

Warszawa, 9 listopada 2020 r.
KL/523/363/AM/2020

Pan

Mateusz Morawiecki

Prezes Rady Ministrów,
Minister Cyfryzacji

Szanowny Panie Premierze,

W nawiązaniu do zaproszenia do konsultacji najnowszej wersji rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE, sygn. 9931/20 (dalej: rozporządzenie *ePrivacy*), które będzie omawiane na najbliższym posiedzeniu grupy roboczej Rady UE (WP TELE) dnia 11 listopada br., w załączeniu, Konfederacja Lewiatan przesyła stanowisko wobec projektu.

Z poważaniem,



Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:

- **Pan Marek Zagórski** - Sekretarz Stanu, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, KPRM
- **Pani Agnieszka Krauzowicz** - Dyrektor Departamentu Telekomunikacji, KPRM
- **Pani Justyna Romanowska** - Radca, Koordynator Referatu Cyfrowego, Stałe Przedstawicielstwo RP przy UE

Załącznik:

Stanowisko Konfederacji Lewiatan wobec projektu rozporządzenia *ePrivacy* z dnia 4.11.2020 r. (sygn. 9931/20).



**Stanowisko Konfederacji Lewiatan wobec projektu rozporządzenia *ePrivacy* z dnia 4.11.2020 r.
(sygn. 9931/20)**

I. Uwagi ogólne

Na wstępie pragniemy wyrazić głębokie rozczarowanie przedstawionym przez Prezydencję niemiecką dokumentem. Mamy świadomość, że Prezydencja może dążyć do finalizacji prac nad tym projektem, dlatego też w przypadku głosowania nad wersją w brzmieniu przedstawionym w wersji z 4 listopada, apelujemy o jej odrzucenie.

W naszej ocenie, projekt wymaga jeszcze wielu zmian, jako że jego przepisy są nieprzystosowane do realiów technicznych, biznesowych i kontraktowych świadczenia usług, których dotyczy. Ponadto, tak rygorystyczne ograniczenie przetwarzania metadanych bardzo odchodzi od ducha RODO i poprzez faktyczne uniemożliwienie dalszego przetwarzania (na podstawie uzasadnionego interesu) z pewnością nie będzie sprzyjać budowaniu konkurencyjnych usług cyfrowych w UE.

Jest dla nas niezrozumiałe, dlaczego projekt w wersji z 4 listopada usuwa, a tym samym wyklucza możliwość przetwarzania danych w oparciu o przesłankę uzasadnionego interesu, jako jedną z podstaw przetwarzania. Oparcie przetwarzania wyłącznie na zgodzie użytkownika (z drobnymi wyjątkami) nie znajduje racjonalnego uzasadnienia, w szczególności w zakresie przetwarzania danych statystycznych (niezbędnych dla badania świadczenia usługi przez dostawcę), które stanowią dane zagregowane, które nie opisują konkretnego użytkownika, a więc nie wydaje się zasadne, aby były oparte o zgodę konkretnego użytkownika. Na gruncie RODO z powodzeniem funkcjonuje i jest w praktyce wykorzystywana przesłanka prawnie uzasadnionego interesu administratora danych, nie skutkując jednocześnie zagrożeniami dla ochrony danych osobowych. Z pełną odpowiedzialnością można powiedzieć, że z perspektywy przedsiębiorców i prowadzenia działalności gospodarczej przesłanki w postaci uzasadnionego interesu oraz niezbędności do zawarcia lub wykonania umowy, obok zgody, stanowią podstawowe przesłanki przetwarzania danych osobowych na gruncie RODO, które gwarantuje wysoki poziom ochrony danych osobowych, bez względu na to, na jakiej podstawie dane są przetwarzane. Biorąc powyższe pod uwagę całkowicie niezrozumiałe i szkodliwe jest przyjęcie odmiennego podejścia w projekcie e-Privacy i usunięcie z niego przesłanki usprawiedliwionego interesu, co powoduje, że projekt tego dokumentu coraz bardziej oddala się nie tylko od potrzeb i realiów społeczeństwa informacyjnego, ale również od RODO, które powinno być punktem odniesienia dla wszystkich innych unijnych i krajowych regulacji dotyczących przetwarzania danych osobowych i ochrony prywatności.

Uzasadniony interes umożliwiłby dostawcom ECS, w tym operatorom telekomunikacyjnym i kablowym, odpowiedzialne wykorzystywanie metadanych w poszczególnych przypadkach, z uwzględnieniem praw użytkowników końcowych, interesów dostawcy i, na przykład, szerszych interesów społecznych. Jest to zgodne z zasadą rozliczalności zapisaną w RODO, która wymaga dokładnej oceny danej operacji przetwarzania danych. Wprowadzenie takiej podstawy prawnej stanowiłoby również znaczną zachętę



do rozwoju sieci europejskich i Internetu rzeczy, w których złożone relacje między wieloma podmiotami opierają się na przetwarzaniu danych.

Można także odnieść wrażenie, że projektodawcy, kierując się słuszną skądinąd potrzebą ochrony prywatności użytkowników, kompletnie nie rozumieją na jakich zasadach (w tym technicznych) oparte jest świadczenie usług i jak istotną rolę odgrywa przewidziana w RODO przesłanka niezbędności do zawarcia lub wykonania umowy, która jest osobną od zgody oraz uzasadnionego interesu podstawą prawną przetwarzania. I tak np. w odniesieniu do danych lokalizacyjnych przetwarzanych przez dostawców usług komunikacji elektronicznej (patrz zmiany w motywie 17 projektu rozporządzenia), jeżeli abonent zawierając umowę na świadczenie usług komunikacji elektronicznej nie wyrazi zgody na przetwarzanie takich danych, to nie będzie można świadczyć mu usług, gdyż dane takie są niezbędne do wykonania usługi w sieci mobilnej. Zatem w przypadku przetwarzania danych lokalizacyjnych, niezbędnych do świadczenia usług komunikacji elektronicznej w sieciach mobilnych, podstawą prawną przetwarzania danych musi być niezbędność do zawarcia i wykonania umowy, a nie zgoda. Oparcie przetwarzania danych na zgodzie spowoduje, że odwołanie zgody przez abonenta (do czego abonent ma zawsze prawo) będzie skutkowało brakiem możliwości wykonania na rzecz abonenta usług komunikacji elektronicznej, pomimo tego, że abonenta będzie wiązała z dostawcą umowa na świadczenie takich usług. Ponadto, w takim scenariuszu trudno powiedzieć jak powinien zachować się dostawca usług, jeśli abonent zawierając umowę na usługi komunikacji elektronicznej jednocześnie nie wyrazi zgody na przetwarzanie danych lokalizacyjnych niezbędnych do wykonania tej umowy (a przecież zgodnie z RODO nie można uzależniać zawarcia umowy od wyrażenia zgody). Tak samo w przypadku zamawianych przez użytkownika usług zapewnienia ochrony przed nadużyciami, ochrony bezpieczeństwa, do działania których niezbędne jest przetwarzanie metadanych (patrz nowe brzmienie motywu 18), podstawą takiego przetwarzania powinna być niezbędność do zawarcia lub wykonania umowy (jak w RODO), a nie zgoda. Pobieranie zgody na coś, co jest niezbędne do wykonania umowy, którą użytkownik przecież dobrowolnie zawiera i co jest niezbędne do wykonania zamówionej przez niego usługi, to jak prośenie użytkownika najpierw o to, aby zgodził się zawrzeć umowę, a potem, odrębnie prośenie go o to, aby zgodził się na wykonanie umowy, którą wcześniej dobrowolnie zawarł. Dlatego na gruncie RODO - bardzo słusznie - zgoda i wykonanie umowy to dwie, odrębne i niezależne podstawy prawne pozwalające na przetwarzanie danych osobowych. Jeżeli dane są przetwarzane na podstawie jednej z nich, to druga nie ma zastosowania.

W przypadku usług komunikacji elektronicznej, jak również usług dodatkowych i towarzyszących, oparcie przetwarzania danych na zgodzie, tam, gdzie chodzi o przetwarzanie danych niezbędnych do wykonania umowy i świadczenia usługi, będzie prowadziło do możliwości zakwestionowania wszystkich umów i relacji z klientami, gdyż powstanie pytanie, co ma się stać z umową zawartą z użytkownikiem, jeśli ten sam użytkownik nie wyrazi albo odwoła zgodę na przetwarzanie danych niezbędnych do wykonania umowy i świadczenia usługi – usługa ma zostać użytkownikowi wyłączona pomimo tego, że będzie on związany umową? Widać więc wyraźnie, że projektowane przepisy doprowadzić mogą do absurdu. Z tego względu postulujemy odrzucenie zmian w motywach 17, 17aa, 17 b (pierwszy akapit); 18 oraz art. 6b (ca) (e).



Zwracamy uwagę, że skreślony motyw 17b odzwierciedlał rozumienie przez prezydencję uzasadnionego interesu i wymieniał kilka przykładów uzasadnionego interesu: oszustwa, fakturowanie i wzajemne połączenia, zarządzanie siecią i optymalizacja, spełnianie obowiązkowych wymogów technicznych dotyczących jakości usług, badania naukowe i obliczenia statystyczne.

Wnosimy ponadto o przywrócenie wykreślonego z art. 6 punktu (d). Przedsiębiorcom zdecydowanie potrzebny jest przepis jak ten, bezpośrednio stosowany, który przesądza wprost, że mogą oni przetwarzać dane w każdym przypadku, w którym przetworzenie danych jest potrzebne do wykonania ciążącego na nich obowiązku prawnego. Analogiczna podstawa prawna istnieje w RODO. Usunięcie tego przepisu spowoduje dla przedsiębiorców niepewność prawną i możliwe wątpliwości interpretacyjne przy zestawianiu przepisów krajowych z przepisami rozporządzenia e-Privacy. Usunięcie tego przepisu spowoduje, że każdy przypadek, w którym przedsiębiorca będzie przetwarzał dane na potrzeby wywiązania się z ciążących na przedsiębiorcy obowiązków prawnych, będzie obarczony niepewnością prawną i ryzykiem regulacyjnym, gdyż na poziomie e-Privacy brakować będzie generalnego przepisu, który na wzór RODO jednoznacznie przesądza, że przetwarzanie danych na potrzeby wywiązania się z obowiązków prawnych jest legalne. Problemu tego nie rozwiązuje w najmniejszym stopniu art. 11 projektu e-Privacy, który de facto odsyła do prawodawstwa krajowego, co spowoduje, że legalność przetwarzania danych na potrzeby wykonania obowiązków prawnych będzie uzależniona od brzmienia poszczególnych przepisów prawa krajowego, nakładających takie obowiązki, co będzie wymagało analizy prawnej każdej takiej sytuacji indywidualnie, w miejsce przepisu, który generalnie i kompleksowo wyjaśnia takie sytuacje.

Ponadto, skomentować należy usunięcie lit. (ca) z art. 6b ust. 1 projektu rozporządzenia. Domyślać się można, że usunięcie tego punktu wiąże się ze zmianami w lit. (b) tego artykułu, a w ocenie autorów tych zmian w obecnym kształcie brzmienie lit. (b) konsumuje treść lit. (ca). Brzmienie lit. (ca) miało stanowić jednoznaczną podstawę do przetwarzania danych niezbędnych do wykonania usług komunikacji elektronicznej. Bez tego punktu legalność przetwarzania danych na potrzeby świadczenia usług komunikacji elektronicznej będzie musiała zostać wyinterpretowana z przepisu dotyczącego wykonania umowy (lit. (b)), a nie wprost z przepisu dotyczącego wykonania usługi (usuwany lit. (ca)), a trzeba pamiętać, że przepis w lit. (ca) jako przykładowe działania w ramach wykonania umowy wymienia naliczanie opłat za korzystanie z usług czy przeciwdziałanie nadużyciom, nie wymieniając świadczenia usługi komunikacji elektronicznej. Biorąc powyższe pod uwagę brzmienie lit. (b) powinno zostać zmienione tak, aby świadczenie usługi komunikacji elektronicznej zostało wskazane (obok naliczania opłat i przeciwdziałania nadużyciom), jako przykład działania mieszczącego się w pojęciu wykonania umowy (co wydaje się oczywistością, ale przy tak skomplikowanym brzmieniu i logice projektowanych przepisów może wprowadzać element całkowicie niepotrzebnej niepewności prawnej, w szczególności, że autorzy kolejnych wersji tekstu wstawiają w kolejnych przepisach sformułowania, które mają zapewnić, że przetwarzania będzie dopuszczalne tylko i wyłącznie w przypadkach wyraźnie wskazanych w rozporządzeniu, wykluczając tym samym wszelkie rozszerzające wykładnie przepisów prawa).



Pragniemy też zwrócić uwagę na nieprecyzyjność proponowanych w motywie 20 określeń:

„genuine choice” oraz „a few alternatives” : „... Conversely, in some cases, making access to website content dependent on the use of such cookies may be considered, in the presence of a clear imbalance between the end user and the service provider as depriving the end-user of a genuine choice (...) Similarly, such imbalance could exist when the end-user has only a few or no alternatives to the service”. Istnieje ryzyko dużej uznaniowości w zakresie tego, co stanowi lub nie autentyczny wybór użytkownika, oraz czy „only a few alternatives” oznacza, że jeśli są dwie opcje do wyboru, użytkownik faktycznie nie ma autentycznego wyboru? W przypadku usług dostępu do treści w modelu reklamowym wydaje się, że możliwość wyboru przez użytkownika alternatywnej opcji usługi płatnej, powinna być wyraźnie wskazana jako jedna z przesłanek spełniających kryterium autentycznego wyboru.

Wyrażamy zastrzeżenia, co do zmiany w motywie 26 - dodanie tekstu” “... including by requiring providers to enable and assist competent authorities in carrying out lawful interception”. Skoro rozporządzenie w zakresie obowiązków na rzecz bezpieczeństwa państwa w art. 11 de facto odsyła do przepisów prawa krajowego, to jednocześnie to samo rozporządzenie nie powinno przesądzać czy określać, jak szeroki zakres obowiązków powinien ciążyć na przedsiębiorcach, jako że to również powinno zostać określone prawem krajowym, w ramach wykonywania art. 11 e-Privacy.

II. Uwagi szczegółowe

1. Organy regulujące e-prywatność zostaną objęte przepisami o niezależności, o których mowa w art. 51-54 RODO (patrz art. 18): nie jest to wystarczające i przepisy powinny wyraźnie uznawać One Stop Shop. Projekt dokonuje deharmonizacji, nie przewidując mechanizmu one-stop-shop znanego z RODO, potencjalnie poddając firmy jurysdykcji nawet 54 (po 2a na każde państwo członkowskie) urzędów regulacyjnych, co w oczywisty sposób będzie szkodziło osiągnięciu w pełni funkcjonalnego jednolitego rynku cyfrowego w UE.
2. Artykuł 8 wymaga ponownego rozważenia. Podstawowym celem artykułu powinno być zajęcie się najważniejszymi problemami wokół „plików cookies”, tzw. „zmęczenie zgodą” (consent fatigue) i brakiem pewności co do tego, jak reguły dotyczące plików cookie odnoszą się w praktyce do RODO oraz zapewnienie kontroli użytkownikom. W szczególności ponownego przemyślenia wymaga propozycja zawężenia wyjątku do przypadku zgody, gdy pliki cookie są „technicznie” niezbędne do świadczenia usług „wyraźnie” żądanych przez użytkownika końcowego. „Wyraźny wniosek” po prostu powraca do mechanizmu zabezpieczenia „zgody”, zawężając wyjątek tak bardzo, że pokrywa się on z wymogiem zgody.
3. Art. 6a ust. 2 powinien zostać usunięty. Dwoch lub więcej wyrażających zgodę użytkowników powinno być w stanie wyrazić zgodę osobie trzeciej wykorzystującej ich treści komunikacyjne, jeśli tego chcą, bez dalszej oceny skutków. Sformułowanie jest również niejasne i można by w sposób domniemany odnieść je do obowiązku oceny skutków w zakresie ochrony danych określonego



w art. 35 RODO (lub nie). Odniesienie do uprzednich konsultacji nie jest ani potrzebne, ani proporcjonalne do poszczególnych ryzyk.

4. Żałujemy, że usunięto z tekstu „zgodne dalsze przetwarzanie” (compatible further processing). Zgodne dalsze przetwarzanie nie jest samą „podstawą prawną” przetwarzania danych, ale zasadą wtórnego przetwarzania danych, które zostały już zebrane i przetworzone. Wzywamy prezydencję do ponownego wprowadzenia tej zasady jako niezbędnego uzupełnienia podstaw prawnych przetwarzania oraz jako kluczowej zasady równoważenia potrzeby ochrony prywatności i innowacji w zakresie danych.
5. Liczenie statystyczne podlega ścisłym warunkom (patrz art. 6b lit. e)), które mogą powodować rozbieżności w sposobie wdrażania i egzekwowania przez organy regulacyjne UE odpowiedzialne za ochronę danych, co jest problemem (w równym stopniu jak w przypadku anonimizacji).
6. Motyw 20 wydaje się wykraczać poza ochronę prywatności osób: opiera się na narracji „cookie wall”, którą CNIL (francuski organ ochrony danych osobowych) forsował w 2020 r., i która została uznana przez francuski Sąd Najwyższy (wyrok z 19 czerwca 2020 r.) za wykraczającą poza wymogi RODO. Ustalenie, czy utworzenie cookie wall może być uznane za niedopuszczalne, nie zostało w żaden sposób jednoznacznie stwierdzone, w szczególności w przypadku odniesienia do tego, w jaki sposób zakaz stosowania *cookie wall* miałby zastosowanie „w przypadku witryn internetowych świadczących określone usługi, na przykład tych świadczonych przez władze” lub gdy „użytkownik końcowy ma niewiele alternatyw dla usługi lub nie ma ich wcale”. Takie oceny są niejasne i wywołują niedopuszczalną niepewność prawną.

Zakaz stosowania cookie wall byłby nieuzasadnioną ingerencją w swobodę prowadzenia działalności gospodarczej, de facto nakazującą świadczenie usługi wbrew woli usługodawcy.

7. Motyw 21, zgodnie z którym zgoda jest systematycznie potrzebna do korzystania z identyfikujących użytkownika plików cookie, powoduje wspomniane wcześniej problemy związane z consent fatigue.

Punkty pozytywne:

1. Ponowna identyfikacja indywidualnych użytkowników w celu wyrażenia zgody została usunięta (zgodnie z art.11 RODO) zgodnie z art. 4a: „2a. *O ile administrator nie jest w stanie zidentyfikować osoby, której dane dotyczą, do wykazania zgody użytkownika końcowego zgodnie z art. 8 ust. 1 lit. b) wystarczy protokół techniczny wykazujący, że zgoda została udzielona przez użytkownika końcowego.*” 2. *Dodanie przetwarzania danych do użytku osobistego (art. 6a lit. a)), co umożliwia i jest zgodne z motywem 18 RODO.*
2. Art. 8(d), przy czym proponujemy korektę treści w taki sposób, aby sformułowanie „where applicable” dotyczyło również Art. 28 GDPR (nie zaś jak w obecnym brzmieniu – jedynie Art. 26 GDPR).
3. Art. 8 (d) i (da) i(e)

Konfederacja Lewiatan, KL/523/363/AM/2020

