Warszawa, dnia 28 listopada 2018 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Marek Zagórski

BM-WOP.072.238.2018

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z 6 listopada br. Posła na Sejm RP Pana Arkadiusza Marchewki w sprawie *tzw. ePrivacy* (interpelacja nr 27072).

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania:

Ad 1) Czy Minister wspiera wprowadzenie do projektu rozporządzenia ePrivacy zasad privacy by default (domyślne ustawienia prywatności) i privacy by design (prywatność w fazie projektowania), w celu zagwarantowania poufności i integralności komunikacji elektronicznej?

Zasady *privacy by default* (domyślne ustawienia prywatności) i *privacy by design* (prywatność w fazie projektowania) stanowią obecnie jedną z fundamentalnych podstaw ochrony danych osobowych. Zostały one uregulowane w rozporządzeniu o ochronie danych osobowych[1]. W projektowanym rozporządzeniu ePrivacy brak jest analogicznej regulacji. Z uwagi jednak na to, że akt ten ma stanowić *lex specialis* w stosunku do RODO, a w zakresie nieuregulowanym w ePrivacy znajdą zastosowanie przepisy RODO, w tym zasady wynikające z art. 25 RODO, nie wydaje się zatem zasadne, aby w rozporządzeniu ePrivacy powtarzać zasady, które uregulowane są w RODO i w tym zakresie również będą stosowane. Poziom ochrony użytkowników telekomunikacyjnych urządzeń końcowych czy aplikacji internetowych nie ulegnie zatem obniżeniu w porównaniu do poziomu ochrony gwarantowanego przez RODO.

Ad 2) Czy Minister sprzeciwia się propozycjom, które pozwalają dostawcom usług elektronicznych stosować technologie śledzące aktywność użytkowników w celach

[1] art. 25 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 (zwanego dalej „RODO")

reklamowych bez ich zgody, jako niezbędne do świadczenia usług finansowanych poprzez reklamę targetowaną?

Ministerstwo Cyfryzacji stoi na stanowisku, że niedopuszczalne są propozycje, które zakładają stosowanie technologii śledzących, których użytkownik nie akceptuje. Należy zwrócić uwagę, że obecnie istnieje znaczna liczba usług, takich jak np. serwisy internetowe, w tym serwisy informacyjne, które oparte są na modelu biznesowym polegającym na finansowaniu funkcjonowania danej strony, serwisu czy aplikacji z wyświetlanych reklam dopasowanych do preferencji użytkownika. Zgoda na stosowanie technik śledzących stanowi tu *de facto* zapłatę za możliwość korzystania z udostępnianych w serwisie treści lub aplikacji. Brak akceptacji na stosowanie technologii śledzących w celach reklamowych jest tu rozumiany jako odmowa zapłaty za dostęp do strony czy aplikacji, a co za tym idzie pociąga za sobą odmowę dostępu użytkownika do danej usługi. Kluczowy jest jednak obowiązek poinformowania użytkownika o stosowaniu takich technologii oraz o ich celu.

Projektowane rozporządzenie wyjaśnia w motywie (21) kwestię, wskazując, że „in some cases the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment may also be necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use.”. Projekt akcentuje zatem to, że stosowanie technologii śledzących, takich jak pliki cookies, dotyczy sytuacji gdy usługa jest zażądana przez użytkownika, użytkownik zaakceptował stosowanie tych technologii, a ponadto udostępniono mu precyzyjne, przystępne informacje o celu stosowania technologii śledzących.

Podkreślić należy, że już obecnie obowiązująca dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.[2] przewiduje również w motywie (25), że dostęp do niektórych treści zamieszczonych na stronach internetowych może być nadal uzależniony od świadomej akceptacji zastosowania „cookie” lub podobnej funkcjonalności, jeżeli służy ono prawnie dopuszczalnemu celowi.

Należy przy tym zauważyć, że udostępnianie danych osobowych czy innych danych (a takie są m.in. zbierane za pośrednictwem technologii śledzących) może stanowić formę wynagrodzenia, zgodnie z projektowanym Europejskim Kodeksem Łączności

[2] dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)

Elektronicznej[3], który znajduje się obecnie na końcowym etapie prac. W motywie (16) Kodeksu wskazano bowiem, że „usługi łączności elektronicznej są często świadczone *na rzecz użytkownika końcowego nie tylko* w zamian za *świadczenie pieniężne, ale coraz częściej i w szczególności w zamian za dostarczenie danych osobowych lub innych danych. Pojęcie wynagrodzenia powinno zatem obejmować sytuacje, gdy usługodawca prosi o dane osobowe (…) lub inne dane, a użytkownik końcowy świadomie, pośrednio lub bezpośrednio, udostępnia usługodawcy takie dane. (…) Powinno ono również obejmować przypadki, gdy użytkownik końcowy zezwala na dostęp do informacji, choć ich aktywnie nie udostępnia, takich jak dane osobowe, w tym adres IP, lub inne automatycznie generowane informacje, takie jak dane gromadzone i przekazywane przez pliki cookie.* (…)". Pojęcie wynagrodzenia, w rozumieniu Kodeksu, obejmuje również sytuacje, gdy użytkownikowi wchodzącemu na daną stronę wyświetlane są reklamy (w serwisach rozrywkowych, czy też we wcześniej wspomnianych serwisach informacyjnych). Kodeks uwzględnia zatem obecnie funkcjonujące modele biznesowe i realia rynkowe, a także to, że w takiej sytuacji użytkownik świadomie godzi się na udostępnienie danych.

Przy ocenie zasadności propozycji zawartych w projektowanym rozporządzeniu ePrivacy należy jeszcze raz podkreślić, że zawiera ono wymóg akceptacji stosowania technologii śledzących w celach reklamowych. Technologie te nie mogą być zatem stosowane bez wiedzy i akceptacji ze strony użytkownika. Należy jednak brać również pod uwagę relację tego przepisu do definicji zgody i wymogów co do prawidłowości jej wyrażania, uregulowanych w RODO. Zgoda w rozumieniu RODO oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. RODO[4] w wskazuje przy tym, że przy ocenie, czy zgody udzielono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy. Na skutek pojawiających się wątpliwości co do relacji proponowanych w projekcie rozporządzenia ePrivacy zapisów do RODO, Polska zwracała się do Prezydencji austriackiej o wystąpienie o opinię do Europejskiej Rady Ochrony Danych, czy tak udzielona zgoda jest dobrowolna przy uwzględnieniu specyfiki obecnych modeli biznesowych.

Biorąc pod uwagę powyższe, należy zaznaczyć, że kwestia stosowania technologii śledzących w celach reklamowych wymaga, zdaniem Ministerstwa Cyfryzacji, dalszych

[33] Projekt dyrektywy Parlamentu Europejskiego i Rady ustanawiającej Europejski Kodeks Łączności Elektronicznej

[4] art. 7 ust. 4 RODO

analiz i dyskusji podczas prac grupy roboczej Rady UE - WP TELE. Konieczne jest wypracowanie rozwiązania kompromisowego, które pogodzi zarówno interesy przedsiębiorców jak i użytkowników końcowych. Należy mieć na uwadze specyfikę sektora cyfrowego, obowiązujące modele biznesowe oparte na reklamach, a także fakt, że wprowadzenie zakazu stosowania technologii śledzących do celów reklamowych może spowodować wprowadzenie opłat za treści ogólnodostępne w Internecie. Regulacja dotycząca w szczególności plików cookies powinna być przy tym przyszłościowa i umożliwiać rozwój metod finansowania usług i treści dostępnych w Internecie.

Ad 3) Czy Minister gwarantuje, że sprzeciwi się każdej propozycji, która nie respektuje wyroków Trybunału Sprawiedliwości Unii Europejskiej dotyczących obowiązkowej retencji danych telekomunikacyjnych, w szczególności w sprawach C-203/15 i C-293/12?

Kwestia retencji danych pozostaje w kręgu zainteresowania Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Sprawiedliwości czy KPRM – w zakresie dostępu służb do danych telekomunikacyjnych. Przedstawiciele MSWiA uczestniczą w posiedzeniach grupy roboczej DAPIX (Friends of the Presidency), która zajmuje się na arenie UE kwestią retencji danych, w tym interpretacją i skutkami wyroków w sprawach C-203/15 i C-698/15 Tele2 Sverige AB oraz w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland Ltd.

Zgodnie ze stanowiskiem Rządu RP wobec projektowanego rozporządzenia ePrivacy, przyjętym przez KSE 27 czerwca 2017 r., Polska powinna w trakcie prac zmierzać do tego, aby projektowane rozporządzenie ePrivacy wyraźnie umożliwiało przyjęcie regulacji krajowych dotyczących retencji danych i ich wykorzystania w postępowaniu karnym. Polska będzie również popierała takie przepisy, na podstawie których będzie mogła podejmować skuteczne działania na rzecz ochrony bezpieczeństwa i porządku publicznego, w tym na rzecz ratowania zdrowia lub życia ludzkiego oraz wsparcia działań poszukiwawczych i ratowniczych. Powyższe stanowisko w zakresie retencji danych, kwestii ochrony bezpieczeństwa i porządku publicznego zostało sformułowane na podstawie opinii MSWiA, MS oraz KPRM i zaakceptowane przez Radę Ministrów.

Niezależnie od powyższego, należy wskazać, że wyroki w połączonych sprawach C-203/15 i C-698/15 Tele2 Sverige AB oraz w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland Ltd, a także ich skutki budzą wątpliwości interpretacyjne. Świadczą o tym wszczęte po tych wyrokach, na wniosek poszczególnych państw członkowskich, kolejne postępowania przed Trybunałem mające m.in. na celu wyjaśnienie lub doprecyzowanie ww. wyroków (przykładowo sprawa C-207/16 Ministerio Fiscal, C-623/17 Privacy International, C-520/18 Ordre des barreaux francophones et germanophone e.a., C-511/18 i C-512/18 La Quadrature du Net i in.). Należy przywołać tu niedawny wyrok TSUE

z dnia 2 października 2018 r. w sprawie C-207/16 Ministerio Fiscal, z którego wynika, że nie należy zbyt restrykcyjnie interpretować wyroku w sprawie C-293/12 i C-594/12 Digital Rights Ireland Ltd[5]. Niezależnie od tego, obecna jest szeroka dyskusja odnośnie sposobu formułowania regulacji dotyczących retencji danych telekomunikacyjnych. Dopiero orzeczenia zapadłe w toczących się postępowaniach przed TSUE oraz wyniki dyskusji na arenie UE umożliwią określenie, jakie regulacje dotyczące zatrzymywania przez przedsiębiorców telekomunikacyjnych i udostępniania uprawnionym podmiotom danych telekomunikacyjnych są dopuszczalne.

Ad 4) Czy Minister popiera szybkie przyjęcie i wdrożenie rozporządzenia ePrivacy?

Należy podkreślić, że w opinii Ministerstwa Cyfryzacji konieczne jest przede wszystkim zagwarantowanie realizacji podstawowego celu projektowanego rozporządzenia ePrivacy, jakim jest zapewnienie odpowiedniego poziomu prywatności w komunikacji elektronicznej. Wprowadzanie nowej regulacji powinno być zatem poprzedzone pogłębioną analizą, która wykaże w jakim zakresie obowiązujące już od maja br. przepisy RODO są niewystarczające do zapewnienia ochrony prywatności i danych w komunikacji elektronicznej oraz uzasadni dalszą potrzebę uregulowania tej ochrony w odrębnym, dedykowanym sektorowi telekomunikacyjnemu akcie prawnym. Taka analiza powinna zostać dokonana przez wnioskodawcę (tj. Komisję Europejską) i stanowić podstawę prowadzonych prac. W związku z obowiązującymi przepisami RODO zasadne wydaje się w pierwszej kolejności przeanalizowanie praktyki jego stosowania, a dopiero w drugiej kolejności kontynuowanie prac nad nowym aktem. W ten sposób doświadczenia związane ze stosowaniem RODO mogłyby zostać uwzględnione również w rozporządzeniu ePrivacy.

Ponadto należy wskazać, że Ministerstwo Cyfryzacji popiera wprowadzenie rozporządzenia ePrivacy, o ile regulacja ta nie będzie budziła wątpliwości interpretacyjnych, wyklarowana zostanie relacja tego aktu do RODO, oceniony zostanie wpływ regulacji na obecne modele biznesowe oraz na konkurencyjność przedsiębiorców z Unii Europejskiej w stosunku do tych z państw trzecich. Tak długo jak przedstawiony

[5] Z wyroku TSUE w sprawie Digital Rights Ireland Ltd wynikało, że tylko walka z poważnymi przestępstwami może uzasadniać nałożenie na firmy świadczące usługi łączności elektronicznej ogólnego obowiązku zatrzymywania danych. Tymczasem TSUE w wyroku w sprawie C-207/16 Ministerio Fiscal wskazał, że art. 15 dyrektywy 2002/58/WE, który jest podstawową do uregulowania w prawie krajowym przepisów, stanowiących odstępstwo od ochrony prywatności, zawiera wyczerpujący katalog celów, dla których to odstępstwo może zostać wprowadzone. Podkreślił, że cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i ściganiu przestępstw kryminalnych, nie został w art. 15 dyrektywy ograniczony do zwalczania poważnych przestępstw, lecz odnosi się ogólnie do „przestępstw kryminalnych". Z uwagi na to, że w przepisie jest mowa o konieczności zachowania zasady proporcjonalności, poważna ingerencja w poufność może być uzasadniona jedynie w odniesieniu do ścigania poważnej przestępczości. Jeżeli ingerencja wynikająca z dostępu do danych nie jest poważna to może być uzasadniona ściganiem, zapobieganiem itp. ogółu przestępstw, a nie tylko poważnych przestępstw.

projekt zawiera wiele niejasności, nie powinien on zostać przyjęty. Do czasu przyjęcia nowego aktu zastosowanie znajdzie obowiązująca obecnie dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady oraz RODO - w zakresie spraw nieuregulowanych w dyrektywie. Na marginesie warto wskazać, że również ten aspekt, czyli brak rozporządzenia ePrivacy wbrew planowanemu jego wejściu w życie wraz z RODO, nie został przez wnioskodawcę przeanalizowany, zwłaszcza w praktyce.

Niezależnie od powyższych informacji, pragnę wskazać, że Ministerstwo Cyfryzacji prowadzi proces negocjacji w sposób transparentny. Na bieżąco konsultuje z zainteresowanymi podmiotami, w szczególności organizacjami zajmującymi się prawami konsumentów oraz ochroną danych w sieci, czy z izbami zrzeszającymi przedsiębiorców telekomunikacyjnych, pracodawców[6], a także z innymi resortami i urzędami (Urzędem Ochrony Konkurencji i Konkurentów, Urzędem Ochrony Danych Osobowych) kolejne wersje tekstu projektowanego rozporządzenia opracowywane przez państwa sprawujące prezydencję w Radzie UE. Ministerstwo korzysta ze stanowisk i uwag przekazywanych w ramach konsultacji. Należy jednak wskazać, że propozycje interesariuszy są niejednokrotnie przeciwstawne. Ministerstwo prowadzi zatem prace nad rozporządzeniem ePrivacy w taki sposób, aby z jednej strony nie utrudniać prowadzenia działalności gospodarczej w zmieniających się warunkach technologicznych, a z drugiej – zabezpieczyć podstawowy cel projektowanej regulacji, jakim jest ochrona prywatności użytkowników.

Z wyrazami szacunku,

Marek Zagórski
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów

[6] Konsultacje prowadzone są w szczególności z: Konfederacją Lewiatan, Federacją Konsumentów, Fundacją Panoptykon, Helsińską Fundacją Praw Człowieka, Startup Poland, IAA Polska – Międzynarodowym Stowarzyszeniem Reklamy, Polską Izbą Informatyki i Telekomunikacji, Krajową Izbą Komunikacji Ethernetowej, Polską Izbą Komunikacji Elektronicznej, Krajową Izbą Gospodarczą Elektroniki i Telekomunikacji, IAB Polska, BCC