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

Data ostatniego posiedzenia grupy: 11 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:

Uwagi generalne

- Polska stoi na stanowisku, iż projekt wymaga dalszych prac zanim zostanie skierowany na dalszy etap procesu legislacyjnego. Należy przy tym wskazać, że PL otrzymuje wiele uwag z sektora prywatnego, który w dalszym ciągu podnosi istnienie niejasności w tekście projektu. W szczególności jako do końca niewyjaśnione wskazuje się rozbieżności między podstawami przetwarzania danych w odniesieniu do treści i metadanych.
- PL 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.
- Polska opowiada się za zasięgnięciem opinii Europejskiej Rady Ochrony Danych co do wprowadzenia mechanizmu one-stop-shop.

Uwagi szczegółowe

Motyw (32)

Przedstawiciel Polski wskaże, że należałoby doprecyzować pojęcie "advertising" (mot. 32) - tj. wskazać w motywach, że należy rozumieć go szeroko, aby nie było wątpliwości, że np. telefon z prośbą o udział w ankiecie również stanowi telemarketing.

Art. 2 [kwestia zagwarantowania level playing field]

Polska zgłasza wątpliwość, czy art. (2)(2) lit. e) i f), końcowa część recitalu 8, druga część recitalu 19, art. 7(1), tj. zmiany związane są ze sformułowaniem "data processing before/after receipt" nie doprowadzą do znacznego wyłączenia podmiotów OTT (np. Gmail) spod regulacji. To może doprowadzić do podważenia zasady *level playing field*.

Dla przykładu: recital 8 stanowi, że strony trzecie (np. dostawcy oprogramowania typu firewall czy inni dostawcy oprogramowania w zakresie bezpieczeństwa, którzy nie są dostawcami usług komunikacji elektronicznej) mogłyby przetwarzać metadane na potrzeby bezpieczeństwa sieci zanim zostały one otrzymane i tym samym nie podlegałyby reżimowi ePrivacy, a jedynie RODO. To prowadziłoby do istnienia przepisów, na podstawie których operatorzy telekomunikacyjni, którzy mogą robić to samo (tj. przetwarzać metadane ze względu na bezpieczeństwo sieci - Art. 6), musieliby być zgodni z rozporządzeniem ePrivacy, podczas gdy strony trzecie, które robią to samo (bezpieczeństwo sieci) podlegałyby jedynie RODO. To w żadnym stopniu nie prowadziłoby do zapewnienia tzw. *level playing field*.

To samo odnosi się do recitalu 19 oraz art. 2 (2) lit. e): sformułowanie „after receipt" powoduje, iż byłoby możliwe, aby zarówno metadane jak i treści były przetwarzane przez np. dostawcę usług chmurowych lub nawet dostawcę usług (jeśli usługa nie jest integralną częścią usługi komunikacyjnej), bez jakichkolwiek dodatkowych ograniczeń, jedynie zgodnie z RODO. W tym samym czasie, operator telekomunikacyjny przetwarzający metadane nie podlegałby RODO, ale ePrivacy.

Art. 3 ust. 1

Przedstawiciel PL zwróci uwagę, że zakres zastosowania projektowanego rozporządzenia jest szerszy niż RODO, RODO wymaga bowiem aktywności od administratora danych. W przypadku art. 3 wystarczy, że użytkownik końcowy jest w UE, o czym dostawca usługi może nie wiedzieć i może nie podejmować jakichkolwiek aktywnych działań w kierunku UE. W praktyce to od działań użytkownika końcowego będzie zależeć czy dostawca usługi zostanie objęty rozporządzeniem.

Art. 4

Art. 4 ust. 3 lit f) Definicja "direct marketing communications"

W zakresie zaproponowanej definicji wprowadzono kategorię “specific end-users” w miejsce “identified or identifiable end-users”. O ile definicja operująca pojęciem zidentyfikowanego lub możliwego do zidentyfikowanego użytkownika końcowego jest instytucją znaną prawu ochrony danych osobowych o tyle wprowadzone zmiany odbiegają od wprowadzonej w RODO nomenklatury w zakresie definicji danych osobowych, w której to definicji jest mowa o „zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”)”. Ponadto, w naszej opinii powinna istnieć zamknięta lista środków komunikacji podpadających pod definicję „direct marketing communications”.

Art. 6b lit. d)

Ponadto, Przedstawiciel PL spyta czy w przypadkach innych niż „emergency” nie można już chronić „vital interests” użytkownika końcowego. Wydaje się, że przepis ten powinien pozwalać na ochronę żywotnych interesów użytkowników końcowych także w innych sytuacjach. Należy zauważyć, że w RODO analogiczna przesłanka nie została ograniczona do przypadków "emergency". [W art. 6 ust. 1 lit. D wskazuje się jako podstawę przetwarzania danych: przetwarzanie niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Natomiast w art. 9 regulującym podstawy przetwarzanie danych wrażliwych wskazano: przetwarzanie niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody]. Należy zatem wyjaśnić czy różnice pomiędzy ePrivacy i RODO są celowe i jakie mogą być tego konsekwencje.

Art. 6d

W odniesieniu do kwestii zwalczania treści o charakterze pornografii dziecięcej należy wskazać, że nie jest jasne z jakiego powodu kwestia walki z pornografią dziecięcą ma w projekcie rozporządzenia własne, odrębne regulacje, podczas gdy takich odrębnych regulacji nie ma w odniesieniu do walki z innymi, nielegalnymi treściami. O ile potrzeba walki z pornografią dziecięcą jest w pełni zrozumiała, o tyle takie podejście grozi fragmentaryzacją przepisów rozporządzenia i rodzi pytania o przewarzanie danych w zakresie niezbędnym do walki z innymi niż pornografia dziecięca typami nielegalnych treści. Wydaje się, że zasady zbierania i przetwarzania danych na potrzeby walki z nielegalnymi treściami powinny być takie same dla wszystkich podmiotów objętych rozporządzeniem E-privacy i opierać się na proporcjonalnych i przejrzystych przesłankach, aby cel, któremu służą mógł być efektywnie osiągnięty. PL wskazuje do rozważenia czy art. 11 nie stanowiłby wystarczającej podstawy do wprowadzenia ewentualnych odrębnych regulacji w zakresie zwalczania treści o charakterze pornografii dziecięcej.
Projektowane art. 6d i art. 29 w zakresie zwalczania treści o charakterze pornografii dziecięcej wydają się wzajemnie wykluczać. Należy wyjaśnić wzajemne relacje obu

przepisów.

Art. 8

W art. 8 ust. 1 lit. d projektu wprowadza się zezwolenie do umieszczania w urządzeniach końcowych abonentów aplikacji badającej oglądalność usług społeczeństwa informacyjnego (chodzi tu głownie o telewizję w internecie IPTV). Uprawnienie to przysługuje wyłącznie dostawcom usług społeczeństwa informacyjnego (w tym przypadku OTT czyli nadawcom IPTV) oraz podmiotom działającym na ich zlecenie. W tym kontekście należy zastanowić się czy wprowadzenie tej możliwości nie powoduje zbytniego uprzywilejowania jednego rodzaju przedsiębiorców. Tradycyjnym operatorzy telekomunikacyjni i podmioty badające oglądalność na ich zlecenie nie mają analogicznych możliwości, tj. badania oglądalności świadczonych przez siebie programów i kanałów, aby móc lepiej dopasować swoje oferty do potrzeb abonentów. Polska wskazuje zatem na zasadność przeanalizowania skutków art. 8 ust. 1 lit. D.

Art. 10

Przedstawiciel PL poprze utrzymanie usunięcia art. 10 i motywów 22-24.

Art. 11

W zależności od przebiegu dyskusji, Przedstawiciel PL może poprzeć ewentualne uwagi zgłaszane przez FR. Zasadne jest usunięcie w art. 6 i 7 projektu odesłania do art. 11. Za rozsądną należy uznać argumentację, że zabezpieczenie przetwarzania i zatrzymywania danych wydaje się być w pełni bezpieczne bez odniesienia się do art. 11.

Art. 16 Unsolicited and direct marketing communications

- W przepisach art. 16 lub przynajmniej w motywach 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.

- Art. 16 ust. 6 lit. d in fine Na chwilę obecną wydaje się, że nie zostało przesądzone co oznacza danie możliwości wycofania zgody w sposób tak łatwy jak została wyrażona „It shall be as easy to withdraw as to give consent". Wydaje się, że powinno zostać to w pełniejszy sposób wyjaśnione.

Art. 18-20

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.

Art. 21

Przedstawiciel Polski wskaże na możliwe negatywne konsekwencje brzmienia art. 21 ust. 1, tj. możliwość 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