



**Stanowisko Izby Gospodarki Elektronicznej
w sprawie wniosku Komisji Europejskiej
dotyczącego Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego
rozporządzenia (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854
oraz dyrektywy 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do
uproszczenia cyfrowych ram legislacyjnych oraz uchylającego rozporządzenia
(UE)
2018/1807, (UE) 2019/1150, (UE) 2022/868 oraz dyrektywę (UE) 2019/1024
(Omnibus Cyfrowy)
i
zmieniającego rozporządzenia (UE) 2024/1689 i (UE) 2018/1139 w odniesieniu
do uproszczenia wdrażania zharmonizowanych zasad dotyczących sztucznej
inteligencji
(Omnibus Cyfrowy w sprawie AI)**

Warszawa, 12.12.2025 r.



Szanowni Państwo,

w nawiązaniu do konsultacji publicznych prowadzonych przez Ministerstwo Cyfryzacji dotyczących pakietu przepisów upraszczających prawo UE opublikowanych przez Komisję Europejską (wniosek dotyczący Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenia (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 oraz dyrektywy 2002/58/WE, (UE) 2022/2555 i (UE) 2022/2557 w odniesieniu do uproszczenia cyfrowych ram legislacyjnych oraz uchylającego rozporządzenia (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 oraz dyrektywę (UE) 2019/1024 (dalej: **Omnibus Cyfrowy**) i zmieniającego rozporządzenia (UE) 2024/1689 i (UE) 2018/1139 w odniesieniu do uproszczenia wdrażania zharmonizowanych zasad dotyczących sztucznej inteligencji (dalej: **Omnibus Cyfrowy w sprawie AI**), Izba Gospodarki Elektronicznej (dalej: **e-Izba**) przedstawia stanowisko dotyczące ww. regulacji.

I. Omnibus Cyfrowy

1. Projekt artykułu 88b RODO (art. 3 ust. 15 projektu Omnibusu Cyfrowego)

Zgodnie z proponowanym artykułem 88b RODO dostawcy przeglądarek internetowych, którzy nie są MŚP, musieliby zapewnić środki techniczne umożliwiające użytkownikom wyrażanie zgody lub jej odmowę oraz wykonywanie prawa do sprzeciwu za pomocą środków zautomatyzowanych i możliwych do odczytu maszynowego. Obowiązek ten ułatwia wprowadzenie scentralizowanych mechanizmów zarządzania plikami cookie, często kontrolowanych przez przeglądarki lub systemy operacyjne.

Zauważamy, że wprowadzenie scentralizowanych mechanizmów zarządzania plikami cookie będzie miało istotny wpływ na europejski rynek, w tym:

- wprowadzenie scentralizowanych mechanizmów zgody, zgodnie z wymogiem artykułu 88b, poważnie zaszkodziłoby szerszej europejskiej gospodarce cyfrowej, w tym MŚP;
- scentralizowany system zarządzania zgodą mógłby nie odpowiadać wszystkim preferencjom użytkowników, którzy wolą zachować sprawczość w zakresie wyborów dotyczących gromadzenia danych, często podejmując odmienne decyzje dla każdej strony internetowej lub aplikacji w zależności od treści lub usług;
- uniemożliwiłoby to europejskim firmom bezpośrednie pozyskiwanie zgody użytkowników lub stosowanie innych podstaw prawnych do przetwarzania danych niezbędnych do funkcjonowania, innowacji i finansowania ich produktów i usług;



- pozbawiłoby europejskie firmy możliwości zarządzania zgodą, w praktyce tworząc nowego pośrednika (przeglądarkę/system centralny) między wydawcą a jego odbiorcą, z ryzykiem powstania nowych „gatekeeperów” bez odpowiedniej refleksji regulacyjnej;
- istniejący już gatekeeperzy (często kontrolujący odpowiednie przeglądarki/systemy operacyjne) nadal uzyskiwaliby zgody na szeroką skalę, stawiając europejskie firmy w strukturalnie gorszej i konkurencyjnie słabszej pozycji oraz niwecząc postępy osiągnięte dzięki Aktowi o rynkach cyfrowych;
- sankcjonowałoby zgodę jako jedyną podstawę dostępu do danych osobowych, utrwalając obecny stan rzeczy, mimo że europejskie ramy prawne oferują wiele podstaw i wyjątków;
- konsolidacja stanów zgody i identyfikatorów w jednym centralnym repozytorium stworzyłaby atrakcyjny cel i pojedynczy punkt podatności/awarii dla cyberataków na wszystkie zależne usługi;
- wprowadziłoby fundamentalne zmiany bez oceny skutków, prowadząc do wysokich kosztów dla europejskich firm bez dowodów na uproszczenie zgodności czy poprawę doświadczeń użytkowników.

Instytucje unijne powinny unikać wprowadzania scentralizowanych systemów zarządzania zgodą. Systemy takie wcześniej nie zyskały akceptacji podczas negocjacji nad Rozporządzeniem ePrivacy i spotkały się z szeroką krytyką podczas „Cookie-Pledge Initiative”. Kluczowe jest, aby europejscy dostawcy stron internetowych i przedsiębiorstwa działające cyfrowo zachowali operacyjną i prawną możliwość pozyskiwania oraz zarządzania zgodą użytkowników – lub stosowania innych podstaw prawnych – bezpośrednio na poziomie strony internetowej, ponieważ bezpośrednia relacja z użytkownikami jest bardzo istotna.

Nakazanie dostawcom stron internetowych wprowadzenia zautomatyzowanych, możliwych do odczytu maszynowego mechanizmów zgody (zgodnie z proponowanym artykułem 88b RODO) otwiera drogę do szkodliwych scentralizowanych systemów zarządzania plikami cookie. Systemy te mogłyby koncentrować władzę, osłabić konkurencyjność europejskich firm cyfrowych i medialnych, zagrażać pluralizmowi mediów oraz tworzyć nowe ryzyka dla bezpieczeństwa, ostatecznie działając wbrew kluczowym celom wzmacniania konkurencyjności i innowacyjności Europy.

2. Projekt artykułu 88c RODO (art. 3 ust. 15 projektu Omnibusu Cyfrowego) - dostosowanie aktu o sztucznej inteligencji (AI Act) i RODO

Zdaniem e-Izby głównym problemem może okazać się niestabilna podstawa prawna dla szkolenia systemów AI, ponieważ powszechne poleganie na uzasadnionym interesie jest wysoce ocenne. Dodatkowo trudno jest przestrzegać zasady minimalizacji danych, ponieważ rozwój AI często wymaga rozległych zbiorów danych, co utrudnia firmom ocenę



minimalnej niezbędnej ilości danych. Z zadowoleniem przyjmujemy ukierunkowane zmiany w Akcie o AI oraz proponowane doprecyzowanie RODO, w szczególności potwierdzenie, że rozwój i szkolenie systemów AI mogą opierać się na podstawie uzasadnionego interesu. Ważne jest jednak, aby zasady regulujące stosowanie uzasadnionego interesu dla rozwoju i szkolenia AI pozostały jasne, spójne i łatwe do zrozumienia dla przedsiębiorstw.

Ponadto prawo do bycia zapomnianym (art. 17 RODO) stanowi poważne wyzwanie techniczne w kontekście modeli AI. Choć dane wejściowe mogą zostać usunięte, usuwanie danych z samych modeli jest technicznie złożone, podobne do usuwania konkretnych danych z systemów kopii zapasowych. Pragmatycznym rozwiązaniem byłoby dostosowanie artykułu 17 RODO poprzez wprowadzenie wyjątku opartego na nieproporcjonalności między wymaganymi działaniami (np. pełnym usunięciem modelu) a skutkami lub ryzykami. Ustanowienie tych dostosowań oraz odrębnej podstawy prawnej zapewniłoby potrzebną jasność co do właściwych podstaw prawnych przetwarzania danych na potrzeby AI.

II. Omnibus Cyfrowy w sprawie AI

1. Projekt artykułu 50 ust. 7 Aktu ws. AI (dalej: AIA)

W art. 50 AIA warto wyraźnie wskazać, że obowiązki dotyczące oznaczania wyników działania systemów AI jako sztucznie wygenerowanych lub zmanipulowanych spoczywają na dostawcach ADK, platform agentowych AI i frameworków. Jeśli dany framework pozwala na tworzenie agentów AI, to jego dostawca powinien zapewnić odpowiednie mechanizmy znakowania wyników (watermarkingu). Nie powinno się wymagać, aby twórca agenta AI, który często jest jedynie użytkownikiem biznesowym i nie ma specjalistycznej wiedzy technicznej, samodzielnie implementował takie rozwiązania. Byłoby to nieproporcjonalne.

Obowiązki związane ze znakowaniem wyników AI w przypadku tekstów powinny być stosowane w sposób proporcjonalny. Nie każdy tekst powinien posiadać techniczny znak wodny. Jeśli agent AI tworzy raporty dla konkretnych firm, a raporty te zawierają jasną informację dla użytkownika, że zostały wygenerowane przez AI i sama architektura danych pokazuje, które zasoby powstały z wykorzystaniem AI, dodatkowe techniczne oznaczenia nie są niezbędne.

Jeśli tekst jest wykorzystywany jako artykuł na blogu lub portalu informacyjnym, zgadzamy się, że techniczny znak wodny może być wymagany. Jednak w przypadkach, gdy:

- architektura techniczna i danych jest zbudowana tak, że jasno wynika, które zasoby są generowane przez AI; lub
- teksty są wykorzystywane wyłącznie wewnętrznie i zawierają informację dla użytkowników (ludzi), że zostały stworzone z użyciem AI,

- nie ma potrzeby wprowadzania dodatkowych wymogów dotyczących znaków wodnych.



2. Projekt art. 113 AIA

Propozycja Komisji, aby przesunąć w czasie stosowanie przepisów dotyczących systemów wysokiego ryzyka, jest rozwiązaniem pragmatycznym, pozwala bowiem zyskać dodatkowy czas na dopracowanie wytycznych, przyjęcie odpowiednich norm oraz przygotowanie się do nowych obowiązków. Problemem jest jednak brak pewności co do harmonogramu tych zmian, ponieważ zależą one od tego, kiedy powstaną narzędzia niezbędne do ich wdrożenia. Bez jasnej informacji o terminach podjęcia odpowiednich decyzji trudno określić, kiedy przepisy faktycznie zaczną obowiązywać. Powoduje to niepewność prawną po stronie przedsiębiorców i utrudnia im planowanie działań zgodnych z regulacją. Z tego względu proponujemy ustalenie bardziej przejrzystych terminów oraz jasnych warunków, które uruchamiałyby stosowanie poszczególnych obowiązków.

3. Uproszczenie i doprecyzowanie wdrożenia AIA

Wdrożenie Aktu o AI w kontekście biznesowym jest obecnie utrudnione przez znaczną niepewność regulacyjną, często zmuszającą firmy do podejmowania ryzykownych założeń. Kluczowe definicje – takie jak definicja AI czy „istotna ogólność ogólnego modelu AI” – są zbyt niejasne. Ponadto niektóre przepisy, np. wymóg mierzenia liczby FLOPS wykorzystanych do trenowania modelu w przypadku modeli dostrajanych, są nierealistyczne i w praktyce niemożliwe do wiarygodnego wdrożenia w całej branży.

Niejasności te wzmacniają wewnętrzne niespójności rozporządzenia, w którym deklarowane cele regulacyjne rozmiągają się z faktycznym brzmieniem przepisów lub z towarzyszącymi im oficjalnymi wytycznymi (np. sugestia, że model jednomodalny może być uznany za model ogólny). Tego rodzaju niepewność, połączona z opóźnieniami we wdrażaniu oraz potencjalnymi różnicami w implementacji krajowej w poszczególnych państwach UE, znacząco utrudnia planowanie strategiczne i operacyjne dużym przedsiębiorstwom międzynarodowym.

Aby uniknąć sytuacji, w której obecne brzmienie przepisów przypadkowo blokowałoby działalność biznesową lub sprzyjało niezamierzonej niezgodności, wszystkie definicje i obowiązki powinny zostać uproszczone i jednoznacznie doprecyzowane. W szczególności warto rozważyć usunięcie nadmiernie szczegółowych kryteriów trudnych do pomiaru lub egzekwowania, zwłaszcza tych dotyczących ryzyka systemowego. Co równie istotne, wszystkie przepisy oraz oficjalne materiały wyjaśniające muszą być spójne, a przejrzysta, wiążąca mapa drogowa wdrażania powinna zostać jasno opublikowana i konsekwentnie przestrzegana przez instytucje nadzorcze. Tylko w ten sposób przedsiębiorcy będą mogli działać w stabilnym otoczeniu regulacyjnym i skutecznie zapewniać zgodność z przepisami.

poświadczenie złożenia podpisów i pieczęci elektronicznych

Certyfikat dla dokumentu o Autenti ID: 31e4a37e-7719-44f7-975c-8c9a299e3f70
utworzonego: 2025-12-12 13:12 (GMT+01:00)

Dokument przekazany do podpisu przez Izba Gospodarki Elektronicznej biuro@eizba.pl, został zabezpieczony pieczęcią elektroniczną Autenti przed wprowadzeniem nieautoryzowanych zmian.



2025-12-12 13:12 (GMT+01:00)

Patrycja Staniszevska

patrycja.staniszevska@eizba.pl

Izba Gospodarki Elektronicznej

NIP: 7010391922 | Prezes Zarządu



**Podpis elektroniczny
zabezpieczony pieczęcią Autenti**

Uwierzytelnienie: e-mail

Powód: Podpisanie dokumentu

Adres IP: 109.206.213.204

2025-12-12 13:14 (GMT+01:00)

Autentyczność oraz integralność podpisanego dokumentu przed wprowadzeniem nieautoryzowanych zmian została zabezpieczona pieczęcią elektroniczną Autenti.



2025-12-12 13:14 (GMT+01:00)

Niniejszy dokument stanowi poświadczenie wykonania usługi zaufania, w tym złożenia podpisów elektronicznych, zgodnie z zasadami opisanymi w Polityce.

Osoby podpisujące dokument złożyły podpisy elektroniczne zgodnie z zasadami opisanymi w Polityce Usług Zaufania Autenti dla podpisów elektronicznych Autenti oraz obsługi podpisywania dokumentów (dostępnej na: <https://autenti.com/pl/regulaminy>) oraz oświadczyły, że znają i akceptują treść podpisywanego dokumentu a także potwierdziły poprawność i prawdziwość danych służących do złożenia podpisu elektronicznego.

W ramach składania podpisów elektronicznych przeprowadzono uwierzytelnienie podpisujących.

Usługa została wykonana zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Rozporządzenie eIDAS).

Karta podpisów stanowi poświadczenie Autenti w zakresie realizacji poszczególnych usług zaufania, zgodnie z zasadami ich świadczenia oraz definicjami zawartymi w Polityce.