PROJEKT STANOWISKA RP

przygotowany w związku z art. 7 ustawy z dnia 8 października 2010 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz. U. Nr 213, poz. 1395)

Dotyczy	Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)

Data przekazania Polsce dokumentu przez instytucje UE	luty 2017 r.

Sygnatura dokumentu	Komisja Europejska	COM (2017) 10
	Numer międzyinstytucjonalny	2017/0003 (COD)

Procedura decyzyjna	zwykła procedura ustawodawcza

Tryb głosowania w Radzie UE	większość kwalifikowana

Instytucja wiodąca	Ministerstwo Cyfryzacji

Instytucje współpracujące	UKE, UOKiK, MSWiA, GIODO, KPRM

Data przyjęcia przez KSE	23 czerwca 2017 r.

I. Cel projektu aktu prawnego

W dniu 10 stycznia 2017 r. Komisja Europejska (dalej także KE) opublikowała projekt rozporządzenia dotyczącego poszanowania życia prywatnego i ochrony danych osobowych w sektorze komunikacji elektronicznej i uchylającego dyrektywę 2002/58/WE, będący wynikiem prac nad przeglądem obowiązującej obecnie dyrektywy 2002/58/WE z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.

Celem projektowanego aktu jest określenie zasad odnoszących się do ochrony podstawowych praw i wolności zarówno osób fizycznych, jak i prawnych w związku z zapewnianiem i korzystaniem z usług komunikacji elektronicznej.

Z zapowiedzianego już w Strategii Jednolitego Rynku Cyfrowego przeglądu obowiązującej dyrektywy 2002/58/WE, wynika, że cele i zasady zawarte w tej dyrektywie, tj. potrzeba zapewnienia prywatności i poufności komunikacji pozostają aktualne. Regulacje dyrektywy 2002/58/WE co do zasady odpowiadają tym celom, jednakże z uwagi na istotny postęp technologiczny oraz rozwój usług internetowych realizowanych w oparciu o komunikację interpersonalną, który nastąpił w ostatnich latach, tj. w okresie od wprowadzenia ostatnich zmian w dyrektywie 2002/58/WE w 2009 r. spowodował, że wystąpiła potrzeba opracowania nowego aktu prawnego mającego zastąpić dyrektywę 2002/58/WE. Postęp technologiczny obejmuje m.in. powstanie nowych rozwiązań technicznych, które umożliwiają śledzenie aktywności użytkowników końcowych w sieci, a które nie są objęte zakresem dyrektyw 2002/58/WE. Należy również wskazać, że obecnie konsumenci i przedsiębiorcy coraz częściej korzystają z usług VoIP (ang. voice over internet protocol), tj. połączeń telefonicznych przez Internet, komunikatorów internetowych, tzw. webmaili[1] w miejsce tradycyjnych usług komunikacji elektronicznej. Dyrektywa 2002/58/WE nie obejmuje jednak podmiotów świadczących usługi OTT[2] (ang. Over the top), co sprawiło, iż wystąpiła asymetria między obowiązkami dostawców tradycyjnych usług komunikacji elektronicznej a obowiązkami „nowych" dostawców usług OTT, a co za tym idzie obecne regulacje nie zapewniają jednolitego i dostatecznego poziomu ochrony komunikacji. Projektowane rozporządzenie ma zatem za zadanie dostosować przepisy w zakresie ochrony prywatności i danych w komunikacji elektronicznej do obecnych realiów rynkowych.

Ponadto, projektowane rozporządzenie ma stanowić *lex specialis* w stosunku do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej także RODO). RODO określa ogólne ramy regulacyjne w zakresie ochrony danych osobowych. Natomiast projektowane rozporządzenie będzie doprecyzowywać i uzupełniać RODO w odniesieniu do danych dotyczących łączności elektronicznej. Jednoczenie należy zaznaczyć, że o ile ogólne rozporządzenie o ochronie danych zapewnia ochronę danych osobowych, to dyrektywa 2002/58/WE i projektowane rozporządzenie zapewniają poufność komunikacji,

[1] aplikacja internetowa pozwalająca użytkownikom korzystać z usług poczty elektronicznej, przy wykorzystaniu przeglądarki internetowej w roli klienta poczty elektronicznej

[2] Over the top services – usługi polegające na dostarczaniu treści video, audio i innych mediów przez Internet, które operatorzy zapewniają swoim abonentom. Nie mają jednak kontroli nad treścią udostępnianej usługi, gdyż jest ona oferowana przez podmioty trzecie.

która może obejmować także dane nie stanowiące danych osobowych oraz dane powiązane z osobami prawnymi (tj. niepodlegające ochronie na podstawie przepisów RODO).

Konieczność dostosowania przepisów projektowanego rozporządzenia do regulacji zawartej w RODO sprawia, że niezbędnym staje się uchylenie części przepisów, które obecnie znajdują się w dyrektywie 2002/58/WE. Do tych przepisów należy zaliczyć m.in. zasady bezpieczeństwa przetwarzania danych uregulowane w art. 4 dyrektywy 2002/58/WE. Kwestie te są obecnie całkowicie objęte zakresem RODO, w związku z czym nie ma potrzeby ich powtarzania w projektowanym rozporządzeniu. Ponadto, brak podjęcia odpowiednich działań legislacyjnych będzie skutkował np. podwójnym obowiązkiem notyfikacyjnym w przypadku naruszenia ochrony danych osobowych. Przepisy RODO stosuje się zatem do kwestii dotyczących przetwarzania danych osobowych w komunikacji elektronicznej w zakresie w jakim nie zostały uregulowane w projektowanym rozporządzeniu.

II. Stanowisko RP

Rząd Polski wspiera wynikający z projektowanego rozporządzenia ogólny kierunek działania Komisji Europejskiej zmierzający do zapewnienia w Europie efektywnej ochrony prywatności i danych w komunikacji elektronicznej, a także ujednolicenia obowiązków dostawców usług OTT z obowiązkami podmiotów świadczących tradycyjne usługi komunikacji elektronicznej.

Jednocześnie Rząd RP stoi na stanowisku, że przyjmowane regulacje powinny zapewniać ochronę bezpieczeństwa i porządku publicznego oraz ochronę interesów konsumenckich. Te dobra często mają pierwszeństwo przed prawem do prywatności i z tego względu przepisy tworzonego rozporządzenia w pierwszej kolejności powinny umożliwiać ochronę prawna tych wartości ;

Głównymi zmianami w porównaniu do obecnie obowiązującej dyrektywy 2002/58/WE jest:

- zmiana zakresu przedmiotowego regulacji poprzez objęcie nią również usług OTT, komunikatów przesyłanych machine-to-machine, publicznych, otwartych sieci WiFi,
- wprowadzenie definicji nowych pojęć niedefiniowanych w dotychczas obowiązującej dyrektywie 2002/58/WE, tj. definicji danych pochodzących z łączności elektronicznej, treści łączności elektronicznej, metadanych pochodzących z łączności elektronicznej,
- brak rozróżnienia na dane o ruchu i dane o lokalizacji poprzez połączenie obu tych kategorii danych w jedno pojęcie metadanych, co ma służyć stworzeniu jednakowych zasad przetwarzania tego rodzaju danych,
- usunięcie przepisów dotyczących kwestii, które uregulowane są także w RODO, m.in. przepisów dotyczących zasad bezpieczeństwa,
- zmiana w zakresie legalnego przetwarzania danych, w szczególności w zakresie przetwarzania za zgodą użytkownika, wprowadzenie wymogu uzyskania zgody użytkownika na przetwarzanie danych w celu dostarczenia usług,
- zmiany w zakresie wykorzystywania plików cookies. Projektowane rozporządzenie zobowiązuje podmioty zarządzające przeglądarkami internetowymi do umożliwienia użytkownikom wprowadzenia na początkowym etapie konfiguracji przeglądarki opcji wyłączenia możliwości używania cookies i podobnych narzędzi,
- ograniczenie wykorzystywania danych generowanych przez urządzenia końcowe,

- wprowadzenie bardziej restrykcyjnych zasad dotyczących marketingu bezpośredniego, wprowadzenie ogólnego wymogu uzyskania zgody na marketing przy wykorzystaniu usług łączności elektronicznej - bez wskazywania w przepisie poszczególnych środków komunikacji (rozporządzenie przewiduje wyjątki od tej zasady),
- wskazanie, że organem odpowiedzialnym za monitorowanie stosowania rozporządzenia będzie organ nadzorczy właściwy do monitorowania stosowania rozporządzenia RODO, który ma jedynie „współpracować w stosownych przypadkach" z krajowym organem regulacyjnym,
- wprowadzenie analogicznie do RODO dwóch limitów kar pieniężnych za naruszenie przepisów rozporządzenia, które w zależności od rodzaju naruszenia mogą skutkować nałożeniem kary, której górna granica może wynosić: 10 milionów Euro (a w przypadku przedsiębiorstwa - 2% całkowitego rocznego światowego obrotu) albo 20 milionów Euro (lub 4% całkowitego rocznego światowego obrotu),
- umożliwienie użytkownikom końcowym, którzy ponieśli szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów projektowanego rozporządzenia dochodzenia odszkodowania od naruszyciela.

Na uwagę zasługuje przede wszystkim rozszerzenie regulacji na podmioty świadczące usługi OTT, ograniczenie śledzenia zachowań użytkowników końcowych w sieci, informowanie użytkowników o ustawieniach prywatności.

Niezależnie zatem od generalnego poparcia dla propozycji projektu rozporządzenia, Rząd RP oraz partnerzy społeczni, z którymi konsultowany był projekt przedmiotowej regulacji, dostrzegają pewne obszary, omówione w uzasadnieniu stanowiska, które w trakcie prac nad przedłożonym projektem wymagać będą pogłębionych analiz i wyjaśnień ze strony projektodawców.

Zastrzeżenia Rządu RP budzi w szczególności proponowana forma regulacji – rozporządzenie zamiast dyrektywy, zbyt krótki termin wejścia w życie projektowanych przepisów, niewystarczająca regulacja odnośnie stosowania plików cookies (regulacja powinna być bardziej przyszłościowa, uwzględniać również przyszłe zmiany technologiczne), niejasna relacja części przepisów do RODO oraz relacja projektowanego rozporządzenia do innych aktów unijnych (dyrektywy 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW, dyrektywy 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW, dyrektywy 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego). Ponadto, należy zaznaczyć, że regulacja powinna uwzględniać najnowsze rozwiązania techniki (takie jak np. sztuczna inteligencja, połączone samochody, sieci sensorów) oraz być zorientowana na przyszłość. Regulacje nie są w stanie nadążyć za zmianami technologicznymi, więc jedynym rozwiązaniem jest projektowanie praw na odpowiednim poziomie ogólności, z dokładnym zrozumieniem aktualnej sytuacji i możliwością przewidzenia tego, co nadchodzi.

Wątpliwości Rządu RP budzi także stopień uwzględnienia w projekcie przedmiotowego rozporządzenia zasady autonomii instytucjonalnej państw członkowskich. Autonomia instytucjonalna oznacza swobodę państw członkowskich w kształtowaniu struktur wewnętrznych wykonujących zobowiązania wynikające z prawa unijnego, w tym udziału w procesie decyzyjnym i instytucjach UE. Powołana zasada przyznaje państwom członkowskim swobodę na dwóch płaszczyznach. Po pierwsze, w wyborze organów odpowiedzialnych za realizację określonych zadań unijnych, a po drugie, swobodę wyposażenia ich we właściwe kompetencje. Ustawodawca unijny dał wyraz pełnemu poszanowaniu wskazanej zasady, przyznając w RODO państwom członkowskim pełną swobodę w określeniu aparatu instytucjonalnego nadzorującego przestrzeganie tego rozporządzenia. W ocenie Rządu RP zasada taka powinna znaleźć swoje odzwierciedlenie również w przedmiotowym rozporządzeniu, poprzez przyznanie państwom członkowskim pełnej swobody w określeniu który z organów państwowych jest najwłaściwszy do nadzoru nad realizacją przepisów dotyczących ochrony prywatności w sieciach łączności elektronicznej. Ze względu na materię regulacji przedmiotowego rozporządzenia oraz dotychczasową praktykę stosowania postanowień dyrektywy 2002/58/WE możliwe jest wiele różnych rozwiązań sprowadzających się nie tylko do przyznania takiej kompetencji organowi nadzorczemu powołanemu na podstawie przepisów RODO ale również pozostawienia nadzoru nad realizacją przepisów dotyczących ochrony prywatności w sieciach łączności elektronicznej krajowemu organowi regulacyjnemu na rynku usług łączności określonemu w Europejskim Kodeksie Łączności Elektronicznej.

Projekt wymaga także dopracowania ze względu na brak precyzji niektórych przepisów powodujący wątpliwości interpretacyjne co z kolei prowadzi do braku pewności prawnej u adresatów projektowanych norm.

III. Uzasadnienie stanowiska RP

I. Cel, zakres i forma regulacji

Rząd RP z niepokojem przyjął propozycję Komisji Europejskiej zastąpienia dyrektywy 2002/58/WE nowym aktem w formie rozporządzenia, a nie dyrektywy. Należy przy tym zaznaczyć, że zrozumiałe jest to, iż przyjęto model spójny z RODO, zakładając przy tym, że regulacja ta ma wejść w życie razem z RODO. W opinii Rządu RP to forma dyrektywy, w przeciwieństwie do rozporządzenia, umożliwia państwom członkowskim jej wdrożenie do narodowych porządków prawnych w sposób uwzględniający zarówno specyfikę własnego systemu prawnego, jak i właściwości krajowego rynku telekomunikacyjnego. Doświadczenia legislacyjne ostatnich regulacji sektora telekomunikacyjnego w postaci rozporządzenia Parlamentu Europejskiego i Rady UE 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii, wskazują iż forma rozporządzenia, pomimo intencji ustawodawcy europejskiego zmierzającej do pełnej harmonizacji przepisów na terenie UE, nie zapewnia spójności stosowania przepisów, a także nie wyklucza pojawienia się poważnych wątpliwości interpretacyjnych co do stosowania przepisów w praktyce.

Należy mieć na uwadze, że ujęcie regulacji w formie rozporządzenia pomimo, iż akt taki stosowany jest bezpośrednio, wymaga jednak dostosowania przepisów krajów, co również jest czasochłonne - wymaga analiz i konsultacji. Termin rozpoczęcia stosowania regulacji - maj

2018 r. jest zatem zbyt krótki (niezależnie od przyjętej formy regulacji) mając również na uwadze to, że nie dostosowano jeszcze przepisów krajowych do przepisów RODO i w ocenie Rządu RP unijnym instytucjom ciężko będzie go dotrzymać. Należy zapewnić odpowiedni czas na przygotowanie się organizacyjne przedsiębiorców do stosowania przepisów nowej regulacji, zwłaszcza w kontekście nowych obowiązków dla przedsiębiorców, rozszerzenia dotychczasowego zakresu podmiotowego o dostawców usług OTT i wysokich kar za niewdrożenie unijnych przepisów.

Projektowane rozporządzenie przewiduje rozszerzenie zakresu podmiotowego poprzez objęcie zasadami ochrony prywatności nowych podmiotów, tj. dostawców usług OTT (over-the-top service providers), świadczących usługi drogą elektroniczną, takie jak np.: WhatsApp, Facebook Messenger, Skype, Viber. Przepisy będą dotyczyły zatem m.in. witryn internetowych, portali społecznościowych oraz komunikatorów. Rozwiązanie to pozwoli na zobligowanie do zapewnienia użytkownikom takiego samego poziomu ochrony w zakresie poufności komunikacji do jakiego są zobowiązani tradycyjni operatorzy telekomunikacyjni i będzie spójne z projektowaną dyrektywą ustanawiającą Europejski Kodeks Łączności Elektronicznej, która również swoją regulację rozszerza na dostawców usług łączności interpersonalnej niewykorzystujących numerów (tj. komunikatorów OTT). Propozycja ta, a także objęcie regulacją komunikatów przesyłanych machine-to-machine zasługuje w pełni na aprobatę Rządu RP. Wątpliwości może budzić jednak to czy objęcie regulacją usług OTT nie spowoduje zmniejszonej konkurencyjności unijnych usług OTT wobec usług spoza UE.

Ponadto, ze względu na wzrastającą liczbę publicznych sieci WiFi i jednoczesną niską świadomość dotyczącą konieczności zachowania ostrożności w korzystaniu z Internetu na urządzeniach mobilnych, objęcie regulacją publicznych, otwartych sieci WiFi wydaje się słusznym kierunkiem.

Rząd RP podkreśla, że konieczne jest wyraźne wyjaśnienie relacji między projektowanym rozporządzeniem a RODO tak, aby dostatecznie jasnym było, które przepisy RODO znajdą zastosowanie w związku z przedmiotowym projektem, a które projekt wyłącza, zważywszy na fakt, iż projektowana regulacja ma stanowić w stosunku do RODO lex specialis. Rząd RP zaznacza również, że RODO dotyczy ochrony danych osobowych, a zatem danych osób fizycznych. Natomiast użytkownikami końcowymi, których dotyczy projektowane rozporządzenie, są poza osobami fizycznymi również osoby/podmioty inne niż osoby fizyczne, w tym osoby prawne. Dane nie stanowiące danych osobowych oraz dane powiązane z osobami prawnymi nie podlegają ochronie na podstawie przepisów RODO. Okoliczność ta powinna zostać uwzględniona w projektowanym rozporządzeniu. Zasadne jest również określenie relacji między projektowanym rozporządzeniem a dyrektywą 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne i zastępującą decyzję ramową Rady 2005/222/WSiSW, która również zakazuje dostępu do systemów informatycznych, w tym urządzeń końcowych – bez zgody właściciela lub osoby uprawnionej. Projekt rozporządzenia powinien się ponadto wyraźnie odnieść do innych przepisów prawa unijnego regulujących kwestię przesyłania niezamówionych komunikatów handlowych (w szczególności w zakresie podstaw legalizujących przesyłanie takich komunikatów), i w jednoznaczny sposób określić, że rozporządzenie jest jedynym aktem unijnym określającym kompleksowo objęte prawem Unii zasady przesyłania niezamówionych komunikatów handlowych (kwestia ta została wyjaśniona w dalszej części stanowiska).

Ponadto, należy zachować spójność przepisów projektowanego rozporządzenia z przepisami dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w

sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW, w kontekście współpracy przedsiębiorców telekomunikacyjnych z organami ścigania, sądami i prokuratorami. Zachowanie spójności jest istotne w zakresie w jakim dane telekomunikacyjne stanowią dane osobowe i o ile są jako takie niezbędne w procesie ścigania przestępstw i powinny być w sposób określony ramami prawnymi przekazane kompetentnym w tym zakresie tym podmiotom.

Odnosząc się do zakresu przedmiotowego projektu, należy wskazać, iż ma on mieć zastosowanie do przetwarzania danych komunikacji elektronicznej w związku z dostarczaniem i korzystaniem z usług komunikacji elektronicznej oraz do informacji związanych z urządzeniami końcowymi użytkowników końcowych (art. 2 ust. 1). Art. 2 ust. 2 zawiera natomiast zamknięty katalog określający obszary, do których rozporządzenie nie będzie mieć zastosowania, do których należą m.in. czynności podejmowane przez właściwe organy dla celów zapobiegania, wykrywania, ścigania przestępstw, wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

W opinii Rządu RP wątpliwości budzi to, czy rozporządzenie będzie miało zastosowanie do czynności podejmowanych w postępowaniach, które nie dotyczą przestępstw, ale które mają charakter quasi-karny lub spełniają standardy dla postępowania w sprawach o przestępstwa, np. postępowania przed Prezesem UOKiK. Problem ten jest istotny z uwagi na to, że przedsiębiorcy w trakcie postępowania mogą zasłaniać się tajemnicą komunikacji.

Zgodnie z art. 2 ust. 2 lit. d projekt rozporządzenia nie ma zastosowania do działania właściwych organów do celów zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych, w tym ochrony przed i zapobiegania zagrożeniom dla bezpieczeństwa publicznego. Wątpliwości budzi zatem, czy zakresem tego wyłączenia objęte są również CERT-y narodowe (Computer Emergency Response Team). Podmioty te przetwarzają wiele danych osobowych, w szczególności w celu wspomagania organów ścigania czy służb. CERT monitoruje cyberprzestrzeń, pojawiające się zagrożenia oraz przeprowadza analizę ryzyka. W przypadku gdy okazuje się, że istnieje zagrożenie cyberterroryzmem, cyberprzestępczością sprawą dalej zajmują się odpowiednie służby. CERT-y nie są według prawa polskiego ani służbą, ani administracją publiczną i z tego względu pojawia się pytanie, czy art. 2 ust. 2 lit. d projektu ma również do nich zastosowanie. Należy zatem rozstrzygnąć tę kwestię.

Ponadto, niejasna jest relacja pomiędzy art. 2 ust. 2 pkt d oraz artykułem 11. Zgodnie z art. 2 przetwarzanie danych telekomunikacyjnych w związku z bezpieczeństwem publicznym powinno być wyjęte spod regulacji rozporządzenia (a zatem objęte RODO). Wydaje się, że jednak art. 11 dotyczy także takiego przetwarzania. Kwestia ta wymaga wyjaśnienia.

Zakres terytorialny projektowanej regulacji został określony w art. 3, zgodnie z którym projektowane rozporządzenie będzie mieć zastosowanie do:

a) dostarczania usług komunikacji elektronicznej do użytkowników końcowych na terytorium Unii Europejskiej, niezależnie czy wymagane jest dokonanie płatności przez użytkownika końcowego;

b) korzystania z tego rodzaju usług;

c) ochrony informacji odnoszących się do urządzeń końcowych użytkowników końcowych zlokalizowanych na terytorium Unii Europejskiej.

Artykuł 3, podobnie jak RODO, nakłada zatem takie same obowiązki na podmioty świadczące usługi klientom na terenie UE. Nie ma przy tym znaczenia kraj siedziby tych podmiotów, czy miejsce przetwarzania danych. Regulacja ta zdecydowanie zasługuje na aprobatę, gdyż chroni użytkowników na terenie UE bez względu na ich obywatelstwo, a ponadto jest zgodna z zasadą „same service, same rules". Jest ona też zbieżna z rozwiązaniami przyjętymi w RODO, które rozszerzają zakres terytorialny stosowania unijnych przepisów poza terytorium UE. Pozytywnym aspektem z punktu widzenia ochrony prywatności jest również zobowiązanie, na mocy art. 3 ust. 2 projektu rozporządzenia, dostawcy usług komunikacji elektronicznej nie posiadającego swojej siedziby na terytorium Unii Europejskiej do ustanowienia swojego przedstawiciela w Unii Europejskiej, co zapewni łatwiejsze egzekwowanie przestrzegania postanowień projektowanego rozporządzenia oraz kontakt użytkowników z dostawcą usług. Wątpliwości budzi jednak to jakie będą sankcje za nieustanowienie przedstawiciela mimo oferowania usług przez podmiot spoza Unii Europejskiej, a ponadto jakie będą szanse na egzekwowanie ewentualnie nakładanych sankcji.

II. Definicje (art. 4)

Artykuł 4 ust. 1 lit. a wskazuje, że dla celów projektowanego rozporządzenia zastosowanie znajdą definicje zawarte w RODO, co ma znaczenie dla spójnego stosowania obydwu aktów prawnych. Projekt ponadto odwołuje się do definicji zawartych w projektowanej dyrektywie ustanawiającej Europejski Kodeks Łączności Elektronicznej, tj. definicji usługi łączności elektronicznej, usługi łączności interpersonalnej, usługi łączności interpersonalnej opartej na numeracji, usługi łączności interpersonalnej nie opartej na numeracji, użytkownika końcowego, połączenia. Pojawia się zatem wątpliwość czy uda się zachować spójność między tymi dwoma aktami na dalszych etapach prac. Jednocześnie ten sam argument przemawia za wszczęciem prac nad przedmiotowym projektem dopiero w momencie, gdy będą już znane ostatecznie definicje zawarte w Kodeksie Łączności Elektronicznej.

Odnosząc się do definicji usług łączności interpersonalnej należy również wskazać, że zgodnie z art. 4 ust. 2 projektu definicja tych usług na potrzeby projektowanego rozporządzenia została rozszerzona o usługi umożliwiające interpersonalną i interaktywną komunikację, która jest jedynie drobną pomocniczą funkcją, nierozerwalnie związaną z inną usługą. Rozwiązanie to, w opinii Rządu RP, jest słuszne, gdyż umożliwi objęcie projektowanymi przepisami nie tylko usług, które mogą być funkcjonalnie równoważne (różnego rodzaju komunikatory tekstowe i głosowe), ale także objęcie wszystkich sytuacji, w których następuje faktyczna komunikacja między użytkownikami. W praktyce przepis ten dotyczy m.in. komunikacji w grach czy innych aplikacjach, gdzie funkcja komunikowania się jest jedynie dodatkiem.

Ponadto, projekt przewiduje wprowadzenie nowych definicji, w szczególności definicji:

- danych pochodzących z łączności elektronicznej (treść łączności elektronicznej oraz metadane pochodzące z łączności elektronicznej),
- treści łączności elektronicznej (treści przekazywane z wykorzystaniem usług łączności elektronicznej, takie jak tekst, głos, nagrania video, obrazy i dźwięki),
- metadanych pochodzących z łączności elektronicznej (dane przetwarzane w sieci łączności elektronicznej w celu transmisji, dystrybucji/rozpowszechniania lub wymiany treści komunikacji elektronicznej, z uwzględnieniem danych służących do śledzenia i

identyfikacji źródła lub przeznaczenia komunikatu, danych o lokalizacji urządzenia generowanych w związku ze świadczeniem usług łączności elektronicznej oraz datę, czas, długość trwania i rodzaj łączności).

Powyższe definicje określają kategorie informacji wymienianych za pomocą środków komunikacji elektronicznej. W obecnie obowiązującej dyrektywie 2002/58/WE powyższym definicjom odpowiada definicja: danych o ruchu, danych dotyczących lokalizacji, komunikatu.

Nowe pojęcie „metadanych pochodzących z łączności elektronicznej" łączy w sobie definicje danych o ruchu i danych dotyczących lokalizacji zawartych w dyrektywie 2002/58/WE. Projekt nie przewiduje zatem kontynuacji rozróżnienia pomiędzy danymi o ruchu a danymi dotyczącymi lokalizacji, umieszczając oba ww. pojęcia w jednej definicji metadanych pochodzących z łączności elektronicznej. Zniesienie rozróżnienia między danymi o ruchu a danymi dotyczącymi lokalizacji zasługuje na aprobatę Rządu RP, gdyż służyć ma stworzeniu jednakowych zasad przetwarzania tego rodzaju danych. Standardy ochrony prywatności określone w orzecznictwie TSUE (m.in. orzeczenia w połączonych sprawach C-293/12 i C-594/12: *Digital Rights Ireland* oraz w połączonych sprawach C-203/15 i C-698/15: *Tele 2)* wskazują, iż tzw. metadane mogą dostarczać informacji pozwalających na odtworzenie wielu aspektów życia prywatnego danej osoby – m.in. sposobach korzystania ze środków komunikacji elektronicznej, osobach, z którymi się kontaktuje czy miejscach, w których przebywa o konkretnej porze dnia. Część z nich może stanowić także tzw. dane wrażliwe, które podlegają specjalnej ochronie na podstawie przepisów o ochronie danych osobowych. Zebranie tego rodzaju danych pozwala na stworzenie dokładnego profilu behawioralnego określonej osoby, co może stanowić istotną ingerencję w prawa do prywatności i prawa do ochrony danych osobowych wynikających z art. 7 i 8 Karty Praw Podstawowych UE. Ponadto, należy zwrócić uwagę, iż rozwój technologii informacyjnych sprawia, iż dane tego typu przetwarzane są nie tylko przez dostawców usług komunikacji elektronicznej w rozumieniu dyrektywy 2002/58/WE, lecz powszechnie przez podmioty świadczące usługi w cyberprzestrzeni. Jej przejawem jest choćby instalowanie plików cookies. Tego rodzaju podmioty świadczące usługi nowego typu, nieprzystające do kategorii pojęciowych zawartych w aktualnie obowiązującej dyrektywie, mogą uzyskiwać szczegółowe informacje dotyczące sposobu życia określonej osoby bez konieczności wykonywania zobowiązań wynikających z dyrektywy, o ile nie uzyskują dostępu do informacji przechowywanych w urządzeniu końcowym użytkownika. Co więcej, podkreślenia wymaga, iż sposób funkcjonowania usług komunikacji elektronicznej nowej generacji sprawia, iż granice pomiędzy danymi o ruchu i danymi o lokalizacji uległy zatarciu[3].

Połączenie pojęć danych o ruchu i danych dotyczących lokalizacji i stworzenie jednej, całościowej definicji metadanych pochodzących z łączności elektronicznej służyć ma ustanowieniu precyzyjnych reguł dotyczących przetwarzania ww. danych obowiązujących wszystkie podmioty uczestniczące w tym procesie, co w opinii Rządu RP jest w pełni uzasadnione.

Wątpliwości może budzić czy w każdym przypadku możliwe będzie precyzyjne oddzielenie treści łączności elektronicznej i metadanych. Przetwarzanie metadanych również może wiązać się z dużą ingerencją w prywatność, niekiedy większą niż w przypadku przetwarzania treści komunikacji. W związku z tym warte zastanowienia jest zapewnienie jak najbardziej zbliżonych

[3] Opinia grupy roboczej ds. art. 29: Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), 19 July 2016.

standardów ochrony w przypadku przetwarzania obu kategorii danych i zapewnienie użytkownikowi skutecznych warunków do rezygnacji z usługi i wycofania danych utrwalających jego profil zachowania.

Projektowane rozporządzenie przewiduje ponadto wprowadzenie zupełnie nowych definicji: komunikaty marketingu bezpośredniego, połączenia głosowe w ramach marketingu bezpośredniego, zautomatyzowane systemy wywoływania i łączności. Na poparcie zasługuje wprowadzenie definicji komunikatów marketingu bezpośredniego, niemniej definicja w zaproponowanym brzemieniu budzi pewne wątpliwości, w szczególności wątpliwości budzi zdefiniowanie marketingu jako formy reklamowania (*means any form of advertising*), może to bowiem zawężać rozumienie marketingu tylko do komunikatów, w ramach których zawarty jest element perswazyjny, a pozostawić poza jego zakresem takie kontakty, które wprost nie mają na celu sprzedaży usług natomiast pośrednio służą ich promocji np. zaproszenia na spotkania sprzedażowe, umówienie spotkania ze sprzedawcą itp. Zawarcie w definicji odwołania do sposobów przekazywania tych komunikaty wydaje się błędne, gdyż to nie sposób przekazywania komunikatu stanowi o jego charakterze, a jego treść.

Jednocześnie proponuje się dokonać nieznacznych zmian w definicji "poczty elektronicznej" - "electronic mail". Definicja "electronic mail" stanowi, że jest to wiadomość elektroniczna zawierająca takie informacje jak tekst, głos, dźwięk lub obraz. Zwrot "electronic mail" pojawia się w projektowanym art. 16 ust. 2 rozporządzenia dotyczącym komunikatów niezamówionych. Mając na uwadze definicję bezpośredniej komunikacji marketingowej, treść motywu 33 i 34 oraz konieczność dostosowania prawa do współczesnych realiów technologicznych zasadne jest rozważenie doprecyzowania treści definicji tak, aby objęła wszelkie formy komunikacji elektronicznej (email, SMS, MMs, komunikacja bluetooth itp.), co rozwiałoby ewentualne wątpliwości interpretacyjne przepisów, które będą miały zastosowanie wprost przez kraje członkowskie. Należy również wskazać, że definicja komunikatów marketingu bezpośredniego zawiera zwrot "poczty elektronicznej, wiadomości tekstowych". Tymczasem definicja "electronic mail" powinna obejmować również SMS (tak jak to jest w obecnej dyrektywie 2002/58/WE), mając na uwadze zasadę neutralności technologicznej.

III. Podstawy przetwarzania danych

Art. 6 projektowanego rozporządzenia reguluje kwestie przetwarzania danych pochodzących z łączności elektronicznej, metadanych oraz treści łączności elektronicznej, przy czym danymi dotyczącymi łączności elektronicznej są metadane i dane o treści.

Wątpliwości Rządu RP budzi kwestia zgody jako podstawy dla przetwarzania zarówno treści, jak i metadanych. Zgodnie z art. 6 ust. 2 pkt c oraz ust. 3 pkt a zgoda jest wymagana przy przetwarzaniu danych w związku z dostarczaniem usług. Warto, aby unijny prawodawca rozważył wpisanie świadczenia usług jako samodzielną podstawę dla przetwarzania danych, w przypadku gdy przetwarzanie konkretnych danych osobowych jest dla takiego świadczenia niezbędne. Istotne jest to w szczególności w odniesieniu do przetwarzania metadanych niezbędnych do świadczenia usług dodatkowych (np. nawigacyjnych). Jeżeli usługa taka wymaga przetwarzania danych o lokalizacji użytkownika, o czym użytkownik został poinformowany, należy uznać, że wymaganie w takiej sytuacji zgody na to przetwarzanie nie znajduje uzasadnienia. Należy w tym miejscu wskazać, że również dyrektywa 2002/58/WE czy RODO, w art. 6 ust. 1 lit. b, nie wymaga zgody użytkownika na przetwarzanie danych niezbędne do wykonania umowy. Wątpliwości również budzi kwestia wpływu cofnięcia przez

użytkownika zgody na istnienie umowy. Mając na uwadze powyższe wątpliwości, Rząd RP proponuje, aby zgoda nie była wymagana na przetwarzanie metadanych, które są niezbędne do wykonania usługi, o ile użytkownikowi zostanie przekazana, w sposób wyczerpujący, jasny i zrozumiały, informacja na ten temat przed aktywacją usługi. Ewentualnie, zgoda klienta na przetwarzanie metadanych na potrzeby oferowania dodatkowych usług mogłaby być wyrażana poprzez odpowiednie ustawienia oprogramowania (analogicznie jak zaproponowano w art. 9 ust. 2 projektu rozporządzenia). Niezależnie od powyższego, w odniesieniu do art. 6 ust. 3 lit. a należy wskazać, że treści łączności elektronicznej mogą zawierać niezwykle wrażliwe dane. Z tego względu należy doprecyzować przesłanki przetwarzania treści łączności elektronicznej, tak aby uniknąć nadużyć.

Ponadto, należy wskazać, że w opinii Rządu RP art. 6 ust. 3 lit. b) umożliwiający przetwarzanie treści łączności elektronicznych jeżeli wszyscy użytkownicy końcowi, których to dotyczy, wyrazili zgodę na przetwarzanie treści ich łączności elektronicznej dla jednego lub kilku celów, które nie mogą być zrealizowane przez przetwarzanie informacji poddanych anonimizacji, a dostawca skonsultował się z organem nadzorczym - jest nieprecyzyjny i nie pozwala na jasne określenie w jakich sytuacjach będzie miał zastosowanie. Wątpliwości budzi przy tym wymóg, aby zgoda została wyrażona przez wszystkich użytkowników (zatem jest sformułowany odmiennie do art. 6 ust. 3 lit. a). Doprecyzowania może wymagać kwestia, iż zwrot „wszyscy użytkownicy" powinien oznaczać osoby uczestniczące w komunikacji pomiędzy tymi użytkownikami, a nie wszystkich użytkowników tej usługi niezależnie od tego czy uczestniczą w danym połączeniu/komunikacji.

Niezależnie od powyższego, jak zostało to już wskazane w niniejszym stanowisku, przetwarzanie metadanych może prowadzić do porównywalnych naruszeń prywatności jak przy przetwarzaniu treści, a także mogą zaistnieć wątpliwości co do rozróżnienia w praktyce metadanych od treści komunikacji. Jak najbardziej zbliżone standardy ochrony powinny być zatem stosowane w odniesieniu do obu kategorii danych.

IV. Przechowywanie i usuwanie danych komunikacji elektronicznej (art. 7)

Dostawca usług komunikacji elektronicznej powinien usunąć lub zanonimizować treść komunikacji elektronicznej po otrzymaniu treści przez odbiorcę, do którego treść była skierowana. Dane te mogą być odtwarzane lub przechowywane przez użytkowników końcowych zgodnie z RODO. W odniesieniu do metadanych projekt przewiduje obowiązek ich usuwania lub anonimizacji przez dostawcę kiedy już nie będą niezbędne do transmisji komunikacji (analogiczny zapis w odniesieniu do danych o ruchu znajduje się w dyrektywie 2002/58/WE).

Metadane mogą być również przetwarzane w celach rozliczeniowych – do końca okresu, w którym rachunek może zostać zgodnie z prawem zakwestionowany lub płatności mogą być realizowane.

Rząd RP, co do zasady popiera ogólny wymóg usuwania lub anonimizacji danych, w przypadku których nie są już one niezbędne dla celów przesyłu komunikatu. Konieczne jest jednak stworzenie faktycznych możliwości prawnych do ochrony interesów konsumentów związanych np. z kwestią płatności za usługi telekomunikacyjne. Opinie publiczną kilka lat temu bulwersowały przykłady wielotysięcznych rachunków za połączenia , które nie były w rzeczywistości wykonane. Z tego względu przepis ust 3 art. 7 projektowanego rozporządzenia, który reguluje kwestię przechowywania danych na potrzeby reklamacji klientów powinien zostać przeformułowany w taki sposób aby tworzył zobowiązanie dla operatorów, a nie tylko

potencjalną możliwość przechowywania danych. W tym drugim przypadku istnieje obawa że operatorzy po wystawieniu rachunków będą usuwać dane powołując się na rozporządzenie, co spowoduje utrudnienie dochodzenia reklamacji przed sądem przez klienta operatora. Projekt rozporządzenia przewiduje przechowywanie przez okres niezbędny do zakwestionowania rachunku według prawa krajowego. Ze względu na ryzyko pokrzywdzenia konsumenta w przypadku nieznajomości przez niego obcych porządków prawnych należy dodać zastrzeżenie, że niezależnie od tego dane powinny być przechowywane przez co najmniej 12 miesięcy. W preambule rozporządzenia należy wskazać że okres ten nie powoduje jednak harmonizacji minimalnej okresów określonych przez prawo krajowe w których można zakwestionować rachunek ale jest to zabezpieczenie praktyczne roszczeń konsumenckich.

V. Zgoda na przetwarzanie danych (art. 9)

Art. 9 reguluje kwestię definicji zgody (odsyłając do definicji z RODO) oraz zasady jej udzielania i wycofania. W art. 9 ust. 2 przewidziana została regulacja, która umożliwia udzielenie zgody za pomocą ustawień oprogramowania pozwalającego na dostęp do Internetu. Pojawia się wątpliwość jakiego konkretnie oprogramowania przepis ten dotyczy. Nie zalicza się tu, jak należy sądzić, np. wyszukiwarek. Wielu użytkowników nie korzysta z żadnego konkretnego oprogramowania a wyłącznie z ustawień systemowych urządzenia końcowego lub komputera. Ponadto warto wskazać na niespójność art. 9 z art. 10 ust. 2, który dotyczy „oprogramowania umożliwiającego łączność elektroniczną, w tym wyszukiwanie i przedstawianie informacji w internecie". Rząd RP proponuje ewentualne uspójnienie obydwu przepisów.

Warte rozważenia przez projektodawcę jest również wprowadzenie przepisu, zgodnie z którym zgoda byłaby udzielana nie tylko za pomocą ustawień oprogramowania, ale również ustawień urządzenia końcowego lub jego oprogramowania. Jednocześnie, domyślne ustawienia oprogramowania powinny zapewnić, że dopiero świadoma akcja użytkownika dokonującego zmian ustawień umożliwiałaby połączenie i w konsekwencji oznaczała zgodę na przetwarzanie danych.

Podkreślenia wymaga fakt, że zgoda powinna zostać wyrażona dobrowolnie i po uzyskaniu odpowiednich informacji. Należy bowiem wskazać, że zdarzają się przypadki stosowania tzw. cookie-wall, tj. uniemożliwienia użytkownikom, którzy nie zaakceptowali plików cookies korzystania ze strony internetowej. Tymczasem wiele plików cookies pozwala na śledzenie użytkownika również po opuszczeniu przez niego konkretnej witryny, umożliwiając firmom dostęp do informacji niezbędnych do profilowania i działań marketingowych. Powyższe praktyki naruszają zasadę swobodnie wyrażanej zgody, która została ujęta w RODO (motyw 42). Rekomendacje w tym zakresie są zbieżne z opinią Europejskiego Inspektora Ochrony Danych[4].

Wątpliwości Rządu RP budzi regulacja zawarta w art. 9 ust. 3, zgodnie z którym użytkownik powinien być informowany w odstępach 6 miesięcy o możliwości odwołania w każdym czasie zgody. Przepis ten wydaje się zbyt restrykcyjny. Jednocześnie w przypadku udzielenia wielu zgód, może prowadzić do zalewu użytkownika końcowego tego typu wiadomościami. Przy udzieleniu zgody klient jest informowany o tym, że udzielił zgody oraz w jaki sposób może ją cofnąć. RODO nawet w odniesieniu do przetwarzania danych sensytywnych nie przewiduje takiego obowiązku.

[4] Opinia 5/2016 „Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), 22 lipiec 2016, str. 16

VI. Domyślne ustawienia prywatności (art. 10)

Artykuł 10 zawiera regulację chroniącą przed śledzeniem aktywności użytkownika przez osoby trzecie. Stosownie do art. 10 ust. 1 dostępne na rynku oprogramowanie, które umożliwia komunikację elektroniczną powinno oferować opcje uniemożliwiające osobom trzecim przechowywanie informacji na urządzeniach użytkowników końcowych, lub przetwarzanie informacji już na tych urządzeniach przechowywanych. Przepis ten zatem ma uniemożliwić ingerowanie zdalnie w dane przechowywane w komunikatorach i innych podobnych aplikacjach. Ponadto, zgodnie z art. 10 ust. 2, przy instalacji oprogramowania, użytkownik będzie miał możliwość konfiguracji ustawień prywatności. Aby kontynuować instalację będzie wymagana zgoda na ustawienia prywatności. Istniejące oprogramowanie będzie musiało zostać zaktualizowane w celu zapewnienia spełnienia przez nie powyższych wymagań, do dnia 25 sierpnia 2018 r.

Rząd RP popiera powyższą regulację, jednocześnie proponuje rozszerzenie przepisu również na komponenty urządzeń końcowych, przy czym ustawienia domyślne – zarówno oprogramowania, jak i komponentów – powinny uniemożliwiać śledzenie przez podmioty trzecie. Zbieranie informacji 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. Rozwiązanie to byłoby zgodne z zasadą ochrony prywatności w opcji domyślnej, którą przewiduje RODO (privacy by default).

W odniesieniu do art. 10 należy wskazać, że przepis ten nie określa na jakich podmiotach ciążyć będą obowiązki w nim wskazane: na producencie, importerze, czy dystrybutorze, czy wszystkich tych podmiotach. Wydaje się, iż obowiązki te powinny być adresowane do producentów i importerów, natomiast nie do dystrybutorów, gdyż dystrybutor nie ma wpływu na to w jakie funkcje dane oprogramowanie zostanie wyposażone. Różnica w faktycznym wpływie producenta, importera oraz dystrybutora na to jakie wymagania spełnia urządzenie znalazło odzwierciedlenie w obowiązkach tych podmiotów określonych w ustawie z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Obowiązki dystrybutora różnią się od obowiązków producenta i importera - dystrybutor ma obowiązek działać z należytą starannością przy udostępnianiu wyrobu na rynku, sprawdzić, przed udostępnieniem wyrobu na rynku, czy producent i importer spełnili określone obowiązki, sprawdzić, czy na wyrób naniesiono oznakowanie CE, nie udostępniać na rynku wyrobu, co do którego istnieją uzasadnione wątpliwości w zakresie spełniania wymagań.

Niezależnie od powyższego należy wskazać, że oprogramowanie najczęściej wprowadzane jest łącznie z urządzeniem stanowiąc jego nieodłączny element. Z tego względu Rząd RP uznaje za zasadne rozważenie przez projektodawcę uregulowania kwestii zawartych w art. 10 projektowanego rozporządzenia w dyrektywie 20014/53/UE w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE. Dyrektywa ta wskazuje bowiem wymagania, jakie muszą spełniać urządzenia radiowe oraz obowiązki podmiotów gospodarczych. Wymagania nie powinny być natomiast materią przedmiotowego rozporządzenia. Pozostawienie regulacji w art. 10 stanowi kolejny argument przemawiający za tym, że regulacja powinna przyjąć formę dyrektywy a nie rozporządzenia. Producent, importer czy dystrybutor będzie poszukiwał bowiem wymagań jakie ma spełnić urządzenie i związane z nim oprogramowanie nie w rozporządzeniu, a raczej w aktach określających te wymagania i obowiązki podmiotów gospodarczych, tj. w ustawie z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne oraz w ustawie o systemach oceny zgodności i nadzoru rynku. Przyjęcie

formy dyrektywy umożliwiłoby implementację art. 10 właśnie do polskiej ustawy - Prawo telekomunikacyjne określającej wymagania, jakie urządzenia radiowe powinny spełnić.

VII. Wyświetlanie i ograniczenie identyfikacji rozmów przychodzących i wychodzących

Art. 12 ust. 1 nakłada wskazane w nim obowiązki wyłącznie na dostawców publicznie dostępnych usług łączności interpersonalnej wykorzystujących numery, nie obejmując tymi obowiązkami dostawców publicznie dostępnych usług łączności interpersonalnej niewykorzystujących numerów. Biorąc pod uwagę fakt, że projektowany Kodeks Łączności Elektronicznej przewiduje, że obie kategorie usług mają charakter konkurencyjny / substytucyjny wobec siebie, należy uznać, że różnicowanie obu usług w zakresie obowiązków wskazanych w art. 12 projektu rozporządzenia nie jest zasadne. W opinii Rządu RP zasadnym jest zatem nałożenie ww. obowiązków generalnie na dostawców usług łączności elektronicznej.

VIII. Blokowanie połączeń przychodzących

W art. 16 ust. 3 projektu rozporządzenia wprowadza się, w odniesieniu do połączeń marketingowych, obowiązek informowania odbiorcy o tym, że jest to połączenie marketingowe poprzez prezentowanie specjalnego kodu lub prefiksu wskazującego na marketingowy charakter połączenia. Należy ocenić tę propozycję kierunkowo pozytywnie, natomiast zaproponowane rozwiązanie wydaje się zbyt mało ambitne. Jednocześnie warto wyjść naprzeciw potrzebom użytkowników końcowych i umożliwić im skuteczną blokadę możliwości realizowania tego typu połączeń na takich samych zasadach, o jakich mowa w art. 14 w odniesieniu do numerów telefonów poprzez dodanie do przepisu art. 14 lit. a wyrazów: "or with specific codes/prefixes".

Rząd RP zwraca również uwagę na to, że art. 14 nakłada wskazane w nim obowiązki na dostawców publicznie dostępnych usług łączności interpersonalnej wykorzystujących numery, nie obejmując tymi obowiązkami dostawców publicznie dostępnych usług łączności interpersonalnej niewykorzystujących numerów, co jak wskazano w analogicznej sytuacji w pkt VII powyżej, również nie znajduje uzasadnienia. Ponadto, należy wskazać, że art. 14 może budzić wątpliwości interpretacyjne, gdyż wynika z niego, że dostawcy poza obowiązkami blokowania połączeń wskazanymi w art. 14 lit. a i b są zobowiązani wdrożyć bliżej nieokreślone najnowocześniejsze środki, aby ograniczyć otrzymywanie przez użytkowników końcowych niepożądanych połączeń. Przepis zatem w opinii Rządu RP powinien zostać przeredagowany w szczególności z uwagi na formę projektowanej regulacji i jej obowiązywaniem wprost.

IX. Zgoda na marketing (art. 16)

Projekt rozporządzenia przewiduje bardziej restrykcyjne, w porównaniu do obecnie obowiązujących, zasady dotyczące e-marketingu, rozszerza zasady wyrażenia zgody na marketing bezpośredni, na marketing z wykorzystaniem wszystkich usług łączności elektronicznej (np. zautomatyzowanych połączeń telefonicznych, wiadomości wysyłanych za pośrednictwem sieci społecznościowych, SMS, MMS, Bluetooth czy poczty elektronicznej) bez wskazywania/rozróżniania poszczególnych środków komunikacji, co generowało wątpliwości interpretacyjne (np. w odniesieniu do kwestii SMS). Bezpośrednie działania e-marketingowe wobec osób fizycznych i prawnych wymagać będą ich zgody (opt-in), z wyjątkiem sytuacji wykorzystania do celów marketingowych poczty elektronicznej użytkownika, której adres został przez użytkownika podany w związku ze sprzedażą produktów/usług (marketing ma tu dotyczyć własnych podobnych produktów/usług), a klienci posiadają możliwość odstąpienia

od otrzymywania tych wiadomości. Umożliwia się wprowadzenie przez państwa członkowskie możliwości wykonywania połączeń głosowych („voice-to-voice" live call) w ramach marketingu bezpośredniego do osób fizycznych, które nie wyraziły sprzeciwu (model opt-out).

W pierwszej kolejności należy wskazać na konieczność wyjaśnienia relacji art. 16 projektu rozporządzenia, który co do zasady ustanawia model opt-in, do art. 6 ust. 1 (zgoda) oraz art. 21 RODO, w którym jest mowa o prawie do sprzeciwu (model opt-out). Należy zaznaczyć, również, że w opinii Rządu RP stosowanie jednocześnie różnych modeli, tj. modelu opt-in i opt-out, nie przyniesie w praktyce oczekiwanych efektów, czego dowodem jest praktyka oparta na obecnych regulacjach zawartych w art. 13 dyrektywy 2002/58/WE. W tym kontekście Rząd RP uważa propozycje Komisji za zbyt mało ambitne, utrzymujące status quo i uniemożliwiające państwom członkowskim wprowadzenie bardziej skutecznych rozwiązań realizujących zasadniczy cel projektowanej regulacji – ochronę prywatności przed nieuprawnioną ingerencją. W tym zakresie, zdaniem Rządu RP, niezbędne jest wypracowanie rozwiązania, które skutecznie realizować będzie cel omawianego rozporządzenia – ochrone prywatności użytkowników usług łączności elektronicznej, w taki sposób który nie naruszy ochrony innych dóbr prawnych mających pierwszeństwo przed prawem do prywatności. Rząd RP w dalszych pracach będzie miał zatem na względzie również uzasadniony interes konsumentów i konieczność osiągnięcia tego celu.

W przypadku pozostawienia modelu zaproponowanego w projektowanym rozporządzeniu Rząd RP wskazuje na poniższe wątpliwości. Należy wskazać w szczególności na wątpliwości interpretacyjne co do ust. 4 przepisu w relacji do ust. 1. Ustęp 1 stanowi bowiem, że wymagana jest zgoda na marketing bezpośredni. Natomiast ust. 4 stanowi, iż mogą zostać ustanowione przepisy krajowe pozwalające na połączenia głosowe w odniesieniu do odbiorców, którzy nie sprzeciwili się otrzymaniu takiej formy marketingu bezpośredniego. Pojawia się zatem pytanie, czy nie należałoby interpretować tak sformułowanego przepisu jako możliwości uzyskania zgody na początku rozmowy (czyli sprzeciw jako remedium na telefony mające na celu uzyskanie zgody) albo też, że sprzeciw neutralizowałby wszelkie uprzednio udzielone (nieświadome) zgody. Wątpliwości Rządu RP budzi to, czy celowa jest rezygnacja w art. 16 ust. 1 z pojęcia „uprzedniej" (ang. „prior") zgody w zaproponowanej oficjalnej wersji rozporządzenia.

W odniesieniu do ochrony osób prawnych art. 16 ust. 5 odsyła do ochrony zapewnionej przez przepisy prawa krajowego. W pierwszej kolejności należy wskazać, że regulacja ta powinna odnosić się nie tylko do osób prawnych ale też innych osób, nie będących osobami fizycznymi (tak ja ma to miejsce w art. 13 ust. 5 dyrektywy 2002/58/WE). W opinii Rządu RP warte rozważenia jest zastosowanie innego mechanizmu dla komunikacji marketingowej, bowiem wymogi dotyczące zgody (dobrowolność, świadomość) w przypadku osób prawnych są trudne do spełnienia. Precyzyjnego rozstrzygnięcia wymagałoby określenie podmiotu, który w przypadku klientów biznesowych wyrażałby zgodę: użytkownik urządzenia, czy abonent. Ponadto, w przypadku podmiotów innych niż osoby fizyczne trudno jest mówić o konieczności ochrony prywatności czy innych praw podstawowych, które ze swej natury przysługują osobom fizycznym. Dyrektywa 2002/58/WE w zakresie osób innych niż osoby fizyczne również odsyła do prawa krajowego, niemniej jednak w przypadku dyrektywy (która wskazuje jedynie cele, pozostawiając Państwom Członkowskim dobór konkretnych narzędzi) takie rozwiązanie może być uzasadnione, o tyle takie odesłanie do prawa krajowego nie powinno mieć miejsca w przypadku rozporządzenia, które w założeniu ma w sposób pełny i wyczerpujący regulować wybrane zagadnienie, aby zapewnić spójność regulacji prawnych w całej UE.

Wątpliwości może również budzić art. 16 ust. 4, który to przepis umożliwia wprowadzenie przez państwa członkowskie połączeń głosowych do osób fizycznych w ramach marketingu bezpośredniego w modelu opt-out (a zatem możliwości wykonywania połączeń w celach marketingowych do osób fizycznych, które nie wyraziły sprzeciwu). Biorąc pod uwagę, iż analizowany projekt ma być rozporządzeniem (a nie dyrektywą), powinien jednoznacznie przesądzać tę kwestię, zamiast pozostawiać taką możliwość Państwom Członkowskim. Należy wskazać również, że w obecnym brzmieniu art. 16 ust. 4 pozwala na stosowanie modelu opt-out w odniesieniu do osób fizycznych, pomijając osoby inne niż osoby fizyczne. A skoro uznano model opt-out za dopuszczalny w przypadku osób fizycznych, to tym bardziej powinien być dopuszczalny w przypadku osób innych niż osoby fizyczne. Problemu nie rozwiązuje art. 16 ust. 5, gdyż na jego podstawie Państwa Członkowskie mogą przyjąć model opt-in dla osób innych niż osoby fizyczne, co może doprowadzić do sytuacji, w których w jednym kraju połącznia typu „voice-to-voice" do osób fizycznych nie będą wymagały uprzedniej zgody (art. 16 ust. 4), natomiast w te same połączenia kierowane do np. osób prawnych będą wymagały uprzedniej zgody (art. 16 ust. 5).

Należy również wskazać, co zostało już wspomniane w niniejszym stanowisku, iż projekt rozporządzenia powinien wyraźnie odnieść się do innych przepisów prawa unijnego regulujących kwestię przesyłania niezamówionych komunikatów handlowych, tj. art. 7 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) oraz art. 10 dyrektywy 2002/65/WE Parlamentu Europejskiego i Rady z dnia 23 września 2002 r. dotyczącej sprzedaży konsumentom usług finansowych na odległość oraz zmieniającej dyrektywę Rady 90/619/EWG oraz dyrektywy 97/7/WE i 98/27/WE.

X. Ochrona bezpieczeństwa i porządku publicznego

Ostatnie orzeczenia TSUE w sprawach C-203/15 i C-698/15, Tele2/Watson zaktualizowały potrzebę uregulowania kwestii związanych z przechowywaniem danych elektronicznych, w tym danych pochodzących z komunikacji elektronicznej, oraz z zasadami i trybem ich udostępniania organom ścigania i wymiaru sprawiedliwości. Mając na względzie dotychczasową linię orzeczniczą TSUE istnieje poważne ryzyko, że w przypadku wejścia w życie rozporządzenia w projektowanym kształcie, przy jednoczesnym braku uregulowania zagadnienia retencji danych na szczeblu europejskim, TSUE mógłby uznawać krajowe przepisy dopuszczające retencję danych, za sprzeczne z prawem europejskim. Nie kwestionując niezaprzeczalnej wartości jaką jest ochrona prywatności, nie można nie zauważyć, że proponowane rozwiązanie negatywnie wpłynie na możliwość zapewnienia bezpieczeństwa obywatelom, pozbawiając uprawnione podmioty ważnego narzędzia umożliwiającego skuteczne działania w tym zakresie. Pozyskiwanie danych telekomunikacyjnych oraz ich wykorzystanie przez uprawnione podmioty, w celu przeprowadzenia badania ex post, będącego podstawową formą prowadzenia analizy kryminalnej, służy bowiem głównie zwalczaniu przestępczości, ochronie życia i zdrowia ludzkiego, co nabiera szczególnego znaczenia w kontekście zagrożenia terrorystycznego.

Mając na względzie fakt, że retencja danych telekomunikacyjnych stanowi jedno z podstawowych narzędzi dla organów ścigania w celu utrzymania wysokiego poziomu bezpieczeństwa Rząd RP będzie popierał przyjęcie rozwiązań umożliwiających podejmowanie skutecznych działań na rzecz ochrony bezpieczeństwa i porządku publicznego, w tym na rzecz ratowania zdrowia lub życia ludzkiego oraz wsparcia działań poszukiwawczych

i ratowniczych. Wśród potencjalnych rozwiązań wskazać należy m.in. na potrzebę podjęcia na szczeblu unijnym prac nad aktem prawnym regulującym zagadnienie retencji danych telekomunikacyjnych.

Rząd RP będzie również dążył do zapewnienia możliwości uregulowania kwestii retencji danych w prawie krajowym. W tym zakresie, należy sformułować wyraźne stwierdzenie (np. w formie motywu w preambule rozporządzenia), że projektowane rozporządzenie nie stoi na przeszkodzie przyjęciu regulacji krajowych dotyczących retencji danych i ich wykorzystania w postępowaniu karnym.

Z powyższych względów Rząd RP, nie kwestionując wartości, jaką jest ochrona prywatności, będzie popierał przyjęcie rozwiązań umożliwiających podejmowanie skutecznych działań na rzecz ochrony bezpieczeństwa i porządku publicznego czy interesów konsumenckich Lista potencjalnych, celów które mają pierwszeństwo przed prawem do prywatności powinna być rozszerzona w stosunku do projektowanego brzmienia i uzupełniona o dobra uprzywilejowane w stosunku do prawa do prywatności Ponadto przepis rozporządzenia nie powinien posługiwać się określeniami relatywizującymi przepisy krajowe a w szczególności usunięte powinno być kryterium proporcjonalności. Zasada proporcjonalności nie budzi zastrzeżeń rządu polskiego ale wpisanie jej do przepisu określającego relacje z przepisami krajowymi rozporządzenia adresowanego do operatorów powoduje wątpliwość czy przepis taki nie stwarza podstaw do kwestionowania przez podmioty prywatne postanowień prawa publicznego, które powinno być dla nich wiążące.

XI. Informacje o wykrytym ryzyku w zakresie bezpieczeństwa sieci i usług

Projektowany art. 17 nakazuje dostawcy usług w przypadku szczególnego ryzyka, które może zagrozić bezpieczeństwu sieci i usług, informowanie użytkowników końcowych o takim zagrożeniu. A jeżeli ryzyko występuje poza zakresem środków zaradczych dostawcy – dostawca powinien informować o wszelkich środkach zaradczych, w tym wskazać prawdopodobne koszty, jakie się z tym wiążą.

W pierwszej kolejności należy wskazać, że przepis ten nie dotyczy kwestii ochrony danych, czy prywatności, odnosi się natomiast do szerszej materii bezpieczeństwa sieci i usług. Z tego względu w opinii Rządu RP kwestie uregulowane w art. 17 mogłyby zostać przeniesione do Europejskiego Kodeksu Łączności Elektronicznej, nad którym trwają obecnie prace. Należy wskazać, że Kodeks w art. 40 i 41 reguluje kwestię bezpieczeństwa sieci i usług.

Niezależnie od powyższego, w opinii Rządu RP, art. 17 może być nieostry dla adresatów. W szczególności wątpliwości może budzić to jaki podmiot będzie decydował o tym, czy wystąpiło szczególne ryzyko. Projektowane rozporządzenie nie zawiera żadnych szczegółowych informacji, które umożliwiłyby wykonanie dyspozycji przepisu, co zwłaszcza w przypadku ujęcia przedmiotowej regulacji w formie rozporządzenia budzi zastrzeżenia Rządu RP. Niezbędne jest w tym zakresie również wyjaśnienie relacji projektowanego art. 17 do dyrektywy Parlamentu i Rady UE nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

XII. Organ nadzorczy

Wątpliwości Rządu RP budzi kwestia nakładania się kompetencji organu właściwego do spraw ochrony danych i organu właściwego do spraw ochrony konkurencji w zakresie wykorzystania danych osobowych na potrzeby marketingu. Zachodzi zatem potrzeba przeanalizowania skutków takiej regulacji w kontekście możliwości nakładania kar przez oba organy za to samo naruszenie. Kwestie związane z marketingiem bezpośrednim stanowią bowiem dużą część postępowań prowadzonych przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów w zakresie ochrony zbiorowych interesów konsumentów. Pojawia się wątpliwość, czy w świetle projektowanych przepisów rozporządzenia, Prezes UOKiK miałby nadal możliwość prowadzenia postępowań na podstawie przepisów tego rozporządzenia dotyczących marketingu bezpośredniego, w zakresie posiadanych kompetencji, wynikających z ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów.

Warte rozważenia przez projektodawcę jest dodanie przepisu wskazującego, że projektowany art. 18 rozporządzenia pozostaje bez uszczerbku dla zadań powierzonych przez państwa członkowskie krajowym organom regulacyjnym lub innym właściwym organom zgodnie z prawem Unii (analogicznie jak w przepisie art. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego internetu oraz zmieniającego dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii). Przepis taki mógłby rozwiać ewentualne wątpliwości i spory kompetencyjne.

Jednocześnie jak zostało to już wskazane w niniejszym dokumencie, w ocenie Rządu RP wartym rozważenia jest również przyznanie państwom członkowskim pełnej swobody w określeniu aparatu instytucjonalnego, sprawującego nadzór nad realizacją przepisów dotyczących ochrony prywatności w sieciach łączności elektronicznej. Mimo stałego wzrostu kontaktów pomiędzy państwami członkowskimi, ich systemy ustrojowe cały czas cechują się znaczną odmiennością ustrojową względem siebie. Zróżnicowanie w zakresie sposobów wykonywania prawa unijnego, uzasadnione autonomią instytucjonalną, nie narusza unijnego wymogu efektywności, o ile spełnione są wszystkie wymogi danej regulacji. W ocenie Rządu RP państwa członkowskie powinny mieć więc pełną swobodę w określeniu jaki organ będzie właściwy do nadzoru nad przestrzeganiem przepisów przedmiotowego rozporządzenia. W ocenie Rządu RP warte rozważenia przez unijnego prawodawcę jest również pozostawienie nadzoru nad realizacją przepisów dotyczących ochrony prywatności w sieciach łączności elektronicznej krajowemu organowi regulacyjnemu na rynku usług łączności określonemu w Europejskim Kodeksie Łączności Elektronicznej ze względu na jego wyspecjalizowany charakter, a także duże obciążenie organu zajmującego się ochroną danych osobowych i znaczące zwiększenie liczby zadań wynikające z RODO.

XIII. Środki ochrony

Projekt rozporządzenia wskazuje, że użytkownicy mają prawo do środków ochrony określonych w art. 77, 78 i 79 RODO. Brak jest jednak odwołania również do art. 80 RODO, stanowiącym o możliwości umocowania organizacji lub zrzeszenia, które nie mają charakteru zarobkowego i które działają w obszarze ochrony danych do reprezentowania użytkowników. Wyłączenie stosowania art. 80 ust. 1 RODO budzi wątpliwości odnośnie spójności projektowanego rozporządzenia z RODO.

XIV. Pozostałe kwestie

Zastrzeżenia Rządu RP budzi delegowanie zbyt dużej ilości kwestii do doregulowanie przez Komisję Europejską w aktach delegowanych, co uniemożliwia dokonanie pełnej oceny skutków regulacji i prowadzi do braku pewności prawnej.

W zakresie uwag o charakterze redakcyjnym należy wskazać, że art. 23 projektu, określający ogólne warunki dotyczące nakładania kar administracyjnych, wskazuje w ust. 1, że rozdział VII rozporządzenia 2016/679/EU, który dotyczy współpracy i spójności ma zastosowanie do naruszeń przepisów projektowanego rozporządzenia. Tymczasem to Rozdział VIII a nie VII dotyczy środków ochrony prawnej, odpowiedzialności i sankcji. Jest to zatem zapewne błąd redakcyjny.

Ocena skutków projektowanego rozporządzenia

Projektowany akt ma formę rozporządzenia a zatem jest bezpośrednio skutecznym aktem prawa unijnego i nie wymaga wdrożenia. Konieczne może okazać się jednak wprowadzenie zmian w prawie krajowym dostosowujących przepisy do rozporządzenia, co biorąc pod uwagę wskazywany przez projektodawcę termin wejścia w życie przedmiotowych przepisów, przemawia za sprzeciwieniem się takiej ścieżce procedowania dokumentu.

Należy również wskazać, że przepisy rozporządzenia w kilku przypadkach przewidują możliwość (art. 11 ust. 1 czy art. 16 ust. 4) lub zobowiązują (art. 13 ust. 2) państwo członkowskie do ustanowienia szczegółowych uregulowań w odniesieniu do przepisów rozporządzenia.

Projektowane rozporządzenie będzie miało wpływ na użytkowników końcowych, przedsiębiorców, producentów i importerów, dystrybutorów oprogramowania. Oczekiwane są pozytywne skutki społeczne przejawiające się w szczególności w zapewnieniu bardziej efektywnej ochrony prywatności i danych w komunikacji elektronicznej.

Komisja Europejska wskazuje, że głównymi korzyściami płynącymi z projektowanej regulacji jest: lepsza ochrona poufności komunikacji elektronicznej poprzez rozszerzenie zakresu stosowania przedmiotowego instrumentu prawnego w celu uwzględnienia nowych, funkcjonalnie równoważnych usług łączności elektronicznej. Ponadto rozporządzenie wzmacnia kontrolę użytkowników końcowych przez doprecyzowanie, że zgoda może być wyrażona poprzez stosowne ustawienia techniczne; wzmocnienie ochrony przed niezamówionymi komunikatami, wraz z wprowadzeniem obowiązku zapewnienia identyfikacji rozmów przychodzących lub obowiązkowego prefiksu dla połączeń marketingowych i lepsze możliwości blokowania połączeń z niepożądanych numerów; uproszczenie i doprecyzowanie otoczenia regulacyjnego poprzez ograniczenie pola manewru państw członkowskich, uchylenie przestarzałych przepisów i rozszerzenie wyjątków od zasad wyrażenia zgody. Regulacją objęto nowe kategorie usług w porównaniu do obecnie obowiązującej dyrektywy 2002/58/UE, m.in. usługi OTT przez co podmioty świadczące te usługi poniosą dodatkowe koszty przestrzegania przepisów.

Komisja Europejska zauważyła, iż część regulacji zawartych w dyrektywie 2002/58/WE stanowiła zbytnie utrudnienie dla przedsiębiorców, jak i konsumentów. Przykładem takich przepisów były regulacje dotyczące zgody w kontekście ochrony poufności odnośnie urządzeń końcowych. Nie sprawdziło się proszenie użytkowników końcowych o akceptację tzw. "tracking cookies" bez zrozumienia przez tych użytkowników na czym te pliki polegają. Zdarzały się również przypadki stosowania plików cookies bez zgody użytkowników.

Komisja uznała zatem, że efektywniejszym rozwiązaniem będzie centralizacja zgody w oprogramowaniu, takim jak np. przeglądarki internetowe i zapewnienie tam użytkownikom możliwości wyboru ustawień prywatności, a zatem prawo do rozporządzania własnymi danymi (decydowania kiedy i komu zostaną one przekazane). Rozszerzono również wyjątki od zasad stosowania plików cookies, co, w opinii Komisji Europejskiej, umożliwi przedsiębiorcom w znacznej części niestosowanie banerów informacyjnych, powiadomień o plikach cookies oraz zapewni oszczędność kosztów.

Ze zewnętrznej analizy wykonanej na zlecenie Komisji Europejski wynika, iż ogólne oszczędności pod względem kosztów przestrzegania przepisów w porównaniu do obecnych ukształtują się na poziomie 70%[5].

Należy wskazać, że precyzyjne określenie skutków i ich kwantyfikacja nie są na tym etapie możliwe, w szczególności w kontekście pozostawienia wielu kwestii do uregulowania przez Komisję Europejską w aktach delegowanych. Z tego powodu zawarte w projekcie rozwiązania konsekwentnie w trakcie prac wymagać będą wyjaśnienia, w szczególności w zakresie ich potencjalnego wpływu na budżety państw członkowskich.

Wpływ na finanse publiczne ma m.in. zakres obowiązków dla organów nadzorczych, w tym również wskazanie, który z organów będzie odpowiedzialny za monitorowanie stosowania

[5] Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector (SMART 2016/0080), Deloitte 2016

rozporządzenia. Pozytywny wpływ na budżet państwa będą stanowiły wpływy z kar nakładanych przez organ nadzorczy.

Analizowana będzie również na dalszym etapie prac nad przedmiotowym dokumentem możliwość oceny jego skutków finansowych dla jednostek sektora finansów publicznych, w tym odnośnie potencjalnych zmian zakresu obowiązków organu odpowiedzialnego za monitorowanie stosowania projektowanego rozporządzenia. Takie szacunki zostaną dokonane, o ile pozwoli na to kształt wynegocjowanych zapisów.

Wyniki konsultacji społecznych projektu rozporządzenia

Polska Izba Informatyki Telekomunikacji (PIIT)

W opinii PIIT duże zaniepokojenie budzi pojawienie się projektu nowego rozporządzenia odnoszącego się m.in. do ochrony danych osobowych w sytuacji, gdy nie zostało jeszcze wdrożone Rozporządzenie 2016/679 UE (RODO). PIIT podkreśla, że już samo wdrożenie RODO będzie dla przedsiębiorców telekomunikacyjnych dużym wyzwaniem pod względem prawnym, organizacyjnym i finansowym, zwłaszcza w obliczu wysokich kar za niedopełnienie obowiązków. Z tego względu propozycja wprowadzenia kolejnej regulacji, która jest miejscami niespójna z RODO i wprowadza większe restrykcje i obowiązki dla przedsiębiorców budzi sprzeciw Izby.

PIIT wskazał ponadto, iż kwestie ochrony prywatności użytkowników i poufności komunikacji zostały już ujęte w Dyrektywie 2013/40/UE PE i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW. Należy określić relację projektu do dyrektyw konsumenckich i dyrektywy o handlu elektronicznym. Ponadto, PIIT wskazał, że mechanizmy samoregulacji lub współregulacji mogłyby bardziej efektywne godzić interes ochrony prywatności użytkowników z interesami przedsiębiorców działających w różnych modelach biznesowych, w tym przy udziale stron trzecich.

Zaproponowane w projekcie przepisy, w opinii Izby, stworzą zagrożenie dla funkcjonowania powszechnie przyjętych i dominujących w Internecie modeli biznesowych, w których użytkownik nie musi płacić za dostęp do treści/usług on-line. PIIT wskazuje, że bezpłatny dostęp do treści/usług będzie niemożliwy, jeżeli zniknie finansowanie z reklam. Modele reklamowe dostępu do treści oparte są w głównej mierze na wykorzystaniu sprofilowanych reklam, dopasowanych od preferencji użytkowników i uwzględniają stosowanie tzw. „*third party cookies*". Przepisy zawarte w projekcie rozporządzenia drastycznie ograniczą takie praktyki oraz bardzo utrudnią m.in. stosowanie plików *cookies* do rejestracji ilości odsłon treści chronionych prawami autorskimi/licencjami na potrzeby rozliczeń z OZZ/licencjodawcami, czy też prowadzenie niezależnych badań oglądalności będących gwarantem funkcjonowania rynku reklamy i usług on-line.

PIIT pozytywnie ocenia art. 3 „*Territorial scope*". Izba podkreśla, iż przedstawiona regulacja będzie miała negatywny wpływ na przetwarzania metadanych na potrzeby statystyczne/analityczne, co w praktyce uniemożliwi rozwój narzędzi Big Data w Europie oraz wielu projektów związanych z tzw. Smart Cities lub ITS. Izba wskazała również na potrzebę wyraźniejszego wyjaśnienia relacji pomiędzy projektowanym rozporządzeniem a RODO.

Izba krytycznie odniosła się do uniemożliwienia przetwarzania metadanych na potrzeby wykonania usług dodatkowych, ograniczenia wyjątków, w których stosowanie „cookies" nie wymaga zgody – do „cookies" służących do mierzenia ruchu na stronie/w serwisie i tylko do

przypadków, w których pomiar jest dokonywany przez dostawcę usługi elektronicznej, z której korzysta użytkownik. Negatywnie oceniono zobowiązanie operatorów do informowania klienta co poł roku o możliwości cofnięcia zgody, nałożenie obowiązków związanych z wyświetlaniem identyfikacji rozmów przychodzących i wychodzących jedynie na *publicly available number-based interpersonal communications services providers*, nie obejmując tymi obowiązkami *publicly available number-independent interpersonal communications services providers (podobnie w przypadku przepisów dotyczących ochrony przez spamem)*. Za kontrowersyjną PIIT uznał propozycję wprowadzenia nowego obowiązku prawnego związanego z gromadzeniem informacji emitowanych przez urządzenia końcowe oraz kwestię wdrażania obowiązku polegającego na zapewnienie użytkownikom końcowym możliwości blokowania niechcianych połączeń głosowych. Izba zgłosiła zastrzeżenia do odesłania do uregulowania w prawie krajowym kwestii ochrony osób innych niż osoby fizyczne przed marketingiem bezpośrednim, a także kwestii umożliwienia „voice-to-voice" live call w modelu opt-out.

Fundacja Panoptykon

W opinii Fundacji projekt rozporządzenia wprowadza wiele zmian zmierzających w dobrym kierunku. Fundacja wskazała, że rozróżnienie metadanych oraz danych dotyczących treści nie powinno przekładać się na odmienny standard ich ochrony, gdyż obecnie nie zawsze jest możliwe precyzyjne rozróżnienie tych danych. Podkreślono konieczność zachowania spójności z definicjami zawartymi w projektowanym Kodeksie na dalszym etapie prac nad obydwoma aktami lub wprowadzenie odrębnych definicji w projekcie.

Fundacja wskazała również, że różnice w zaproponowanych podstawach przetwarzania poszczególnych rodzajów danych mogą prowadzić do wątpliwości interpretacyjnych. Za kontrowersyjne Fundacja uznała wymóg uzyskania zgody na przetwarzanie danych w związku z dostarczaniem usług. Panoptykon proponował, aby projekt odwoływał się do zasad minimalizacji danych, proporcjonalności, definicji anonimizacji zawartej w RODO. Wskazano również, że co do zasady każda możliwość zapisywania danych na urządzeniach końcowych użytkowników końcowych powinna być uzależniona od ich świadomej zgody, a wyjątki od tej zasady powinny dotyczyć tylko sytuacji, w których istnieje znikome zagrożenie dla prywatności lub gdy pojawia się dodatkowa korzyść. Gromadzenie danych emitowanych przez urządzenia końcowe powinno podlegać tym samym ograniczeniom, co zapisywanie danych na takim urządzeniu i co do zasady wymagać zgody użytkownika. Projekt rozporządzenia powinien wyraźnie zakazać praktyk tzw. cookie wall, polegających na tym, że użytkownicy, którzy nie zaakceptowali plików cookies nie są w stanie korzystać ze strony internetowej.

Fundacja z aprobatą przyjęła zawarty w art. 10 obowiązek oferowania w oprogramowaniu opcji ochrony użytkownika przed śledzeniem aktywności użytkownika przez podmioty trzecie. Zaproponowała rozszerzenie tego przepisu na komponenty urządzeń końcowych oraz wskazała, że ustawienia – zarówno oprogramowania, jak i komponentów – powinny uniemożliwiać śledzenie przez podmioty trzecie w opcji domyślnej. Fundacja w odniesieniu do środków ochrony, wskazanych w art. 21, zaproponowała umożliwienie stosowania oprócz art. 77, 78, 79 RODO, również art. 80 RODO, który dopuszcza możliwość reprezentowania użytkowników przez organizacje lub zrzeszenia, które nie mają charakteru zarobkowego i które działają w obszarze ochrony danych. Ponadto podkreślono, że użytkownicy powinni mieć prawo do szyfrowanej komunikacji.

Digital Economy Lab UW

Z aprobatą przyjęto propozycję uregulowania przedmiotowych kwestii w formie rozporządzenia, do objęcia regulacja dostawców usług OTT, komunikatów przesyłanych maschine-to-maschine, możliwości zróżnicowania ustawień prywatności (motyw 28). Za wart rozważenia uznano wariant art. 16 ust. 3, w którym przy połączeniach wykonywanych w celu marketingu bezpośredniego stosowany byłby jednocześnie wymóg dotyczący podawania danych kontaktowych jak i stosowania specjalnego prefiksu. W opinii DELab UW na uwzględnienie zasługują trudności techniczne związane z zagadnieniem anonimizacji metadanych. Ponadto ściślejszej regulacji domagają się, w świetle linii orzeczniczej TSUE odnośnie do tego zagadnienia, kwestie retencji danych w projektowanym rozporządzeniu.

Fundacja Wiedza To Bezpieczeństwo

W opinii Fundacji niezbędnym jest, aby przedmiotowy dokument przyjął formę rozporządzenia. Fundacja zgłosiła wątpliwość odnośnie do uregulowanej w art. 3 kwestii przedstawiciela dostawcy usług w Unii. Doprecyzowania wymaga kwestia, gdy użytkownicy końcowi znajdują się w kilku państwach członkowskich – czy wystarczy powołanie jednego przedstawiciela czy powinien być odrębny w każdym państwie? Zdaniem Fundacji również ustęp 5 tego artykułu jest zbyt ogólny i wymaga doprecyzowania. Ponadto kwestia marketingu powinna zostać uregulowana w sposób bardziej precyzyjny, w szczególności w odniesieniu do uprzedniej zgody. Rozstrzygnięcia wymaga również to czy zgodę należy uzyskać na każde z telekomunikacyjnych urządzeń końcowych odrębnie. Fundacja wskazała również, że w odniesieniu do kwestii śledzenia użytkowników urządzeń końcowych niedopuszczalne jest zbieranie danych ponad te, które są absolutnie niezbędne do wykonania usługi.

IV. Informacja w sprawie zgodności projektu aktu z zasadą pomocniczości

Komisja Europejska wskazuje, że poszanowanie prawa do prywatności w odniesieniu do komunikacji jest jednym z praw podstawowych zawartych w art. 7 Karty Praw Podstawowych Unii Europejskiej. Treść komunikacji elektronicznej, jak i metadane pochodzące z komunikacji elektronicznej mogą ujawnić wiele wrażliwych, osobistych informacji na temat użytkowników końcowych - uczestników komunikacji. Większość państw członkowskich również traktuje ochronę komunikacji jako konstytucyjne prawo. Zapewnienie ekwiwalentnego poziomu ochrony osób fizycznych i prawnych oraz swobody przepływu danych w ramach Unii nie są jednak możliwe do osiągnięcia w wystarczającym stopniu poprzez krajowe regulacje państw członkowskich. Realizacja powyższych celów będzie efektywniejsza w przypadku uregulowania tych kwestii w sposób jednolity na poziomie unijnym. Ponadto, aby zachować spójność z RODO konieczne jest przyjęcie nowego aktu będącego wynikiem przeglądu dyrektywy 2002/58/WE zapewniającego zbliżenie do siebie obu instrumentów.

V. Przedstawiciel Rządu upoważniony do prezentowania stanowiska

Marek Zagórski – Sekretarz Stanu w Ministerstwie Cyfryzacji