FUNDACJA PANOPTYKON

Warszawa, 17 stycznia 2017 r.

Uwagi Fundacji Panoptykon dotyczące projektu rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej

Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej (dalej: **projekt rozporządzenia)** wprowadza nowe zasady przetwarzania danych w sektorze usług łączności elektronicznej. Naszym zdaniem wiele z proponowanych w projekcie rozporządzenia zmian zmierza w dobrym kierunku, zapewniając lepsze gwarancje poszanowania praw użytkowników. Nie mniej jednak niektóre z propozycji wymagają zmian na dalszym etapie prac legislacyjnych.

Naszym zdaniem dalsze prace nad projektem rozporządzeniem powinny być wyznaczone przez następujące cele:

- Zagwarantowanie wysokiego poziomu ochrony poufności komunikacji oraz prawa do ochrony danych osobowych użytkowników (art. 7 i 8 Karty Praw Podstawowych).
- Zachowanie spójności z zasadami ujętymi w rozporządzeniu ogólnym o ochronie danych osobowych (dalej: **RODO**). Uzupełnienie i doprecyzowanie rozwiązań wynikających z RODO do usług łączności elektronicznej.
- Dostosowanie nowych przepisów do zmian technologicznych i społecznych. Objęcie zakresem projektu rozporządzenia nowych form komunikacji bez względu na to, czy są świadczone przez tradycyjnych dostarczycieli usług czy np. dostarczycieli usług telefonii internetowej czy komunikatorów. Zakres projektu powinien obejmować usługi funkcjonalnie równoważne oraz takie które oferują nowe możliwości komunikacji.
- Zapewnienie by podstawą dla przetwarzania danych dotyczących łączności elektronicznej były jasno i precyzyjnie określonych cele. W wyjątkowych sytuacjach taką podstawą może być zgoda użytkownika. Udzielanie i wycofywanie zgody powinno odbywać się za pomocą skutecznych i przyjaznych użytkownikom narzędzi (np. poprzez przeglądarki bądź inne oprogramowania lub systemy operacyjne). Wszelkie formy śledzenia użytkowników, monitorowania i wykorzystywania danych bez ich zgody powinny stanowić wyjątek.
- Nowe rozwiązania prawne powinny zapewnić użytkownikom możliwość korzystania z szyfrowanej komunikacji a stosowanie tzw. tylnych wejść do oprogramowania (ang. *backdoors*), nakazów odszyfrowywania czy monitorowania komunikacji szyfrowanej co do zasady powinno być zakazane.

Nasze stanowisko w sprawie projektu rozporządzenia opiera się przede wszystkim na wcześniejszych uwagach Europejskiego Inspektora Ochrony Danych (nr opinii 5/2016), Grupy Roboczej art. 29 (nr opinii 03/2016) oraz European Digital Rights – koalicji

europejskich organizacji pozarządowych zajmujących się prawami cyfrowymi.

1. Forma aktu prawnego

Komisja Europejska zdecydowała, że nowe zasady ochrony prywatności w sektorze łączności elektronicznej zostaną ujęte w formie rozporządzenia. Popieramy ten wybór z kilku względów: a) jest on kompatybilny z modelem regulacji przyjętym dla ogólnych zasad ochrony danych osobowych (RODO); b) gwarantuje podmiotom danych spójne zasady traktowania przez wszystkie podmioty, których przepisy będą dotyczyć; c) zapewnia w miarę jednolitą implementację we wszystkich krajach członkowskich, d) minimalizuje ryzyka wynikające z mechanizmu one-stop-shop.

2. Zakres materialny i definicje

a. Definicje danych dotyczących treści i metadanych

Projekt rozporządzenia wprowadza nowe pojęcia: dane dotyczące łączności elektronicznej, treść łączności elektronicznej oraz metadane dotyczące łączności elektronicznej. Odejście od stosowanego w obowiązującej obecnie dyrektywie podziału na dane dotyczące ruchu i lokalizacji zasługuje na poparcie. Podział ten prowadził do niespójnej interpretacji na etapie wdrażania i stosowania konkretnych przepisów.

Nadal pozostaje jednak wątpliwość, czy w dzisiejszym stanie technologicznym za każdym razem można precyzyjnie oddzielić dane dotyczące treści od metadanych. Na przykład istnieją wątpliwości czy pełny adres URL (wskazujący dokładnie na odwiedzoną stronę) stanowi daną dotyczącą treści czy metadaną. Co więcej, przetwarzanie metadanych może w taki sam (a czasami nawet bardziej inwazyjny) sposób naruszać prywatność użytkowników jak przetwarzanie treści komunikacji. Dlatego rozróżnianie tych dwóch kategorii danych nie powinno się przekładać na odmienny standard ich ochrony.

b. Usługi funkcjonalnie równoważne

Definicje danych wprowadzone przez projekt rozporządzenia odnoszą się do tych zawartych w projekcie dyrektywy ustanawiającej tzw. Europejski kodeks łączności elektronicznej (pojęcia „usług łączności elektronicznej" oraz „sieci łączności elektroniczne"). Definicje te zostały rozszerzone i uwzględniają m.in. usługi funkcjonalnie równoważne (jak VoIP, komunikatory internetowe, operatorzy OTT). Jest to dobre rozwiązanie, zbieżne m.in. z rekomendacjami organów ochrony danych osobowych. Niepokoi nas jednak ścisły związek projektu rozporządzenia z projektem dyrektywy, nad którym prace wciąż trwają. Jeżeli w trakcie prac legislacyjnych nad projektem tej dyrektywy zajdą zmiany mające wpływ na zakres przedmiotowy i podmiotowy komentowanego projektu rozporządzenia, niezbędne będzie wprowadzenie odpowiednich poprawek. Należy również zastanowić, się czy projekt rozporządzenia w kluczowych dla niego punktach nie powinien operować definicjami, niezależnymi od innych aktów prawnych.

Zgodnie z art. 4 ust. 2 definicja usług łączności interpersonalnej (wchodzących w skład usług łączności elektronicznej) została rozszerzona o komunikację interpersonalną, która stanowi jedynie dodatek do usługi głównej. Popieramy takie rozwiązanie ponieważ rozszerza ono zakres projektu nie tylko o usługi, które mogą być funkcjonalnie równoważne (różnego rodzaju

komunikatory tekstowe i głosowe), ale obejmuje wszystkie sytuacje, w których następuje faktyczna komunikacja między użytkownikami. Dotyczy to np. komunikacji w grach czy innych aplikacjach, gdzie opcja komunikatorów ma drugorzędne znaczenie. Skoro jednak te aplikacje wyposażone są w funkcję komunikowania się, ich użytkownicy mają prawo oczekiwać takiego samego prawa do zachowania poufności i prywatności, jak w usługach, których główną funkcją jest komunikacja.

3. Zakres terytorialny (art. 3)

Zakres terytorialny projektu rozporządzenia odpowiada założeniom wynikającym z art. 3 ust. 2 RODO. Ekstraterytorialne obowiązywanie nowego rozporządzenia i objęcie jego zakresem tych podmiotów, które oferują usługi osobom pozostającym na terytorium Unii Europejskiej, jest niezbędne dla zrealizowania celów reformy przepisów o ochronie danych osobowych i zasługuje na pełne poparcie.

4. Poufność łączności (art. 5)

Projekt rozporządzenia w art. 5 ustanawia ogólny zakaz ingerencji w poufność danych łączności komunikacyjnej. Powtórzenie tego obowiązującego obecnie standardu uważamy za dobre rozwiązanie. Jednak naszym zdaniem w motywach projektu należy wskazać, że ingerencja i nadzór nad tymi danymi powinien być rozumiany szeroko i uwzględniać zmiany technologiczne (jak chociażby umieszczenie w urządzeniach użytkowników audio beacons, super cookies itp.).

5. Podstawy przetwarzania danych dotyczących łączności elektronicznej (art. 6)

Art. 6 projektu rozporządzenia ustanawia zasady przetwarzania danych dotyczących łączności elektronicznej, danych dotyczących treści oraz metadanych. Naszą uwagę zwróciły różnice w podstawach przetwarzania poszczególnych rodzajów danych. Różnice te mogą prowadzić do problemów interpretacyjnych, zwłaszcza gdy zachodzą wątpliwości co do tego, czy konkretna informacja jest treścią komunikacji czy metadaną.

Art. 6 ust. 1 wskazuje, że przetwarzanie danych dotyczących łączności elektronicznej pozostaje legalne, gdy jest niezbędne dla przekazywania informacji lub zapewnienia bezpieczeństwa komunikacji. Tak sformułowane wyjątki nie budzą naszych wątpliwości, ale uważamy, że w kontekście różnych praktyk biznesowych należy je doprecyzować w motywach projektu rozporządzenia. W szczególności należy wskazać, że dostarczenie reklam ani inne działania marketingowe, w tym badania, nie są potrzebne dla technicznego nawiązania i utrzymywania połączenia

Warunki przetwarzania metadanych oraz treści zostały określone w art. 6 ust. 2 i 3. Jak wskazuje art. 6 ust. 2 pkt b metadane mogą być przetwarzane m.in. do wykrywania nadużyć. Cele te same w sobie wydają się uzasadnione, ale zwracamy uwagę na to, że są one podatne na swobodną interpretację, co w praktyce biznesowej może prowadzić do nadużyć. Niektórzy usługodawcy, powołując się na cele rozliczeniowe, przetwarzają np. pełną historię wejść na strony internetowe. W związku z tym zagrożeniem projekt rozporządzenia powinien doprecyzować

zakres danych niezbędnych dla przetwarzania danych dla celów rozliczeniowych lub odwołać się do zasady minimalizacji danych.

Szczególnie kontrowersyjne i wątpliwości wiążą się z ze zgodą jako podstawą dla przetwarzania zarówno treści, jaki i metadanych. Art. 6 ust. 2 pkt c i ust. 3 pkt a wskazują, że zgoda jest wymagana przy przetwarzaniu danych w związku z dostarczaniem usług. Warto rozważyć, czy samo świadczenie usług nie może być samodzielną podstawą dla przetwarzania danych. Należy również dogłębnie przemyśleć, czy zgoda (obwarowana jedynie uprzednią konsultacją z organem nadzorującym) może być podstawą dla przetwarzania danych dotyczących treści w innych sytuacjach niż związanych z dostarczaniem usług. Przetwarzanie, w tym analiza treści komunikacji, stanowi bardzo głęboką ingerencję w prywatność jednostki. Dlatego też wymaga podwyższonego standardu ochrony. W sytuacji gdy użytkownicy są zmuszeni do zapoznawania się z długimi regulaminami usług oraz politykami prywatności, kwestie dotyczące przetwarzania treści mogą po prostu umykać ich uwadze i zostać opatrznie ocenione.

Z kolei art. 6 ust. 2 pkt c wskazuje, że przetwarzanie metadanych jest możliwie za zgodą użytkownika zarówno dla świadczenia , jak i innych celów. Przy czym nie stosuje się tutaj rozróżnienia wskazanego w art. 6 ust.3. Tymczasem przetwarzanie metadanych może prowadzić do porównywalnych naruszeń prywatności jak przetwarzanie treści. Mogą też zaistnieć wątpliwości dotyczące tego, czy konkretna informacja jest metadaną czy treścią – pod tym względem uważamy, że projekt rozporządzenia przynajmniej powinien stosować zbliżone (w stopniu uwzględniającym różnice technologiczne) standardy ochrony zarówno dla treści, jak i metadanych

Uważamy również, że komentowany przepis powinien bezpośrednio odwoływać się do zasad proporcjonalności i minimalizacji danych ujętych w RODO.

6. Gromadzenie i usuwanie danych(art. 7)

Popieramy ogólny wymóg usuwania lub anonimizacji danych, w przypadku których nie istnieje dalsza podstawa przetwarzania przez dostawcę usług. Jednocześnie zwracamy uwagę na praktyczne trudności związane ze skutecznym przeprowadzeniem anonimizacji. W związku z tym uważamy, że projekt rozporządzenia – przynajmniej w motywach – powinien odnosić się do definicji danych zanonimizowanych zawartej w RODO (motyw 26) oraz wziąć pod uwagę inne wymogi dotyczące anonimizacji, które zostały przedstawione w opinii Grupy Roboczej art. 29 nr 05/2014. Zawracamy również uwagę na ustanowiony w art. 7 ust. 3 projektu rozporządzenia wyjątek dotyczący danych niezbędnych do celów rozliczeniowych. Również w tym punkcie powinno zostać wprowadzone wyraźne odwołanie do zasady minimalizacji danych, aby ograniczyć ryzyko jego nadinterpretacji.

7. Ochrona informacji gromadzonych w urządzeniach końcowych (śledzenie aktywności użytkowników) (art. 8)

W art. 8 projektu rozporządzenia wprowadzono zasady ochrony informacji gromadzonych w urządzeniach końcowych. Naszym zdaniem projekt powinien stworzyć jeszcze silniejsze gwarancje ochrony prywatności użytkowników w tym kontekście i wyeliminować najgorsze praktyki, jak tzw. cookie-wall (patrz pkt 8). Co do zasady, możliwość zapisywania jakichkolwiek danych na urządzeniach końcowych użytkowników powinna być uzależniona od ich świadomej

i poinformowanej zgody. Wyjątki od tej zasady powinny dotyczyć tylko takich sytuacji, w których istnieje znikome zagrożenie dla prywatności (chociażby w przypadku tzw. analitical cookies), a wręcz pojawia się dodatkowa korzyść (np. większa stabilność sieci) oraz towarzyszy temu odpowiednia informacja dla użytkownika.

Uważamy, że sytuacje ujęte w art. 8 powinny zostać jeszcze przenalizowane pod kątem tych wymogów. Pod tym względem nasze szczególne wątpliwości wzbudza treść art. 8 ust. 2 pkt b Gromadzenie danych emitowanych przez urządzenie końcowe (w celu nawiązania połączenia z innym urządzeniem) powinno podlegać tym samym ograniczeniom, co zapisywanie danych na takim urządzeniu i, co do zasady, wymagać zgody użytkownika. Ta zasada, powinna obowiązywać w szczególności, gdy dane emitowane przez urządzenie mają być wykorzystywane do profilowania użytkowników lub marketingu bezpośredniego (np. przy wykorzystaniu beaconów).

8. Zgoda (art. 9)

Art. 9 zawiera definicję zgody oraz zasady jej udzielania i wycofania. Popieramy konstrukcję przewidzianą w art. 9 ust. 2, który umożliwia skuteczne udzielenie zgodny za pomocą ustawień oprogramowania pozwalającego na dostęp do Internetu. Uważamy też, że taki sposób wyrażenia zgody powinien być obligatoryjny wtedy, gdy pozwalają na to warunki technologiczne (zmienić słowa „may" przez „shall"). Takie rozwiązanie ograniczyłoby ekspozycję użytkowników na mniej efektywne metody pozyskiwana zgody (np. pop-upy). Uważamy również, że zgoda mogła by być udzielana nie tylko z poziomu oprogramowania, ale również urządzenia końcowego lub jego oprogramowania. Np. zgoda na przetwarzania danych przez konkretne aplikacje mogłaby być wyrażana poprzez odpowiednie ustawienia w smartfonie.

Zwracamy również uwagę na to, że zgoda na przetwarzanie danych powinna być wyrażona dobrowolnie i po uzyskaniu odpowiednich informacji. Obecne praktyki biznesowe rzadko stwarzają użytkownikom taką możliwość. W wielu przypadkach mamy do czynienia ze zjawiskiem tzw. cookie-wall, które sprowadza się do tego, że użytkownicy, którzy nie zaakceptowali plików cookies, nie są w stanie korzystać ze strony internetowej. Tymczasem wiele cookies pozwala na śledzenie użytkownika również po opuszczeniu przez niego konkretnej witryny. Podmiotom biznesowym zapewnia to informacje do profilowania i działań marketingowych, ale jednocześnie poważnie narusza autonomię informacyjną użytkowników. Naszym zdaniem zjawisko cookie-wall przeczy idei swobodnie wyrażanej zgody, która została ujęta w RODO (motyw 42). Dlatego projekt rozporządzenia powinien wyraźnie zakazać podobnych praktyk. Rekomendacje w tym zakresie zawiera opinia EDPS (nr 5/2016, str. 16).

9. Domyślne ustawienia prywatności (art. 10)

Zgodnie z art. 10 projektu dostępne na rynku oprogramowania umożliwiające komunikację elektroniczną powinny oferować opcję ochrony przed śledzeniem aktywności użytkownika przez podmioty trzecie. O ile rozwiązanie to zmierza w dobrym kierunku, uważamy je za zdecydowanie niewystarczające. Po pierwsze, art. 10 powinien nie tylko obejmować oprogramowanie, ale również komponenty urządzeń końcowych. Po drugie, ustawienia – zarówno oprogramowania, jak i komponentów – powinny uniemożliwiać śledzenie przez podmioty trzecie w opcji domyślnej. Zbieranie danych o aktywności użytkowników w sieci (jeśli nie są one niezbędne do świadczenia zamówionej usługi ani wymagane przez prawo) powinno

być możliwe dopiero w wyniku wyrażenia przez nich wyraźnej zgody, a nie tak długo, jak nie skorzystają oni z opcji, jaką przewiduje ich urządzenie czy oprogramowanie. Takie rozwiązanie byłoby zgodnie z zasadą ochrony prywatności w opcji domyślnej, którą przewiduje RODO, i byłoby bardzo pożądanym przełomem w ochronie praw użytkowników.

10. Wyłączenia dla ustawodawstwa krajowego (art. 11)

Projekt rozporządzenia przewiduje możliwość ustanowienia wyłączeń w ustawodawstwie krajowym od ogólnych zasad przetwarzania danych m.in. w celach zapewnienia bezpieczeństwa czy walki z przestępczością. Uważamy, że wszelkie w tego typu wyjątki powinny być ograniczone zasadami niezbędności i proporcjonalności.

W przypadku gromadzenia przez instytucje publiczne danych o łączności elektronicznej i ich pozyskiwania od dostawców usług przejrzystość odgrywa kluczowe znaczenie. W związku z tym popieramy rozwiązanie przewidziane w art. 11 ust. 2, które przewiduje jasne procedury udostępniania tego typu danych oraz informowania (na żądanie) organu nadzoru o zapytaniach kierowanych do dostawców usług. Uważamy jednak, że jest ono niewystarczające. Po stronie dostawców usług powinien istnieć obowiązek przekazywania organowi nadzorującemu informacji o zapytaniach i danych udostępnianych wszelkim organom publicznym (np. w cyklu rocznym). Organ nadzorujący powinien zaś upubliczniać ww. dane w zagregowanej formie.

11. Organy nadzoru (art. 18)

Zgodnie z art. 18 projektu rozporządzenia organem odpowiedzialnym za monitorowanie jego realizacji będą organy odpowiedzialne za monitorowanie RODO. To dobre rozwiązanie, które zwiększa szansę na spójne i konsekwentne stosowanie zasad wynikających z obu instrumentów. Zwracamy jednak uwagę, że przekazaniu dodatkowych obowiązków powinno towarzyszyć zapewnienie organom nadzorującym również odpowiednich środków finansowych, osobowych i technicznych, aby mogły te obowiązki realizować.

12. Środki ochrony (art. 21)

Art. 21 projektu rozporządzenia wskazuje, że użytkownicy mają prawo do środków ochrony określonych w art. 77, 78 i 79 RODO. Niestety, projektodawca zrezygnował z możliwości reprezentowania użytkowników przez organizacje lub zrzeszenia, które nie mają charakteru zarobkowego, i które działają w obszarze ochrony danych. Taka decyzja wydaje się niezrozumiała, a co więcej taka możliwość była uwzględniona w wersji projektu rozporządzenia, która wyciekła w grudniu 2016 r. przez co jej usunięcie budzi jeszcze większe wątpliwości.

Udział w postępowaniu organizacji społecznych, posiadających wyspecjalizowaną wiedzę i udzielających pomocy prawnej, może wzmocnić pozycję i ochronę użytkowników, których prawa naruszono. Taki model z powodzeniem funkcjonuje m.in. w prawie konsumenckim. Wyłączenie możliwości reprezentacji użytkowników przez organizacje społeczne budzi też wątpliwości pod kątem spójności z RODO, a szczególnie jego art. 80. Nie dostrzegamy argumentów, które uzasadniałyby stosowanie odmiennych standardów postępowania w bardzo podobnych przypadkach, do których odnoszą się RODO i projektowane rozporządzenie. Co więcej, na gruncie konkretnych postępowań przed sądami mogą pojawić się wątpliwości, czy w

konkretnej sprawie zastosowanie znajdą przepisy wynikające z RODO czy *lex specialis* w postaci projektu rozporządzenia lub też obydwa akty prawne tylko w różnym zakresie. Takie rozwiązanie mogłoby prowadzić do niepewności prawnej i problemów w intepretacji.

13. Szyfrowanie

Jak wskazuje w swojej opinii Grupa Robocza art. 29 „szyfrowanie stało się krytycznym narzędziem służącym ochronie poufności komunikacji w ramach sieci łączności elektronicznej" (opinia nr 3/2016). Sytuacja ta naszym zdaniem powinna znaleźć odzwierciedlenie w projekcie rozporządzenia. Uważamy, że użytkownicy powinni uzyskać *explicite* prawo do szyfrowanej komunikacji. Jednocześnie powinien zostać wprowadzony zakaz monitorowania szyfrowanej komunikacji, deszyfrowania oraz wprowadzania tzw. tylnych drzwi (ang. *back-doors*).