



Stanowisko Izby Gospodarki Elektronicznej w sprawie projektowanych rozwiązań pakietu Digital Omnibus dotyczących zarządzania zgodą na poziomie przeglądarki („browser-level consent”)

1. Uwagi wprowadzające

Z aprobatą odnosimy się do deklarowanego przez Komisję Europejską celu uproszczenia ram prawnych regulujących ochronę danych osobowych i prywatności w środowisku cyfrowym oraz do potrzeby przeciwdziałania zjawisku tzw. „zmęczenia zgodami”, które w praktyce znacząco osłabia funkcję informacyjną i ochronną instytucji zgody.

Natomiast stoimy na zdecydowanym stanowisku, że propozycje przedstawione w pakiecie Digital Omnibus, w szczególności w zakresie projektowanych art. 88a i 88b RODO, w obecnym kształcie nie realizują w pełni deklarowanych celów uproszczenia i poprawy doświadczeń użytkowników. Przeciwnie – niosą one ze sobą istotne ryzyka systemowe, prawne i gospodarcze, które mogą prowadzić do dalszego skomplikowania reżimu regulacyjnego, wzrostu niepewności interpretacyjnej oraz pogorszenia warunków funkcjonowania europejskiego rynku cyfrowego, zwłaszcza dla małych i średnich przedsiębiorstw.

2. Pozytywna ocena wybranych zmian systemowych

Popieramy zmiany zaproponowane w art. 3 pkt 1 lit. a wniosku, przewidujące doprecyzowanie definicji danych osobowych w art. 4 RODO. Wyraźne wskazanie, że informacje nie mają charakteru danych osobowych dla danego podmiotu, jeżeli podmiot ten – przy uwzględnieniu środków, co do których istnieje uzasadnione prawdopodobieństwo ich wykorzystania – nie jest w stanie zidentyfikować osoby fizycznej, której dane dotyczą, wprowadza potrzebną klarowność pojęciową. Zmiana ta potwierdza, że dane pseudonimizowane nie zawsze powinny być traktowane jako dane osobowe dla wszystkich uczestników procesu przetwarzania, co ma istotne znaczenie dla pewności prawa i proporcjonalności obowiązków nakładanych na podmioty przetwarzające.

3. Zasadnicze wątpliwości wobec koncepcji browser-level consent

Pomimo zasadności diagnozy problemu „zmęczenia zgodami” (ang. *consent fatigue*), proponowany mechanizm scentralizowanego wyrażania preferencji użytkownika na poziomie przeglądarki, oparty na automatycznych i maszynowo odczytywalnych sygnałach, budzi daleko idące zastrzeżenia.

Przede wszystkim centralizacja decyzji użytkownika na poziomie przeglądarki prowadzi do oderwania zgody od konkretnego kontekstu przetwarzania. Zgoda wyrażana w sposób ogólny, w oderwaniu od informacji o tożsamości administratora, szczegółowych celach przetwarzania, kategoriach odbiorców danych czy warunkach jej wycofania, może w praktyce nie spełniać wymogów zgody „konkretnej” i „świadomej” w rozumieniu RODO. Kwestie prywatności są bowiem z natury kontekstowe – użytkownicy podejmują odmienne decyzje w



zależności od rodzaju usługi, treści, zaufania do danej marki czy charakteru relacji z lokalnym przedsiębiorcą. Mechanizm przeglądarkowy nie daje realnej możliwości odzwierciedlenia takich indywidualnych, zależnych od sytuacji wyborów. Co więcej ogranicza on autonomię jednostki i stoi w sprzeczności z założeniami ochrony prawa do prywatności.

W konsekwencji użytkownicy mogą być skłaniani do dokonywania masowych, uproszczonych decyzji, takich jak globalne odrzucenie wszelkich plików cookies, co niekoniecznie odpowiada ich rzeczywistym preferencjom. Mogłoby okazać się, że odmowa zgody na przetwarzanie danych byłaby relatywnie łatwa i uproszczona (opt-out), natomiast wyrażenie skutecznej, prawnie ważnej zgody o charakterze aktywnym i pozytywnym stawałoby się istotnie trudniejsze (opt-in). Paradoksalnie może to prowadzić do ograniczenia ich sprawczości, a nie jej wzmocnienia, oraz do obniżenia poziomu personalizacji usług, której użytkownicy coraz częściej oczekują.

Na szczególną uwagę zasługuje wyjątek przewidziany dla dostawców usług medialnych, który w praktyce umożliwia dalsze samodzielne pozyskiwanie zgód na dotychczasowych zasadach mimo sygnałów browser-level consent. Rozwiązanie to osłabia zasadniczy cel reformy, jakim jest ograniczenie „zmęczenia zgodami”, a jego uzasadnienie nie wydaje się spójne względem innych kategorii usług online. Krytycznie do tego wyjątku odnoszą się również EROD i EIOD, wskazując dodatkowo, że działania reklamowe i trackingowe w środowisku medialnym są często realizowane nie tylko przez sam podmiot medialny, lecz również przez podmioty trzecie obecne na stronie lub w aplikacji. Poza tym nie jest jasne, dlaczego akurat jedynie dostawcy usług medialnych mieliby być objęci wyjątkiem. Abstrahując od dodatkowych komplikacji regulacyjnych, powoduje to tworzenie nierównych warunków dla różnych podmiotów działających w gospodarce cyfrowej.

Zastrzeżenia budzi także projektowane wyłączenie niektórych obowiązków wobec dostawców przeglądarek będących MŚP. Również w tym zakresie EROD i EIOD wskazały na brak przekonującego uzasadnienia dla różnicowania sytuacji poszczególnych uczestników rynku.

Dodatkowo może dojść do osłabienia zaufania do prawodawstwa unijnego ze względu na wprowadzenie tak istotnej zmiany w zakresie przetwarzania danych bez oceny skutków regulacji (impact assessment). Skuteczność samego rozwiązania technicznego, na której opierać się mają proponowane założenia pozostaje niesprawdzona, a dostępne dowody nie potwierdzają, że mogłaby realnie uprościć proces przestrzegania przepisów lub poprawić doświadczenie użytkowników.

4. Zaburzenie systemowej spójności RODO i ePrivacy

Projektowane rozwiązania pogłębiają również problem „rozszczepienia” reżimu ochrony informacji na urządzeniach końcowych pomiędzy RODO a dyrektywę ePrivacy ze względu na niejasne ostatecznie kryterium, czy dochodzi do przetwarzania danych osobowych czy nie. Utrzymanie art. 5 ust. 3 dyrektywy ePrivacy w odniesieniu do informacji niebędących danymi osobowymi przy jednoczesnym wprowadzaniu równoległych regulacji do RODO skutkuje dalszym nakładaniem się podstaw normatywnych oraz potencjalną wielotorowością nadzoru.



W praktyce identyfikatory techniczne i pliki cookie często zawierają zarówno elementy o charakterze danych osobowych, jak i informacje czysto techniczne. Powoduje to, że te same operacje mogą jednocześnie podlegać RODO oraz przepisom implementującym dyrektywę ePrivacy, co prowadzi do zwiększenia niepewności prawnej, ryzyka sprzecznych interpretacji i dublowania obowiązków. Zamiast upraszczania systemu, projekt w obecnej formie może jeszcze bardziej go skomplikować.

Proponujemy, aby w ostatecznym kształcie przepisów przyjmowanych w ramach pakietu Digital Omnibus zasady dotyczące dostępu do informacji przechowywanych na urządzeniach końcowych oraz ich zapisywania zostały uregulowane w sposób zapewniający jednolity mechanizm stosowania prawa oraz spójny system nadzoru. Kluczowe jest wyeliminowanie równoległego funkcjonowania odrębnych podstaw prawnych odnoszących się do tych samych czynności.

W tym celu zasadne byłoby uchylenie art. 5 ust. 3 dyrektywy ePrivacy i przeniesienie ujętych w nim regulacji dotyczących urządzeń końcowych do RODO. Rozwiązanie to pozwoliłoby na stworzenie jednolitego i spójnego modelu egzekwowania przepisów, bez uszczerbku dla bezpieczeństwa. Nieuprawniony dostęp do urządzeń nadal pozostawałby bowiem surowo zakazany na podstawie obowiązujących krajowych regulacji dotyczących przestępczości komputerowej.

5. Ryzyko nieskuteczności i nowych form „zmęczenia zgodą”

Istnieje ponadto poważne ryzyko, że projektowane rozwiązanie nie tylko nie wyeliminuje zjawiska „consent fatigue”, lecz doprowadzi do jego nowej, bardziej intensywnej formy. W warunkach ograniczonego dostępu do reklamy cyfrowej upowszechnić się mogą modele biznesowe typu „pay or OK”, w których użytkownik stawiany jest przed alternatywą: zmiana ustawień przeglądarki i akceptacja cookies albo odpłatny dostęp do usług. W efekcie zamiast uproszczenia doświadczenia użytkownika powstanie mechanizm zwiększający presję ekonomiczną i poznawczą.

6. Wątpliwości dotyczące okresu 6 miesięcy bez ponownego pytania o zgodę

Dodatkowe zastrzeżenia budzi projektowany obowiązek respektowania odmowy zgody przez okres co najmniej sześciu miesięcy. Okres ten jawi się jako nieproporcjonalnie długi i niedostosowany do realiów korzystania z usług cyfrowych. Użytkownicy mogą zmieniać zdanie, chcieć skorzystać z usług wymagających zgody lub nie być w stanie łatwo odnaleźć odpowiednich ustawień. W praktyce może to prowadzić do niedogodności, zwłaszcza w kontekście transakcji e-commerce.

Z punktu widzenia technicznego obowiązek ten rodzi również poważne problemy wykonalności, ponieważ jego realizacja wymagałaby stosowania trwałych mechanizmów identyfikacji użytkowników w środowisku wielourzędzeniowym, co pozostaje w sprzeczności z zasadą minimalizacji danych. Zasadne byłoby rozważenie znaczącego skrócenia tego okresu, np. do jednego miesiąca.

7. Skutki gospodarcze i rynkowe



Z perspektywy rynku cyfrowego – w szczególności e-commerce, reklamy internetowej oraz MŚP – wprowadzenie browser-level consent wiąże się z istotnymi ryzykami ekonomicznymi. Automatyczne sygnały przeglądarskie mogą w praktyce uniemożliwić wielu podmiotom dotarcie do nowych użytkowników i rozwój działalności w oparciu o dotychczasowe modele marketingowe. Szczególnie dotkliwe będzie to dla mniejszych przedsiębiorstw, które nie dysponują własnymi, rozbudowanymi bazami danych klientów i w większym stopniu polegają na narzędziach reklamy cyfrowej.

Dostępne analizy wskazują, że mechanizm zgody na poziomie przeglądarki może prowadzić do odmowy zgody przez około 60–65% użytkowników, co przekłada się na szacowany spadek przychodów z reklamy cyfrowej w Unii Europejskiej rzędu 40–50 mld euro rocznie (30–35% obecnych przychodów). Każdy dodatkowy 1% użytkowników odmawiających zgody oznacza dalszy spadek przychodów reklamodawców o 600–800 mln euro rocznie. Negatywne skutki obejmą również reklamę kontekstową, której koszty konwersji mogą wzrosnąć od 31 do nawet 73% ze względu na ograniczenie możliwości pomiaru i optymalizacji kampanii¹.

Podmioty z branży e-commerce będą ponosić wyższe koszty marketingu przy jednoczesnym spadku jego efektywności, co przełoży się na wzrost cen dla konsumentów. Odmowa zgody przez użytkowników spowoduje natychmiastowy spadek dostępnych danych first-party, ograniczy modelowanie atrybucji, osłabi kampanie performance i może uniemożliwić remarketing oraz budowanie profili klientów. Centralne sygnały przeglądarskie zredukują różnice między stronami i pozbawią administratorów możliwości zwiększania współczynnika zgód poprzez lepszy design czy sposób prezentacji banerów, prowadząc do ujednolicenia i mniejszej kreatywności serwisów. Dodatkowo brak możliwości ponownego zapytania o zgodę przez co najmniej sześć miesięcy oraz silniejsza zależność skuteczności kampanii od ustawień przeglądarek pogłębią zależność europejskich przedsiębiorstw od podmiotów spoza UE.

W dalszej perspektywie reforma może sprzyjać marginalizacji europejskich MŚP oraz monopolizacji rynku przez największe globalne podmioty technologiczne, które dysponują własnymi ekosystemami danych i bezpośrednimi relacjami z użytkownikami.

8. Podsumowanie

Uważamy, że przeciwdziałanie zjawisku „zmęczenia zgodami” jest potrzebne. W pełni podpisujemy się również pod inicjatywami mającymi na celu upraszczanie otoczenia regulacyjnego. Stoimy jednocześnie na stanowisku, że projektowane rozwiązania w zakresie browser-level consent w obecnym kształcie niosą ze sobą ryzyko skutków odwrotnych w stosunku do zamierzonych. Zamiast zwiększenia przejrzystości będą prowadzić do niepewności prawnej, a zamiast wzmocnienia ochrony prywatności – do wymuszania bardziej inwazyjnych mechanizmów technicznych oraz osłabienia konkurencyjności europejskiej gospodarki cyfrowej.

¹ Gone in one click. Assessing the socio-economic impact of browser-level consent in the EU, an Implement Consulting Group analysis commissioned by Google, <https://implementconsultinggroup.com/article/gone-in-one-click> (dostęp: 9.04.2026 r.).



W związku z tym apelujemy o ponowne, pogłębione przeanalizowanie projektowanych przepisów, przeprowadzenie rzetelnej oceny skutków regulacji oraz skoncentrowanie dalszych prac legislacyjnych na rozwiązaniach proporcjonalnych, technicznie wykonalnych i rzeczywiście wspierających zarówno ochronę praw użytkowników, jak i rozwój europejskiego rynku cyfrowego.