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

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 20

Przedstawiciel PL zaproponuje wskazanie zamiast art. 5 wprost art. 5 ust. 1 lit. b) RODO, oraz zapyta o powody wprowadzenia odniesienia do art. 8 RODO.

Motyw 21

Przedstawiciel PL poprze dodanie odniesienia do inteligentnych liczników i urządzeń medycznych

Art. 2 ust. 3

Przedstawiciel PL wskaże, że rozporządzenie 2018/1725 odsyła wprost do obecnej dyrektywy o handlu elektronicznym, a w przepisie tym wyłączamy :

Art. 37 2018/1725:
Union institutions and bodies shall protect the information transmitted to, stored in, related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC. (Art. 5 ust. 3 to obowiązek informacyjny)

Motyw 54 2018/1725
Union institutions and bodies should ensure the confidentiality of electronic communications provided for by Article 7 of the Charter. In particular, Union institutions and bodies should ensure the security of their electronic communications networks. They should protect the information related to the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with the Directive 2002/58/EC of the European Parliament and of the Council (8). They should also protect the personal data stored in directories of users.

SECTION 3

Confidentiality of electronic communications

Article 36

Confidentiality of electronic communications

Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks.

Article 37

Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment

Union institutions and bodies shall protect the information transmitted to, stored in,

related to, processed by and collected from the terminal equipment of users accessing their publicly available websites and mobile applications, in accordance with Article 5(3) of Directive 2002/58/EC.

Article 38

Directories of users

1. Personal data contained in directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.

2. Union institutions and bodies shall take all the necessary measures to prevent personal data contained in those directories from being used for direct marketing purposes regardless of whether they are accessible to the public or not.

Art. 3 ust. 1

Przedstawiciel PL zwróci uwagę, że zakres zastosowania projektowanego rozporządzenia jest szerszy niż RODO, RODO wymaga bowiem aktywności od administrator 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. 3 ust. 3 i 4

Przedstawiciel PL zwróci uwagę, że toczy się obecnie dyskusja co do przedstawicieli wyznaczonych pod RODO. Stąd pytanie do KE czy w jej ocenie przedstawiciel wyznaczony w oparciu o art. 3 ust. 2 powinien móc być pociągnięty do odpowiedzialności zamiast podmiotu, który reprezentuje. EDPB bowiem poważnie rozważa dopuszczenie takiej możliwości, nakładania sankcji bezpośrednio na przedstawicieli, gdy ten kto ich wyznaczył znajduje się poza UE.

Art. 4

Przedstawiciel PL zgłosi zastrzeżenia analityczne do definicji „direct marketing communications”

Art. 6a ust. 2

Przedstawiciel PL wskaże, że w art. 6a ust. 2 powinno zostać użyte sformułowanie „consult” zamiast „consulted”.

Art. 6b lit. d)

Przedstawiciel PL zaproponuje zmianę „normally" na „in general", wskazując iż lepiej oddaje to intencje tego przepisu. 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.

Art. 6c ust. 1 lit. e)

Przedstawiciel PL zaproponuje, żeby obok pseudonimizacji dodać też odniesienie do szyfrowania (encryption)

Art. 6d

Przedstawiciel PL zgłosi zastrzeżenia analityczne do propozycji PREZ FI. 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.

Art. 7 ust. 1

Przedstawiciel PL spyta o kwestię chmury obliczeniowej, czy jeżeli dostawca usługi jest też hostingodawcą, to czy musi usuwać dane czy też może je nadal przetwarzać będąc zarówno dostawcą usługi łączności elektronicznej, jak i hostingu?

Art. 8

Przedstawiciel PL zwróci uwagę, że koncepcja administratora danych i podmiotu przetwarzającego została stworzona na potrzeby RODO i nie przystaje ona do realiów usług łączności elektronicznej. Stąd odniesienie do art. 28 RODO w art. 8 ust. 1 lit. d, a więc do procesora, może mieć nieprzewidziane konsekwencje, czy możemy zostawić w tekście tylko „provided that conditions laid down in Regulation (EU)

2016/679 are met”?

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 i BE, nawiązujące do przedłożonego przez te państwa non-paper’a.

Art. 18-20

Przedstawiciel PL zgłosi zastrzeżenia analityczne do propozycji PREZ FI. 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).

Art. 23

Przedstawiciel PL spyta czy przepis ten nie powinien wprost wskazywać organów, które mają nakładać kary. W przypadku RODO nie potrzeba było takiego wskazania bo właściwe są wyłącznie organy ochrony danych osobowych.

Sporządziła: Agnieszka Chruszcz, starszy specjalista DT

Zatwierdziła: Agnieszka Krauzowicz, Dyrektor Departamentu Telekomunikacji