INSTRUKCJA
DLA PRZEDSTAWICIELA POLSKI
na posiedzenie grupy roboczej Rady UE ds. telekomunikacji i społeczeństwa informacyjnego (H.05)
26 października 2018 r.

Data poprzedniego posiedzenia grupy roboczej: 27 września 2018 r.

Informacje na temat przedstawicieli Polski na posiedzenie:

Imię i nazwisko/stanowisko: Pani Justyna Romanowska /kierownik Referatu
Instytucja/Komórka organizacyjna: Stałe Przedstawicielstwo RP przy UE/Referat ds. cyfrowych
Adres e-mail: justyna.romanowska@msz.gov.pl

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)

- Examination of the Presidency text

Rozpatrywany dokument:
ST 13256/18

Stanowisko Polski do zaprezentowania:

1. Uwagi ogólne:

- Polska docenia starania prezydencji austriackiej o przedstawienie nowych propozycji w kluczowych kwestiach. Uważamy jednak, że cała propozycja dotycząca ePrivacy, w szczególności zakres regulacji, wymaga dalszej dyskusji. Przeanalizowanie skutków proponowanych przepisów wymaga szczególnej uwagi, ponieważ regulacja ta będzie miała ogromny wpływ zarówno na obywateli, jak i przedsiębiorstwa. Należy bardzo dokładnie zastanowić się jak regulacja będzie działać w praktyce? Jaki wpływ będą miały te przepisy na istniejące modele biznesowe i na firmy europejskie, zwłaszcza małe i średnie? Zastanawiamy się również, czy wybrany model jest najlepszy do ochrony prywatności obywateli w cyfrowym świecie?
- Wątpliwości Polski budzi prowadzenie prac nad ePrivacy, podczas gdy GDPR jest dopiero od niedawna stosowane i nie wiadomo, jak będzie funkcjonowało. GDPR nakłada szereg nowych obowiązków, trudnych do wdrożenia dla adresatów i związanych z wysokimi karami za nieprzestrzeganie przepisów. Tym bardziej zatem wątpliwe jest dokładanie nowych obowiązków w ePrivacy. Zasadne by było w pierwszej kolejności, aby obserwować praktykę stosowania

GDPR a dopiero w drugiej kolejności pracować nad ePrivacy. Pozwoliłoby to na uwzględnienie w pracach nad ePrivacy doświadczeń i wniosków zdobytych po wejściu w życie GDPR.

- W odniesieniu do przedstawionego przez KE dokumentu dotyczącego relacji GDPR do dyrektywy 2002/58/WE należy wskazać, że Polska oczekiwała głębszej refleksji. Zasady dotyczące relacji lex specialis do lex generali są znane, tak samo jak treść art. 94 czy 95 GDPR. Zasadna wydaje się także taka analiza, która wykaże, na podstawie już obowiązujących przepisów – że dyrektywa 2002/58/WE jest obecnie już niewystarczająca, a co więcej że w dalszym ciągu konieczna jest w danym zakresie regulacja szczególna. Należy dobrze uzasadnić dlaczego przepisy GDPR nie są wystarczające. Już teraz przesłanki przetwarzania danych coraz bardziej upodobniają się do przesłanek z GDPR. Wydaje się, iż jest to fundamentalne pytanie.

2. **Motyw 17 - Polska raz jeszcze zwraca uwagę na wątpliwości co do braku objęcia przetwarzania danych lokalizacyjnych pochodzących z GPS rozporządzeniem ePrivacy**. Dane dotyczące lokalizacji powinny być traktowane tak samo, niezależnie od technologii, która stanowi ich podstawę.

[nawiązanie do dotychczasowych uwag PL:
Projektowane rozporządzenie ePrivacy rozciąga obowiązek przestrzegania zasady poufności w zakresie łączności elektronicznej na wszystkich dostawców usług łączności elektronicznej (włączając w to graczy typu OTT oferujących usługi komunikacji interpersonalnej), co oczywiście jest ważnym krokiem w kierunku zapewnienia lepszej ochrony prywatności dla użytkowników, a także stworzenia równych warunków konkurowania pomiędzy dostawcami tradycyjnych usług telekomunikacyjnych a graczami OTT.

Wydaje się jednak, że regulacja nie obejmie swoim zakresem (lub obejmie mniej restrykcyjnymi zasadami) pozostałych graczy OTT, którzy przetwarzają dane lokalizacyjne, ale nie są dostawcami usług komunikacji interpersonalnej. Zasada level playing field może doznać istotnego ograniczenia.

Usługi takie jak Gmail, WhatsApp, Skype, itp. zostaną objęte zakresem proponowanego art. 6 rozporządzenia ePrivacy. Natomiast Polska ma nadal wątpliwości czy usługi oparte o dane lokalizacyjne GPS, np. Google Maps, UBER, Pokémon Go, Galileo nie zostaną objęte zakresem art. 6 ePrivacy, ponieważ nie mogą one zostać zakwalifikowane jako *"usługi łączności elektronicznej"*. Stanie się tak, pomimo iż przy świadczeniu tych usług uzyskiwane są dane o znacznie większym poziomie granulacji niż przy świadczeniu usług łączności interpersonalnej. Jednakże recital 17 projektu ePrivacy wyraźnie stanowi, iż dane lokalizacyjne, które są generowane w innym kontekście niż dostarczanie usług łączności elektronicznej, nie powinny być uznawane za metadane w rozumieniu tego rozporządzenia.

Obawiamy się, że dane lokalizacyjne o wysokiej granulacji, generowane w ramach usług opartych o lokalizację GPS, nie będą objęte zakresem art. 6 ePrivacy. Metadane

pochodzące z tego typu usług będą regulowane w oparciu o podejście oparte o ryzyko na podstawie GDPR lub art. 8 ePrivacy (który jest mniej restrykcyjny niż art. 6).]

3. **Motyw (19b)**

Polska ma wątpliwości odnośnie do następującego zdania w motywie (19b): „In some cases, the legal entity having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned." Uzyskanie zgody pracownika w takich przypadkach będzie w praktyce problematyczne, zwłaszcza gdy subskrybent usługi jest dużą organizacją, w której kilka osób korzysta z jednego komputera / urządzenia / interfejsu. Czy dostawca usług będzie wiedział, że usługa nie jest wykorzystywana przez przedstawiciela podmiotu, który zawarł umowę (pracodawca), ale przez konkretnego pracownika?

4. **Art. 2 i art. 11 – zakres, retencja**

- Pozostaje wątpliwość (ta sama co od początku dyskusji nad ePR) co do potencjalnych problemów interpretacyjnych związanych z relacją art. 2 ust. 2 lit. d) (generalne wyłączenie spod regulacji ePR obszaru bezpieczeństwa ścigania przestępstw etc.) i art. 11 stanowiącym szczególne upoważnienie do odrębnego uregulowania (w związku z bezpieczeństwem, ściganiem przestępstw etc.) obszaru wymienionego w art. 5 – 8 ePR (poufność danych w komunikacji, przetwarzanie danych, przetrzymywanie i usuwanie danych, zabezpieczenie danych w urządzeniach użytkownika).
- PL opowiada się za wprowadzeniem do projektu jasnych zapisów, z których wynikałaby możliwość ustanawiania przez państwa członkowskie skutecznych mechanizmów retencji danych telekomunikacyjnych na potrzeby zwalczania przestępstw, zapewnienia bezpieczeństwa publicznego, w tym - co równie istotne - działań poszukiwawczo-ratowniczych. Ważne jest, aby przepisy projektu nie generowały niepewności prawnej oraz nie prowadziły do nieuzasadnionego pozbawienia skuteczności instrumentu retencji danych, który jest jednym z podstawowych mechanizmów pozwalających na efektywne działanie organów ścigania oraz zapewniających realizację prawa do bezpieczeństwa obywateli. Istotne jest także, że Rada Europejska zwracała dotychczas uwagę na priorytetowy charakter zapewnienia dostępu organów ścigania do niezbędnych danych, co stanowi ważny element struktury bezpieczeństwa wewnętrznego UE. Polska opowiada się za kontynuacją dyskusji w tym zakresie, tak aby wypracowane zostały akceptowalne rozwiązania. Istotne jest także zapewnienie koordynacji oraz przepływu informacji pomiędzy FoP DAPIX – data retention oraz WP TELE

5. **Art. 6 – podstawy przetwarzania danych**

- **Art. 6.2.a**

W odniesieniu do podstawy przetwarzania metadanych - w celu optymalizacji i zarządzania siecią wskazano, że przetwarzanie to jest dopuszczalne przez okres niezbędny do tego celu. Należy podnieść, że działania związane z zarządzaniem

siecią i jej optymalizacją to zadanie ciągłe, sieć musi być zarządzana i optymalizowana stale, aby zapewnić właściwy poziom jakości usług, także w przypadkach wymagających przetwarzania danych z łączności elektronicznej.

- **Further processing (art. 6.2a)**

Na gruncie samego GDPR może budzić wątpliwości interpretacyjne wymóg wzięcia pod uwagę charakteru przetwarzanych danych, w tym tego czy dane mają charakter sensytywny. Nie jest nadal jasne co oznacza w tym kontekście, powtórzone również w ePrivacy, pojęcie "wzięcia pod uwagę … charakteru danych osobowych". Jakie działania ma podjąć administrator? Czy na takiej samej zasadzie może dalej przetwarzać dane sensytywne i niesensytywne? Wątpliwe jest również to w jaki sposób określić czy cel dalszego przetwarzania jest zgodny z pierwotnym celem przetwarzania. Należy podkreślić, że dyskusja nad przesłankami dalszego przetwarzania danych powinna mieć szerszy zakres i zmierzać również do wykazania czy regulacja zawarta w tym zakresie w GDPR jest wystarczająca czy nie. Wydaje się, że dopiero obserwacja praktyki funkcjonowania przepisów GDPR da odpowiedź na to pytanie.

[dodatkowe wiadomości: kwestia ta była podnoszona podczas poprzedniego posiedzenia grupy H5. KE wskazała wówczas dość ogólnie, że w GDPR kwestie przetwarzania danych sensytywnych zostały uregulowane w art. 9 i 10 i to te przepisy determinują zasady przetwarzania danych sensytywnych. Sensytywność powinna zostać wzięta pod uwagę przy przetwarzaniu.
W dalszym jednak ciągu pozostaje pytanie: w jaki sposób należy „wziąć pod uwagę" sensytywność danych. Czy chodzi o to, że dalszego przetwarzania danych sensytywnych nie można opierać na innej podstawie niż z art. 9 GDPR? Ale z drugiej strony możliwość dalszego przetwarzania jest samodzielną, dodatkową podstawą]

W odniesieniu do wymogu, aby dalsze przetwarzanie nie prowadziło do tworzenia profili użytkowników należy wyjaśnić czy zakaz tworzenia profili odnosi się do zakazu profilowania w rozumieniu art. 22.1 GDPR[1]. Jeśli zatem zakaz tworzenia profili dotyczy profilowania z art. 22.1 GDPR należy się zastanowić czy nie będzie to stanowiło zbytniego zawężenia ochrony użytkownika. W art. 22.1. GDPR jest bowiem mowa o podejmowania decyzji dotyczącej danej osoby, polegającej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołującej wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływającej. Przepis zatem mówi tylko o skutkach prawnych lub innym podobnym wpływie.

- **Art. 6.2.f** – warte zastanowienia jest czy wymóg oparcia się na prawie

[1] Art. 22.1 GDPR: „1.Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa."

krajowym lub prawie unijnym nie doprowadzi do fragmentacji pomiędzy państwami członkowskimi i nie stoi w sprzeczności z celem rozporządzenia, którym jest przyjęcie zharmonizowanego podejścia. Wymóg ten trzeba przeanalizować pod kątem brzmienia art. 89 GDPR, który nie przewiduje, aby potrzeby statystyczne były co do zasady przedmiotem prawa unijnego lub prawa państwa członkowskiego (zob. art. 5(1) GDPR). W art. 9.2.j jest natomiast analogiczny wymóg odnoszący się do danych sensytywnych. W ePrivacy rozciągnięto wymóg na wszystkie dane bez rozróżniania czy są to dane sensytywne czy nie. Polska nie sugeruje wykreślenia wymogu ale przeanalizowanie skutków.

- **Art. 6.3.**
  Wątpliwości wzbudza tekst: **Without prejudice to paragraph 1,**Providers of the electronic communications **networks and** services may **shall be permitted to** process electronic communications content only: (…)
  (aa) for the purpose of the provision of an explicitly requested service by an end-user for purely individual use if the requesting end-user has given consent and where such requested processing does not adversely affect fundamental rights and interests of another person concerned and does not exceed the duration necessary for the provision of the requested services and is limited to that purpose only; or (…)
  Czy powyższy zapis oznacza, że nawet jeśli przetwarzanie treści jest konieczne do dostarczenia usługi, dodatkowo użytkownik musi wyrazić zgodę na przetwarzanie. Czy w efekcie mamy do czynienia z podwójną przesłanką przetwarzania danych? W RODO zasadą jest oparcie się na jednej przesłance przetwarzania danych.

- **Polska zwraca uwagę na wysoką sensytywność danych lokalizacyjnych i potrzebę zapewnienia właściwej ochrony tych danych.**

6. **Art. 8 – pliki cookies**

W odniesieniu do kwestii cookie walls [tj. możliwości uzależnienia dostępu do treści dostępnych w internecie od udzielenia zgody na stosowanie plików cookies] jeszcze raz PL proponuje zwrócić się o opinię do Europejskiej Rady Ochrony Danych w kwestii zbadania czy tak udzielona zgoda jest dobrowolna – biorąc jednak pod uwagę specyfikę obecnych modeli biznesowych. Należy jednak wskazać, że projektowany Europejski Kodeks Łączności Elektronicznej w motywie (16) wskazuje udostępnienie danych osobowych jako formę wynagrodzenia za usługę.

[dodatkowa wiadomość: na uwagę zasługuje podniesiona na ostatniej grupie H5 propozycja, aby w przypadku oferowania bezpłatnego dostępu do treści w internecie (przy którym istniałby wymóg zgody na cookies), przedsiębiorca oferował również płatny dostęp (bez możliwości stosowania plików cookies). Wydaje się, że w większym stopniu zapewniona by była dobrowolność wyboru, udzielenia zgody na cookies. Konieczne będzie również wzmocnienie obowiązków informacyjnych, m.in. o

celach stosowania plików cookies. Należy mieć na uwadze specyfikę sektora, obowiązujące modele biznesowe oparte na reklamach, to, iż wprowadzenie zakazu cookie walls może spowodować wprowadzenie opłat za treści dostępne w internecie.]

7. **Art. 10 – ustawienia prywatności**

W związku z wykreśleniem z tekstu art. 10, który dotyczył ustawień prywatności warto rozważyć, aby w motywach wskazać, że zasada privacy by default zawarta w art. 25 GDPR ma zastosowanie również do ePrivacy. Na skutek wykreślenia art. 10 wykreślono bowiem również motyw 23, który wskazywał właśnie na art. 25 GDPR.
Zasada privacy by design oraz privacy by default są jednymi z kluczowych zasad GDPR. Zapewnienie takiego standardu ochrony prywatności powinno być obowiązkiem również producentów urządzeń końcowych czy aplikacji internetowych. Należy jeszcze raz zastanowić się nad tym, czy na skutek wykreślenia w całości art. 10 nie zostanie obniżony poziom ochrony użytkowników.

8. **Art. 16 – marketing bezpośredni**

Art. 16 co do zasady ustanawia obowiązek uzyskania zgody na przesłanie wiadomości marketingu bezpośredniego. Nie ma tu mowy o uprzedniej zgodzie („prior consent"). KE wyjaśniała już tę kwestię wskazując, iż doprecyzowanie to było zbędne, gdyż oczywistym jest, iż zgoda powinna być uprzednia.
Istnieją jednak wątpliwości odnośnie etapu, na jakim owa zgoda powinna zostać uzyskana. W Polsce są rozbieżne interpretacje odnośnie przykładowo tego czy zgoda może być wydana w trakcie tej samej rozmowy co przekaz marketingowy. Niektóre organy przyjmowały restrykcyjną interpretację wskazującą, że przesyłanie zapytań o zgodę na marketing bezpośredni bez uprzedniej zgody na kontakty stanowiło naruszenie przepisów.
Polska proponuje zatem, aby rozważyć doprecyzowanie kwestii wyrażania zgody na marketing w motywach.

9. **Art. 18 – organ nadzorczy**

PL z zadowoleniem przyjęła zmiany dokonane w art. 18. Jednakże wątpliwości budzi wskazanie w art. 18 ust. 1ab, że organ nadzorczy powinien mieć prawo do zapewnienia środków zaradczych zgodnie z artykułem 21.1. oraz 23 ePrivacy. Art. 21.1. odsyła natomiast do środków wskazanych w art. 77, 78, 79 GDPR. Tymczasem art. 78 i 79 GDPR dotyczą prawa do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu lub przeciwko administratorowi – a zatem, jak należy sądzić to nie w gestii organu nadzorczego leży zapewnienie tych środków. Jedynie art. 77 GDPR dotyczy prawa do wniesienia środka odwoławczego do organu nadzorczego.
PL podziela ponadto wątpliwości podniesione przez Litwę, czy treść art. 18 ust. 1ab daje możliwość do ustanowienia innych niż wskazane w art. 21.1. i 23 ePrivacy środków oraz wskazanie organu nadzorczego innego niż organ ochrony danych. Należy zatem przeanalizować skutki proponowanego przepisu czy daje on dowolność w wyborze organu nadzorczego.

10. **Art.29.2 – PL** popiera wydłużenie terminu rozpoczęcia obowiązywania regulacji do 2 lat od jej publikacji. Stosownych zmian wymagają także daty wskazane w art. 27 i 28.

Przedstawiciel Polski może zadawać dodatkowe pytania w zależności od przebiegu dyskusji.

Opracowała:
Agnieszka Chruszcz, Starszy specjalista, Departament Telekomunikacji
Wydział Regulacyjny Ministerstwo Cyfryzacji
e-mail: agnieszka.chruszcz@mc.gov.pl

Zaakceptował:
Dariusz Dąbek, Zastępca Dyrektora, Departament Telekomunikacji
e-mail: dariusz.dabek@mc.gov.pl