

Jak sprawować funkcję IOD bez ryzyka kar?

Nowe wytyczne

W TYM WYDANIU:

IOD – jak sprawować funkcję, żeby nie narazić się na karę administracyjną?

1

- Jak zapewnić niezależność IOD?

3

Praktyczne aspekty stosowania RODO i AI Act w organizacjach wykorzystujących sztuczną inteligencję

4

- Jak zarządzać systemami AI w firmie

8



Włodzimierz Dola
Legal Counsel

IOD – jak sprawować funkcję, żeby nie narazić się na karę administracyjną

W lutym 2025 r. na stronach Urzędu Ochrony danych osobowych ukazała się druga wersja Poradnika na gruncie RODO Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. Treść Poradnika wywołała poruszenie w środowisku ochrony danych osobowych ze względu na wyrażane w jego treści wskazówki dotyczące roli Inspektorów Ochrony Danych u administratorów. Zaznaczyć należy, że Prezes UODO nie ma uprawnień do dokonywania wiążącej wykładni przepisów prawa, a treści zamieszczone w Poradniku stanowią wskazówki będące emanacją uprawnień Prezesa UODO w zakresie upowszechnia wiedzy.

Poradnik jednak daje administratorom i podmiotom przetwarzającym sygnał, jak Prezes UODO podchodzi i będzie w przyszłości podchodził do pełnienia roli IOD w organizacji. Powyższe podejście ma już też wymiar praktyczny, bowiem przykładowo **Prezes UODO nałożył już w grudniu 2024 r. na Toyota Bank Polska S.A. karę w wysokości około 260 tys. zł za nieprawidłowe usytuowanie inspektora ochrony danych osobowych, niezapewniające mu niezależności**. Myślę, że w razie kontroli UODO, należy się spodziewać, że ocena roli IOD będzie sprawdzana i weryfikowana w tym kontekście.

Rola IOD w RODO

Motyw 97 RODO i art. 37-39 RODO określają rolę, pozycję u administratora, zadania i obowiązki Inspektorów Ochrony Danych. Jednym z najważniejszych elementów statuujących rolę IOD w świetle powyżej cytowanych przepisów jest gwarancja statusu niezależności IOD, a w zakresie jego odpowiedzialności powinien on być wolny od konfliktu interesów. Gwarantami powyższego jest przede wszystkim to, że:

- IOD ma podlegać bezpośrednio pod najwyższe kierownictwo administratora
- powinien być właściwie i niezwłocznie włączany przez administratora we wszystkie sprawy dotyczące ochrony danych osobowych
- powinien też otrzymać od administratora niezbędne zasoby, w tym dostęp do wiedzy fachowej, dotyczące sprawowania jego funkcji oraz dostęp do danych osobowych i operacji przetwarzania
- nie może też otrzymywać instrukcji dotyczących wykonywania tych zadań.



Zadania IOD zgodnie ze wskazówkami wynikającymi z poradnika UODO

Poradnik wskazuje, że zadania IOD to przede wszystkim:

-  doradzanie organizacji i personelowi w zakresie ochrony danych osobowych
-  monitorowanie przestrzegania przepisów RODO w organizacji
-  podnoszenie świadomości personelu na temat ochrony danych osobowych
-  współpraca z organem nadzorczym
-  pełnienie funkcji punktu kontaktowego dla organu nadzorczego i osób, których dane dotyczą

W zakresie będącym przedmiotem poradnika, czyli w obsłudze naruszeń ochrony danych osobowych poradnik wskazuje, że rola IOD polega na:

- pomocy administratorowi w zapobieganiu naruszeniom, np. poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowaniu szkoleń oraz formułowaniu zaleceń dotyczących bezpieczeństwa przetwarzania danych
- udzielaniu wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym zarządzania im, zgłaszania ich Prezesowi UODO oraz zawiadamiania osób, których dane dotyczą
- doradztwie w zakresie dokumentowania naruszeń i zarządzania dokumentacją
- przekazywaniu dodatkowych informacji o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

Poradnik wymienia również czynności, których IOD w procesie obsługi naruszeń ochrony danych osobowych nie może wykonywać, bowiem mogą one wpłynąć na jego niezależność.

Poradnik w tym zakresie wskazuje, że IOD nie może:



zgłaszać naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń



zawiadamiać w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych



dokumentować naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określeniem działań zaradczych)



podejmować zobowiązań dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających



działać na podstawie pełnomocnictwa w sprawach dotyczących ochrony danych osobowych.

Jestem przekonany, że część wymienionych zadań do tej pory u dużej ilości administratorów wykonywali de facto IOD, traktując je jako część swojego zakresu obowiązków. Wskazówki na pewno pozwolą na to, aby administratorzy mogli rozdzielić obowiązki IOD innego personelu zajmującego się kwestią obsługi naruszeń ochrony danych osobowych.

Jakich czynności nie powinien wykonywać IOD, żeby zachować niezależność i nie popadać w konflikt interesów?

Choć poradnik z jednej strony w zakresie obsługi naruszeń danych osobowych kompleksowo wyjaśnił zakres czynności, które IOD może wykonywać oraz tych, których nie powinien, to z drugiej strony stworzył w środowisku ochrony danych osobowych dyskusję w zakresie pozostałych obowiązków wynikających z RODO i roli IOD.

Przedstawiam w związku z tym otwarty i przykładowy zakres działań, których w mojej opinii IOD **nie powinien** realizować, aby nie narażać administratora na ryzyko nałożenia przez Prezesa UODO kary administracyjnej:

- sprawować roli u administratora, która powoduje, że może popaść w konflikt interesów
- prowadzić rejestrów: czynności przetwarzania i kategorii czynności przetwarzania
- określać celów i sposobów przetwarzania danych
- przygotowywać treści klauzul zgód lub obowiązków informacyjnych
- decydować o podstawie prawnej przetwarzania danych osobowych
- opracowywać umowy powierzenia przetwarzania danych osobowych
- opracowywać postanowień w relacjach z podmiotami trzecimi w zakresie danych osobowych
- opracowywać środki techniczne lub organizacyjne, podejmować decyzji o stosowanych środkach
- przeprowadzać ocenę skutków dla ochrony danych osobowych
- wydawać polecenia podmiotowi przetwarzającemu.



Jak zapewnić niezależność IOD?

Praktyka u wielu administratorów, szczególnie tych mniejszych, jest taka, że IOD jest w Organizacji jedyną osobą odpowiedzialną za ochronę danych osobowych. Z biznesowego punktu widzenia jest to słuszne. Wyspecjalizowana osoba dba o ochronę danych osobowych, jednocześnie nie generuje nadmiernych kosztów u administratora. Przy obecnej praktyce Ustawodawca powinien w moim odczuciu poszukać rozwiązania pozwalającego IOD w mikro i małych podmiotach (szczególnie tych, które mogą a nie muszą powoływać IOD), wykonywać większą ilość obowiązków w zakresie ochrony danych osobowych niż teraz na to pozwalają przepisy prawa. W mojej opinii będzie to z pewnością z korzyścią dla ochrony i bezpieczeństwa danych osobowych w takiej Organizacji.

W aktualnym stanie prawnym, przy obecnym podejściu organów nadzorczych oraz zasadzie rozliczalności, aby IOD mógł swoją funkcję sprawować niezależnie, administratorzy danych powinni zweryfikować, czy z jakiegoś powodu IOD nie wykonuje obowiązków, które nie powodują, że jego rola w Organizacji nie jest prawidłowa. **LexDigital jako firma specjalizująca się w doradztwie z tego obszaru kompleksowo wyręcza swoich klientów zarówno w pełnieniu funkcji IOD, jak i wsparciu administratorów w realizacji obowiązków wynikających z RODO.** Realizujemy powyższe między innymi poprzez rozdzielenie obu usług, tj. outsourcingu funkcji IOD i wsparciu administratorów danych w realizacji obowiązków wynikających z RODO oraz dedykowania osobnych zespołów do obu obszarów.



Aleksander Markiewicz
Legal Counsel

Praktyczne aspekty stosowania RODO i AI Act w organizacjach wykorzystujących sztuczną inteligencję

W erze cyfrowej transformacji sztuczna inteligencja staje się coraz bardziej integralną częścią działalności wielu organizacji. Pozwala ona na optymalizację procesów, wdrożenie innowacji produktowych oraz lepszego zrozumienia potrzeb klientów. Wraz z rosnącym znaczeniem AI, pojawiają się istotne wyzwania prawne i etyczne, zwłaszcza w kontekście ochrony danych osobowych i regulacji takich jak AI Act. Organizacje wykorzystujące AI muszą zatem świadomie podejść do kwestii zgodności z przepisami, aby w pełni wykorzystać potencjał tej technologii, minimalizując jednocześnie ryzyka prawne i reputacyjne. Niniejszy artykuł ma na celu omówienie **praktycznych aspektów** stosowania RODO i AI Act w organizacjach wykorzystujących sztuczną inteligencję, przedstawiając kluczowe obowiązki, wyzwania i strategie zarządzania.

Obowiązki wynikające z AI Act

AI Act ma na celu ustanowienie zharmonizowanych ram prawnych dla rozwoju, wprowadzania do obrotu i stosowania systemów AI w Unii Europejskiej. Jego głównym celem jest zapewnienie wysokiego poziomu bezpieczeństwa i zagwarantowania praw

podstawowych. Akt ten wprowadza podejście oparte na ryzyku, dzieląc systemy AI na różne kategorie w zależności od potencjalnego zagrożenia, jakie stwarzają.

Systemy AI wysokiego ryzyka podlegają najsurowszym wymogom. Obejmują one systemy wykorzystywane w obszarach krytycznych, takich jak infrastruktura krytyczna, edukacja, zatrudnienie, dostęp do usług publicznych i prywatnych, egzekwowanie prawa, zarządzanie migracjami i granicami oraz wymiar sprawiedliwości.

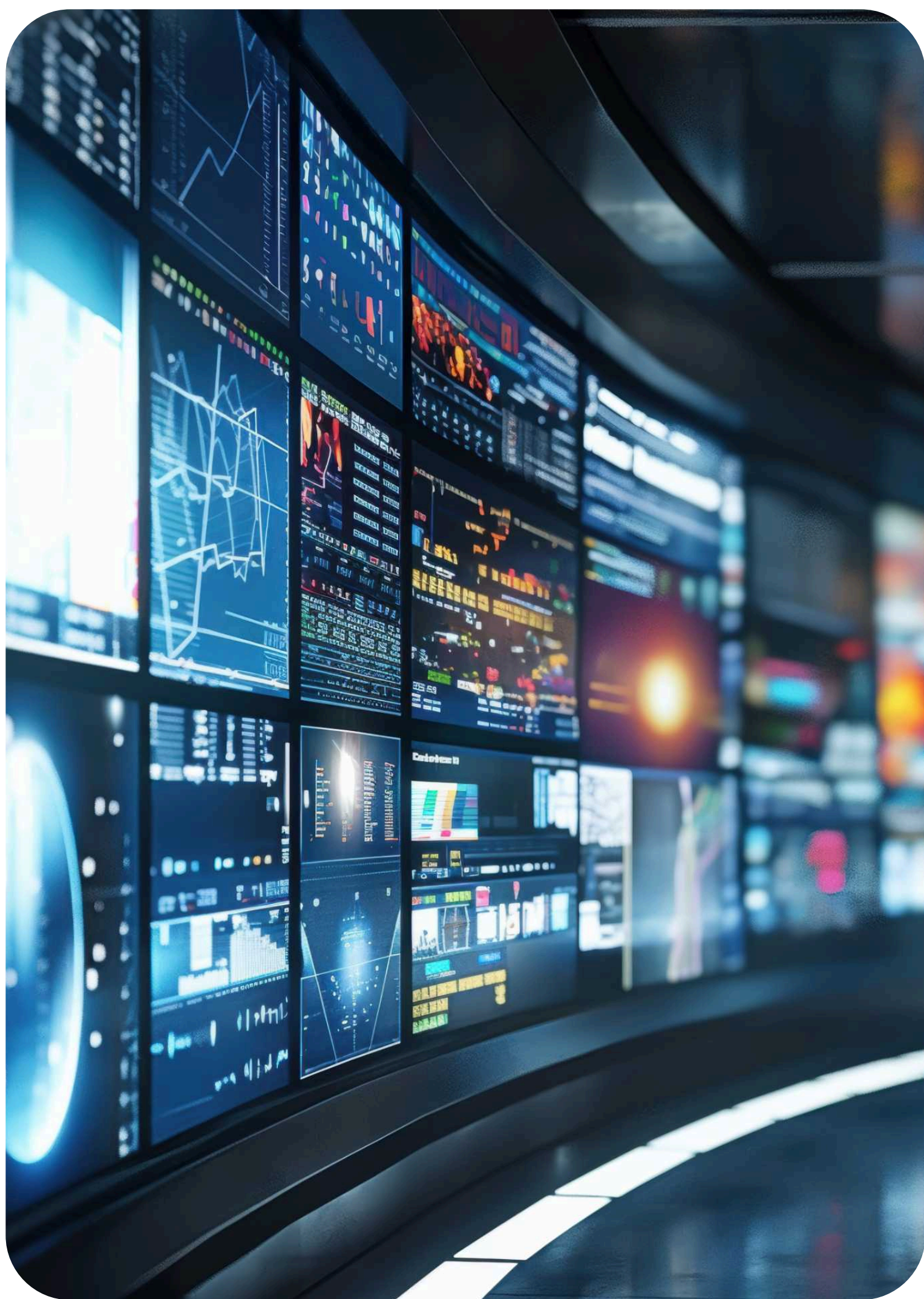
Organizacje wdrażające systemy AI wysokiego ryzyka będą musiały spełnić szereg obowiązków. Należą do nich:



Ocena zgodności – przed wprowadzeniem systemu do obrotu lub oddaniem go do użytku, organizacje będą musiały przeprowadzić ocenę zgodności z wymogami AI Act



Dokumentacja techniczna – niezbędne będzie prowadzenie szczegółowej dokumentacji technicznej systemu AI, która umożliwi ocenę jego zgodności z prawem



AI Act zakazuje pewnych praktyk, które są uznawane za niedopuszczalne ze względu na ich potencjał do naruszania praw podstawowych. Należą do nich m.in. systemy wykorzystujące techniki podprogowe do manipulowania zachowaniem, systemy biometrycznej identyfikacji zdalnej w czasie rzeczywistym w przestrzeni publicznej (z pewnymi wyjątkami), systemy oceny społecznej oparte na zachowaniu społecznym czy cechach osobowości.

Obowiązki wynikające z RODO

RODO ustanawia ramy prawne dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. **Podmioty wykorzystujące narzędzia AI często przetwarzają duże ilości danych osobowych, co sprawia, że RODO ma kluczowe znaczenie.**

Jednym z kluczowych obowiązków jest posiadanie podstawy prawnej przetwarzania danych osobowych. Przetwarzanie danych osobowych przez systemy AI musi opierać się na jednej z legalnych podstaw wymienionych w RODO, takich jak zgoda, wykonanie umowy, obowiązek prawny, ochrona żywotnych interesów, zadanie realizowane w interesie publicznym lub prawnie uzasadniony interes administratora. W kontekście AI, uzyskanie świadomej i jednoznacznej zgody może być wyzwaniem, zwłaszcza gdy przetwarzanie jest złożone i trudne do pełnego zrozumienia przez osobę, której dane dotyczą.



Przejrzystość i informowanie – użytkownicy systemów AI wysokiego ryzyka będą musieli być informowani o tym, że korzystają z takiego systemu oraz o jego możliwościach i ograniczeniach. W przypadku systemów interakcyjnych użytkownicy powinni być informowani o tym, że wchodzi w interakcję z systemem AI



Nadzór człowieka – systemy AI wysokiego ryzyka powinny być zaprojektowane w sposób umożliwiający skuteczny nadzór człowieka, tak aby w razie potrzeby można było interweniować lub cofnąć decyzję podjętą przez system



Dokładność i solidność – systemy AI wysokiego ryzyka muszą być zaprojektowane i testowane w taki sposób, aby osiągały wysoki poziom dokładności, solidności i cyberbezpieczeństwa.



Rejestracja – niektóre systemy AI wysokiego ryzyka będą musiały zostać zarejestrowane w publicznej bazie danych UE.

Przetwarzanie danych osobowych musi odbywać się zgodnie z zasadami określonymi w RODO. Wśród nich znajduje się zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, integralność i poufność. W kontekście AI, zapewnienie przejrzystości algorytmów i procesów decyzyjnych może być szczególnie trudne, zwłaszcza w przypadku złożonych modeli uczenia maszynowego.



Kolejnym istotnym obowiązkiem jest zapewnienie **realizacji praw podmiotów danych**. Osoby, których dane są przetwarzane mają szereg praw, w tym prawo dostępu do danych, prawo do sprostowania, prawo do usunięcia danych ("prawo do bycia zapomnianym"), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu oraz prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, która wywołuje wobec nich skutki prawne lub w podobny sposób istotnie na nie wpływa.

Przetwarzając dane osobowe Administrator zobowiązany jest do realizacji obowiązków z art. 13 i 14 RODO – realizacji obowiązku informacyjnego. Administratorzy danych są zobowiązani do informowania osób, których dane dotyczą, o sposobie przetwarzania ich danych, w tym o celach przetwarzania, kategoriach danych, odbiorcach danych, okresie przechowywania danych oraz o ich prawach. W przypadku wykorzystywania AI do podejmowania decyzji, informacje te powinny być jasne i zrozumiałe, wyjaśniając logikę działania systemu.

Administrator danych jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych, uwzględniając ryzyko związane z przetwarzaniem, w tym ryzyko wynikające z wykorzystania AI w procesie przetwarzania.

Istotnym obowiązkiem administratora jest przeprowadzanie analizy ryzyka, a w razie konieczności również oceny skutków dla ochrony danych (DPIA). **W przypadku przetwarzania danych osobowych z wykorzystaniem AI, które może wiązać się z wysokim ryzykiem dla praw i wolności osób fizycznych (np. profilowanie na dużą skalę, podejmowanie zautomatyzowanych decyzji o istotnych skutkach), administratorzy są zobowiązani do przeprowadzenia oceny skutków dla ochrony danych.**

Obowiązki wynikające ze stosowania AI

Niezależnie od obowiązków wynikających bezpośrednio z przepisów AI Act i RODO, samo stosowanie AI w organizacjach wiąże się z licznymi obowiązkami i wyzwaniem. Ustalenie i przestrzeganie podstawowych zasad pozwoli organizacjom na zagwarantowanie przetwarzania danych i wykorzystywania systemów AI w sposób zgodny z przepisami i poszanowaniem interesów podmiotów danych.



Istotne jest ustalenie zasad odpowiedzialności i rozliczalności działań. Określenie odpowiedzialności za decyzje podejmowane przez systemy AI może być złożone. Organizacje muszą ustanowić jasne procedury dotyczące nadzoru nad systemami AI, monitorowania ich działania i interweniowania w przypadku błędów lub niepożądanych skutków. Ważne jest, aby móc wyjaśnić, jak system AI doszedł do określonej decyzji (rozliczalność). Organizacje powinny uwzględniać aspekty etyczne związane z wykorzystaniem AI, takie jak unikanie uprzedzeń w danych i algorytmach, zapewnienie sprawiedliwości i niedyskryminacji, oraz poszanowanie prywatności i autonomii użytkowników.

Dla efektywnego wykorzystania systemów AI konieczne jest wprowadzenie zasad zarządzania danymi. Skuteczne wykorzystanie AI wymaga dostępu do wysokiej jakości danych. Organizacje muszą zapewnić odpowiednie procesy gromadzenia, przechowywania, czyszczenia i zarządzania danymi, z uwzględnieniem wymogów RODO dotyczących minimalizacji danych i ograniczenia przechowywania.

Istotnym aspektem korzystania z systemów AI jest nadzór człowieka nad tymi systemami. Konieczne jest wdrażanie mechanizmów nadzoru człowieka nad systemami AI, umożliwiających interwencję i korygowanie decyzji z wykorzystaniem czynnika ludzkiego.

Dla prawidłowego wykorzystania systemów AI niezbędne są odpowiednie kompetencje. Wdrożenie i zarządzanie systemami AI wymaga specjalistycznej wiedzy i umiejętności.

Organizacje muszą inwestować w rozwój kompetencji swoich pracowników w zakresie AI, a także podnosić świadomość na temat potencjalnych ryzyk i korzyści związanych z tą technologią.

Równie istotnym elementem systemu zarządzania AI jest **monitorowanie i audyt**. Systemy AI powinny być regularnie monitorowane i poddawane audytom w celu oceny ich wydajności, dokładności, bezpieczeństwa i zgodności z przepisami. Jednym z elementów zarządzania systemami AI powinno być testowanie tych systemów. Przeprowadzanie rygorystycznych testów i walidacji systemów AI pozwoli zapewnić ich dokładność, solidność i bezpieczeństwo.

Dla zapewnienia rozliczalności realizacji obowiązków i przestrzegania wewnętrznych zasad niezbędne jest prowadzenie dokumentacji, w szczególności prowadzenie dokumentacji dotyczącej rozwoju, wdrożenia i użytkowania systemów AI, w tym ocen zgodności, analiz ryzyka i opisów technicznych. Istotnym aspektem jest zapewnienie szkolenia i podnoszenia świadomości wśród personelu.

Regularne szkolenie pracowników w zakresie RODO, AI Act, zasad bezpiecznego korzystania z AI oraz etycznych aspektów stosowania AI pozwoli na realizację wszystkich powyższych obowiązków.



Zagrożenia wynikające ze stosowania AI

Niewłaściwe stosowanie AI może prowadzić do szeregu poważnych zagrożeń, w tym:



Naruszenia prywatności

– nieuprawniony dostęp do danych osobowych, profilowanie bez podstawy prawnej, brak przejrzystości w przetwarzaniu danych przez systemy AI.



Dyskryminacji i uprzedzenia

– występowanie uprzedzeń w danych treningowych może prowadzić do dyskryminujących wyników i decyzji podejmowanych przez systemy AI.



Braku odpowiedzialności – trudności w ustaleniu odpowiedzialności za szkody spowodowane przez autonomiczne systemy AI.



Manipulacji i dezinformacji

– wykorzystanie AI do tworzenia fałszywych informacji (deepfakes) i manipulowania opinią publiczną.



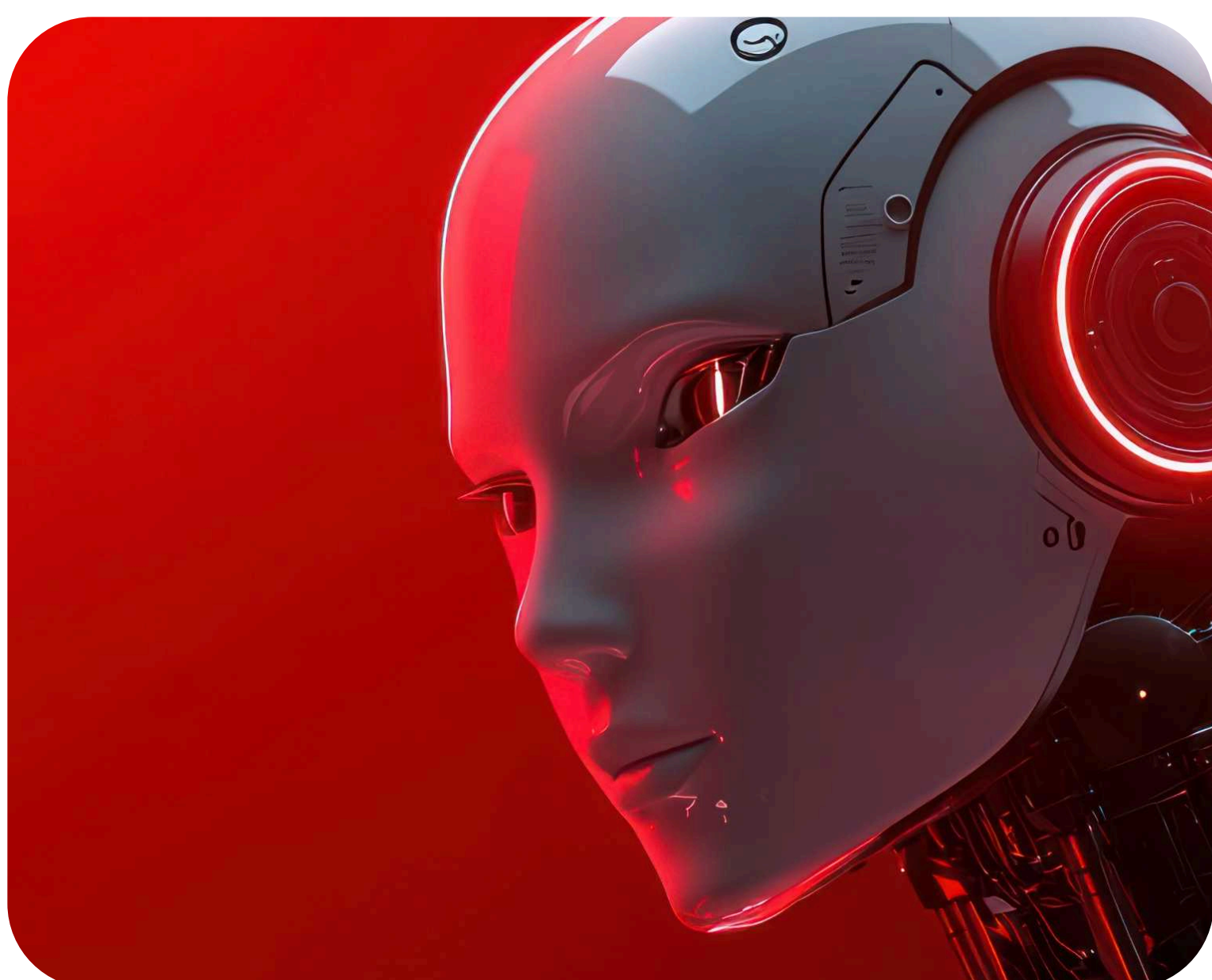
Zagrożenia dla bezpieczeństwa

– wykorzystanie AI do cyberataków i innych działań przestępczych.



Utraty zaufania

– niewłaściwe stosowanie AI może prowadzić do utraty zaufania publicznego do tej technologii.



Jak zarządzać systemami AI w firmie

Skuteczne zarządzanie systemami AI w organizacji wymaga holistycznego podejścia, obejmującego aspekty prawne, etyczne, techniczne i organizacyjne.

Istotnym elementem jest ustanowienie polityk i procedur związanych z wykorzystaniem AI. Każda organizacja powinna dążyć do opracowania wewnętrznych polityk i procedur dotyczących rozwoju, wdrażania, audytowania, testowania i użytkowania systemów AI.

Wewnętrzne procedury powinny określać:



Zadania ciążące na organizacji – np. ocena ryzyka, szkolenie personelu, testowanie systemów AI



Obowiązki pracowników – przestrzeganie wewnętrznych zasad, zwiększanie kompetencji



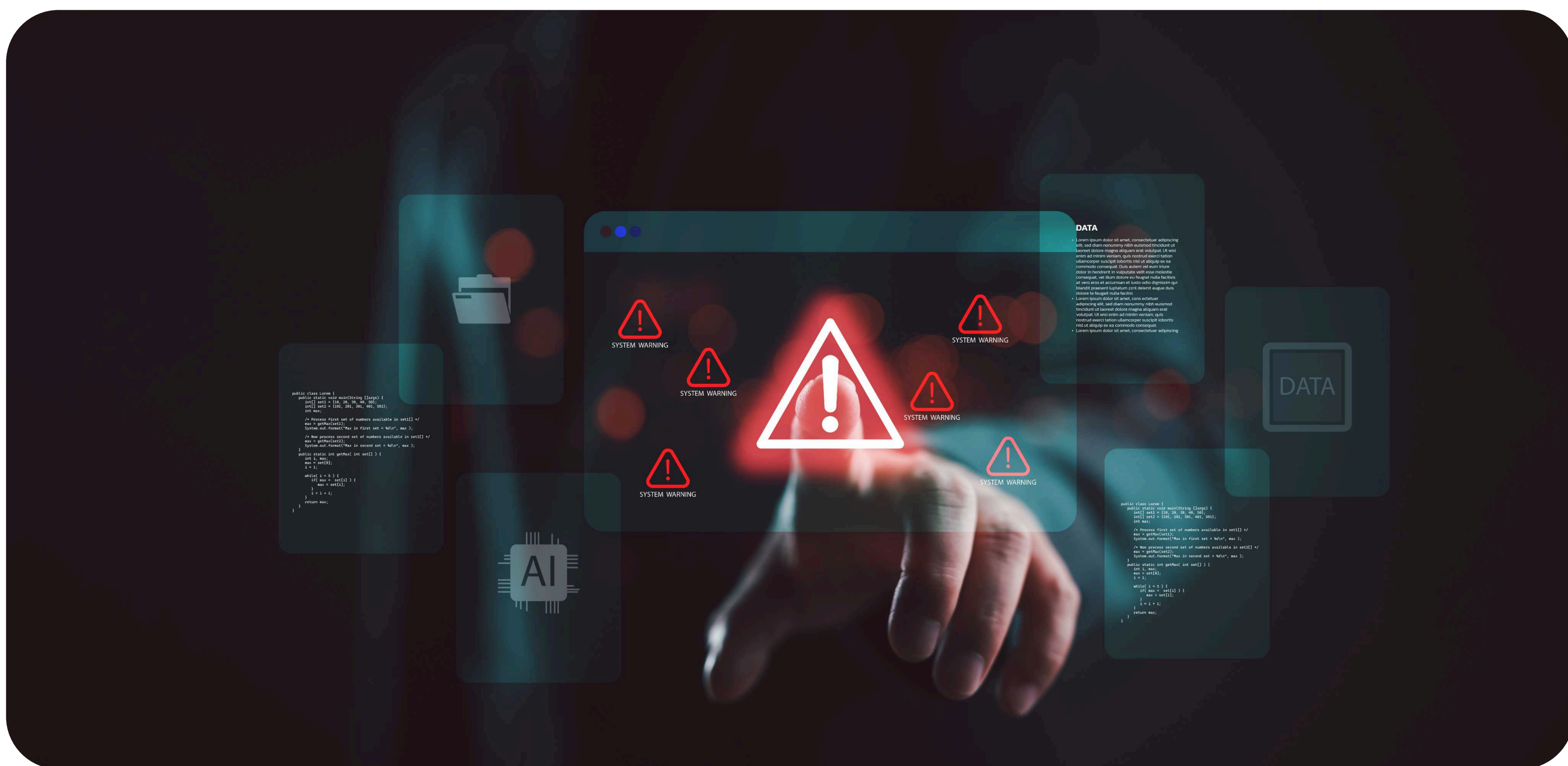
Zasady dopuszczenia systemu AI do użytku – obowiązek weryfikacji narzędzia od strony prawnej i technicznej



Zasady wykorzystania narzędzi AI – zakres i rodzaj danych wprowadzanych do konkretnego narzędzia.

Aby system zarządzania AI był skuteczny, niezbędne jest powierzenie odpowiedzialności – wyznaczenie osób lub zespołów odpowiedzialnych za nadzór nad systemami AI, zapewnienie ich zgodności z przepisami i monitorowanie ich działania.

Podobnie jak w obszarze ochrony danych, istotne jest regularne przeprowadzanie ocen ryzyka związanego z systemami AI oraz niezależnych audytów w celu weryfikacji ich zgodności i skuteczności z przepisami prawa i wewnętrznymi regulacjami.



Istotnym elementem nadzoru nad systemami sztucznej inteligencji jest zarządzanie danymi w systemach AI. Wdrożenie procesów zarządzania danymi wykorzystywanymi przez systemy AI, z uwzględnieniem jakości, bezpieczeństwa i zgodności z RODO pozwala na respektowanie powszechnie obowiązujących przepisów oraz zapewnienie realizacji wewnętrznych procedur.

Nadzór człowieka nad działaniem systemów AI oraz mechanizmy interwencji pozwalają zagwarantować bieżącą weryfikację sposobu działania systemów wykorzystujących AI oraz jakość i poprawność danych wyjściowych.

Testowanie i monitorowanie wydajności oraz jakości systemów AI w rzeczywistych warunkach pozwala na identyfikowanie i usuwanie potencjalnych problemów, błędów i niedoskonałości.

Jak zostało wskazane wyżej, szkolenie i edukacja personelu w zakresie systemów AI, etyki AI, RODO i AI Act pozwala na zwiększenie świadomości wśród pracowników, a co za tym idzie na minimalizację ryzyka wystąpienia incydentów. Równie ważne jest

organizowanie współpracy między zespołami technicznymi, prawnymi, etycznymi i biznesowymi w celu zapewnienia odpowiedzialnego oraz zgodnego z przepisami stosowania i rozwoju AI wewnątrz organizacji. Wszystkie powyższe działania powinny zmierzać do budowanie zaufania klientów i opinii publicznej do systemów AI stosowanych przez organizację, poprzez transparentność i odpowiedzialność.

Podsumowanie

Podsumowując, organizacje wykorzystujące sztuczną inteligencję stoją przed złożonym zadaniem zapewnienia zgodności z dynamicznie zmieniającym się otoczeniem prawnym, obejmującym RODO i AI Act. Kluczem do zgodności jest proaktywne podejście, uwzględniające aspekty prawne, etyczne i techniczne na każdym etapie cyklu życia systemów AI. Poprzez wdrożenie odpowiednich polityk, procedur i mechanizmów nadzoru, organizacje mogą wykorzystać ogromny potencjał AI, minimalizując jednocześnie ryzyka i budując zaufanie. Świadome i odpowiedzialne stosowanie AI jest nie tylko obowiązkiem prawnym, ale także strategiczną koniecznością w budowaniu trwałej wartości i reputacji organizacji w erze cyfrowej.



Newsletter RODO

Czerwiec 2025 nr 6/2025

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI