**Opinia 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji**

**(tłumaczenie nieoficjalne)**

**Przyjęta 17 grudnia 2024 r.**

|  |
| --- |
| **Streszczenie**Technologie sztucznej inteligencji stwarzają wiele możliwości i korzyści w wielu sektorach i działaniach społecznych.Chroniąc podstawowe prawo do ochrony danych, RODO wspiera te możliwości i promuje inne prawa podstawowe UE, w tym prawo do wolności myśli, wypowiedzi i informacji, prawo do edukacji lub wolności prowadzenia działalności gospodarczej. W ten sposób RODO stanowi ramy prawne, które zachęcają do odpowiedzialnych innowacji.W tym kontekście, biorąc pod uwagę kwestie ochrony danych związane z tymi technologiami, irlandzki organ nadzorczy zwrócił się do EROD o wydanie opinii w sprawach mających charakter ogólny zgodnie z art. 64 ust. 2 RODO. Wniosek dotyczy przetwarzania danych osobowych w kontekście faz opracowywania i wdrażania modeli sztucznej inteligencji ("**AI**"). Bardziej szczegółowo, we wniosku zapytano: (1) kiedy i w jaki sposób model sztucznej inteligencji można uznać za "anonimowy"; (2) w jaki sposób administratorzy mogą wykazać odpowiedniość prawnie uzasadnionego interesu jako podstawy prawnej w fazach opracowywania i (3) wdrażania; oraz (4) jakie są konsekwencje niezgodnego z prawem przetwarzania danych osobowych w fazie opracowywania modelu sztucznej inteligencji dla późniejszego przetwarzania lub działania modelu sztucznej inteligencji.**W odniesieniu do pierwszego pytania** w opinii wspomniano, że twierdzenia dotyczące anonimowości modelu sztucznej inteligencji powinny być oceniane przez właściwe organy nadzorcze indywidualnie dla każdego przypadku, ponieważ EROD uważa, że modele sztucznej inteligencji szkolone z wykorzystaniem danych osobowych nie mogą we wszystkich przypadkach być uznawane za anonimowe. Aby model sztucznej inteligencji można było uznać za anonimowy, zarówno (1) prawdopodobieństwo bezpośredniego (w tym probabilistycznego) pozyskania danych osobowych dotyczących osób fizycznych, których dane osobowe wykorzystano do opracowania modelu, jak i (2) prawdopodobieństwo uzyskania, celowo lub nie, takich danych osobowych z zapytań, powinno być nieznaczne, biorąc pod uwagę "wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane" przez administratora lub inną osobę.Aby przeprowadzić ocenę, organy nadzorcze powinny dokonać przeglądu dokumentacji dostarczonej przez administratora w celu wykazania anonimowości modelu. W tym względzie opinia zawiera nie nakazowy i niewyczerpujący wykaz metod, które mogą być stosowane przez administratorów w celu wykazania anonimowości, a tym samym mogą być brane pod uwagę przez organy nadzorcze przy ocenie twierdzenia administratora o anonimowości. Obejmuje to na przykład podejścia przyjęte przez administratorów w fazie opracowywania, aby zapobiec lub ograniczyć gromadzenie danych osobowych wykorzystywanych do szkolenia, zmniejszyć ich identyfikowalność, zapobiec ich pozyskiwaniu lub zapewnić odporność na ataki zgodnie z aktualnym stanem wiedzy.**W odniesieniu do drugiego i trzeciego pytania** opinia zawiera ogólne uwagi, które organy nadzorcze powinny wziąć pod uwagę przy ocenie, czy administratorzy mogą powoływać się na prawnie uzasadniony interes jako odpowiednią podstawę prawną przetwarzania prowadzonego w kontekście opracowywania i wdrażania modeli sztucznej inteligencji.W opinii przypomniano, że nie ma hierarchii między podstawami prawnymi przewidzianymi w RODO oraz że do administratorów należy określenie odpowiedniej podstawy prawnej dla ich działań związanych z przetwarzaniem. Następnie w opinii przypomniano trzystopniowy test, który należy przeprowadzić przy ocenie wykorzystania prawnie uzasadnionego interesu jako podstawy prawnej, tj. (1) identyfikację prawnie uzasadnionego interesu realizowanego przez administratora lub stronę trzecią; (2) analizę konieczności przetwarzania do celów wynikających z prawnie uzasadnionych interesów (zwaną również "testem konieczności"); oraz (3) ocenę, czy prawnie uzasadnione interesy nie są podrzędne wobec interesów lub podstawowych praw i wolności osób, których dane dotyczą (zwaną również "testem równowagi"). |

|  |
| --- |
| W odniesieniu do pierwszego kroku w opinii przypomniano, że interes można uznać za prawnie uzasadniony, jeżeli spełnione są łącznie następujące trzy kryteria: interes (1) jest zgodny z prawem; (2) jest jasno i precyzyjnie sformułowany; oraz (3) jest rzeczywisty i obecny (tj. nie jest spekulacyjny). Taki interes może dotyczyć na przykład rozwoju modelu sztucznej inteligencji - opracowania usługi konsultanta rozmawiającego z użytkownikiem pomagającego użytkownikom lub jego wdrożenia - usprawnienia wykrywania zagrożeń w systemie informatycznym.W odniesieniu do drugiego kroku, w opinii przypomniano, że ocena konieczności obejmuje rozważenie: (1) czy czynność przetwarzania pozwoli na realizację prawnie uzasadnionego interesu; oraz(2) czy nie istnieje mniej inwazyjny sposób realizacji tego interesu. Oceniając, czy warunek konieczności jest spełniony, organy nadzorcze powinny zwrócić szczególną uwagę na ilość przetwarzanych danych osobowych oraz na to, czy jest to proporcjonalne do realizacji danego prawnie uzasadnionego interesu, również w świetle zasady minimalizacji danych.W odniesieniu do trzeciego etapu w opinii przypomniano, że test równowagi powinien być przeprowadzany z uwzględnieniem szczególnych okoliczności każdej sprawy. Następnie przedstawia przegląd elementów, które organy nadzorcze mogą wziąć pod uwagę przy ocenie, czy interes administratora lub strony trzeciej jest podrzędny w stosunku do interesów, praw podstawowych i wolności osób, których dane dotyczą.W ramach trzeciego kroku w opinii podkreślono szczególne zagrożenia dla praw podstawowych, które mogą pojawić się zarówno na etapie opracowywania, jak i wdrażania modeli AI. Wyjaśnia również, że przetwarzanie danych osobowych, które ma miejsce na etapie opracowywania i wdrażania modeli sztucznej inteligencji, może mieć różny wpływ na osoby, których dane dotyczą, który może być pozytywny lub negatywny. Aby ocenić taki wpływ, organy nadzorcze mogą wziąć pod uwagę charakter danych przetwarzanych przez modele, kontekst przetwarzania i możliwe dalsze konsekwencje przetwarzania.W opinii dodatkowo podkreśla się rolę prawnie uzasadnionych oczekiwań osób, których dane dotyczą, w teście równowagi. Może to być ważne ze względu na złożoność technologii wykorzystywanych w modelach sztucznej inteligencji oraz fakt, że osobom, których dane dotyczą, może być trudno zrozumieć różnorodność potencjalnych zastosowań tych technologii, jak również związanych z nimi różnych czynności przetwarzania. W związku z tym zarówno informacje przekazywane osobom, których dane dotyczą, jak i kontekst przetwarzania mogą być jednymi z elementów, które należy wziąć pod uwagę, aby ocenić, czy osoby, których dane dotyczą, mają rozsądne przesłanki, by spodziewać się, że ich dane osobowe będą przetwarzane. W odniesieniu do kontekstu może to obejmować: to, czy dane osobowe były publicznie dostępne, charakter relacji między osobą, której dane dotyczą, a administratorem (i czy istnieje między nimi związek), charakter usługi, kontekst, w którym dane osobowe zostały zebrane, źródło, z którego dane zostały zebrane (tj. strona internetowa lub usługa, w której dane osobowe zostały zebrane i oferowane przez nie ustawienia prywatności), potencjalne dalsze zastosowania modelu oraz czy osoby, których dane dotyczą, są rzeczywiście świadome, że ich dane osobowe są w ogóle online.W opinii przypomniano również, że jeżeli interesy, prawa i wolności osób, których dane dotyczą, wydają się nadrzędne wobec prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, administrator może rozważyć wprowadzenie środków łagodzących w celu ograniczenia wpływu przetwarzania na te osoby, których dane dotyczą. Środków łagodzących nie należy mylić ze środkami, które administrator i tak jest prawnie zobowiązany przyjąć w celu zapewnienia zgodności z RODO. Ponadto środki te powinny być dostosowane do okoliczności sprawy i cech modelu AI, w tym jego zamierzonego zastosowania. W tym względzie Opinia zawiera niewyczerpujący wykaz przykładów środków łagodzących w odniesieniu do fazy opracowywania (również w odniesieniu do web scrapingu) i fazy wdrażania. Środki łagodzące mogą podlegać szybkim zmianom i powinny być dostosowane do okoliczności danej sprawy. W związku z tym ocena adekwatności wdrożonych środków łagodzących w poszczególnych przypadkach pozostaje w gestii organów nadzorczych. |

|  |
| --- |
| **W odniesieniu do czwartego pytania,** w opinii ogólnie przypomniano, że organy nadzorcze mają swobodę decyzyjną w zakresie oceny możliwego naruszenia (naruszeń) i wyboru odpowiednich, niezbędnych i proporcjonalnych środków, biorąc pod uwagę okoliczności każdej indywidualnej sprawy. Następnie w opinii rozważono trzy scenariusze.W scenariuszu 1 dane osobowe są przechowywane w modelu sztucznej inteligencji (co oznacza, że modelu nie można uznać za anonimowy, jak wyszczególniono w pierwszym pytaniu) i są następnie przetwarzane przez tego samego administratora (na przykład w kontekście wdrożenia modelu). W opinii stwierdzono, że to, czy fazy opracowywania i wdrażania wiążą się z odrębnymi celami (stanowiąc tym samym odrębne czynności przetwarzania) oraz zakres, w jakim brak podstawy prawnej dla początkowej czynności przetwarzania wpływa na zgodność z prawem późniejszego przetwarzania, należy oceniać indywidualnie dla każdego przypadku, w zależności od kontekstu sprawy.W scenariuszu 2 dane osobowe są zatrzymywane w modelu i przetwarzane przez innego administratora w kontekście wdrożenia modelu. W związku z tym w opinii stwierdza się, że organy nadzorcze powinny wziąć pod uwagę, czy administrator wdrażający model przeprowadził odpowiednią ocenę w ramach swoich obowiązków w zakresie rozliczalności w celu wykazania zgodności z art. 5 ust. 1 lit. a) i art. 6 RODO, aby upewnić się, że model sztucznej inteligencji nie został opracowany poprzez niezgodne z prawem przetwarzanie danych osobowych. Ocena ta powinna uwzględniać na przykład źródło danych osobowych oraz to, czy przetwarzanie w fazie opracowywania było przedmiotem stwierdzenia naruszenia, w szczególności jeśli zostało ono stwierdzone przez organ nadzorczy lub sąd, i powinna być mniej lub bardziej szczegółowa w zależności od ryzyka związanego z przetwarzaniem w fazie wdrażania.W scenariuszu 3 administrator bezprawnie przetwarza dane osobowe w celu opracowania modelu sztucznej inteligencji, a następnie zapewnia ich anonimizację, zanim ten sam lub inny administrator rozpocznie dalsze przetwarzanie danych osobowych w kontekście wdrożenia. W tym względzie w opinii stwierdzono, że jeżeli można wykazać, że późniejsze działanie modelu sztucznej inteligencji nie wiąże się z przetwarzaniem danych osobowych, EROD uważa, że RODO nie będzie miało zastosowania. W związku z tym niezgodność z prawem początkowego przetwarzania nie powinna mieć wpływu na późniejsze działanie modelu. Ponadto EROD uważa, że jeżeli administratorzy dokonują dalszego przetwarzania danych osobowych zebranych w fazie wdrażania, po tym jak model został zanonimizowany, RODO będzie miało zastosowanie w odniesieniu do tych operacji przetwarzania. W takich przypadkach w opinii uznano, że w odniesieniu do RODO niezgodność z prawem początkowego przetwarzania danych nie powinna mieć wpływu na zgodność z prawem przetwarzania przeprowadzonego w fazie wdrażania. |

Spis treści

Spis treści

[1 Wprowadzenie 6](#_Toc195612006)

[1.1 Podsumowanie faktów 6](#_Toc195612007)

[1.2 Dopuszczalność wniosku o wydanie opinii na podstawie art. 64 ust. 2 RODO 8](#_Toc195612008)

[2 Zakres i kluczowe pojęcia 9](#_Toc195612009)

[2.1 Zakres opinii 9](#_Toc195612010)

[2.2 Kluczowe pojęcia 11](#_Toc195612011)

[2.3 Modele sztucznej inteligencji w kontekście opinii 11](#_Toc195612012)

[3 Istota wniosku 12](#_Toc195612013)

[3.1 Charakter modeli sztucznej inteligencji w odniesieniu do definicji danych osobowych 12](#_Toc195612014)

[3.2 Okoliczności, w których modele sztucznej inteligencji można uznać za anonimowe i związane z tym wykazanie 14](#_Toc195612015)

[3.2.1 Ogólne rozważania dotyczące anonimizacji w omawianym kontekście. 14](#_Toc195612016)

[3.2.2. Elementy służące do oceny szczątkowego prawdopodobieństwa identyfikacji 16](#_Toc195612017)

[Wybór źródeł 17](#_Toc195612018)

[Przygotowanie i minimalizacja danych 17](#_Toc195612019)

[Wybory metodologiczne dotyczące szkolenia 17](#_Toc195612020)

[Środki dotyczące wyników modelu 17](#_Toc195612021)

[3.3. Odpowiedniość prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania danych osobowych w kontekście opracowywania i wdrażania modeli AI 19](#_Toc195612022)

[3.3.1 Uwagi ogólne 19](#_Toc195612024)

[3.3.2 Rozważania na temat trzech etapów oceny prawnie uzasadnionego interesu w kontekście rozwoju i wdrażania modeli sztucznej inteligencji 21](#_Toc195612025)

[3.3.2.1 Pierwszy krok - realizacja prawnie uzasadnionego interesu przez administratora lub osobę trzecią 21](#_Toc195612026)

[Interesy, podstawowe prawa i wolności osób, których dane dotyczą 23](#_Toc195612027)

[Wpływ przetwarzania na osoby, których dane dotyczą 24](#_Toc195612028)

[Rozsądne oczekiwania osób, których dane dotyczą 26](#_Toc195612029)

[Środki łagodzące 27](#_Toc195612030)

[3.4 Możliwy wpływ niezgodnego z prawem przetwarzania w ramach opracowywania modelu AI na zgodność z prawem późniejszego przetwarzania lub działania modelu AI 30](#_Toc195612031)

[3.4.1 Scenariusz 1. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowania modelu, dane osobowe są przechowywane w modelu i są następnie przetwarzane przez tego samego administratora (na przykład w kontekście wdrożenia modelu). 31](#_Toc195612032)

[3.4.2. Scenariusz 2. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowania modelu, dane osobowe są zatrzymywane w modelu i przetwarzane przez innego administratora w kontekście wdrożenia modelu. 32](#_Toc195612033)

[3.4.3. Scenariusz 3. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowywania modelu, a następnie zapewnia anonimizację modelu, zanim ten sam lub inny administrator rozpocznie dalsze przetwarzanie danych osobowych w kontekście wdrożenia. 33](#_Toc195612034)

[4. Uwagi końcowe 34](#_Toc195612035)

**Europejska Rada Ochrony Danych**

uwzględniając art. 63 oraz art. 64 ust. 2 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 (dalej "RODO"),

uwzględniając Porozumienie EOG, w szczególności jego załącznik XI i protokół 37, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r. ,[[1]](#footnote-2)

uwzględniając art. 10 i art. 22 swojego regulaminu wewnętrznego, a także mając na uwadze, co następuje:

1. Główną rolą Europejskiej Rady Ochrony Danych (zwanej dalej **"EROD"**) jest zapewnienie spójnego stosowania RODO w całym Europejskim Obszarze Gospodarczym (**"EOG"**). Artykuł 64 ust. 2 RODO stanowi, że każdy organ nadzorczy (**"organ nadzorczy"**), przewodniczący Rady lub Komisja mogą wystąpić o przeanalizowanie przez Europejską Radę Ochrony Danych w celu uzyskania opinii każdej sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim EOG. Celem niniejszej opinii jest przeanalizowanie sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim EOG.
2. Opinię EROD przyjmuje się zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od podjęcia przez przewodniczącego i właściwy organ nadzorczy decyzji o kompletności akt. Na podstawie decyzji przewodniczącego termin ten może zostać przedłużony o kolejne sześć tygodni, biorąc pod uwagę złożony charakter sprawy.

**WYDAŁA NASTĘPUJĄCĄ OPINIĘ**

# Wprowadzenie

## Podsumowanie faktów

1. 4 września 2024 r. irlandzki organ nadzorczy ("**ON IE** " lub "**wnioskujący ON**") zwrócił się do EROD o wydanie opinii na podstawie art. 64 ust. 2 RODO w odniesieniu do modeli sztucznej inteligencji i przetwarzania danych osobowych ("**wniosek**").
2. 13 września 2024 r. przewodnicząca EROD i ON IE uznali akta za kompletne. Następnego dnia roboczego, 16 września 2024 r., akta zostały przesłane przez sekretariat EROD. Przewodnicząca Rady, biorąc pod uwagę złożony charakter sprawy, podjęła decyzję o przedłużeniu ustawowego terminu zgodnie z art. 64 ust. 3 RODO i art. 10 ust. 4 regulaminu wewnętrznego EROD.
3. Wniosek dotyczy niektórych elementów szkolenia, aktualizacji, opracowywania i obsługi modeli sztucznej inteligencji, w przypadku których dane osobowe stanowią część odpowiedniego zbioru danych. ON IE podkreśla, że wniosek dotyczy kluczowych kwestii, które mają duży wpływ na osoby, których dane dotyczą, i administratorów danych w EOG, oraz że na tym etapie nie ma zharmonizowanego stanowiska wśród krajowych organów nadzorczych[[2]](#footnote-3) .

Terminologię, która będzie stosowana do celów niniejszej opinii, przedstawiono w sekcjach 2.2 i 2.3 poniżej.

1. Następujące pytania zostały zadane przez ON IE:

**Pytanie 1**: Czy ostateczny model sztucznej inteligencji, który został przeszkolony przy użyciu danych osobowych, we wszystkich przypadkach nie spełnia definicji danych osobowych (zgodnie z art. 4 ust. 1 RODO)?

Jeśli odpowiedź na pytanie 1 brzmi "tak":

* 1. Na jakim etapie operacji przetwarzania prowadzących do powstania modelu AI dane osobowe nie są już przetwarzane?
		1. W jaki sposób można wykazać, że model sztucznej inteligencji nie przetwarza danych osobowych?
	2. Czy są jakieś czynniki, które spowodowałyby, że działanie ostatecznego modelu sztucznej inteligencji nie byłoby już uważane za anonimowe?
		1. Jeśli tak, w jaki sposób można wykazać środki podjęte w celu złagodzenia, zapobiegania lub ochrony przed tymi czynnikami (aby zapewnić, że model sztucznej inteligencji nie przetwarza danych osobowych)?

Jeśli odpowiedź na pytanie 1 brzmi "nie":

 i. W jakich okolicznościach może to nastąpić?

a) Jeśli tak, w jaki sposób można wykazać kroki podjęte w celu zapewnienia, że model sztucznej inteligencji nie przetwarza danych osobowych?

**Pytanie 2**: W przypadku gdy administrator danych opiera się na prawnie uzasadnionych interesach jako podstawie prawnej przetwarzania danych osobowych w celu tworzenia, aktualizowania i/lub rozwijania modelu sztucznej inteligencji, w jaki sposób powinien on wykazać odpowiedniość prawnie uzasadnionych interesów jako podstawy prawnej, zarówno w odniesieniu do przetwarzania danych osób trzecich, jak i danych własnych?

i. Jakie względy powinien wziąć pod uwagę administrator, aby zapewnić, że interesy osób, których dane dotyczą, których dane osobowe są przetwarzane, są odpowiednio zrównoważone z interesami administratora w kontekście:

* + 1. Dane osób trzecich
		2. Dane własne

**Pytanie 3**: Po szkoleniu, w przypadku gdy administrator danych opiera się na prawnie uzasadnionych interesach jako podstawie prawnej przetwarzania danych osobowych odbywającego się w ramach modelu AI lub systemu AI, którego częścią jest model AI, w jaki sposób administrator powinien wykazać odpowiedniość prawnie uzasadnionych interesów jako podstawy prawnej?

**Pytanie 4**: Jeżeli stwierdzono, że model sztucznej inteligencji został utworzony, zaktualizowany lub opracowany przy użyciu danych osobowych przetwarzanych niezgodnie z prawem, jaki jest wpływ tego faktu, jeżeli w ogóle, na zgodność z prawem dalszego lub późniejszego przetwarzania lub działania modelu sztucznej inteligencji, samodzielnie lub jako część systemu sztucznej inteligencji, w przypadku gdy:

1. Model AI, samodzielnie lub jako część systemu AI, przetwarza dane osobowe?
2. ii. Ani Model AI, ani model AI jako część systemu AI nie przetwarza danych osobowych?

## Dopuszczalność wniosku o wydanie opinii na podstawie art. 64 ust. 2 RODO

1. Art. 64 ust. 2 RODO stanowi w szczególności, że każdy organ nadzorczy może zażądać, aby każda sprawa mająca charakter ogólny lub wywołująca skutki w więcej niż jednym państwie członkowskim została przeanalizowana przez EROD w celu wydania opinii.
2. Wnioskujący organ nadzorczy skierował do EROD pytania dotyczące aspektów ochrony danych w kontekście modeli sztucznej inteligencji. We wniosku stwierdzono, że chociaż wiele organizacji korzysta obecnie z modeli sztucznej inteligencji, w tym dużych modeli językowych ("**LLM**"), ich działanie, szkolenie i wykorzystanie budzą "*wiele szeroko zakrojonych* obaw dotyczących *ochrony danych*"[[3]](#footnote-4) , które "*mają wpływ na osoby, których dane dotyczą, w całej* UE/EOG"[[4]](#footnote-5) .
3. Wniosek podnosi zasadnicze kwestie dotyczące (i) stosowania pojęcia danych osobowych; (ii) zasady zgodności z prawem, ze szczególnym uwzględnieniem podstawy prawnej jaką jest prawnie uzasadniony interes, w kontekście modeli sztucznej inteligencji; a także (iii) konsekwencji niezgodnego z prawem przetwarzania danych osobowych na etapie opracowywania modeli sztucznej inteligencji dla późniejszego przetwarzania lub działania modelu.
4. EROD uważa, że wniosek dotyczy "*sprawy mającej charakter ogólny*" w rozumieniu art. 64 ust. 2 RODO. W szczególności sprawa dotyczy interpretacji i stosowania art. 4 ust. 1, art. 5 ust. 1 lit. a) i art. 6 RODO w odniesieniu do przetwarzania danych osobowych przy opracowywaniu i wdrażaniu modeli sztucznej inteligencji. Jak podkreślił wnioskujący organ nadzorczy, zastosowanie tych przepisów do modeli sztucznej inteligencji wiąże się z systemowymi, abstrakcyjnymi i nowymi kwestiami[[5]](#footnote-6) . Szybki rozwój i wdrażanie modeli sztucznej inteligencji przez coraz więcej organizacji wiąże się z konkretnymi kwestiami i, jak wskazano we wniosku, *"EROD odniesie znaczne korzyści z wypracowania wspólnego stanowiska w kwestiach poruszonych w niniejszym wniosku, ponieważ kwestie te mają kluczowe znaczenie dla planowanych prac EROD w perspektywie krótko- i* średnioterminowej"[[6]](#footnote-7) . Ponadto technologie sztucznej inteligencji stwarzają wiele możliwości i korzyści w wielu sektorach i działaniach społecznych. Poza tym RODO stanowi ramy prawne, które zachęcają do odpowiedzialnych innowacji. Wynika z tego, że w ogólnym interesie leży dokonanie tej oceny w formie opinii EROD, aby zapewnić spójne stosowanie niektórych przepisów RODO w kontekście modeli sztucznej inteligencji.
5. Alternatywny warunek zawarty w art. 64 ust. 2 RODO odnosi się do kwestii "*wywołujących skutki w więcej niż jednym państwie członkowskim"*. EROD przypomina, że termin "skutki" należy interpretować *sensu largo*, a zatem nie ogranicza się on wyłącznie do skutków prawnych[[7]](#footnote-8). Ponieważ coraz więcej modeli sztucznej inteligencji jest szkolonych i wykorzystywanych przez rosnącą liczbę organizacji w EOG, mają one wpływ na dużą liczbę osób, których dane dotyczą w całym EOG, z których niektóre zgłosiły już swoje zastrzeżenia do właściwego organu nadzorczego[[8]](#footnote-9) . W związku z tym EROD uważa, że kwestia podniesiona przez wnioskujący organ nadzorczy również spełnia ten warunek.
6. Wniosek zawiera pisemne uzasadnienie dotyczące kontekstu i motywów przedłożenia pytań EROD, w tym odpowiednich ram prawnych. W związku z tym EROD uważa, że wniosek jest uzasadniony zgodnie z art. 10 ust. 3 regulaminu EROD.
7. Zgodnie z art. 64 ust. 3 RODO[[9]](#footnote-10) EROD nie wydaje opinii, jeżeli wcześniej wydała już opinię w takiej samej sprawie. EROD nie wydała opinii w takiej samej sprawie i nie udzieliła jeszcze odpowiedzi na pytania wynikające z wniosku.
8. Z tych powodów EROD uważa, że wniosek jest dopuszczalny, a kwestie z niego wynikające powinny zostać przeanalizowane w niniejszej opinii ("**opinia**") przyjętej zgodnie z art. 64 ust. 2 RODO.

# Zakres i kluczowe pojęcia

## Zakres opinii

1. EROD zgadza się z wnioskującym organem nadzorczym, że z perspektywy ochrony danych, rozwój i wdrażanie modeli sztucznej inteligencji wiąże się z podstawowymi kwestiami dotyczącymi ochrony danych. Pytania te dotyczą w szczególności: (i) kiedy i w jaki sposób model sztucznej inteligencji można uznać za "anonimowy" (pytanie 1 wniosku); (ii) w jaki sposób administratorzy mogą wykazać odpowiedniość prawnie uzasadnionego interesu jako podstawy prawnej w fazie opracowywania (pytanie 2 wniosku) i wdrażania (pytanie 3 wniosku); oraz (iii) czy niezgodne z prawem przetwarzanie danych osobowych w fazie opracowywania ma konsekwencje dla zgodności z prawem późniejszego przetwarzania lub działania modelu sztucznej inteligencji (pytanie 4 wniosku).
2. EROD przypomina, że organy nadzorcze są odpowiedzialne za monitorowanie stosowania RODO i powinny przyczyniać się do jego spójnego stosowania w całej Unii[[10]](#footnote-11) . W związku z tym do kompetencji organów nadzorczych należy badanie konkretnych modeli sztucznej inteligencji, a tym samym przeprowadzanie oceny poszczególnych przypadków.
3. Niniejsza opinia stanowi ramy dla właściwych organów nadzorczych do oceny konkretnych przypadków, w których mogą pojawić się (niektóre) kwestie poruszone we wniosku. Niniejsza opinia nie ma na celu wyczerpania tematu, lecz raczej przedstawienie ogólnych rozważań na temat interpretacji odpowiednich przepisów, które właściwe organy nadzorcze powinny w jak największym stopniu uwzględnić przy korzystaniu ze swoich uprawnień do prowadzenia postępowań wyjaśniających. Chociaż niniejsza opinia jest skierowana do właściwych organów nadzorczych i odnosi się do ich działań i uprawnień, pozostaje ona bez uszczerbku dla obowiązków administratorów i podmiotów przetwarzających wynikających z RODO. W szczególności, zgodnie z zasadą rozliczalności zapisaną w art. 5 ust. 2 RODO, administratorzy są odpowiedzialni za przestrzeganie wszystkich zasad związanych z przetwarzaniem przez nich danych osobowych i są w stanie wykazać ich przestrzeganie.
4. W niektórych przypadkach w opinii można podać pewne przykłady, ale biorąc pod uwagę szeroki zakres pytań zawartych we wniosku, a także różne rodzaje modeli sztucznej inteligencji w nim uwzględnionych, nie wszystkie możliwe scenariusze zostaną uwzględnione w niniejszej opinii. Technologie związane z modelami sztucznej inteligencji podlegają szybkiej ewolucji; w związku z tym rozważania EROD zawarte w niniejszej opinii należy interpretować w tym świetle.
5. **W niniejszej opinii nie przeanalizowano poniższych przepisów, które nadal mogą odgrywać ważną rolę przy ocenie wymogów ochrony danych mających zastosowanie do modeli sztucznej inteligencji:**
	* **Przetwarzanie szczególnych kategorii danych:** EROD przypomina zakaz zawarty w art. 9 ust. 1 RODO dotyczący przetwarzania szczególnych kategorii danych oraz ograniczone wyjątki zawarte w art. 9 ust. 2 RODO[[11]](#footnote-12) . W tym względzie Trybunał Sprawiedliwości Unii Europejskiej (**"TSUE"**) wyjaśnił dalej, że "*w przypadku gdy* przedmiotem takich czynności jest zbiór danych zawierający jednocześnie dane wrażliwe i takie, które nie podlegają takiej szczególnej ochronie, a w szczególności jest pozyskiwany jako jedna całość, a dane te nie mogą zostać w momencie tego pozyskiwania oddzielone od siebie, przetwarzanie tego zbioru danych należy uznać za zabronione w rozumieniu art. 9 ust. 1 RODO, w sytuacji gdy zawiera on co najmniej jedną daną wrażliwą i jednocześnie nie ma zastosowania żadne z odstępstw, o których mowa w art. 9 ust. 2 tego rozporządzenia"[[12]](#footnote-13) . Ponadto TSUE podkreślił również, że *"że do celów zastosowania wyjątku przewidzianego w art. 9 ust. 2 lit. e) RODO należy sprawdzić, czy osoba, której dane dotyczą, zamierzała, w drodze wyraźnej czynności potwierdzającej, udostępnić rozpatrywane dane osobowe ogółowi opinii publicznej.*"[[13]](#footnote-14) . Rozważania te należy wziąć pod uwagę, gdy przetwarzanie danych osobowych w kontekście modeli sztucznej inteligencji obejmuje szczególne kategorie danych.
	* **Zautomatyzowane podejmowanie decyzji, w tym profilowanie**: Operacje przetwarzania prowadzone w kontekście modeli sztucznej inteligencji mogą wchodzić w zakres art. 22 RODO, który nakłada dodatkowe obowiązki na administratorów i zapewnia dodatkowe zabezpieczenia osobom, których dane dotyczą. EROD przypomina w tym względzie swoje Wytyczne w sprawie zautomatyzowanego indywidualnego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679[[14]](#footnote-15) .
	* **Zgodność celów**: Art. 6 ust. 4 RODO przewiduje, w odniesieniu do niektórych podstaw prawnych, kryteria, które administrator powinien wziąć pod uwagę, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, dla którego dane osobowe zostały pierwotnie zebrane. Przepis ten może mieć znaczenie w kontekście opracowywania i wdrażania modeli sztucznej inteligencji, a jego zastosowanie powinno zostać ocenione przez organy nadzorcze.
	* **Oceny skutków dla ochrony danych**  (art. 35 RODO): Oceny skutków dla ochrony danych są ważnym elementem rozliczalności, gdy przetwarzanie w kontekście modeli sztucznej inteligencji może spowodować wysokie ryzyko dla praw i wolności osób fizycznych[[15]](#footnote-16) .
	* **Zasada uwzględniania ochrony danych w fazie projektowania** (art. 25 ust. 1 RODO): Ochrona danych w fazie projektowania jest podstawowym zabezpieczeniem, które ma być oceniane przez organy nadzorcze w kontekście opracowywania i wdrażania modelu sztucznej inteligencji.

## Kluczowe pojęcia

18. Na wstępie EROD pragnie przedstawić wyjaśnienia dotyczące terminologii i pojęć, których używa w niniejszej opinii, i wyłącznie do celów niniejszej opinii:

* "**Dane własne**" odnoszą się do danych osobowych, które administrator zebrał od osób, których dane dotyczą.
* "**Dane osób trzecich**" odnoszą się do danych osobowych, których administratorzy nie uzyskali od osób, których dane dotyczą, ale które zebrali lub otrzymali od strony trzeciej, na przykład od brokera danych lub zebrali za pomocą pozyskiwania danych ze stron internetowych.
* "**Web scraping**" to powszechnie stosowana technika zbierania informacji z publicznie dostępnych źródeł internetowych. Informacje pozyskane na przykład z serwisów informacyjnych, mediów społecznościowych, forów dyskusyjnych i osobistych stron internetowych mogą zawierać dane osobowe.
* Wniosek odnosi się do **"cyklu życia" modeli AI**, a także do różnych etapów dotyczących między innymi "tworzenia", "rozwoju", "szkolenia", "aktualizacji", "dostrajania", "działania" lub "fazy poszkoleniowej" modeli AI. EROD przyznaje, że w zależności od okoliczności takie etapy mogą mieć miejsce podczas opracowywania i wdrażania modeli AI i mogą obejmować przetwarzanie danych osobowych do różnych celów przetwarzania. Niemniej jednak do celów niniejszej opinii EROD uważa, że ważne jest usprawnienie kategoryzacji etapów, które mogą wystąpić. W związku z tym na potrzeby niniejszej opinii EROD odnosi się do "**fazy opracowywania**" i "**fazy wdrażania**". Opracowanie modelu sztucznej inteligencji obejmuje wszystkie etapy przed jakimkolwiek wdrożeniem modelu sztucznej inteligencji i obejmuje między innymi opracowanie kodu, gromadzenie szkoleniowych danych osobowych, wstępne przetwarzanie szkoleniowych danych osobowych oraz szkolenie. Wdrożenie modelu AI obejmuje wszystkie etapy związane z wykorzystaniem modelu AI i może obejmować wszelkie operacje przeprowadzone po fazie opracowywania. EROD jest świadoma różnorodności przypadków użycia i ich potencjalnych konsekwencji w zakresie przetwarzania danych osobowych; w związku z tym organy nadzorcze powinny rozważyć, czy uwagi przedstawione w niniejszej opinii są istotne dla przetwarzania, które jest przedmiotem ich oceny.
* EROD podkreśla również, że w razie potrzeby termin "**szkolenie**" odnosi się do części fazy opracowywania, w której modele sztucznej inteligencji uczą się na podstawie danych, aby wykonać zamierzone zadanie (jak wyjaśniono w następnej sekcji niniejszej opinii).
* Pojęcie i zakres **modeli sztucznej** inteligencji, tak jak są one rozumiane przez EROD do celów niniejszej opinii, zostały szczegółowo określone w poniższej sekcji.

## Modele sztucznej inteligencji w kontekście opinii

1. Unijny akt o sztucznej inteligencji ("**AI** **Act**")[[16]](#footnote-17) definiuje "system sztucznej inteligencji" jako "*system* maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne"[[17]](#footnote-18) . Motyw (12) aktu o sztucznej inteligencji wyjaśnia dalej pojęcie "systemu AI". W związku z tym kluczową cechą systemów AI jest ich zdolność do wnioskowania.

Techniki, które umożliwiają wnioskowanie podczas tworzenia systemu sztucznej inteligencji, obejmują uczenie maszynowe, podejścia oparte na logice i wiedzy.

1. Z drugiej strony "modele AI" są jedynie pośrednio zdefiniowane w akcie o sztucznej inteligencji: "Chociaż modele AI są zasadniczymi elementami systemów AI, nie stanowią same w sobie systemów AI. Aby model AI mógł stać się systemem AI należy dodać do niego dodatkowe elementy, takie jak na przykład interfejs użytkownika. Modele AI są zwykle zintegrowane z systemami AI i stanowią ich część.*"[[18]](#footnote-19) .*
2. EROD rozumie, że definicja modelu sztucznej inteligencji zaproponowana we wniosku jest węższa niż ta zawarta w akcie o sztucznej inteligencji, ponieważ odnosi się do *"*modelu sztucznej inteligencji*"* jako "*obejmującego produkt wynikający z mechanizmów szkoleniowych, które są stosowane do zestawu danych szkoleniowych, w kontekście sztucznej inteligencji, uczenia maszynowego, głębokiego uczenia się lub innych powiązanych kontekstów przetwarzania"*, a ponadto precyzuje, że "*termin ten ma zastosowanie do modeli sztucznej inteligencji, które mają być poddawane dalszemu szkoleniu, dostrajaniu lub rozwojowi, a także do modeli sztucznej inteligencji, które nie mają podlegać takim operacjom*"[[19]](#footnote-20) .
3. Na tej podstawie EROD przyjęła niniejszą opinię przy założeniu, że system sztucznej inteligencji będzie polegał na modelu sztucznej inteligencji w celu osiągnięcia zamierzonego celu poprzez włączenie modelu do szerszych ram (np. system sztucznej inteligencji do obsługi klienta może wykorzystywać model sztucznej inteligencji wyszkolony na podstawie historycznych danych konwersacji w celu udzielania odpowiedzi na zapytania użytkowników).
4. Ponadto modele sztucznej inteligencji (lub "**modele**") istotne dla niniejszej opinii to modele opracowane w procesie szkolenia. Taki proces szkolenia jest częścią fazy opracowywanie, w której modele uczą się na podstawie danych, aby wykonać zamierzone zadanie. W związku z tym proces szkolenia wymaga zbioru danych, na podstawie których model będzie identyfikował i "uczył się" wzorców. W takich przypadkach model wykorzysta różne techniki do zbudowania reprezentacji wiedzy wyodrębnionej ze zbioru danych szkoleniowych. Dotyczy to w szczególności uczenia maszynowego.
5. W praktyce każdy model sztucznej inteligencji jest algorytmem, którego działanie jest określone przez zestaw elementów. Przykładowo, modele głębokiego uczenia często mają postać sieci neuronowej z wieloma warstwami składającymi się z węzłów połączonych krawędziami, które mają wagi, które są dostosowywane podczas uczenia, aby nauczyć się relacji między wejściami i wyjściami. Cechy prostego modelu głębokiego uczenia to: (i) typ i rozmiar każdej warstwy, (ii) waga przypisana do każdej krawędzi (czasami nazywana "parametrami"), (iii) funkcje aktywacji[[20]](#footnote-21) między warstwami i ewentualnie (iv) inne operacje, które mogą mieć miejsce między warstwami. Na przykład, podczas trenowania prostego modelu głębokiego uczenia się do klasyfikacji obrazów, dane wejściowe ("**piksele obrazu**") będą powiązane z danymi wyjściowymi, a wagi mogą być dostosowywane, tak aby przez większość czasu generować prawidłowe dane wyjściowe.
6. Inne przykłady modeli głębokiego uczenia się obejmują LLM i generatywną sztuczną inteligencję, które są wykorzystywane np. do generowania treści podobnych do tych tworzonych przez człowieka i tworzenia nowych danych.
7. **W oparciu o powyższe rozważania, zgodnie z wnioskiem, zakres niniejszej opinii obejmuje jedynie podzbiór modeli sztucznej inteligencji, które są wynikiem szkolenia takich modeli z wykorzystaniem danych osobowych.**

# Istota wniosku

## Charakter modeli sztucznej inteligencji w odniesieniu do definicji danych osobowych

1. Artykuł 4 ust. 1 RODO definiuje dane osobowe jako "*wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*" (tj. osoby, której dane dotyczą). Ponadto motyw 26 RODO stanowi, że zasady ochrony danych nie powinny mieć zastosowania do informacji anonimowych, a mianowicie informacji, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, biorąc pod uwagę "wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane" przez administratora lub inną osobę. Obejmuje to: (i) dane, które nigdy nie były związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną; oraz (ii) dane osobowe, które zostały zanonimizowane w taki sposób, że osoba, której dane dotyczą, nie jest lub nie jest już możliwa do zidentyfikowania.
2. W związku z tym na pytanie 1[[21]](#footnote-22) zawarte we wniosku można odpowiedzieć, analizując, czy model sztucznej inteligencji powstały w wyniku szkolenia, które obejmuje przetwarzanie danych osobowych, powinien we wszystkich przypadkach być uznawany za anonimowy. W oparciu o sformułowanie pytania EROD odniesie się w tej sekcji do procesu "szkolenia" modelu AI.
3. Przede wszystkim EROD pragnie przedstawić następujące ogólne uwagi. Modele sztucznej inteligencji, niezależnie od tego, czy są szkolone z wykorzystaniem danych osobowych, czy też nie, są zazwyczaj zaprojektowane do prognozowania lub wyciągania wniosków, tj. są zaprojektowane do wnioskowania. Co więcej, modele sztucznej inteligencji trenowane z wykorzystaniem danych osobowych są często zaprojektowane do wyciągania wniosków na temat osób innych niż te, których dane osobowe zostały wykorzystane do trenowania modelu sztucznej inteligencji. Niektóre modele sztucznej inteligencji są jednak specjalnie zaprojektowane do dostarczania danych osobowych dotyczących osób, których dane osobowe zostały wykorzystane do szkolenia modelu, lub w jakiś sposób do udostępniania takich danych. W takich przypadkach takie modele sztucznej inteligencji będą z natury (i zazwyczaj koniecznie) zawierać informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a zatem będą obejmować przetwarzanie danych osobowych. W związku z tym tego rodzaju modeli AI nie można uznać za anonimowe. Dotyczy to na przykład (i) modelu generatywnego dostrojonego na podstawie nagrań głosowych danej osoby w celu naśladowania jej głosu; lub (ii) dowolnego modelu zaprojektowanego tak, aby odpowiadał danymi osobowymi ze szkolenia, gdy zostanie poproszony o podanie informacji dotyczących konkretnej osoby.
4. W oparciu o powyższe rozważania, odpowiadając na pytanie 1 z wniosku, EROD koncentruje się na sytuacji modeli sztucznej inteligencji, które nie są zaprojektowane w celu dostarczania danych osobowych związanych z danymi szkoleniowymi.
5. EROD uważa, że nawet jeżeli model sztucznej inteligencji nie został celowo zaprojektowany do generowania informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej z danych szkoleniowych, informacje ze szkoleniowego zbioru danych, w tym dane osobowe, mogą nadal pozostać "wchłonięte" przez parametry modelu, a mianowicie reprezentowane przez obiekty matematyczne. Mogą one różnić się od oryginalnych punktów danych szkoleniowych, ale nadal mogą zachowywać oryginalne informacje z tych danych, które ostatecznie mogą zostać wyodrębnione lub w inny sposób uzyskane, bezpośrednio lub pośrednio, z modelu. W każdym przypadku, gdy informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, których dane osobowe zostały wykorzystane do szkolenia modelu, można uzyskać z modelu sztucznej inteligencji za pomocą rozsądnie prawdopodobnych sposobów, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane, można stwierdzić, że taki model nie jest anonimowy.
6. W tym względzie we wniosku stwierdzono, że "*istniejące publikacje badawcze podkreślają pewne potencjalne luki, które mogą istnieć w modelach sztucznej inteligencji, które mogą skutkować przetwarzaniem danych osobowych,[[22]](#footnote-23) , a także przetwarzaniem danych osobowych, które może mieć miejsce, gdy modele są wdrażane do użytku z innymi danymi, za pośrednictwem interfejsów programowania aplikacji (****"API"****) lub* interfejsów *"prompt"*"[[23]](#footnote-24) .
7. W tym samym duchu, badania nad ekstrakcją danych szkoleniowych są szczególnie dynamiczne[[24]](#footnote-25) . Pokazują one, że w niektórych przypadkach możliwe jest wykorzystanie środków, które z dużym prawdopodobieństwem pozwolą na wydobycie danych osobowych z niektórych modeli sztucznej inteligencji lub po prostu przypadkowe uzyskanie danych osobowych w wyniku interakcji z modelem sztucznej inteligencji (na przykład w ramach systemu sztucznej inteligencji). Ciągłe wysiłki badawcze w tej dziedzinie pomogą w dalszej ocenie ryzyka szczątkowego związanego z regurgitacją[[25]](#footnote-26) i pozyskiwaniem danych osobowych w każdym konkretnym przypadku.
8. **W oparciu o powyższe rozważania EROD uważa, że modele sztucznej inteligencji szkolone na danych osobowych nie mogą we wszystkich przypadkach być uznawane za anonimowe. Zamiast tego ustalenie, czy model sztucznej inteligencji jest anonimowy, powinno być oceniane indywidualnie w oparciu o określone kryteria.**

## Okoliczności, w których modele sztucznej inteligencji można uznać za anonimowe i związane z tym wykazanie

1. W odniesieniu do pytania 1 z wniosku[[26]](#footnote-27) , EROD proszona jest o wyjaśnienie okoliczności, w których model sztucznej inteligencji, który został wyszkolony z wykorzystaniem danych osobowych, można uznać za anonimowy. W odniesieniu do pytania 1(i)(a) z wniosku[[27]](#footnote-28) , EROD proszona jest o wyjaśnienie, jakie dowody lub dokumentację organy nadzorcze powinny wziąć pod uwagę przy ocenie, czy model sztucznej inteligencji jest anonimowy.

### 3.2.1 Ogólne rozważania dotyczące anonimizacji w omawianym kontekście.

1. Użycie wyrażenia " *informacje*" w definicji "*danych osobowych*" w art. 4 ust. 1 RODO odzwierciedla cel przypisania temu pojęciu szerokiego zakresu, który obejmuje wszystkie rodzaje informacji, pod warunkiem, że "*odnoszą się" one do* osoby, której dane dotyczą, która jest zidentyfikowana lub może zostać zidentyfikowana bezpośrednio lub pośrednio.
2. Informacje mogą odnosić się do osoby fizycznej, nawet jeśli są technicznie zorganizowane lub zakodowane (na przykład w formacie nadającym się wyłącznie do odczytu maszynowego, zastrzeżonym lub otwartym) w sposób, który nie sprawia, że związek z tą osobą fizyczną jest natychmiast widoczny. W takich przypadkach aplikacje mogą być wykorzystywane do łatwej identyfikacji, rozpoznawania i wyodrębniania określonych danych. Jest to szczególnie widoczne w przypadku modeli sztucznej inteligencji, w których parametry reprezentują statystyczne zależności między danymi szkoleniowymi i w których istnieje możliwość wyodrębnienia dokładnych lub niedokładnych (ponieważ wywnioskowanych statystycznie) danych osobowych, bezpośrednio z relacji między danymi zawartymi w modelu lub poprzez odpytywanie modelu.
3. Modele sztucznej inteligencji zwykle nie zawierają danych, które można bezpośrednio wyodrębnić lub powiązać, ale raczej parametry reprezentujące probabilistyczne relacje między danymi zawartymi w modelu. Nie mniej jednak w realistycznych scenariuszach może być możliwe wywnioskowanie informacji[[28]](#footnote-29) z modelu, takich jak wnioskowanie o członkostwie. Dlatego, aby organ nadzorczy mógł zgodzić się z administratorem, że dany model sztucznej inteligencji można uznać za anonimowy, powinien przynajmniej sprawdzić, czy otrzymał wystarczające dowody na to, że przy użyciu rozsądnych środków: (i) nie można wyodrębnić z modelu danych osobowych związanych z danymi szkoleniowymi[[29]](#footnote-30) ; oraz (ii) żadne dane wyjściowe generowane w wyniku zapytań do modelu nie odnoszą się do osób, których dane osobowe zostały wykorzystane do szkolenia modelu.
4. Trzy elementy powinny być brane pod uwagę przez organy nadzorcze, aby ocenić, czy te warunki zostały spełnione.
5. Po pierwsze organy nadzorcze powinny wziąć pod uwagę elementy określone w najnowszych opiniach Grupy Roboczej Art. 29 lub wytycznych Europejskiej Rady Ochrony Danych dotyczących tej kwestii. W odniesieniu do anonimizacji, na dzień wydania niniejszej opinii, organy nadzorcze powinny wziąć pod uwagę elementy zawarte w opinii Grupy Roboczej Art. 29 nr 05/2014 w sprawie technik anonimizacji (**"opinia Grupy Roboczej Art. 29 nr 05/2014"**), w której stwierdza się, że jeżeli nie jest możliwe wyodrębnienie, powiązanie i wywnioskowanie informacji z rzekomo anonimowego zbioru danych, dane można uznać za anonimowe[[30]](#footnote-31) . Stwierdza się w niej również, że "*w każdym przypadku, gdy wniosek nie spełnia jednego z kryteriów, należy* przeprowadzić *dokładną ocenę ryzyka związanego z identyfikacją*”[[31]](#footnote-32) . **Biorąc pod uwagę wyżej wspomniane prawdopodobieństwo wyodrębnienia i wnioskowania, EROD uważa, że modele sztucznej inteligencji z dużym prawdopodobieństwem będą wymagały tak dokładnej oceny ryzyka identyfikacji.**
6. Po drugie ocena ta powinna zostać przeprowadzona z uwzględnieniem "*wszystkich środków, które z uzasadnionym prawdopodobieństwem mogą zostać użyte*" przez administratora lub inną osobę w celu zidentyfikowania osób fizycznych[[32]](#footnote-33) , a określenie tych środków powinno opierać się na obiektywnych czynnikach, jak wyjaśniono w motywie 26 RODO, które mogą obejmować:
	* + 1. charakterystykę samych danych szkoleniowych, modelu sztucznej inteligencji i procedury szkoleniowej[[33]](#footnote-34)

;

* + - 1. kontekst, w którym model AI jest udostępniany i/lub przetwarzany ;[[34]](#footnote-35)
			2. dodatkowe informacje, które umożliwiłyby identyfikację i mogą być dostępne dla danej osoby;
			3. koszty i czas, jaki dana osoba musiałaby poświęcić na uzyskanie takich dodatkowych informacji (jeżeli nie są one jeszcze dla niej dostępne) ; oraz[[35]](#footnote-36)
			4. dostępne technologie w czasie przetwarzania, jak również rozwój technologiczny[[36]](#footnote-37) .
1. Po trzecie organy nadzorcze powinny rozważyć, czy administratorzy dokonali oceny ryzyka identyfikacji zarówno przez administratora jak i przez różne rodzaje "*innych osób*", w tym niezamierzone osoby trzecie uzyskujące dostęp do modelu sztucznej inteligencji. Należy również uwzględnić, czy te osoby mogą być racjonalnie uznane za zdolne do uzyskania dostępu lub przetwarzania danych, o których mowa.
2. **Podsumowując, EROD uważa, że aby model sztucznej inteligencji można było uznać za anonimowy, przy użyciu rozsądnych środków zarówno (i) prawdopodobieństwo bezpośredniego (w tym probabilistycznego) wyodrębnienia danych osobowych dotyczących osób, których dane osobowe zostały użyte do szkolenia modelu, jak i (ii) prawdopodobieństwo uzyskania takich danych osobowych w wyniku zapytań, celowo lub nie, powinny być znikome[[37]](#footnote-38) dla każdej osoby, której dane dotyczą**. **Domyślnie organy nadzorcze powinny zakładać, że modele sztucznej inteligencji wymagają dokładnej oceny prawdopodobieństwa identyfikacji, aby móc wyciągnąć wnioski na temat ich potencjalnie anonimowego charakteru.** Ocena tego prawdopodobieństwa powinna uwzględniać **"*wszystkie środki, które mogą być racjonalnie użyte*" przez administratora lub inną osobę, a także niezamierzone (ponowne) użycie lub ujawnienie modelu.**

### 3.2.2. Elementy służące do oceny szczątkowego prawdopodobieństwa identyfikacji

1. Chociaż środki mogą być podejmowane zarówno na etapie tworzenia, jak i wdrażania modelu AI w celu zmniejszenia prawdopodobieństwa uzyskania danych osobowych z modelu AI, ocena anonimowości modelu sztucznej inteligencji powinna również uwzględniać możliwość bezpośredniego dostępu do modelu.
2. Ponadto, organy nadzorcze powinny ocenić, indywidualnie w każdym przypadku, czy środki wdrożone przez administratora w celu zapewnienia i udowodnienia, że model sztucznej inteligencji jest anonimowy, są odpowiednie i skuteczne.
3. W szczególności, wnioski z oceny organu nadzorczego (SA) mogą różnić się w przypadku modelu AI dostępnego publicznie, który jest dostępny dla nieznanej liczby osób i nieznanych metod wyodrębniania danych osobowych, a modelu AI wewnętrznego, dostępnego tylko dla pracowników. Chociaż w obu przypadkach organy nadzorcze powinny zweryfikować, czy administratorzy wywiązali się z obowiązku rozliczalności na mocy art. 5 ust. 2 i art. 24 RODO, "*środki, co do których istnieje uzasadnione prawdopodobieństwo, że zostaną użyte*" przez inne osoby, mogą mieć wpływ na zakres i charakter możliwych scenariuszy, które należy wziąć pod uwagę. W związku z tym, w zależności od kontekstu opracowania i wdrożenia modelu, organy nadzorcze mogą rozważyć różne poziomy testowania i odporności na ataki.
4. W tym względzie EROD przedstawia poniżej nienormatywną i niewyczerpującą listę możliwych elementów, które mogą być brane pod uwagę przez organy nadzorcze podczas oceny twierdzenia administratora o anonimowości.. Inne podejścia mogą być możliwe, jeżeli zapewniają równoważny stopień ochrony, w szczególności biorąc pod uwagę aktualny stan wiedzy.
5. Obecność lub brak wymienionych poniżej elementów nie jest rozstrzygającym kryterium oceny anonimowości modelu sztucznej inteligencji.

#### 3.2.2.1 Projektowanie modeli AI

1. Jeśli chodzi o projektowanie modeli sztucznej inteligencji, organy nadzorcze powinny ocenić podejścia przyjęte przez administratorów w fazie opracowywania. W tym względzie należy rozważyć zastosowanie i skuteczność czterech kluczowych obszarów (określonych poniżej).

Wybór źródeł

1. Pierwszy obszar oceny obejmuje analizę wyboru źródeł wykorzystywanych do trenowania modelu sztucznej inteligencji. W tym zakresie organy nadzorcze powinny ocenić wszelkie kroki podjęte w celu uniknięcia lub ograniczenia gromadzenia danych osobowych, w tym między innymi (i) stosowności kryteriów wyboru; (ii) trafności i adekwatności wybranych źródeł, biorąc pod uwagę zamierzony cel (cele); oraz (iii) czy wykluczono nieodpowiednie źródła*.*

### Przygotowanie i minimalizacja danych

1. Drugi obszar oceny dotyczy przygotowania danych do fazy szkoleniowej. Organy nadzorcze powinny w szczególności zbadać: (i) czy rozważono wykorzystanie danych anonimowych i/lub danych osobowych, które zostały poddane pseudonimizacji; oraz (ii) w przypadku podjęcia decyzji o niestosowaniu takich środków, powody tej decyzji, biorąc pod uwagę zamierzony cel; (iii) strategie i techniki minimalizacji danych zastosowane w celu ograniczenia ilości danych osobowych uwzględnionych w procesie szkolenia; oraz (iv) wszelkie procesy filtrowania danych wdrożone przed szkoleniem modelu w celu usunięcia nieistotnych danych osobowych.

### Wybory metodologiczne dotyczące szkolenia

1. Trzeci obszar oceny dotyczy wyboru solidnych metod opracowywania modeli sztucznej inteligencji. Niezależne organy nadzorcze powinny ocenić wybory metodologiczne, które mogą znacznie zmniejszyć lub wyeliminować możliwość identyfikacji, w tym między innymi: (i) czy metodologia ta wykorzystuje metody regularyzacji w celu poprawy generalizacji modelu i zmniejszenia przeuczenia (overfitting); oraz, co najważniejsze, (ii) czy administrator wdrożył odpowiednie i skuteczne techniki ochrony prywatności (np. prywatność różnicową).

### Środki dotyczące wyników modelu

1. Ostatni obszar oceny dotyczy wszelkich metod lub środków dodanych do samego modelu sztucznej inteligencji, które mogą nie mieć wpływu na ryzyko bezpośredniego wyodrębnienia danych osobowych z modelu przez przez osoby mające do niego bezpośredni dostęp ale które mogą zmniejszyć prawdopodobieństwo uzyskania danych osobowych związanych z danymi szkoleniowymi na podstawie zapytań.

#### 3.2.2.2. Analiza modelu AI

1. Aby organy nadzorcze mogły ocenić solidność zaprojektowanego modelu sztucznej inteligencji pod względem anonimizacji, pierwszym krokiem jest upewnienie się, że projekt został opracowany zgodnie z planem i podlega skutecznemu zarządzaniu inżynieryjnemu. Organy nadzorcze powinny ocenić, czy administratorzy przeprowadzili audyty oparte na dokumentach (wewnętrzne lub zewnętrzne), które obejmują ocenę wybranych środków i ich wpływu na ograniczenie prawdopodobieństwa identyfikacji. Może to obejmować analizę raportów z przeglądów kodu, a także analizę teoretyczną dokumentującą stosowność wybranych środków, mających na celu zmniejszenie prawdopodobieństwa ponownej identyfikacji danego modelu.

#### 3.2.2.3 Testowanie modeli AI i odporność na ataki

1. Wreszcie, organy nadzorcze powinny wziąć pod uwagę zakres, częstotliwość, ilość i jakość testów, które administrator przeprowadził na modelu. W szczególności, organy nadzorcze powinny uwzględnić fakt, że pomyślne testowanie, które obejmuje szeroko znane, nowoczesne ataki, może stanowić jedynie dowód na odporność na te ataki.. Na dzień wydania niniejszej opinii może to obejmować, między innymi, strukturalne testowanie pod kątem: (i) wnioskowania o atrybutach i członkostwie; (ii) eksfiltracji; (iii) regurgitacji danych szkoleniowych; (iv) inwersji modelu; lub (v) ataków rekonstrukcyjnych.

#### 3.2.2.4 Dokumentacja

1. Artykuły 5, 24, 25 i 30 RODO a w przypadkach, gdy istnieje prawdopodobne wysokie ryzyko dla praw i wolności osób, których dane dotyczą, art. 35 RODO, wymagają od administratorów odpowiedniego dokumentowania swoich operacji przetwarzania. Dotyczy to również każdego przetwarzania, które obejmuje szkolenie modelu sztucznej inteligencji, nawet jeśli celem przetwarzania jest anonimizacja. Organy nadzorcze powinny wziąć pod uwagę taką dokumentację i wszelkie regularne oceny ryzyka związanego z przetwarzaniem prowadzonym przez administratorów, ponieważ są to podstawowe kroki mające na celu wykazanie, że dane osobowe nie są przetwarzane.
2. **EROD uważa, że organy nadzorcze powinny uwzględniać dokumentację za każdym razem, gdy konieczna jest ocena twierdzenia o anonimowości w odniesieniu do danego modelu sztucznej inteligencji. EROD zauważa, że jeżeli organ nadzorczy nie jest w stanie potwierdzić, po dokonaniu oceny twierdzenia o anonimowości, w tym w świetle dokumentacji, że podjęto skuteczne środki w celu zanonimizowania modelu AI, organ nadzorczy może uznać, że administrator nie wypełnił swoich obowiązków w zakresie rozliczalności na mocy art. 5 ust. 2 RODO. W związku z tym należy również rozważyć zgodność z innymi przepisami RODO.**
3. Najlepiej byłoby, gdyby organy nadzorcze zweryfikowały, czy dokumentacja administratora zawiera:
	1. wszelkie informacje dotyczące ocen wpływu na ochronę dla ochrony danych (),, w tym wszelkie oceny i decyzje, w których stwierdzono, że ocena wpływu skutku dla ochrony danych nie była konieczna;
	2. wszelkie porady lub opinie przekazane przez inspektora ochrony danych ("**IOD**") (w przypadku, gdy IOD został - lub powinien zostać - wyznaczony);
	3. informacje na temat środków technicznych i organizacyjnych podjętych podczas projektowania modelu sztucznej inteligencji w celu zmniejszenia prawdopodobieństwa identyfikacji, w tym modelu zagrożeń i ocen ryzyka, na których opierają się te środki. Powinno to obejmować konkretne środki dla każdego źródła zbiorów danych szkoleniowych, w tym odpowiednie adresy URL źródeł i opisy podjętych środków (lub już podjętych przez dostawców zbiorów danych stron trzecich);
	4. środki techniczne i organizacyjne podjęte na wszystkich etapach cyklu życia modelu, które przyczyniły się lub potwierdziły brak danych osobowych w modelu;
	5. dokumentację wykazującą dokumentację wykazującą teoretyczną odporność modelu sztucznej inteligencji na techniki ponownej identyfikacji, a także środki kontrolne zaprojektowane w celu ograniczenia lub oceny powodzenia i wpływu głównych ataków (takich jak regurgitacja, ataki związane z członkostwem, eksfiltracja itp.) Może to obejmować w szczególności: (i) stosunek między ilością danych szkoleniowych a liczbą parametrów w modelu, w tym analizę jego wpływu na model ; (ii) wskaźniki prawdopodobieństwa ponownej identyfikacji w oparciu o aktualny stan wiedzy; (iii) raporty dotyczące sposobu testowania modelu (przez kogo, kiedy, w jaki sposób i w jakim zakresie) oraz (iv) wyniki testów[[38]](#footnote-39) ;
	6. dokumentację przekazaną administratorowi(om)administratorowi(-om) wdrażającemu (-ym) model i/lub osobom, których dane dotyczą, w szczególności dokumentację dotyczącą podjętych środków mających na celu zmniejszenia prawdopodobieństwa identyfikacji oraz dotyczącą ewentualnych ryzyk resztkowych.

# 3.3. Odpowiedniość prawnie uzasadnionego interesu jako podstawy prawnej przetwarzania danych osobowych w kontekście opracowywania i wdrażania modeli AI

1. Aby odpowiedzieć na pytania 2 i 3 zawarte we wniosku, EROD najpierw przedstawi ogólne uwagi dotyczące niektórych ważnych aspektów, które organy nadzorcze powinny wziąć pod uwagę, niezależnie od podstawy prawnej przetwarzania, oceniając, w jaki sposób administratorzy mogą wykazać zgodność z RODO w kontekście modeli sztucznej inteligencji. Następnie, opierając się na Wytycznych 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO[[39]](#footnote-40) , EROD rozważy trzy kroki wymagane w ramach oceny prawnie uzasadnionego interesu w kontekście opracowywania i wdrażania modeli sztucznej inteligencji.
	1.

### Uwagi ogólne

1. EROD przypomina, że RODO nie ustanawia żadnej hierarchii między różnymi podstawami prawnymi

określonymi w art. 6 ust. 1 RODO[[40]](#footnote-41) .

1. W art. 5 RODO określono zasady dotyczące przetwarzania danych osobowych. EROD podkreśla te, które są istotne dla niniejszej opinii i które powinny być przynajmniej uwzględnione przez organy nadzorcze przy ocenie konkretnych modeli sztucznej inteligencji, a także najistotniejsze wymogi wynikające z innych przepisów RODO, z uwzględnieniem zakresu niniejszej opinii.
2. **Zasada rozliczalności** (art. 5 ust. 2 RODO) - zasada ta stanowi, że administrator danych jest odpowiedzialny za zgodność z RODO i jest w stanie ją wykazać. W związku z tym role i obowiązki stron przetwarzających dane osobowe w kontekście opracowywania lub wdrażania modelu sztucznej inteligencji należy ocenić przed rozpoczęciem przetwarzania, aby od samego początku określić obowiązki administratorów lub współadministratorów oraz podmiotów przetwarzających (jeśli istnieją).
3. **Zasady zgodności z prawem, rzetelności i przejrzystości** (art. 5 ust. 1 lit. a) RODO) - Oceniając zgodność z prawem przetwarzania w kontekście modeli sztucznej inteligencji, w świetle art. 6 ust. 1 RODO, EROD uważa za przydatne rozróżnienie różnych etapów przetwarzania danych osobowych[[41]](#footnote-42) . Zasada rzetelności, która jest ściśle powiązana z zasadą przejrzystości, wymaga, aby dane osobowe nie były przetwarzane nierzetelnymi metodami, podstępem lub w sposób, który jest " „bezzasadnie szkodliwy, bezprawnie dyskryminujący, nieoczekiwany *lub* wprowadzający w błąd osobę, której dane dotyczą[[42]](#footnote-43) . Biorąc pod uwagę złożoność stosowanych technologii, informacje na temat przetwarzania danych osobowych w ramach modeli sztucznej inteligencji powinny być zatem przekazywane w sposób dostępny, zrozumiały i przyjazny dla użytkownika[[43]](#footnote-44) . Przejrzystość w zakresie przetwarzania danych osobowych obejmuje w szczególności spełnienie obowiązków informacyjnych określonych w art. 12-14 RODO[[44]](#footnote-45), które wymagają również, w przypadku zautomatyzowanego podejmowania decyzji, w tym profilowania, dostarczenia istotnych informacji na temat zastosowanej logiki, a także znaczenia i przewidywanych konsekwencji przetwarzania dla osoby, której dane dotyczą[[45]](#footnote-46). Mając na uwadze, że fazy opracowywania modeli sztucznej inteligencji mogą wiązać się z gromadzeniem dużych ilości danych z publicznie dostępnych źródeł (takich jak techniki web scrapingu), powoływanie się na wyjątek przewidziany w art. 14 ust. 5 lit. b) RODO jest ściśle ograniczone do sytuacji, gdy wymogi tego przepisu są w pełni spełnione[[46]](#footnote-47) .
4. **Zasady ograniczenia celu i minimalizacji danych** (art. 5 ust. 1 lit. b), c) RODO) - Zgodnie z zasadą minimalizacji danych opracowanie i wdrożenie modeli sztucznej inteligencji wymaga, aby dane osobowe były adekwatne, stosowne i niezbędne w stosunku do celu. Może to obejmować przetwarzanie danych osobowych w celu uniknięcia ryzyka potencjalnych uprzedzeń i błędów, gdy jest to jasno i wyraźnie określone w celu, a dane osobowe są niezbędne do (np. nie można skutecznie osiągnąć poprzez przetwarzanie innych danych, w tym danych syntetycznych lub zanonimizowanych)[[47]](#footnote-48) . Grupa Robocza Art. 29 podkreśliła już, że "cel gromadzenia danych musi być jasno i wyraźnie określony "[[48]](#footnote-49) . Oceniając, czy realizowany cel jest zgodny z prawem, konkretny i wyraźny oraz czy przetwarzanie jest zgodne z zasadą minimalizacji danych, należy najpierw zidentyfikować daną czynność przetwarzania. W niektórych przypadkach możliwe jest określenie celu, który będzie realizowany podczas wdrażania modelu sztucznej inteligencji na wczesnym etapie rozwoju. Nawet jeśli tak nie jest, pewien kontekst tego wdrożenia powinien być już jasny, a zatem należy rozważyć, w jaki sposób kontekst ten wpływa na cel rozwoju. Dokonując przeglądu celu przetwarzania na danym etapie rozwoju, organy nadzorcze powinny oczekiwać od administratora (administratorów) pewnego stopnia szczegółowości oraz wyjaśnienia, w jaki sposób te szczegóły wpływają na cel przetwarzania. Może to obejmować na przykład informacje na temat rodzaju opracowanego modelu sztucznej inteligencji, jego oczekiwanych funkcji i wszelkich innych istotnych kontekstów, które są już znane na tym etapie. Kontekst wdrożenia może również obejmować, na przykład, czy model jest opracowywany do wdrożenia wewnętrznego, czy administrator zamierza sprzedać lub udostępnić model osobom trzecim po jego opracowaniu, w tym czy model ma być przede wszystkim wykorzystywany do celów badawczych lub komercyjnych.
5. **Prawa osób, których dane dotyczą** (rozdział III RODO) - niezależnie od potrzeby zapewnienia przez organy nadzorcze poszanowania wszystkich praw osób, których dane dotyczą, podczas opracowywania i wdrażania modeli sztucznej inteligencji przez administratorów, EROD przypomina, że w każdym przypadku, gdy administrator powołuje się na prawnie uzasadniony interes jako podstawę prawną, zastosowanie ma prawo do sprzeciwu na mocy art. 21 RODO, które należy zapewnić[[49]](#footnote-50) .

# 3.3.2 Rozważania na temat trzech etapów oceny prawnie uzasadnionego interesu w kontekście rozwoju i wdrażania modeli sztucznej inteligencji

1. W celu ustalenia, czy przetwarzanie danych osobowych może opierać się na art. 6 ust. 1 lit. f) RODO, organy nadzorcze powinny sprawdzić, czy administratorzy dokładnie ocenili i udokumentowali, czy spełnione są łącznie trzy następujące warunki: (i) realizacja prawnie uzasadnionego interesu przez administratora lub przez stronę trzecią; (ii) przetwarzanie jest niezbędne do realizacji prawnie uzasadnionego interesu; oraz (iii) prawnie uzasadniony interes nie jest podrzędny wobec interesów lub podstawowych praw i wolności osób, których dane dotyczą[[50]](#footnote-51) .

### 3.3.2.1 Pierwszy krok - realizacja prawnie uzasadnionego interesu przez administratora lub osobę trzecią

1. Interes to szerszy interes lub korzyść, jaką administrator danych lub strona trzecia może odnieść w związku z zaangażowaniem się w określoną czynność przetwarzania[[51]](#footnote-52) . Podczas gdy RODO i TSUE uznały kilka interesów za uzasadnione[[52]](#footnote-53), ocena zasadności danego interesu powinna być wynikiem indywidualnej analizy każdego przypadku.
2. Jak przypomniała EROD w swoich Wytycznych w sprawie prawnie uzasadnionego interesu[[53]](#footnote-54) , interes można uznać za prawnie uzasadniony, jeżeli spełnione są łącznie następujące trzy kryteria:
	1. Interes jest zgodny] z prawem[[54]](#footnote-55) ;
	2. Interes jest jasno i precyzyjnie sformułowany; oraz
	3. Interes jest rzeczywisty i obecny, a nie spekulacyjny
3. Z zastrzeżeniem dwóch innych kroków wymaganych w ramach oceny prawnie uzasadnionego interesu, następujące przykłady mogą stanowić prawnie uzasadniony interes w kontekście modeli sztucznej inteligencji: (i) opracowanie usługi - konsultanta rozmawiającego z użytkownikiem w celu pomocy użytkownikom; (ii) opracowanie systemu sztucznej inteligencji w celu wykrywania oszukańczych treści lub zachowań; oraz (iii) poprawa wykrywania zagrożeń w systemie informatycznym.

#### 3.3.2.2 Krok drugi - Analiza konieczności przetwarzania w celu realizacji prawnie uzasadnionego interesu

1. Drugi etap oceny polega na ustaleniu, czy przetwarzanie danych osobowych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych interesów[[55]](#footnote-56) ("test konieczności").
2. Motyw 39 RODO wyjaśnia, że "*dane osobowe powinny być przetwarzane tylko wtedy, gdy cel przetwarzania nie może być osiągnięty w inny sposób"*. Zgodnie z TSUE i wcześniejszymi wytycznymi EROD, warunek dotyczący konieczności przetwarzania należy zbadać w świetle podstawowych praw i wolności osób, których dane dotyczą, oraz w związku z zasadą minimalizacji danych zapisaną w art. 5 ust. 1 lit. c) RODO[[56]](#footnote-57) .
3. Metodologia, do której odwołuje się TSUE, uwzględnia kontekst przetwarzania, a także skutki dla administratora i osób, których dane dotyczą. Ocena konieczności obejmuje zatem dwa elementy: (i) czy czynność przetwarzania pozwoli na realizację celu[[57]](#footnote-58); oraz (ii) czy nie istnieje mniej inwazyjny sposób realizacji tego celu[[58]](#footnote-59).
4. Na przykład, w zależności od przypadku, zamierzoną ilość danych osobowych zaangażowanych w model sztucznej inteligencji należy ocenić w świetle mniej inwazyjnych alternatyw, które mogą być racjonalnie dostępne, aby równie skutecznie osiągnąć cel realizowanego prawnie uzasadnionego interesu. Jeżeli osiągnięcie celu jest również możliwe za pomocą modelu sztucznej inteligencji, który nie wiąże się z przetwarzaniem danych osobowych, wówczas przetwarzanie danych osobowych należy uznać za niekonieczne. Jest to szczególnie istotne w przypadku opracowywania modeli sztucznej inteligencji. Oceniając, czy warunek niezbędności jest spełniony, organy nadzorcze powinny zwrócić szczególną uwagę na ilość przetwarzanych danych osobowych oraz na to, czy jest to proporcjonalne do realizacji prawnie uzasadnionego interesu, również w świetle zasady minimalizacji danych.
5. Ocena konieczności powinna również uwzględniać szerszy kontekst zamierzonego przetwarzania danych osobowych. Istnienie środków mniej ingerujących w podstawowe prawa i wolności osób, których dane dotyczą, może się różnić w zależności od tego, czy administrator danych ma bezpośredni związek z osobami, których dane dotyczą (dane własne), czy też nie (dane osoby trzeciej). TSUE przedstawił pewne uwagi, które należy wziąć pod uwagę przy analizie konieczności przetwarzania danych osób trzecich w celu realizacji prawnie uzasadnionych interesów (aczkolwiek w kontekście ujawniania takich danych osobom trzecim)[[59]](#footnote-60) .
6. Wdrożenie zabezpieczeń technicznych w celu ochrony danych osobowych może również przyczynić się do spełnienia testu konieczności. Może to obejmować na przykład wdrożenie środków, takich jak te określone w sekcji 3.2.2, w taki sposób, aby nie osiągnąć anonimizacji, ale nadal zmniejszać łatwość identyfikacji osób, których dane dotyczą. EROD zauważa, że niektóre z tych środków, jeśli nie są wymagane do zapewnienia zgodności z RODO, mogą stanowić dodatkowe zabezpieczenia, jak dalej przeanalizowano w podsekcji "środki łagodzące" w sekcji 3.3.2.3[[60]](#footnote-61) .

#### 3.3.2.3 Trzeci krok – test równowagi

1. Trzecim etapem oceny prawnie uzasadnionego interesu jest "**wyważenie**" (zwane również w niniejszym dokumencie "**testem równowagi**")[[61]](#footnote-62) . Etap ten polega na zidentyfikowaniu i opisaniu różnych przeciwstawnych praw i interesów, które są zaangażowane[[62]](#footnote-63) , tj. z jednej strony interesów, podstawowych praw i wolności osób, których dane dotyczą, a z drugiej strony interesów administratora lub strony trzeciej. Następnie należy rozważyć szczególne okoliczności sprawy, aby wykazać, że prawnie uzasadniony interes jest odpowiednią podstawą prawną dla przedmiotowych czynności przetwarzania[[63]](#footnote-64) .

### Interesy, podstawowe prawa i wolności osób, których dane dotyczą

1. Artykuł 6 ust. 1 lit. f) RODO stanowi, że oceniając różne elementy w kontekście testu równowagi, administrator powinien wziąć pod uwagę interesy, podstawowe prawa i wolności osób, których dane dotyczą. Interesy osób, których dane dotyczą, to te, na które może mieć wpływ przedmiotowe przetwarzanie. W kontekście fazy opracowywania modelu sztucznej inteligencji mogą one obejmować między innymi interes w samostanowieniu i zachowaniu kontroli nad własnymi danymi osobowymi (np. danymi zebranymi w celu opracowania modelu). W kontekście wdrożenia modelu sztucznej inteligencji interesy osób, których dane dotyczą, mogą obejmować między innymi interesy związane z zachowaniem kontroli nad własnymi danymi osobowymi (np. danymi przetwarzanymi po wdrożeniu modelu), interesy finansowe gdy model sztucznej inteligencji jest wykorzystywany przez osobę, której dane dotyczą, do generowania przychodów lub jest wykorzystywany przez osobę fizyczną w kontekście jej działalności zawodowej), korzyści osobiste (np. gdy model sztucznej inteligencji jest wykorzystywany do poprawy dostępności niektórych usług) lub interesy społeczno-gospodarcze (np. gdy model sztucznej inteligencji umożliwia dostęp do lepszej opieki zdrowotnej lub ułatwia korzystanie z prawa podstawowego, takiego jak dostęp do edukacji)[[64]](#footnote-65) .
2. Im bardziej precyzyjnie zostanie zdefiniowany interes w świetle zamierzonego celu przetwarzania, tym lepiej umożliwi to jasne zrozumienie rzeczywistych korzyści i zagrożeń, które należy wziąć pod uwagę w test równowagi.
3. W odniesieniu do podstawowych praw i wolności osób, których dane dotyczą, opracowywanie i wdrażanie modeli sztucznej inteligencji może wiązać się z poważnym ryzykiem dla praw chronionych Kartą praw podstawowych UE **("Karta praw podstawowych UE"**), w tym między innymi prawa do życia prywatnego i rodzinnego (art. 7 Karty praw podstawowych UE) oraz prawa do ochrony danych osobowych (art. 8 Karty praw podstawowych UE). Ryzyko to może wystąpić na etapie opracowywania, na przykład gdy dane osobowe są pobierane wbrew woli osób, których dane dotyczą, lub bez ich wiedzy. Ryzyko to może również wystąpić w fazie wdrażania, na przykład gdy dane osobowe są przetwarzane przez model (lub jako jego część) w sposób, który narusza prawa osób, których dane dotyczą, lub gdy możliwe jest wywnioskowanie, przypadkowo lub poprzez ataki (np. wnioskowanie o członkostwie, wyodrębnienie lub inwersję modelu), jakie dane osobowe są zawarte w uczącej się bazie danych. Takie sytuacje stanowią zagrożenie dla prywatności osób, których dane dotyczą, których dane mogą pojawić się w fazie wdrażania systemu sztucznej inteligencji (np. ryzyko utraty reputacji, kradzieży tożsamości lub oszustwa, ryzyko bezpieczeństwa w zależności od charakteru danych).
4. W zależności od rozpatrywanej sprawy mogą również istnieć zagrożenia dla innych praw podstawowych. Na przykład masowe gromadzenie danych przez modele sztucznej inteligencji w fazie opracowywania może stwarzać poczucie nadzoru dla osób, których dane dotyczą, zwłaszcza biorąc pod uwagę trudności w zapobieganiu gromadzeniu danych publicznych. Może to prowadzić do autocenzury osób fizycznych i stwarzać ryzyko naruszenia ich wolności wypowiedzi (art. 11 Karty praw podstawowych Unii Europejskiej). W fazie wdrożeniaj ryzyko dla wolności wypowiedzi występuje również wtedy, gdy modele AI są wykorzystywane do blokowania publikacji treści od osób, których dane dotyczą. Ponadto model sztucznej inteligencji zalecający osobom podatnym na zagrożenia nieodpowiednie treści może stanowić zagrożenie dla ich zdrowia psychicznego (art. 3 ust. 1 Karty praw podstawowych Unii Europejskiej). W innych przypadkach wdrożenie modeli AI może również prowadzić do negatywnych konsekwencji dla prawa danej osoby do podjęcia pracy (art. 15 Karty praw podstawowych Unii Europejskiej), na przykład gdy podania o pracę są wstępnie selekcjonowane przy użyciu modelu AI. W ten sam sposób model sztucznej inteligencji może stanowić zagrożenie dla prawa do niedyskryminacji (art. 21 Karty praw podstawowych UE), jeżeli dyskryminuje osoby fizyczne ze względu na pewne cechy osobiste (takie jak narodowość lub płeć).Ponadto, wdrażanie modeli AI może również stanowić zagrożenie dla bezpieczeństwa danej osoby (np. gdy model AI jest wykorzystywany w złych zamiarach), a także dla jej integralności fizycznej i psychicznej[[65]](#footnote-66) .
5. Wdrożenie modeli AI może mieć również pozytywny wpływ na niektóre prawa podstawowe, np. model może wspierać prawo do integralności psychicznej osoby (art. 3 Karty), na przykład gdy model AI jest wykorzystywany do identyfikowania szkodliwych treści w Internecie; lub model może ułatwiać dostęp do niektórych podstawowych usług lub ułatwiać korzystanie z praw podstawowych, takich jak dostęp do informacji (art. 11 Karty praw podstawowych UE) lub dostęp do edukacji (art. 14 Karty praw podstawowych UE).

### Wpływ przetwarzania na osoby, których dane dotyczą

1. Przetwarzanie danych osobowych, które ma miejsce podczas opracowywania i wdrażania modeli sztucznej inteligencji, może wpływać na osoby, których dane dotyczą, na różne sposoby, które mogą być pozytywne lub negatywne.[[66]](#footnote-67) Na przykład, jeżeli czynność przetwarzania wiąże się z korzyściami dla osoby, której dane dotyczą, mogą one zostać uwzględnione w teście równowagi. Chociaż istnienie takich korzyści może prowadzić do wniosku organu nadzorczego, że interesy administratora lub strony trzeciej nie są nadrzędne wobec interesów, podstawowych praw i wolności osób, których dane dotyczą, taki wniosek może wynikać jedynie z analizy poszczególnych przypadków, uwzględniającej wszystkie odpowiednie czynniki.
2. Wpływ przetwarzania na osoby, których dane dotyczą, może zależeć od (i) charakteru danych przetwarzanych przez modele; (ii) kontekstu przetwarzania; oraz (iii) dalszych konsekwencji, jakie może mieć przetwarzanie[[67]](#footnote-68) .
3. W odniesieniu do **charakteru przetwarzanych danych** należy przypomnieć, że - oprócz szczególnych kategorii danych osobowych oraz danych dotyczących wyroków skazujących i naruszeń prawa, które są objęte dodatkową ochroną na mocy art. 9 i 10 RODO - przetwarzanie niektórych innych kategorii danych osobowych może mieć poważne konsekwencje dla osób, których dane dotyczą. W tym kontekście przetwarzanie niektórych rodzajów danych osobowych ujawniających wysoce prywatne informacje (np. dane finansowe lub dane dotyczące lokalizacji) w celu opracowania i wdrożenia modelu sztucznej inteligencji należy uznać za mogące mieć poważny wpływ na osoby, których dane dotyczą. W fazie wdrażania konsekwencje takiego przetwarzania dla osób, których dane dotyczą, mogą być na przykład ekonomiczne (np. dyskryminacja w kontekście zatrudnienia) i/lub reputacyjne (np. zniesławienie).
4. W odniesieniu do **kontekstu przetwarzania** należy najpierw zidentyfikować elementy, które mogą stwarzać ryzyko dla osób, których dane dotyczą (np. sposób, w jaki model został opracowany, sposób, w jaki model może zostać wdrożony i/lub czy środki bezpieczeństwa stosowane w celu ochrony danych osobowych są odpowiednie). Charakter modelu i zamierzone zastosowania operacyjne odgrywają kluczową rolę w identyfikacji takich potencjalnych przyczyn.
5. Konieczna jest również ocena wagi tych zagrożeń dla osób, których dane dotyczą. Można rozważyć, między innymi, w jaki sposób przetwarzane są dane osobowe (np. czy są one łączone z innymi zbiorami danych), jaka jest skala przetwarzania i ilość przetwarzanych danych osobowych [[68]](#footnote-69) (np. ogólna ilość danych, ilość danych na osobę, której dane dotyczą, liczba osób, których dane dotyczą)[[69]](#footnote-70) status osoby, której dane dotyczą (np. dzieci lub inne wrażliwe osoby, których dane dotyczą) oraz jej relacje z administratorem (np. jeśli osoba, której dane dotyczą, jest klientem). Przykładowo, wykorzystanie web scrapingu w fazie opracowywania może prowadzić - przy braku wystarczających zabezpieczeń - do znaczącego wpływu na osoby fizyczne, ze względu na dużą ilość gromadzonych danych, dużą liczbę osób, których dane dotyczą, oraz masowe gromadzenie danych osobowych.
6. Przy ocenie wpływu przetwarzania na osoby, których dane dotyczą, należy również wziąć pod uwagę **dalsze konsekwencje**, jakie może mieć przetwarzanie. Powinny one być oceniane przez organy nadzorcze indywidualnie dla każdego przypadku, z uwzględnieniem konkretnych faktów.
7. Takie konsekwencje mogą obejmować (ale nie ograniczają się do) ryzyko naruszenia praw podstawowych osób, których dane dotyczą, jak opisano w poprzedniej podsekcji[[70]](#footnote-71) . Ryzyko to może różnić się prawdopodobieństwem i dotkliwością oraz może wynikać z przetwarzania danych osobowych, które może prowadzić do szkód fizycznych, materialnych lub niematerialnych, w szczególności gdy przetwarzanie może prowadzić do dyskryminacji[[71]](#footnote-72) .
8. Jeżeli wdrożenie modelu sztucznej inteligencji wiąże się z przetwarzaniem danych osobowych zarówno (i) osób, których dane dotyczą, których dane osobowe są zawarte w zbiorze danych wykorzystywanym w fazie opracowywania; oraz (ii) osób, których dane dotyczą, których dane osobowe są przetwarzane w fazie wdrażania, organy nadzorcze powinny rozróżnić i rozważyć ryzyko wpływające na interesy, prawa i wolności każdej z tych kategorii osób, których dane dotyczą, podczas weryfikacji testu równowagi przeprowadzonego przez administratora.
9. **Wreszcie, analiza możliwych dalszych konsekwencji przetwarzania powinna również uwzględniać prawdopodobieństwo zmaterializowania się tych dalszych konsekwencji**. Oceny takiego prawdopodobieństwa należy dokonać z uwzględnieniem obowiązujących środków technicznych i organizacyjnych oraz szczególnych okoliczności sprawy. Na przykład, organy nadzorcze mogą rozważyć, czy wdrożono środki w celu uniknięcia potencjalnego niewłaściwego wykorzystania modelu sztucznej inteligencji. W przypadku modeli sztucznej inteligencji, które mogą być wdrażane do różnych celów, takich jak generatywna sztuczna inteligencja, może to obejmować kontrole ograniczające w jak największym stopniu ich wykorzystanie do szkodliwych praktyk, na przykład: tworzenia deepfake'ów; chatbotów wykorzystywanych do dezinformacji, phishingu i innych rodzajów oszustw; oraz manipulacyjnych AI/agentów AI(w szczególności gdy są antropomorficzne lub dostarczają wprowadzających w błąd informacji).

### Rozsądne oczekiwania osób, których dane dotyczą

1. Zgodnie z motywem 47 RODO " każdym razie istnienie prawnie uzasadnionego interesu wymagałoby starannej oceny, w tym ustalenia, czy osoba, której dane dotyczą, może oczekiwać, w czasie i w kontekście gromadzenia danych osobowych, że przetwarzanie w tym celu może mieć miejsce. Interesy i podstawowe prawa osoby, której dane dotyczą, mogą w szczególności przeważać nad interesem administratora, jeżeli dane osobowe są przetwarzane w okolicznościach, w których osoby, których dane dotyczą, nie oczekują dalszego przetwarzania"[[72]](#footnote-73).
2. Rozsądne oczekiwania odgrywają kluczową rolę w teście równowagi, między innymi ze względu na złożoność technologii wykorzystywanej w modelach sztucznej inteligencji oraz fakt, że osobom, których dane dotyczą, może być trudno zrozumieć różnorodność potencjalnych zastosowań modelu sztucznej inteligencji i związanego z nim przetwarzania danych[[73]](#footnote-74) . W tym celu informacje przekazywane osobom, których dane dotyczą, mogą być brane pod uwagę przy ocenie, czy osoby, których dane dotyczą, mogą rozsądnie oczekiwać, że ich dane osobowe będą przetwarzane. Jednakże, chociaż pominięcie informacji może przyczynić się do tego, że osoby, których dane dotyczą, nie oczekują określonego przetwarzania, samo spełnienie wymogów przejrzystości określonych w RODO nie jest wystarczające do uznania, że osoby, których dane dotyczą, mogą rozsądnie oczekiwać określonego przetwarzania[[74]](#footnote-75) . Ponadto sam fakt, że informacje dotyczące fazy opracowywania modelu sztucznej inteligencji są zawarte w polityce prywatności administratora, niekoniecznie oznacza, że osoby, których dane dotyczą, mogą rozsądnie oczekiwać, że tak się stanie; powinno to raczej zostać przeanalizowane przez organy nadzorcze w oparciu o konkretne okoliczności sprawy i z uwzględnieniem wszystkich istotnych czynników.
3. Oceniając uzasadnione oczekiwania osób, których dane dotyczą, w odniesieniu do przetwarzania, które ma miejsce w fazie opracowywania, ważne jest, aby odnieść się do elementów wymienionych w Wytycznych EROD dotyczących prawnie uzasadnionego interesu[[75]](#footnote-76) . Ponadto w ramach przedmiotu niniejszej opinii ważne jest, aby wziąć pod uwagę szerszy kontekst przetwarzania. Może to obejmować, choć nie ogranicza się do tego, czy dane osobowe były publicznie dostępne, charakter relacji między osobą, której dane dotyczą, a administratorem danych (i czy istnieje między nimi związek), charakter usługi, kontekst, w którym dane osobowe zostały zebrane, źródło, z którego dane zostały zebrane (np. strona internetowa lub usługa, w której dane osobowe zostały zebrane i oferowane przez nie ustawienia prywatności), potencjalne dalsze zastosowania modelu oraz czy osoby, których dane dotyczą, są rzeczywiście świadome, że ich dane osobowe są w ogóle online.
4. Na etapie opracowywania modelu uzasadnione oczekiwania osób, których dane dotyczą, mogą się różnić w zależności od tego, czy dane przetwarzane w celu opracowania modelu są upubliczniane przez osoby, których dane dotyczą, czy nie. Co więcej, rozsądne oczekiwania mogą się również różnić w zależności od tego, czy osoby te bezpośrednio dostarczyły dane administratorowi (np. w kontekście korzystania przez nie z usługi), czy też administrator uzyskał je z innego źródła (np. za pośrednictwem strony trzeciej lub scrapingu). W obu przypadkach przy ocenie rozsądnych oczekiwań należy wziąć pod uwagę kroki podjęte w celu poinformowania osób, których dane dotyczą, o czynnościach przetwarzania.
5. W fazie wdrażania modelu AII równie ważne jest uwzględnienie rozsądnych oczekiwań osób, których dane dotyczą, w kontekście konkretnych możliwości modelu. Na przykład w przypadku modeli sztucznej inteligencji, które mogą dostosowywać się do dostarczonych danych wejściowych, istotne może być rozważenie, czy osoby, których dane dotyczą, były świadome, że dostarczyły dane osobowe, aby model sztucznej inteligencji mógł dostosować swoje reakcje do ich potrzeb i aby mogli uzyskać usługi dostosowane do ich potrzeb. Ponadto istotne może być również rozważenie, czy ta czynność przetwarzania miałaby wpływ tylko na usługę świadczoną osobom, których dane dotyczą (np. personalizacja treści dla konkretnego użytkownika), czy też byłaby wykorzystywana do modyfikacji usługi świadczonej wszystkim klientom (np. w celu ogólnego ulepszenia modelu). Podobnie jak na etapie opracowywania, szczególnie istotne może być również rozważenie, czy istnieje bezpośredni związek między osobami, których dane dotyczą, a administratorem. Takie bezpośrednie powiązanie może na przykład umożliwić administratorowi łatwe dostarczenie osobom, których dane dotyczą, informacji na temat czynności przetwarzania i modelu, które mogłyby następnie wpłynąć na rozsądne oczekiwania tych osób.

### Środki łagodzące

1. Jeżeli interesy, prawa i wolności osób, których dane dotyczą, wydają się podrzędne wobec prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią, administrator może rozważyć wprowadzenie środków łagodzących w celu ograniczenia wpływu przetwarzania na te osoby, których dane dotyczą. Środki łagodzące to zabezpieczenia, które powinny być dostosowane do okoliczności sprawy i zależeć od różnych czynników, w tym od zamierzonego zastosowania modelu AI. Te środki łagodzące miałyby na celu zapewnienie, że interesy administratora lub strony trzeciej nie będą nadrzędne, tak aby administrator mógł polegać na tej podstawie prawnej.
2. Jak przypomniano w Wytycznych EROD dotyczących prawnie uzasadnionego interesu, środków łagodzących nie należy mylić ze środkami, które administrator i tak jest prawnie zobowiązany przyjąć w celu zapewnienia zgodności z RODO, niezależnie od tego, czy przetwarzanie opiera się na art. 6 ust. 1 lit. f) RODO[[76]](#footnote-77) . Jest to szczególnie ważne w przypadku środków, które na przykład wymagają zgodności z zasadami RODO, takimi jak zasada minimalizacji danych.
3. Poniższa lista środków ma charakter niewyczerpujący i nie nakazowy, a ich wdrożenie należy rozpatrywać indywidualnie dla każdego przypadku. Chociaż, w zależności od okoliczności, niektóre z poniższych środków mogą być wymagane w celu spełnienia określonych obowiązków wynikających z RODO, w przeciwnym razie mogą one być brane pod uwagę jako dodatkowe zabezpieczenia. Ponadto niektóre z wymienionych poniżej środków odnoszą się do obszarów, które podlegają szybkiej ewolucji i nowym zmianom, i powinny być brane pod uwagę przez organy nadzorcze przy rozpatrywaniu konkretnego przypadku.
4. **W odniesieniu do fazy opracowywania modeli sztucznej inteligencji** można podjąć szereg środków w celu złagodzenia ryzyka związanego z przetwarzaniem zarówno danych własnych, jak i danych osób trzecich (w tym w celu złagodzenia ryzyka związanego z praktykami skrobania stron internetowych). Na podstawie powyższego EROD przedstawia kilka przykładów środków, które można wdrożyć w celu złagodzenia zagrożeń zidentyfikowanych w teście równowagi i które powinny zostać uwzględnione przez organy nadzorcze podczas oceny konkretnych modeli sztucznej inteligencji w poszczególnych przypadkach.
5. **Środki techniczne:**
	1. Środki wymienione w sekcji 3.2.2, które są odpowiednie do ograniczenia istniejącego ryzyka, jeżeli środki te nie skutkują anonimizacją modelu i nie są wymagane do spełnienia innych obowiązków wynikających z RODO lub w ramach testu konieczności (drugi etap oceny prawnie uzasadnionego interesu).
6. Oprócz tych, inne istotne środki mogą obejmować:
	1. Środki pseudonimizacji: mogą to być na przykład środki zapobiegające łączeniu danych opartych na indywidualnych identyfikatorach. Środki te mogą nie być odpowiednie, jeżeli organ nadzorczy uzna, że administrator wykazał uzasadnioną potrzebę gromadzenia różnych danych dotyczących konkretnej osoby fizycznej w celu opracowania danego systemu lub modelu sztucznej inteligencji[[77]](#footnote-78) .
	2. Środki mające na celu maskowanie danych osobowych lub zastępowanie ich fałszywymi danymi osobowymi w zestawie szkoleniowym (np. zastępowanie nazwisk i adresów e-mail fałszywymi nazwiskami i fałszywymi adresami e-mail).

Środek ten może być szczególnie odpowiedni, gdy faktyczna zawartość merytoryczna danych nie jest istotna dla ogólnego przetwarzania (np. w szkoleniach LLM).

1. **Środki ułatwiające korzystanie z praw jednostki:**
	1. Przestrzeganie rozsądnego okresu między zebraniem szkoleniowego zbioru danych a jego wykorzystaniem. To dodatkowe zabezpieczenie może umożliwić osobom, których dane dotyczą, wykonywanie ich praw w tym okresie, przy czym rozsądny okres czasu jest oceniany w zależności od okoliczności każdego przypadku.
	2. Proponowanie bezwarunkowej "rezygnacji" od samego początku, na przykład poprzez zapewnienie osobom, których dane dotyczą, uznaniowego prawa do sprzeciwu przed rozpoczęciem przetwarzania, w celu wzmocnienia kontroli osób fizycznych nad ich danymi, co wykracza poza warunki art. 21 RODO
	3. Zezwolenie osobom, których dane dotyczą, na skorzystanie z prawa do usunięcia danych, nawet jeśli szczególne powody wymienione w art. 17 ust. 1 RODO nie mają zastosowania[[78]](#footnote-79) .
	4. Umożliwienie osobom, których dane dotyczą, zgłaszania roszczeń dotyczących regurgitacji lub zapamiętywania danych osobowych oraz okoliczności i środków, za pomocą których roszczenia te mogą być odtwarzane, umożliwiając administratorom danych odtwarzanie i ocenę odpowiednich technik oduczania się w celu uwzględnienia roszczeń.
2. **Środki przejrzystości:** w niektórych przypadkach środki łagodzące mogą obejmować środki zapewniające większą przejrzystość w odniesieniu do opracowywania modelu sztucznej inteligencji. Niektóre środki, oprócz zgodności z obowiązkami wynikającymi z RODO, mogą pomóc w przezwyciężeniu asymetrii informacyjnej i umożliwić osobom, których dane dotyczą, lepsze zrozumienie przetwarzania danych w fazie opracowywania:
	1. Publiczne i łatwo dostępne komunikaty, które wykraczają poza informacje wymagane na mocy art. 13 lub 14 RODO, na przykład poprzez podanie dodatkowych szczegółów dotyczących kryteriów gromadzenia i wszystkich wykorzystywanych zbiorów danych, z uwzględnieniem szczególnej ochrony dzieci i osób wymagających szczególnej opieki.
	2. Alternatywne formy informowania osób, których dane dotyczą, na przykład: kampanie medialne z różnymi mediami w celu informowania osób, których dane dotyczą, kampania informacyjna za pośrednictwem poczty elektronicznej, wykorzystanie wizualizacji graficznej, często zadawane pytania, oznaczenia przejrzystości i karty modeli, których usystematyzowanie mogłoby uporządkować prezentację informacji na temat modeli sztucznej inteligencji, oraz dobrowolne roczne sprawozdania dotyczące przejrzystości.
3. **Szczególne środki łagodzące w kontekście web scrapingu:** Biorąc pod uwagę, że, jak wspomniano powyżej, web scraping wiąże się ze szczególnym ryzykiem[[79]](#footnote-80) , w tym kontekście można zidentyfikować szczególne środki łagodzące. W stosownych przypadkach mogą one zostać uwzględnione przez organy nadzorcze, oprócz środków łagodzących wspomnianych powyżej, podczas badania administratorów prowadzących web scraping.
4. Konkretne środki, o ile nie są konieczne w ramach drugiego etapu oceny prawnie uzasadnionego interesu, mogą okazać się przydatne w celu ograniczenia ryzyka w kontekście web scrapingu. Mogą one **obejmować środki techniczne**, takie jak:
	1. Wykluczenie treści danych z publikacji, które mogą zawierać dane osobowe wiążące się z ryzykiem dlaokreślonych osób lub grup osób (np. osób, które mogą być narażone na nadużycia, uprzedzenia lub nawet szkody fizyczne w przypadku publicznego ujawnienia danych).
	2. Zapewnienie, że niektóre kategorie danych nie są gromadzone lub że niektóre źródła są wyłączone z gromadzenia danych; może to obejmować na przykład niektóre strony internetowe, które są szczególnie inwazyjne ze względu na wrażliwość ich przedmiotu.
	3. Wykluczenie gromadzenia ze stron internetowych (lub sekcji stron internetowych), które wyraźnie sprzeciwiają się web scrapingowi i ponownemu wykorzystywaniu ich treści w celu tworzenia szkoleniowych baz danych sztucznej inteligencji (na przykład poprzez przestrzeganie plików robots.txt lub ai.txt lub innego uznanego mechanizmu wyrażającego wykluczenie z automatycznego indeksowania lub scrapingu).
	4. Nałożenie innych odpowiednich ograniczeń na gromadzenie danych, w tym ewentualnie kryteriów opartych na okresach.
5. W kontekście web scrapingu przykłady konkretnych środków **ułatwiających wykonywanie praw osób fizycznych i przejrzystość** mogą obejmować: utworzenie listy opt-out, zarządzanej przez administratora i umożliwiającej osobom, których dane dotyczą, sprzeciwienie się gromadzeniu ich danych na niektórych stronach internetowych lub platformach internetowych poprzez podanie informacji identyfikujących je na tych stronach internetowych, w tym przed rozpoczęciem gromadzenia danych[[80]](#footnote-81) .
6. **Szczególne uwagi dotyczące środków łagodzących w fazie wdrażania:** Chociaż niektóre z wyżej wymienionych środków mogą być również istotne dla fazy wdrażania, w zależności od okoliczności, EROD przedstawia poniżej niewyczerpujący wykaz dodatkowych środków wspierających, które mogą zostać wdrożone i które powinny zostać ocenione przez organy nadzorcze na zasadzie indywidualnej.
	1. **Środki techniczne** mogą na przykład zostać wprowadzone w celu zapobiegania przechowywaniu, regurgitacjilub generowaniu danych osobowych, zwłaszcza w kontekście generatywnych modeli sztucznej inteligencji (takich jak filtry wyjściowe) i/lub w celu ograniczenia ryzyka niezgodnego z prawem ponownego wykorzystania przez modele sztucznej inteligencji ogólnego przeznaczenia (np. cyfrowy znak wodny wyników generowanych przez sztuczną inteligencję).
	2. **Środki, które ułatwiają lub przyspieszają wykonywanie praw osób fizycznych** w fazie wdrażania, wykraczające poza to, co jest wymagane przez prawo, dotyczące w szczególności, ale nie wyłącznie, wykonywania prawa do usunięcia danych osobowych z danych wyjściowych modelu lub deduplikacji oraz technik poszkoleniowych, które próbują usunąć lub ukryć dane osobowe.
7. Badając wdrożenie konkretnego modelu sztucznej inteligencji, organy nadzorcze powinny rozważyć, czy administrator opublikował przeprowadzony przez siebie test równowagi, ponieważ może to zwiększyć przejrzystość i rzetelność. Jak wspomniano w wytycznych EROD[[81]](#footnote-82) dotyczących prawnie uzasadnionego interesu, można rozważyć inne środki w celu dostarczenia osobom, których dane dotyczą, informacji z testu równowagi przed jakimkolwiek gromadzeniem danych osobowych . EROD wskazuje również[[82]](#footnote-83) , że elementem, który należy wziąć pod uwagę, jest to, czy administrator danych zaangażował inspektora ochrony danych, jeśli ma to zastosowanie.

# 3.4 Możliwy wpływ niezgodnego z prawem przetwarzania w ramach opracowywania modelu AI na zgodność z prawem późniejszego przetwarzania lub działania modelu AI

1. Niniejsza część opinii odnosi się do pytania 4 wniosku. Pytanie to ma na celu wyjaśnienie możliwego wpływu niezgodnego z prawem przetwarzania w fazie opracowywania na późniejsze przetwarzanie (na przykład w fazie wdrażania modelu sztucznej inteligencji) lub na działanie modelu. Pytanie ma na celu odniesienie się zarówno do sytuacji, w której taki model sztucznej inteligencji przetwarza dane osobowe, które są przechowywane w modelu (pytanie 4(i) wniosku), jak i do sytuacji, w której do wdrożenia modelu sztucznej inteligencji nie wykorzystuje się już przetwarzania danych osobowych(tj. model jest anonimowy) (pytanie 4(ii) wniosku).
2. Przed odniesieniem się do konkretnych scenariuszy, EROD przedstawia następujące ogólne uwagi.
3. Po pierwsze, wyjaśnienia przedstawione w niniejszej sekcji będą koncentrować się na przetwarzaniu danych osobowych w fazie opracowywania prowadzonym z naruszeniem zasady zgodności z prawem określonej w art. 5 ust. 1 lit. a) RODO, a w szczególności w art. 6 RODO (zwanej dalej "**niezgodnością z prawem**")[[83]](#footnote-84) . W tym samym duchu rozważania EROD będą koncentrować się na wpływie niezgodności z prawem przetwarzania na etapie opracowywania na zgodność z prawem (tj. zgodność z art. 5 ust. 1 lit. a) RODO i art. 6 RODO) późniejszego przetwarzania lub działania modelu sztucznej inteligencji. EROD zwraca jednak uwagę, że przetwarzanie prowadzone w fazie opracowywania może również prowadzić do naruszenia innych przepisów RODO, takich jak brak przejrzystości wobec osób, których dane dotyczą, lub ochrona danych w fazie projektowania lub domyślna ochrona danych, które nie są analizowane w niniejszej opinii.
4. Po drugie, przy rozpatrywaniu tej kwestii kluczową rolę odgrywa zasada rozliczalności, która wymaga od administratorów odpowiedzialności i wykazania zgodności *m.in.* z art. 5 ust. 1 RODO i art. 6 RODO[[84]](#footnote-85) . Odnosi się to również do potrzeby oceny, która organizacja jest administratorem danych w odniesieniu do danej czynności przetwarzania oraz czy występują sytuacje współadministrowania (ponieważ mogą być one nierozerwalnie związane)[[85]](#footnote-86) . Biorąc pod uwagę znaczenie okoliczności faktycznych każdej sprawy, w tym w odniesieniu do roli odgrywanej przez każdą ze stron zaangażowanych w przetwarzanie, uwagi EROD należy rozumieć jako ogólne spostrzeżenia, które powinny być oceniane indywidualnie przez organy nadzorcze.
5. Po trzecie, EROD podkreśla, że zgodnie z art. 51 ust. 1 RODO "Każde państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszego rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (zwany dalej ,,organem nadzorczym”)*"*. Do kompetencji organów nadzorczych należy zatem ocena zgodności z prawem przetwarzania danych oraz wykonywanie uprawnień przyznanych im na mocy RODO zgodnie z krajowymi ramami prawnymi[[86]](#footnote-87). W takich przypadkach organy nadzorcze korzystają z uprawnień dyskrecjonalnych do oceny możliwego naruszenia (naruszeń) i wyboru odpowiednich, niezbędnych środków spośród wymienionych w art. 58 RODO, z uwzględnieniem okoliczności każdego indywidualnego przypadku[[87]](#footnote-88) .

**W przypadku stwierdzenia naruszenia, organy nadzorcze mogą nałożyć środki naprawcze, takie jak nakazanie administratorom, z uwzględnieniem okoliczności każdego przypadku, podjęcia działań w celu usunięcia niezgodności z prawem pierwotnego przetwarzania**. Mogą one obejmować na przykład nałożenie administracyjnej kary pieniężnej, nałożenie tymczasowego ograniczenia przetwarzania, usunięcie części zbioru danych, które były przetwarzane niezgodnie z prawem lub, jeżeli nie jest to możliwe, w zależności od okoliczności faktycznych, z uwzględnieniem proporcjonalności środka, nakazanie usunięcia całego zbioru danych wykorzystanego do opracowania modelu sztucznej inteligencji/lub samego modelu sztucznej inteligencji. Oceniając proporcjonalność planowanego środka, organy nadzorcze mogą wziąć pod uwagę środki, które mogą zostać zastosowane przez administratora w celu zaradzenia niezgodności z prawem pierwotnego przetwarzania (np. ponowne szkolenie).

1. EROD podkreśla również, że gdy dane osobowe są przetwarzane niezgodnie z prawem, osoby, których dane dotyczą, mogą zażądać usunięcia swoich danych osobowych, z zastrzeżeniem warunków określonych w art. 17 RODO, oraz że organy nadzorcze mogą nakazać usunięcie danych osobowych *z urzędu[[88]](#footnote-89) .*
2. Oceniając, czy środek jest odpowiedni, konieczny i proporcjonalny, organy nadzorcze mogą wziąć pod uwagę między innymi ryzyko dla osób, których dane dotyczą, wagę naruszenia, techniczną i finansową wykonalność środka, a także ilość danych osobowych, których dotyczy.
3. Ponadto EROD przypomina, że środki podejmowane przez organy nadzorcze na mocy RODO pozostają bez uszczerbku dla środków podejmowanych przez właściwe organy na mocy Aktu o sztucznej inteligencji lub na mocy innych mających zastosowanie ram prawnych (np. przepisów dotyczących odpowiedzialności cywilnej).
4. W kolejnych sekcjach EROD zajmie się trzema scenariuszami objętymi pytaniem 4 wniosku, w których różnice polegają na tym, czy dane osobowe przetwarzane w celu opracowania modelu są zatrzymywane w modelu i/lub czy dalsze przetwarzanie jest wykonywane przez tego samego lub innego administratora danych.

### 3.4.1 Scenariusz 1. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowania modelu, dane osobowe są przechowywane w modelu i są następnie przetwarzane przez tego samego administratora (na przykład w kontekście wdrożenia modelu).

1. Scenariusz ten odnosi się do pytania 4(i) wniosku, w sytuacji, gdy administrator niezgodnie z prawem przetwarza dane osobowe (tj. niezgodnie z art. 5 ust. 1 lit. a) RODO i art. 6 RODO) w celu opracowania modelu sztucznej inteligencji, model sztucznej inteligencji zachowuje informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a zatem nie jest anonimowy. Dane osobowe są następnie przetwarzane przez tego samego administratora (na przykład w kontekście wdrożenia modelu). W odniesieniu do tego scenariusza EROD przedstawia następujące uwagi.
2. Uprawnienie organu nadzorczego do nałożenia środków naprawczych na początkowe przetwarzanie (jak wyjaśniono w pkt 113, 114 i 115 powyżej) miałoby zasadniczo wpływ na późniejsze przetwarzanie (np. jeżeli organ nadzorczy nakazałby administratorowi usunięcie danych osobowych, które były przetwarzane niezgodnie z prawem, takie środki naprawcze nie pozwoliłyby administratorowi na późniejsze przetwarzanie danych osobowych, które podlegały tym środkom).
3. W szczególności w odniesieniu do wpływu niezgodnego z prawem przetwarzania w fazie opracowywania na późniejsze przetwarzanie (na przykład w fazie wdrażania), EROD przypomina, że do organów nadzorczych należy przeprowadzenie indywidualnej analizy, która uwzględnia szczególne okoliczności każdego przypadku.
4. **To, czy fazy opracowywania i wdrażania wiążą się z odrębnymi celami (stanowiąc tym samym odrębne czynności przetwarzania) oraz zakres, w jakim brak podstawy prawnej dla początkowej czynności przetwarzania wpływa na zgodność z prawem późniejszego przetwarzania, należy oceniać indywidualnie dla każdego przypadku, w zależności od kontekstu sprawy.**
5. Na przykład, w szczególności w odniesieniu do podstawy prawnej art. 6 ust. 1 lit. f) RODO, gdy dalsze przetwarzanie opiera się na prawnie uzasadnionym interesie, fakt, że początkowe przetwarzanie było niezgodne z prawem, powinien zostać uwzględniony w ocenie prawnie uzasadnionego interesu (np. w odniesieniu do ryzyka dla osób, których dane dotyczą, lub faktu, że osoby, których dane dotyczą, mogą nie oczekiwać takiego dalszego przetwarzania). W takich przypadkach niezgodność z prawem przetwarzania w fazie opracowywania może mieć wpływ na zgodność z prawem późniejszego przetwarzania.

### 3.4.2. Scenariusz 2. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowania modelu, dane osobowe są zatrzymywane w modelu i przetwarzane przez innego administratora w kontekście wdrożenia modelu.

1. Scenariusz ten odnosi się do pytania 4(i) wniosku. Różni się on od scenariusza 1 (w sekcji 3.4.1 niniejszej opinii), ponieważ dane osobowe są następnie przetwarzane przez innego administratora w kontekście wdrożenia modelu sztucznej inteligencji.
2. EROD przypomina, że ustalenie ról przypisanych tym różnym podmiotom w ramach ochrony danych jest niezbędnym krokiem w celu określenia, które obowiązki wynikające z RODO mają zastosowanie i kto jest za nie odpowiedzialny, oraz że przy ocenie obowiązków każdej ze stron wynikających z RODO należy również uwzględnić sytuacje współadministrowania. W związku z tym poniższe uwagi należy traktować jako ogólne elementy, które w stosownych przypadkach powinny zostać uwzględnione przez organy nadzorcze. W odniesieniu do scenariusza 2 EROD przedstawia następujące uwagi.
3. Po pierwsze, należy przypomnieć, że zgodnie z art. 5 ust. 1 lit. a) RODO, w świetle art. 5 ust. 2 RODO, każdy administrator powinien zapewnić zgodność z prawem przetwarzania, którego dokonuje, i być w stanie to wykazać. W związku z tym organy nadzorcze powinny ocenić zgodność z prawem przetwarzania prowadzonego przez (i) administratora, który pierwotnie opracował model sztucznej inteligencji; oraz (ii) administratora, który nabył model sztucznej inteligencji i samodzielnie przetwarza dane osobowe.
4. Po drugie, rozważania poczynione w pkt 113, 114 i 115 powyżej są istotne w niniejszej sprawie w odniesieniu do uprawnień organów nadzorczych do interwencji w związku z początkowym przetwarzaniem. Art. 17 ust. 1 lit. d) RODO (prawo do usunięcia danych przetwarzanych niezgodnie z prawem) i art. 19 RODO (obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania) mogą, w zależności od okoliczności sprawy, być również istotne w tym kontekście, na przykład w odniesieniu do zgłoszenia, które administrator opracowujący model powinien dokonać administratorowi wdrażającemu model.
5. Po trzecie, w odniesieniu do ewentualnego wpływu niezgodności z prawem pierwotnego przetwarzania na późniejsze przetwarzanie prowadzone przez innego administratora, taka ocena powinna być przeprowadzana przez organy nadzorcze indywidualnie dla każdego przypadku.
6. **Organy nadzorcze powinny wziąć pod uwagę, czy administrator wdrażający model przeprowadził odpowiednią ocenę w ramach swoich obowiązków w zakresie rozliczalności[[89]](#footnote-90) i w celu wykazania zgodności z art. 5 ust. 1 lit. a) i art. 6 RODO, aby upewnić się, że model sztucznej inteligencji nie został opracowywany w wyniku niezgodnego z prawem przetwarzania danych osobowych.** Taka ocena dokonywana przez organy nadzorcze powinna uwzględniać to, czy administrator ocenił niektóre niewyczerpujące kryteria, takie jak źródło danych i to, czy model sztucznej inteligencji jest wynikiem naruszenia RODO, w szczególności jeśli zostało to ustalone przez organ nadzorczy lub sąd, tak aby administrator wdrażający model nie mógł zignorować faktu, że początkowe przetwarzanie było niezgodne z prawem.
7. Administrator powinien rozważyć na przykład, czy dane pochodzą z naruszenia ochrony danych osobowych lub czy przetwarzanie było przedmiotem stwierdzenia naruszenia przez organ nadzorczy lub sąd. **Stopień oceny administratora i poziom szczegółowości oczekiwany przez organy nadzorcze mogą się różnić w zależności od różnych czynników, w tym od rodzaju i stopnia ryzyka związanego z przetwarzaniem w modelu sztucznej inteligencji, podczas jego wdrażania w odniesieniu do osób, których dane zostały wykorzystane do opracowywania modelu.**
8. EROD zauważa, że akt o sztucznej inteligencji wymaga od dostawców systemów sztucznej inteligencji wysokiego ryzyka sporządzenia unijnej deklaracji[[90]](#footnote-91) zgodności i że taka deklaracja zawiera oświadczenie, że odpowiedni system sztucznej inteligencji jest zgodny z unijnymi przepisami o ochronie danych.[[91]](#footnote-92) EROD zauważa, że taka własna deklaracja nie może stanowić rozstrzygającego ustalenia zgodności z RODO. Może ono jednak zostać uwzględnione przez organy nadzorcze podczas badania danego modelu sztucznej inteligencji.
9. Te same rozważania, poczynione w punkcie 123 powyżej, są również istotne w tym przypadku. Gdy organy nadzorcze weryfikują, czy i w jaki sposób administrator ocenił odpowiedniość prawnie uzasadnionego interesu jako podstawy prawnej prowadzonego przez siebie przetwarzania, niezgodność z prawem początkowego przetwarzania powinna zostać uwzględniona, jako część oceny prawnie uzasadnionego interesu, na przykład poprzez ocenę potencjalnego ryzyka, które może powstać dla osób, których dane dotyczą, których dane osobowe były przetwarzane niezgodnie z prawem w celu opracowywania modelu. W ramach testu równowagi o należy odpowiednio uwzględnić różne aspekty, zarówno o charakterze technicznym (np. istnienie filtrów lub ograniczeń dostępu wprowadzonych podczas opracowywania modelu, których późniejszy administrator nie może obejść ani na nie wpłynąć, a które mogą uniemożliwić dostęp do danych osobowych lub ich ujawnienie), jak i o charakterze prawnym (np. charakter i waga niezgodności z prawem początkowego przetwarzania).

### Scenariusz 3. Administrator niezgodnie z prawem przetwarza dane osobowe w celu opracowywania modelu, a następnie zapewnia anonimizację modelu, zanim ten sam lub inny administrator rozpocznie dalsze przetwarzanie danych osobowych w kontekście wdrożenia.

1. Scenariusz ten odnosi się do pytania 4(ii) wniosku i dotyczy przypadku, w którym administrator niegodnie z prawem przetwarza dane osobowe w celu opracowania modelu sztucznej inteligencji, ale robi to w sposób zapewniający anonimizację danych osobowych, zanim ten sam lub inny administrator rozpocznie dalsze przetwarzanie danych osobowych w kontekście wdrożenia. Po pierwsze, EROD przypomina, że organy nadzorcze są właściwe i mają uprawnienia do interweniowania w odniesieniu do przetwarzania związanego z anonimizacją modelu, a także do przetwarzania prowadzonego w fazie opracowywania. W związku z tym organy nadzorcze mogą, w zależności od konkretnych okoliczności sprawy, nałożyć środki naprawcze na to początkowe przetwarzanie (jak wyjaśniono w pkt 113, 114, 115 powyżej).
2. Jeżeli można wykazać, że późniejsze działanie modelu sztucznej inteligencji nie wiąże się z przetwarzaniem danych osobowych, EROD uważa, że RODO nie miałoby zastosowania[[92]](#footnote-93). W związku z tym niezgodność z prawem początkowego przetwarzania nie powinna mieć wpływu na późniejsze działanie modelu. EROD podkreśla jednak, że samo twierdzenie o anonimowości modelu nie wystarcza do wyłączenia go z zakresu stosowania RODO, i zauważa, że organy nadzorcze powinny dokonać oceny, biorąc pod uwagę, indywidualnie dla każdego przypadku, względy przedstawione przez EROD w odpowiedzi na pytanie 1 wniosku.
3. **Gdy administratorzy będą następnie przetwarzać dane osobowe zebrane w fazie wdrożenia, po zanonimizowaniu modelu, RODO będzie miało zastosowanie w odniesieniu do tych czynności przetwarzania. W takich przypadkach, w odniesieniu do RODO, niezgodność z prawem przetwarzania przeprowadzonego w fazie wdrożenia nie powinna mieć wpływu na zgodność z prawem początkowego przetwarzania.**

# 4. Uwagi końcowe

1. Niniejsza opinia jest skierowana do wszystkich organów nadzorczych i zostanie podana do wiadomości publicznej zgodnie z art. 64 ust. 5 lit. b) RODO.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

Anu Talus

1. Odniesienia do "państw członkowskich" w niniejszej opinii należy rozumieć jako odniesienia do "państw członkowskich EOG". Odniesienia do "Unii" w niniejszej opinii należy rozumieć jako odniesienia do "EOG". [↑](#footnote-ref-2)
2. Wniosek, str. 1. [↑](#footnote-ref-3)
3. Wniosek, str. 1. [↑](#footnote-ref-4)
4. Tamże. [↑](#footnote-ref-5)
5. Wniosek, str. 2. [↑](#footnote-ref-6)
6. Wniosek, s. 1. Jak wspomniano w programie prac EROD na lata 2024-2025, przyjętym w dniu 8 października 2024 r., dostępnym pod adresem [https://www.edpb.europa.eu/system/files/2024-10/edpb work programme 2024-2025 en.pdf,](http://www.edpb.europa.eu/system/files/2024-10/edpbworkprogramme2024-2025en.pdf) EROD planuje wydać *m.in.* wytyczne dotyczące anonimizacji, pseudonimizacji i zbierania danych w kontekście generatywnej sztucznej inteligencji. [↑](#footnote-ref-7)
7. EROD, dokument wewnętrzny 3/2019 w sprawie wewnętrznych wytycznych dotyczących art. 64 ust. 2 RODO, przyjęty w dniu 8 października 2019 r., pkt 15, dostępny pod adresem; [https://www.edpb.europa.eu/system/files/2022- 07/internaledpb document 201903 art64.2 en.pdf](https://www.edpb.europa.eu/system/files/2022-%2007/internaledpb%20document%20201903%20art64.2%20en.pdf). [↑](#footnote-ref-8)
8. Wniosek, str. 1-2. [↑](#footnote-ref-9)
9. Art. 64 ust. 3 RODO i art. 10 ust. 4 regulaminu EROD. [↑](#footnote-ref-10)
10. Artykuł 51 ust. 1 RODO i artykuł 51 ust. 2 RODO. [↑](#footnote-ref-11)
11. Zob. również sprawozdanie EROD z prac podjętych przez grupę zadaniową ds. ChatGPT, przyjęte w dniu 23 maja 2024 r., pkt 18: "W odniesieniu do przetwarzania szczególnych kategorii danych osobowych, aby przetwarzanie było zgodne z prawem, dodatkowo musi mieć zastosowanie jeden z wyjątków określonych w art. 9 ust. 2. *Zasadniczo jednym z tych wyjątków może być art. 9 ust. 2 lit. e) RODO. Jednak sam fakt, że dane osobowe są publicznie dostępne, nie oznacza, że "osoba, której dane dotyczą, wyraźnie upubliczniła takie dane" [...]*". [↑](#footnote-ref-12)
12. Wyrok TSUE z dnia 4 lipca 2023 r., sprawa C-252/21, *Meta przeciwko Bundeskartellamt* (ECLI:EU:C:2023:537), pkt 89. [↑](#footnote-ref-13)
13. Wyrok TSUE z dnia 4 lipca 2023 r., sprawa C-252/21, *Meta przeciwko Bundeskartellamt* (ECLI:EU:C:2023:537), pkt 77. [↑](#footnote-ref-14)
14. Wytyczne Grupy Roboczej Art. 29 (**"WP29"**) w sprawie zautomatyzowanego indywidualnego podejmowania decyzji i profilowania do celów rozporządzenia 2016/679, ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r., zatwierdzone przez EROD w dniu 25 maja 2018 r. Zob. również wyrok TSUE z dnia 7 grudnia 2023 r., sprawa C-634/21, *SCHUFA Holding i inni* (ECLI:EU:C:2023:957). [↑](#footnote-ref-15)
15. Wytyczne Grupy Roboczej Art. 29 w sprawie oceny skutków dla ochrony danych (DPIA) i ustalania, czy przetwarzanie "może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, zmienione i przyjęte w dniu 4 października 2017 r., zatwierdzone przez EROD w dniu 25 maja 2018 r. [↑](#footnote-ref-16)
16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji oraz zmieniające rozporządzenia (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797. i (UE) 2020/1828 (akt o sztucznej inteligencji). [↑](#footnote-ref-17)
17. Art. 3 ust. 1 aktu o sztucznej inteligencji. [↑](#footnote-ref-18)
18. Motyw 97 aktu o sztucznej inteligencji. [↑](#footnote-ref-19)
19. Wniosek, s. 3. [↑](#footnote-ref-20)
20. Tj. funkcje, które obliczają, na podstawie danych wejściowych i wag, wyjście węzła neuronowego, które zostanie następnie wysłane do następnej warstwy sieci neuronowej. [↑](#footnote-ref-21)
21. "*Czy ostateczny model sztucznej inteligencji, który został wytrenowany przy użyciu danych osobowych, jest we wszystkich przypadkach uznawany za niespełniający definicji danych osobowych (określonej w art. 4 ust. 1 RODO)?*"*.* [↑](#footnote-ref-22)
22. Takie jak ataki polegające na wnioskowaniu o członkostwie (OWASP) i ataki polegające na odwróceniu modelu (OWASP & Veale et al, 2018). [↑](#footnote-ref-23)
23. Wniosek, str. 1-2. [↑](#footnote-ref-24)
24. Zob. w tym względzie na przykład: (i) Veale M., Binns R., Edwards L., 2018, *Algorithms that remember: model inversion attacks and data protection law*. Phil. Trans. R. Soc. A 376: 20180083, dostępny pod adresem <http://dx.doi.org/10.1098/rsta.2018.0083>; (ii) Brown H., Lee K., Mireshghallah F., Shokri R., and Tramèr F., *What Does it Mean for a Language Model to Preserve Privacy?*, 2022, ACM Digital Library, FAccT '22, June 20, 2022, Seoul, Republic of Korea, dostępny pod adresem <https://dl.acm.org/doi/abs/10.1145/3531146.3534642>; (iii) Vassilev A., Oprea A., Fordyce A., Anderson H., *Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations*, styczeń 2024 r.,

National Institute of Standards and Technology, dostępny pod adresem https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.1002.e2023.pdf; (iv) Carlini N., Tramèr F., Wallace E., Jagielski M., Herbert-Voss A., Lee K., Roberts A., Brown T., Song D., Erlingsson U., Oprea A., Raffel C., *Extracting Training Data from Large Language Models*, arXiv:2012.07805v2 [cs.CR] 15 Jun 2021, dostępny pod adresem <https://arxiv.org/pdf/2012.07805>; (v) Fredrikson M., Jha S., Ristenpart T., *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures*, ACM Digital Library, 12 października 2015, dostępne pod adresem <https://dl.acm.org/doi/abs/10.1145/2810103.2813677>; (vi) Zhang Y., Jia R., Pei H., Wang W., Li B., Song D., *The Secret Revealer: The Generative Model-Inversion Attacks Against Deep Neural Networks*, arXiv:1911.07135v2 [cs.LG] 18 kwietnia 2020 r., dostępne pod adresem <https://arxiv.org/pdf/1911.07135>. [↑](#footnote-ref-25)
25. W przypadku systemu sztucznej inteligencji opartego na generatywnej sztucznej inteligencji regurgitacja odpowiada sytuacji, w której dane wyjściowe byłyby bezpośrednio powiązane z danymi szkoleniowymi. [↑](#footnote-ref-26)
26. "*W jakich okolicznościach może to nastąpić?*". [↑](#footnote-ref-27)
27. "*Jeśli tak, w jaki sposób można wykazać kroki podjęte w celu zapewnienia, że model sztucznej inteligencji nie przetwarza danych osobowych?*". [↑](#footnote-ref-28)
28. (i) Carlini N., Chien S., Nasr M., Song S., Terzis A., Tramer F., *Membership Inference Attacks From First Principles,* arXiv:2112.03570, dostępny pod adresem [https://arxiv.org/abs/2112.03570;](https://arxiv.org/abs/2112.03570)

	* 1. Creţu A.M, Guépin F. i De Montjoye Y.A, *Ataki polegające na wnioskowaniu korelacyjnym na modele uczenia maszynowego*. Sci. Adv.10, eadj9260(2024).DOI:10.1126/sciadv.adj9260 dostępny pod adresem [https://www.science.org/doi/10.1126/sciadv.adj9260;](https://www.science.org/doi/10.1126/sciadv.adj9260)

	* 1. Dana L., Pydi M. S., Chevaleyre Y., Memorization in Attention-only Transformers arXiv:2411.10115v1 15 listopada 2024, dostępny pod adresem: <https://arxiv.org/abs/2411.10115>;
		2. Gehrke M., Liebenow J., Mohammadi E. & Braun T. et al. *Lifting in Support of Privacy-Preserving Probabilistic Inference*. Künstl Intell, 13 czerwca 2024 r., dostępny pod adresem: <https://doi.org/10.1007/s13218-024-00851-y>;
		3. Hu H., *Membership Inference Attacks and Defenses on Machine Learning Models Literature*, dostępny pod adresem: <https://github.com/HongshengHu/membership-inference-machine-learning-literature>;
		4. Nasr M., Carlini N., Hayase J., Jagielski M., Cooper A. F., Ippolito D., Choquette-Choo C. A., Wallace E., Tramèr F., and Lee K., *Scalable Extraction of Training Data from (Production) Language Models*, arXiv:2311.17035 28 listopada 2023, dostępny pod adresem: <https://arxiv.org/abs/2311.17035>;
		5. Shokri R., Stronati M., Song C., Shmatikov V., Membership Inference Attacks against Machine Learning Models arXiv:1610.05820v2 , 31 marca 2017, dostępny pod adresem <https://arxiv.org/abs/1610.05820>;
		6. Staab R., Vero M., Mislav Balunović, Martin Vechev, 2024, *Beyond Memorization: Violating Privacy Via Inference with Large Language Models*, arXiv:2310.07298v2, 6 maja 2024, dostępny pod adresem <https://arxiv.org/abs/2310.07298>;
		7. Wu F., Cui L., Yao S., Yu S., Inference Attacks in Machine Learning as a Service: A Taxonomy, Review, and Promising Directions arXiv:2406.02027v1 , 27 czerwca 2024 r., dostępny pod adresem <https://arxiv.org/abs/2406.02027v1>;
		8. Zhang J., Das D., Kamath G., Tramèr F., *Membership Inference Attacks Cannot Prove that a Model Was Trained On Your*Data arXiv:2409.19798v1, , 29 września 2024, dostępny pod adresem <https://arxiv.org/abs/2409.19798>;

Zhou Z., Xiang J., Chen C., and Su S., Quantifying and Analyzing Entity-Level Memorization in Large Language Models, arXiv:2308.15727v2 5 Nov 2023, dostępne na: <https://arxiv.org/abs/2308.15727> [↑](#footnote-ref-29)
29. Ekstrakcja obejmuje w szczególności przypadek, w którym dane osobowe są wydedukowane z samego modelu sztucznej inteligencji, przy niewielkim lub zerowym wykorzystaniu interfejsów zapytań. [↑](#footnote-ref-30)
30. Opinia Grupy Roboczej Art. 29 05/2014, s. 24 [↑](#footnote-ref-31)
31. Opinia Grupy Roboczej Art. 29 05/2014, s. 24 [↑](#footnote-ref-32)
32. Wyrok TSUE z dnia 19 października 2016 r., sprawa C-582/14, Breyer przeciwko Republice Federalnej Niemien (ECLI:EU:C:2016:779), pkt 43. [↑](#footnote-ref-33)
33. Obejmuje to takie cechy, jak unikalność rekordów w danych szkoleniowych, precyzja informacji, agregacja, randomizacja, a w szczególności to, jak wpływają one na podatność na identyfikację. [↑](#footnote-ref-34)
34. Obejmuje to elementy kontekstowe, takie jak ograniczenie dostępu tylko do niektórych osób i zabezpieczenia prawne [↑](#footnote-ref-35)
35. Wyrok TSUE z dnia 7 marca 2024 r., sprawa C-479/22 P, OC przeciwko Komisji Europejskiej (ECLI:EU:C:2024:215), pkt 50. [↑](#footnote-ref-36)
36. Wyrok TSUE z dnia 7 marca 2024 r., sprawa C-479/22 P, OC przeciwko Komisji Europejskiej (ECLI:EU:C:2024:215), pkt 50. [↑](#footnote-ref-37)
37. Wyrok TSUE z dnia 19 października 2016 r., sprawa C-582/14, Breyer przeciwko Republice Federalnej Niemiec (ECLI:EU:C:2016:779), pkt 46 oraz wyrok TSUE z dnia 7 marca 2024 r., sprawa C-479/22 P, OC przeciwko Komisji Europejskiej (ECLI:EU:C:2024:215), pkt 51. [↑](#footnote-ref-38)
38. Ricciato F., A Cautionary Reflection on (Pseudo-)Synthetic Data from Deep Learning on Personal Data, Privacy in Statistical Databases conference (PSD 2024), Antibes, France, September 2024, slajdy dostępne pod adresem: [https://cros.ec.europa.eu/system/files/2024 10/20240926 PSD2024 Ricciato v6 1.pdf](https://cros.ec.europa.eu/system/files/2024%2010/20240926%20PSD2024%20Ricciato%20v6%201.pdf) oraz Belkin M., Hsu D., Ma S., & Mandal S. (2019), Reconciling modern machine-learning practice and the classical bias-variance tradeoff. Proceedings of the National Academy of Sciences, 24 lipca 2019 r., 116(32) 15849-15854, dostępne pod adresem: <https://www.pnas.org/doi/10.1073/pnas.1903070116>. [↑](#footnote-ref-39)
39. Zob. wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r. [↑](#footnote-ref-40)
40. Tamże, pkt 1 [↑](#footnote-ref-41)
41. Sprawozdanie EROD z prac podjętych przez grupę zadaniową ChatGPT, przyjęte w dniu 23 maja 2024 r., pkt 14. [↑](#footnote-ref-42)
42. Sprawozdanie EROD z prac podjętych przez grupę zadaniową ChatGPT, przyjęte 23 maja 2024 r., pkt 23; Wytyczne EROD 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych na podstawie art. 25, wersja 2.0, przyjęte 20 października 2020 r., pkt 69; Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, zmienione i zatwierdzone przez EROD 25 maja 2018 r., pkt 2.przyjęte w dniu 11 kwietnia 2018 r., zatwierdzone przez EROD w dniu 25 maja 2018 r., pkt 2. [↑](#footnote-ref-43)
43. Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679, zmienione i przyjęte w dniu 11 kwietnia 2018 r., zatwierdzone przez EROD w dniu 25 maja 2018 r., pkt 5. [↑](#footnote-ref-44)
44. Zob. również motyw 39 RODO, który stanowi, że „powinno być przejrzyste dla osób fizycznych, że dotyczące ich dane osobowe są gromadzone, wykorzystywane, konsultowane lub w inny sposób przetwarzane oraz w jakim zakresie dane osobowe są lub będą przetwarzane [...]”. [↑](#footnote-ref-45)
45. Art. 13. ust 2 lit. f , RODO oraz art. 14 ust 2 lit. g RODO. [↑](#footnote-ref-46)
46. Sprawozdanie EROD z prac podjętych przez grupę zadaniową ChatGPT, przyjęte w dniu 23 maja 2024 r., pkt 27. [↑](#footnote-ref-47)
47. Ponadto art. 10 ust. 5 aktu o sztucznej inteligencji przewiduje szczegółowe zasady przetwarzania szczególnych kategorii danych osobowych w odniesieniu do systemów sztucznej inteligencji wysokiego ryzyka w celu zapewnienia wykrywania i korygowania uprzedzeń. [↑](#footnote-ref-48)
48. Opinia Grupy Roboczej Art. 29 03/2013 w sprawie ograniczenia celu (WP203), s. 15-16. [↑](#footnote-ref-49)
49. Zgodnie z art. 21 RODO, jeżeli osoba, której dane dotyczą, wniesie sprzeciw - z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych, administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. W związku z tym, dwa aspekty, które muszą zostać wzięte pod uwagę przez organy nadzorcze, to to, czy administrator jest w stanie wykazać takie istotne nadrzędne uzasadnione podstawy oraz czy można skorzystać z prawa do sprzeciwu. [↑](#footnote-ref-50)
50. TSUE, wyrok z dnia 4 lipca 2023 r., sprawa C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537), pkt. 106; TSUE, wyrok z dnia 11 grudnia 2019 r., sprawa C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA (ECLI:EU:C:2019:1064), pkt 40. Zob. również Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0 przyjęta w dniu 8 października 2024 r., pkt 12 i nast. Jak przypomniano w tych Wytycznych, ta „ocena powinna zostać przeprowadzona na początku przetwarzania, z udziałem inspektora ochrony danych (DPO) (jeżeli został wyznaczony) i powinna zostać udokumentowana przez administratora zgodnie z zasadą rozliczalności określoną w art. 5 ust. 2 RODO”. [↑](#footnote-ref-51)
51. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 14. [↑](#footnote-ref-52)
52. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 16. [↑](#footnote-ref-53)
53. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 17. [↑](#footnote-ref-54)
54. TSUE, wyrok z dnia 4 października 2024 r., sprawa C-621/22, Koninklijke Nederlandse Lawn Tennisbond (ECLI:EU:C:2024:857), pkt 49, w którym TSUE podkreślił, że prawnie uzasadniony interes nie może być sprzeczny z prawem. W tym względzie EROD podkreśla, że w zależności od przypadku przy ocenie zgodności z prawem danego interesu należy wziąć pod uwagę ramy prawne. Zob. na przykład: art. 26 ust. 3 i art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmieniającego dyrektywę 2000/31/WE (akt o usługach cyfrowych) („DSA”) w sprawie zakazanej reklamy ukierunkowanej na małoletnich; art. 5 ust. 1 i 2 aktu o sztucznej inteligencji w sprawie zakazanych praktyk sztucznej inteligencji (praktyki manipulacyjne i poniżej progu świadomości); przetwarzanie z naruszeniem praw własności intelektualnej oraz przepisy dyrektywy (UE) 2019/790 w sprawie praw autorskich i pokrewnych na jednolitym rynku cyfrowym. [↑](#footnote-ref-55)
55. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 28-30. [↑](#footnote-ref-56)
56. TSUE, wyrok z dnia 4 lipca 2023 r., sprawa C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537), pkt. 108 i 109, odnoszący się również do TSUE, wyrok z dnia 11 grudnia 2019 r., sprawa C-708/18, Asociaţia de Proprietari bloc M5AScaraA (ECLI:EU:C:2019:1064), pkt 48; TSUE, wyrok z dnia 9 listopada 2010 r., sprawy połączone C-92/09 i C93/09, Volker und Markus Schecke (ECLI: EU:C:2010:662), pkt 85 i 86; TSUE, wyrok z dnia 22 czerwca 2021 r., sprawa C-439/19, Latvijas Republikas Saeima (ECLI:EU:C:2021:504), pkt 98, 109, 110, 113. Zob. również na przykład: Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pośrednictwem urządzeń wideo, wersja 2.0, przyjęte w dniu 29 stycznia 2020 r., pkt 24-26 i 73; Wytyczne EROD 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online osobom, których dane dotyczą, wersja 2.0, przyjęte w dniu 8 października 2019 r., pkt 23-25; Opinia EROD 11/2024 w sprawie wykorzystania rozpoznawania twarzy w celu usprawnienia przepływu pasażerów na lotniskach, wersja 1.1, przyjęta w dniu 23 maja 2024 r., pkt 27. [↑](#footnote-ref-57)
57. Zob. TSUE, wyrok z dnia 16 grudnia 2008 r., sprawa C-524/06, Heinz Huber przeciwko Republice Federalnej Niemiec (ECLI:EU:C:2008:724), pkt 66. Również w tej samej sprawie zob. opinia rzecznika generalnego Poiaresa Maduro w sprawie C-524/06, Heinz Huber przeciwko Republice Federalnej Niemiec (ECLI:EU:C:2008:194), pkt 16, stwierdzająca: „właściwym testem jest tutaj test skuteczności, a jego zastosowanie należy do sądu krajowego. Musi on zadać pytanie, czy istnieją inne sposoby przetwarzania danych, za pomocą których organy imigracyjne mogłyby egzekwować przepisy dotyczące statusu pobytu. Jeśli odpowie na to pytanie twierdząco, scentralizowane przechowywanie i przetwarzanie danych obywateli Unii powinno zostać uznane za niezgodne z prawem. Nie jest konieczne, aby alternatywny system był najbardziej skuteczny lub odpowiedni; wystarczy, że będzie w stanie działać odpowiednio. Innymi słowy, nawet jeśli centralny rejestr jest bardziej skuteczny, wygodny lub przyjazny dla użytkownika niż jego alternatywy (takie jak zdecentralizowane, lokalne rejestry), te ostatnie są zdecydowanie preferowane, jeśli mogą być wykorzystane do wskazania statusu pobytu obywateli Unii”. [↑](#footnote-ref-58)
58. Zob. TSUE, wyrok z dnia 27 września 2017 r., sprawa C-73/16, Peter Puškár (ECLI:EU:C:2017:725), pkt 113: „Do sądu krajowego należy zatem ustalenie, czy sporządzenie kwestionowanego wykazu i umieszczenie nazwisk osób, których dane dotyczą, w takim rejestrze jest odpowiednie do osiągnięcia zamierzonych przez nie celów i czy nie istnieją inne, mniej restrykcyjne środki służące osiągnięciu tych celów”; zob. również na przykład opinia rzecznika generalnego Rantosa w sprawie C-252/21, Meta przeciwko Bundeskartellamt, ECLI:EU:C:2022:704, pkt 61. Bundeskartellamt, ECLI:EU:C:2022:704, pkt 61, w której stwierdzono: „[...] Konieczne jest zatem, aby istniał ścisły związek między przetwarzaniem a realizowanym interesem, w przypadku braku alternatyw, które są bardziej przyjazne dla ochrony danych, ponieważ nie wystarczy, aby przetwarzanie było jedynie użyteczne dla administratora”. [↑](#footnote-ref-59)
59. TSUE, wyrok z dnia 4 października 2024 r., sprawa C-621/22, Koninklijke Nederlandse Lawn Tennisbond (ECLI:EU:C:2024:857), pkt 51-53. [↑](#footnote-ref-60)
60. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 57. [↑](#footnote-ref-61)
61. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 31-60. [↑](#footnote-ref-62)
62. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 32. [↑](#footnote-ref-63)
63. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 32, odnoszące się również do wyroku TSUE z dnia 4 lipca 2023 r. w sprawie C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537), pkt 110. [↑](#footnote-ref-64)
64. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 38. [↑](#footnote-ref-65)
65. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 46. [↑](#footnote-ref-66)
66. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 39. [↑](#footnote-ref-67)
67. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 32. [↑](#footnote-ref-68)
68. Zob. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 43. [↑](#footnote-ref-69)
69. TSUE, wyrok z dnia 4 lipca 2023 r., sprawa C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537), pkt 116 [↑](#footnote-ref-70)
70. Patrz podsekcja „Interesy, podstawowe prawa i wolności osób, których dane dotyczą” powyżej. [↑](#footnote-ref-71)
71. Sekcja 2.3 Wytycznych EROD 1/2024 dotyczących przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjętych w dniu 8 października 2024 r. Więcej przykładów znajduje się również w motywie 75 RODO. [↑](#footnote-ref-72)
72. Zob. również TSUE, wyrok z dnia 4 lipca 2023 r., sprawa C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537, pkt 112); TSUE, wyrok z dnia 11 grudnia 2019 r., sprawa C-708/18, Asociaţia de Proprietari Bundeskartellamt (ECLI:EU:C:2023:537), pkt 112; TSUE, wyrok z dnia 11 grudnia 2019 r., sprawa C-708/18, Asociaţia de Proprietari bloc M5A-ScaraA (ECLI:EU:C:2019:1064), pkt 58; TSUE, wyrok z dnia 4 października 2024 r., sprawa C-621/22, Koninklijke Nederlandse Lawn Tennisbond (ECLI:EU:C:2024:857), pkt 55. [↑](#footnote-ref-73)
73. Na przykład w wyroku z dnia 4 lipca 2023 r. w sprawie C-252/21, Meta przeciwko Bundeskartellamt (ECLI:EU:C:2023:537), pkt 123, podczas gdy TSUE stwierdził, że „ulepszenia produktu” nie można co do zasady wykluczyć jako prawnie uzasadnionego interesu, stwierdził również, że „wątpliwe jest, czy [...] cel »ulepszenia produktu«, biorąc pod uwagę skalę tego przetwarzania oraz fakt, że użytkownik nie może racjonalnie oczekiwać, że dane te będą przetwarzane [...], może przeważać nad prawnie uzasadnionym interesem”. ] cel „ulepszenia produktu”, biorąc pod uwagę skalę tego przetwarzania i jego znaczący wpływ na użytkownika, a także fakt, że użytkownik nie może racjonalnie oczekiwać, że dane te będą przetwarzane [...], może przeważać nad interesami i prawami podstawowymi takiego użytkownika, w szczególności w przypadku, gdy użytkownik ten jest dzieckiem”. [↑](#footnote-ref-74)
74. Wytyczne 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 53. [↑](#footnote-ref-75)
75. Wytyczne 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 50-54. [↑](#footnote-ref-76)
76. Wytyczne 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 57. [↑](#footnote-ref-77)
77. Tamże. [↑](#footnote-ref-78)
78. Tamże. [↑](#footnote-ref-79)
79. Praktyki te mogą również wiązać się z dodatkowymi kwestiami, które nie są objęte niniejszą opinią, zob. na przykład Pagallo U., Ciani Sciolla J., Anatomy of web data scraping: ethics, standards, and the troubles of the law. European Journal of Privacy Law & Technologies, (2023) 2 s. 1 - 19, dostępny pod adresem: <https://doi.org/10.57230/EJPLT232PS> [↑](#footnote-ref-80)
80. Chyba że administrator wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. [↑](#footnote-ref-81)
81. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 68. [↑](#footnote-ref-82)
82. Wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, przyjęte w dniu 8 października 2024 r., pkt 12. [↑](#footnote-ref-83)
83. TSUE, wyrok z dnia 4 maja 2023 r., sprawa C-60/22, Bundesrepublik Deutschland (ECLI:EU:C:2023:373), pkt 55-57 [↑](#footnote-ref-84)
84. TSUE, wyrok z dnia 4 maja 2023 r., sprawa C-60/22, Bundesrepublik Deutschland (ECLI:EU:C:2023:373), pkt 53. [↑](#footnote-ref-85)
85. Wytyczne EROD 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego w RODO, wersja 2.1, przyjęte w dniu 7 lipca 2021 r., pkt 55. [↑](#footnote-ref-86)
86. Konieczne może być uwzględnienie szczególnych przepisów krajowych. Zob. na przykład art. 2-decies włoskiego kodeksu ochrony danych (dekret ustawodawczy 196/2003), który stanowi, że dane przetwarzane z naruszeniem zasad ochrony danych nie mogą być wykorzystywane. Pozostaje to bez uszczerbku dla innych krajowych ram prawnych, takich jak przepisy prawa karnego. [↑](#footnote-ref-87)
87. Zob. w tym względzie motyw 129 RODO, a także wyrok TSUE z dnia 26 września 2024 r. w sprawie C-768-21, TR przeciwko Land Hessen (ECLI:EU:C:2024:785), pkt 37; wyrok TSUE z dnia 7 grudnia 2023 r. w sprawach połączonych C-26/22 i C-64/22, SCHUFA Holding (Libération de reliquat de dette) (ECLI: EU:C:2023:958), pkt 57; oraz wyrok TSUE z dnia 14 marca 2024 r., sprawa C-46/23, Újpesti Polgármesteri Hivatal (ECLI:EU:C:2024:239), pkt 34. [↑](#footnote-ref-88)
88. W tym względzie opinia EROD 39/2021 w sprawie tego, czy art. 58 ust. 2 lit. g) RODO może służyć jako podstawa prawna dla organu nadzorczego do nakazania z urzędu usunięcia danych osobowych w sytuacji, gdy taki wniosek nie został złożony przez osobę, której dane dotyczą, pkt 28. Zob. również w tym względzie wyrok TSUE z dnia 14 marca 2024 r. w sprawie C46/23 Újpesti Polgármesteri Hivatal (ECLI:EU:C:2024:239), pkt 42. [↑](#footnote-ref-89)
89. Art. 5 ust 2 RODO i art. 24 RODO. [↑](#footnote-ref-90)
90. Art.16 lit. g i art. 47 aktu o sztucznej inteligencji. [↑](#footnote-ref-91)
91. Załącznik 5 pkt. 5 aktu o sztucznej inteligencji. [↑](#footnote-ref-92)
92. Motyw 26 RODO. [↑](#footnote-ref-93)