INSTRUKCJA
DLA PRZEDSTAWICIELA POLSKI
na posiedzenie grupy roboczej Rady UE ds. telekomunikacji i społeczeństwa informacyjnego (H.05)
7 listopada 2019 r.

Data ostatniego posiedzenia grupy: 22 października 2019 r.

Dane przedstawiciela Polski:
Michał Czerniawski, I Sekretarz, Stałe Przedstawicielstwo RP przy UE
michal.czerniawski@msz.gov.pl; tel. +32 2 7804 342

Rozpatrywany dokument:

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Stanowisko Polski do zaprezentowania:

I. Uwagi generalne

- Wyznaczony czas na zapoznanie się z zaproponowanymi zmianami był zbyt krótki i znacznie utrudnił przeprowadzenie konsultacji z zainteresowanymi podmiotami i dokonanie szczegółowej analizy skutków proponowanych zmian. Polska otrzymuje z rynku wiele zastrzeżeń dotyczących braku spójności i jasności proponowanych przepisów, zagrożenia dla zasady level playing field.
- PL w dalszym ciągu dostrzega zasadność rozważenia przez Komisję przeprowadzenia dodatkowej analizy wskazującej, czy odrębna regulacja ePriv, stanowiąca lex specialis względem RODO jest w chwili obecnej potrzebna. Z tego względu zasadne byłoby również przeprowadzenie ponownej oceny skutków regulacji (Impact Assessment) uwzględniającej analizę sytuacji faktycznej i prawnej po wejściu w życie RODO, a także wykazującej niezbędność utrzymania regulacji lex specialis.

- Potencjalnie na rozwagę zasługuje też ograniczenie zakresu projektu wyłącznie do kwestii wykraczających poza RODO.

II. Uwagi szczegółowe

1) Ad. Pkt I. Zakres zastosowania e-Privacy

Polska kierunkowo popiera opcję 2.
Na uwagę zasługują zmiany zaproponowane w art. 6(1)(a) w opcji 2:

"(a) it is necessary to provide the electronic communication service ~~achieve the transmission of the communication.:~~

Przesłanka przetwarzania danych koniecznego do świadczenia usługi jest szersza i bardziej elastyczna od przesłanki przetwarzania w celu dokonania transmisji komunikacji i może objąć, jak wskazuje Prezydencja, również przechowywanie wiadomości jeśli jest to konieczne do świadczonej usługi. Wydaje się, że dostawcy powinni mieć możliwość przetwarzania danych w zakresie, w jakim są one niezbędne do świadczenia zamówionej usługi, również jeżeli usługa dotyczy etapu po zakończeniu transmisji.

2) **Ad. Pkt II. Pojęcie strony trzeciej**

Odnosząc się do propozycji nadania nowego brzmienia motywowi 19 definiującemu pojęcie strony trzeciej, Polska zgłasza zastrzeżenia analityczne. Jako priorytet należy potraktować takie sformułowanie tego motywu, aby nie stwarzać możliwości do omijania przepisów rozporządzenia.

Polska ma jednak wątpliwości odnośnie tego, czy propozycje zagwarantują level playing field, w szczególności w przypadku opcji 3. Wynika z niej, że przedsiębiorca telekomunikacyjny dostarczający powiązane z usługą telekomunikacyjną usługi opisane w motywie 19a jest w gorszej sytuacji, niż dostarczający takie same funkcjonalnie usługi inny przedsiębiorca. Przykładowo – gromadzenie i przechowywanie w chmurze wiadomości wysyłanych i odbieranych przez użytkownika ma podlegać odmiennym reżimom prawnym w zależności od tego, czy usługa ta będzie powiązana z usługą telekomunikacyjną, czy dostarczana przez zewnętrzny podmiot. W pierwszym przypadku stosuje się e-Privacy, a w drugim przypadku nie.
Ponadto, należało by przeanalizować jak rozumieć stronę trzecią – czy chodzi de facto o podmiot inny niż użytkownik (a nie koniecznie podmiot inny niż dostawca usługi łączności elektronicznej)? Należy również zwrócić uwagę czy z punktu widzenia ochrony prywatności użytkownika istnieje różnica pomiędzy tym, czy usługę związaną z późniejszym przetwarzaniem na zlecenie klienta treści przekazów dostarcza przedsiębiorca telekomunikacyjny łącznie z usługą transmisji, czy zewnętrzny podmiot jako osobną usługę?
Polska kierunkowo może poprzeć opcję nr 1.

3) **Zmiana w motywie 20**

*(20) ...„Conversely, in some cases, making access to website content conditional to dependent on consent to the use of such cookies may be considered**, <u>in the presence of a clear imbalance between the end-user and the service provider</u>*~~*to be disproportionate*~~ *<u>as depriving the end-user of a genuine choice</u>. This would normally*

*be the case for websites providing certain services, such as those provided by public authorities **or by undertakings in a dominant position**, where the user could be seen as having few or no other options but to use the service, and thus having no real choice as to the usage of cookies.*"

Polska popiera potrzebę ochrony użytkowników przed uzależnianiem dostępu do treści od wyrażenia zgody na pliki cookies, w sytuacji, gdy użytkownik nie ma de facto realnej możliwości wyboru - np. w przypadku stron podmiotów publicznych. Prezydencja zaproponowała przy tym, iż analogiczna ochrona powinna dotyczyć treści udostępnianych przez podmiot o dominującej pozycji. Wątpliwości budzi czy taki zapis nie będzie polem do nadinterpretacji oraz czy samo pojęcie "przedsiębiorstwa o dominującej pozycji", jako że jest to pojęcie z zakresu prawa konkurencji, nie zdefiniowane w ePriv będzie wystarczająco jasne i zasadne.

4) Marketing bezpośredni

Polska podtrzymuje dotychczasowe uwagi w zakresie marketingu bezpośredniego:

- W przepisach art. 16 zasadne jest jednoznaczne wskazanie, że zgoda na kontakt marketingowy musi być uprzednia, tj. uzyskana przed jego nawiązaniem. Zakazane powinno być wykonywanie połączeń telefonicznych w celu uzyskania zgody. Wymaga tego ochrona prywatności użytkowników. Obecnie są zalewani smsami czy rozmowami z pytaniami czy „wyraża Pan/Pani zgodę na przedstawienie oferty". Jeśli dane Państwo wybiera system opt-in to powinna być zapewniona należyta ochrona użytkowników końcowych z tym związana. Obecna treść przepisów pozostawia zbyt dużo wątpliwości w tym zakresie.
- W zakresie art. 16 ust. 2a dla zapewnienia spójności warto rozważyć określenie maksymalnego czasu wykorzystywania danych konsumenta (np. okres 2 lat). Przepis w obecnym brzmieniu zostawia zbytnią swobodę, która może znacząco różnicować stopień ochrony użytkowników. Rozważyć można różnicowanie okresu wykorzystywania danych od rodzaju produktów/usług.
- W zakresie art. 16 ust. 6 lit. b sformułowanie „the identity of the legal or natural person on behalf of whom the direct marketing communication is transmitted sent" jest niewystarczające. Przy tym brzmieniu podmiot kontaktujący się mógłby podać np. działam w imieniu Jana Kowalskiego. Nie pozwoli to na ewentualną identyfikację podmiotu w imieniu którego przesyłany jest komunikat marketingowy. Konieczne jest doprecyzowanie, że „identity" obejmuje również adres i pełną nazwę podmiotu oraz ewentualnie dane rejestrowe.

5) Organ nadzoru i zasady współpracy organów

Polska podtrzymuje dotychczasowe uwagi dotyczące konieczności zagwarantowania elastyczności państw członkowskich w wyborze organu nadzoru **oraz zakresu**

współpracy organów nadzorczych

[treść uwagi do ewentualnego wykorzystania:
Dla PL ważna jest kwestia zapewnienia państwom członkowskim elastyczności w wyborze organu nadzorczego. W opinii PL nie znajduje uzasadnienia stawianie organom, odpowiedzialnym za monitorowanie stosowania ePriv, wymagań z RODO. Należy podkreślić, że regulacja ePriv ma szerszy niż RODO zakres i obejmuje również kwestie ochrony prywatności, przetwarzania treści, przetwarzania danych osób prawnych. Z powyższego względu państwa członkowskie powinny mieć wybór czy organem nadzorczym ustanowić NRA czy inny organ krajowy, posiadający odpowiednią wiedzę i doświadczenie do monitorowania regulacji ePriv. W tym kontekście, biorąc pod uwagę zakres regulacji ePriv, wykraczający poza kwestię ochrony danych osobowych, wątpliwości mogą budzić przyznane w ePriv kompetencje Europejskiej Rady Danych Osobowych, przy pominięciu roli BEREC (Organ Europejskich Regulatorów Łączności Elektronicznej).

W zakresie art. 18 ust. 1 b konieczność współpracy organów nadzorczych jest nieograniczona i praktycznie obowiązkowa w każdym przypadku. Przy podziale obowiązków nadzorczych mogłoby to prowadzić do przedłużania i komplikowania weryfikacji wykonywania obowiązków. Jeśli zostaną utrzymane w Polsce NRA i DPA jako organy nadzorcze to konieczność współpracy przy każdej kontroli czy postępowaniu w przedmiocie nałożenia kary wydaje się nadmiarowa. Zasadne wydaje się doprecyzowanie, że organy współpracują w sprawach np. dotyczących zakresu działań obu organów, ewentualnie w niezbędnym zakresie.]

6) Art. 21

Przedstawiciel Polski podtrzyma zgłaszane już zastrzeżenia odnośnie możliwych negatywnych konsekwencji brzmienia art. 21 ust. 1, tj. możliwości doprowadzenia, w praktyce, do paraliżu organów nadzorczych. W przepisie wskazano, prawo użytkownika końcowego do: „lodge a complaint with a supervisory authority and the right to an effective judicial remedy against any decision of a supervisory authority". Sugeruje to, że każda skarga na naruszenie przepisów np. dotyczących niezamówionych komunikatów (w tym wiadomości elektronicznych) wszczynałoby postępowanie przed organem nadzorczym, którego stroną byłby skarżący. Co więcej przyznaje się prawo do zaskarżania wydanych w następstwie skargi decyzji. Może to oznaczać tysiące postępowań w skali roku. Polska wskazuje na konieczność zmiany przepisu.

Sporządziła: Agnieszka Chruszcz, główny specjalista DT
Zatwierdziła: Agnieszka Krauzowicz, Dyrektor Departamentu Telekomunikacji