design i privacy-by-default;

(iv) halucynacje i zasada prawidłowości;

(v) zasady weryfikowania wygenerowanych treści, szczególnie jeżeli służą do podejmowania decyzji względem osób fizycznych (...);

DPO in the loop

[Dopuszczalne narzędzia GenAI] Jakie narzędzia GenAI są dozwolone? (blokowanie wykorzystywania określonych narzędzi)

[Osoby upoważnione do korzystania z GenAI] Kto może korzystać z GenAI? Zidentyfikuj osoby lub role upoważnione do korzystania z GenAI

[Zasady formułowania promptów] Jakie dane mogą być wykorzystywane podczas używania GenAI (input data)?

[Zapewnienie zgodności z RODO]

[Zapewnienie zgodności z innymi przepisami]

[Zasady oznaczania treści wygenerowanych treści]

[Wewnętrzne ścieżki nadzoru i konsultacji – punkt kontaktowy dla pracowników; osoba odpowiedzialna za wdrażanie polityki]

[Mechanizm aktualizacji polityki i regularny audyt wykorzystywanych narzędzi GenAI] dynamiczny charakter GenAI

Szkolenia pracowników!

RODO a AI Act – co powinniśmy wiedzieć

- AI Act i RODO (np. art. 2(5a)– RODO znajduje zastosowanie niezależnie od AIA
- W Akcie w sprawie sztucznej inteligencji (AI Act) systemy generatywnej SI mieszczą się w kategorii *general purpose AI system*, czyli systemów AI ogólnego przeznaczenia (zob. art. 3(44e) i art. 52a i n. AIA)
- *system AI oparty na **modelu AI ogólnego przeznaczenia**, który może służyć różnym celom, zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI;*
- *Gdy model SI ogólnego przeznaczenia jest zintegrowany z systemem SI lub stanowi jego część, system ten uznaje się za system SI ogólnego przeznaczenia, gdy ze względu na tę integrację system ten może służyć różnym celom.*
- Obowiązki nałożone głównie na **dostawców** (providers) modeli SI ogólnego przeznaczenia (obowiązki mają zastosowanie w ciągu 12 miesięcy od daty wejścia w życie AIA – ich realizacja będzie istotna dla użytkowników systemów AI ogólnego przeznaczenia)

Podsumowanie

GenAI to nowe wyzwania dla organizacji z perspektywy ochrony danych (ochrony informacji i nie tylko...) – świadomość ryzyk (!)

Korzystanie z GenAI może wiązać się z określonymi ryzykami dla organizacji – ryzyka zależą od rodzaju organizacji (np. sektor bankowy) i celu wykorzystywania AI (np. HR i procesy rekrutacyjne v. chatbot jako wsparcie obsługi klienta)

Potrzeba „inwentaryzacji"/przeglądu wykorzystywania systemów GenAI w organizacji

Analiza dostępnych narzędzi GenAI i wybór takich, które odpowiednio chronią dane (osobowe)

„DPO in the loop" – zaangażowanie IOD

Monitorowanie zmian (AI Act i stanowiska właściwych organów nadzorczych)

Dr Iga Małobęcka-Szwast, LL.M.

radczyni prawna

iga.malobecka-szwast@wardynski.com.pl

Wardyński i Wspólnicy

Al. Ujazdowskie 10
00-478 Warszawa
tel.: 22 437 82 00, 22 537 82 00
faks: 22 437 82 01, 22 537 82 01

e-mail: warsaw@wardynski.com.pl
www.wardynski.com.pl