Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 11.01.2018 r.
KIGEiT/132/01/2018

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dot. prac nad rozporządzeniem w sprawie prywatności i łączności elektronicznej

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***"), odnosząc się do trwających prac nad rozporządzeniem w sprawie prywatności i łączności elektronicznej (dalej „***Rozporządzenie ePrivacy***") Izba przedstawia stanowisko.

Na samym wstępie pragniemy wyrazić wątpliwości co do tego, czy w świetle 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 (ogólne rozporządzenie o ochronie danych) (dalej „***RODO***") istnieje potrzeba wprowadzenia dalszych, szczególnych obowiązków dotyczących sektora łączności elektronicznej. W ocenie Izby definicja danych osobowych wynikającą z RODO jest na tyle pojemna, że pozwala ona na postawienie tezy, zgodnie z którą dalej idące obowiązki dotyczące sektora łączności elektronicznej są zbędne. Jednocześnie warto rozważyć, czy dla sektora łączności elektronicznej nie należy wprowadzić jedynie rozwiązań, które łagodzą wymagania RODO, a to z uwagi na specyfikę działalności w tym sektorze.

Utrzymywanie różnych rozwiązań prawnych dotyczących często tego samego stanu faktycznego nie zapewnia wymaganej pewności prawnej, potrzebnej dla prowadzenia działalności gospodarczej. Przy założeniu wejścia w życie projektowanego Rozporządzenia ePrivacy przedsiębiorcy działający na rynku telekomunikacyjnym mogą być zmuszeni do analizowania przepisów krajowych, przepisów RODO oraz postanowień ww. projektowanego aktu. W tym kontekście niezbędne jest w ocenie Izby wprowadzenie czytelnych rozwiązań kolizyjnych, wskazujących na to, że pierwszeństwo mają regulacje sektorowe, ze szczególnym uwzględnieniem przepisów dotyczących kar pieniężnych, tak aby uniknąć sytuacji, w której ten sam stan faktyczny mógłby prowadzić do nałożenia kar pieniężnych na podstawie trzech różnych systemów prawnych. W naszej ocenie nie budzi wątpliwości, że taka sytuacja naruszałaby zakaz wielokrotnego karania za ten sam czyn i tego rodzaju sytuacje mogłyby zostać skorygowane na etapie odwołań od decyzji poszczególnych organów, jednakże sam fakt wydania choćby nieprawomocnej (nieostatecznej) decyzji o

ul. Stępińska 22/30, 00-739 Warszawa, tel.: +48 22 8510309, 8406522, fax: +48 22 8510300, e-mail: kigeit@kigeit.org.pl
http://www.kigeit.org.pl; NIP 526-00-29-121 Konto: BGŻ BNP Paribas O/Warszawa nr: 52160013740003005222791001

nałożeniu kary stanowić będzie istotną niedogodność związaną m.in. z koniecznością założenia rezerw finansowych czy też poniesienia nakładów na obsługę prawną związaną ze skorzystaniem z przewidzianych środków odwoławczych.

Zdając sobie również sprawę, iż przekazujemy komentarze do dokumentu roboczego, który będzie jeszcze podlegał zmianom, pragniemy zwrócić uwagę na konieczność określenia realnych i możliwych do spełnienia dat związanych z wejściem w życie Rozporządzenia ePrivacy. Jesteśmy także głęboko przekonani, iż wszelkie zmiany do obowiązującej obecnie dyrektywy 2002/58/WE powinny być rozważane co najmniej po rocznym okresie od obowiązywania nowych wymogów RODO, tak aby można było w efektywny i konstruktywny sposób czerpać z doświadczeń, problemów i wniosków zidentyfikowanych przez wszystkich interesariuszy, a w szczególności przedsiębiorców, regulatorów i użytkowników usług.

Izba podziela również stanowisko wyrażone w dokumencie „*Joint Industry Statement*", przekazywanym już w ramach wcześniej zgłaszanych uwag.

UWAGI SZCZEGÓŁOWE

Art. 1 i 2

Izba popiera zmiany wprowadzone w stosunku do poprzednich wersji ww. przepisów.

Art.3 ust.1 (a)

Izba popiera wprowadzenie pojęcia „*content in transmission*". Dla zachowania spójności, odpowiednia modyfikacja powinna być też wprowadzona w definicjach (art. 4) oraz w art. 6.

Art. 3 ust. 1 (cc)

Izba wnosi o usunięcie słów "*or presenting*", tak aby postanowienie brzmiało: "***the sending ~~or presenting~~ of direct marketing communications to end-users who are in the Union***". Na podstawie dotychczas proponowanej treści można byłoby uznać, że baner reklamowy wyskakujący na stronie www podpada pod te ograniczenia, co byłoby nadmiernym i nieuzasadnionym ograniczeniem reklamy i obowiązkiem nieproporcjonalnym do celów rozporządzenia.

Art. 4

Z ostrożności zwracamy uwagę na konieczność uwzględnienia w dalszych pracach kwestii zgodności definicji z pozostałymi aktami prawnymi pozostającymi w związku z Rozporządzeniem ePrivacy, w szczególności RODO.

Art. 4a ust. 3

W ocenie Izby obowiązek cyklicznego przypominania użytkownikom o możliwości cofnięcia zgody stanowi zbędne obciążenie dla dostawców usług oraz uciążliwość dla samych użytkowników. Zdecydowanie opowiadamy się za rezygnacją z tego obowiązku.

Art.4 ust.3 (b)

Izba postuluje zachowanie spójności ze znaczeniem pojęcia *electronic communciations content*, jakie przyjęto w art. 3 ust. 1 (a) i odpowiednie zmodyfikowanie definicji poprzez dodanie słów "*in transmission*": '*electronic communications content' means the content in transmission exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;...*"

Art.4 ust.3 (f)

Zgodnie z argumentacją dot. art. 3 ust. 1 (cc) postulujemy usunięcie słów "*or presented*": '*direct marketing communications' means any form of advertising, whether written or oral, sent ~~or presented~~ to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems...* "

Art. 5 ust. 1

Izba postuluje przywrócenie pierwotnego brzmienia tego postanowienia, którego istotą była ochrona tajemnicy komunikowania się, a nie zakaz przetwarzania danych. Zakaz wszelkiego przetwarzania danych jest niezgodny z założeniami RODO, jak również z art. 1 ust. 2 Rozporządzenia ePrivacy, który ustawia swobodę przepływu danych w ramach UE (a taki przepływ jest bez wątpienia przetwarzaniem danych, co z kolei na mocy obecnie proponowanego brzmienia art. 5 ust. 1 miałoby być zakazane). Ponadto, obecne brzmienie tego ustępu 1 uniemożliwiłoby w praktyce przetwarzanie danych na potrzeby usług M2M oraz IoT.

Art. 5 ust. 2

Izba stoi na stanowisku, że komunikacja M2M powinna być wyłączona z zakresu tej regulacji, jeżeli jednak nie jest to możliwe, wnosimy o modyfikację przepisu, proponując następującą treść:

1. *Electronic communications data shall be confidential. Listening, tapping, storing, monitoring, scanning, interception, surveillance or any other interference with electronic communications data, by persons other than the end-users, shall be prohibited, except when permitted by this Regulation.*
2. *Confidentiality of electronic communications shall apply to the transmission of machine-to-machine electronic communications content where carried out via an electronic communications service, on the grounds of art. 6 and 7 of this Regulation. Articles 6 and 7 of this Regulation shall not apply to the processing of electronic communications metadata generated by machine-to-machine electronic communications transmissions, which shall be permitted by providers of electronic communications networks and services if the processing is unlikely to result in a*

serious risk to the rights and freedoms of end-users, taking into account the nature, context, scope and purposes of the processing.

Art.6

Izba co do zasady pozytywnie ocenia kierunek wprowadzanych zmian w stosunku do poprzedniej wersji projektu, w szczególności zbliżenie proponowanych przepisów do RODO, dodanie możliwości przetwarzania przez osoby trzecie i w celach naukowych oraz statystycznych. Jednocześnie dostrzegamy potrzebę jeszcze szerszego podejścia do dopuszczalnych podstaw przetwarzania, tak aby do tego rozporządzenia miały zastosowanie te same przesłanki przetwarzania, które przyjęto w RODO, w szczególności art.6.4 oraz 6 ust.1 lit. (f), tym bardziej że metadane nie powinny być traktowanie bardziej restrykcyjnie niż np. dane wrażliwe według RODO.

Wskazujemy, że brak jest jakiegokolwiek uzasadnienia, aby ograniczać możliwość przetwarzania metadanych i treści, jeśli podstawą przetwarzania jest zgoda, tylko do przypadków, w których „*purpose or purposes concerned could not be fulfilled by processing information that is made anonymous*". Nie jest jasne jakiemu celowi takie ograniczenie ma służyć. Zwracamy uwagę, że RODO nie stawia takich wymogów w przypadkach, w których podstawą przetwarzania jest zgoda, co jest w pełni uzasadnione biorąc pod uwagę warunki, jakim musi odpowiadać zgoda.

W kontekście art. 6 ust. 2 lit. c zwracamy uwagę, że proponowana treść przepisu spowoduje poważne trudności praktyczne, gdyż wprowadza ryzyko i niepewność prawną w każdym przypadku przetwarzania takich danych, nawet jeśli dane są przetwarzane na podstawie prawidłowo wyrażonych zgód. Co więcej, nie będzie jasne jak należy traktować zgodę abonenta (wyrażoną świadomie i dobrowolnie) w sytuacji, gdy organ kontrolny uzna, że pomimo zgody przetwarzanie nie było legalne, gdyż w ocenie organu cel przetwarzania mógł być osiągnięty z wykorzystaniem danych anonimowych. Powyższe dotycz również art. 6 ust.3 lit. b.

Ponadto proponujemy wykreślenie warunku, o którym mowa w art.6 ust. 3 lit. a, dotyczącym niezbędności przetwarzania treści dla świadczenia usługi. Odwołując się do powyższej argumentacji stoimy na stanowisku, że za wystarczające należy uznać wyrażenie zgody przez użytkownika.

Art. 6 ust 3

Pierwsze zdanie: "***Without prejudice to paragraph 1,*** *Providers of the electronic communications* ***networks and*** *services may* ***shall be permitted to*** *process electronic communications content ...;*" jest niespójne z art. 3. ust. 1 (aa), w którym jest odniesienie do "*content in transmission*". Z tego względu powinno ono zostać uzupełnione o słowa "*in transmission*" na końcu zdania.

Art. 6 ust.3 (b)

W tym zakresie aktualne pozostają uwagi dotyczące art. 6 ust. 2 (c). Ponadto, w ocenie Izby przepis wskazujący, iż potrzebna jest zgoda "*wszystkich*" użytkowników końcowych dotkniętych / zainteresowanych usługą jest niejasny, nie wiadomo jakich realnych usług miałby dotyczyć.

Ponadto zwracamy uwagę na potrzebę uporządkowania i zapewnienia spójności postanowień odnoszących się do osób prawnych, także w relacji do RODO.

Art.7 ust.2

Generalnie stoimy na stanowisku, iż art. 7 jest nadmiarowy ze względu na fakt, iż lista dopuszczalnych podstaw przetwarzania jest zamknięta.

W ocenie Izby wątpliwości budzi celowość dodania odnoszącego się do metadanych postanowienia, zgodnie z którym „*Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679*".

Nie jest także jasne jakie wynikałyby z niego obowiązki dla dostawcy usług, np. gdyby to była konieczność zapewnienia przenoszalności metadanych, byłby to obowiązek nadmiarowy.

Podobnie uważamy także za niezasadne umieszczenie tego samego zapisu w art. 7 ust.1.

Art. 8

Jeśli chodzi o art. 8, to chcielibyśmy podkreślić, że w naszym przekonaniu, zakresy art. 6 oraz art. 8 powinny być ściśle rozdzielone od siebie. Art. 6 odnosi się do przetwarzania danych w powiązaniu z dostarczaniem usług komunikacji elektronicznej, podczas gdy art. 8 przewiduje zbieranie oraz przetwarzanie danych przez urządzenia. Dlatego nie powinien on, w naszym przekonaniu mieć zastosowania do standardowego dostarczania usług komunikacji elektronicznej. Obecne brzmienie wymaga zatem doprecyzowania w celu uniknięcia wątpliwości interpretacyjnych

Izba pozytywnie ocenia generalny kierunek wprowadzonych zmian. Postulujemy jednak poddanie kwestii przetwarzania danych gromadzonych w oparciu o technologie wykorzystujące cookies pod RODO. W odniesieniu do art. 8 ust.1 lit. e popieramy zmienione postanowienia w punktach (i) oraz (ii), natomiast postulujemy usunięcie fragmentu dotyczącego wyłączenia automatycznej instalacji aktualizacji lub usunięcie całego podpunktu.

Biorąc pod uwagę rosnącą skalę różnego rodzaju ataków o charakterze cyberprzestępczym, możliwość wyłączania przez użytkownika automatycznej instalacji koniecznych aktualizacji zabezpieczeń może spowodować, że użytkownik będzie narażony na ataki, które mogą skutkować zarówno narażeniem prywatności, jak i szkodami majątkowymi. Ponadto, danie użytkownikowi możliwości odłożenia w czasie aktualizacji, aczkolwiek wygodne dla użytkowników, może także prowadzić do niebezpiecznych dla użytkownika skutków. Doskonałym przykładem do czego może doprowadzić odłożenie w czasie lub zaniechanie aktualizacji bezpieczeństwa jest niedawny głośny przypadek ataku ransomware WANNACRY, który atakował komputery z systemem Windows, których użytkownicy nie zainstalowali wcześniej wydanych poprawek bezpieczeństwa (https://niebezpiecznik.pl/post/zamkniete-szpitale-i-zaklady-pracy-uderzenie-robaka-wannacry-i-olbrzymie-straty-na-calym-swiecie/).

Ponadto, za konieczne uważamy dodanie w art. 8 ust. 1 kolejnych podpunktów (aa) i (f) o następującym brzmieniu:

(aa) processing is necessary for the performance of a contract to which the end user is party or in order to take steps at the request of the end user prior to entering into a contract"

„(f) it is necessary for compliance with a legal obligation".

Artykuł ten powinien zostać uzupełniony o dodatkową przesłankę, pozwalającą na przetwarzanie danych jeśli jest to konieczne dla spełnienia wymogów narzuconych przez prawo. W szczególności taka podstawa jest konieczna w świetle wymogów stawianych przez

art. 10 Rozporządzenia ePrivacy, w tym wymogu, aby oprogramowanie zainstalowane przed datą wejścia w życie rozporządzenia zostało dostosowane do nowych wymogów (art. 10 ust. 3 Rozporządzenia ePrivacy). Bez tej podstawy prawnej przetwarzania konieczne będzie uzyskanie zgody użytkownika na aktualizację oprogramowania, również w tych przypadkach, gdzie aktualizacja jest wymagana przez przepisy prawa. To z kolei pozostaje w ścisłym związku z odpowiedzialnością i karami finansowymi za brak aktualizacji wymaganych prawem, gdzie przyczyną braku aktualizacji jest brak zgody użytkownika.

W art.8 ust.2 Izba postuluje wprowadzenie możliwości stosowania pseudonimizacji danych, a nie ograniczenie się tylko do pełnej anonimizacji i usuwania danych.

Art.10

W ocenie Izby optymalnym rozwiązaniem byłoby usunięcie całego artykułu, zgodnie z sugestią przedstawioną w dokumencie „Joint Industry Statement". Gdyby postulat ten nie został uwzględniony wnosimy o uwzględnienie poniższej propozycji:

"2a. The software referred to in paragraph 1 shall provide in a clear manner easy ways for end-users to change the privacy setting consented to under paragraph 2 at any time during the use."

Ponadto, pragniemy zwrócić uwagę, iż zgodnie z Rozporządzeniem ePrivacy, w sytuacji gdy usługodawca posiada zgodę użytkownika na realizację określonych celów z wykorzystaniem technologii opartych o cookies, będzie on mógł umieścić cookies na urządzeniu użytkownika. Tym samym, przeglądarka nie powinna co do zasady blokować usługodawcom możliwości umieszczania plików cookies. Z tego względu należy zapewnić, że funkcjonalność przeglądarki powinna być ograniczona do wysłania sygnału do usługodawców, którzy będą następnie weryfikować, czy posiadają zgodę (inne podstawy prawne) na wykorzystywanie technologii opartych o cookies.

Art. 12 ust. 4

Odnosząc się do komentowanego przepisu w kontekście obowiązków informacyjnych dostawców usług Izba stoi na stanowisku, że zamieszczenie na stronach internetowych dostawców usług żądanych informacji powinno być uznawane za podanie do publicznej wiadomości.

Art. 13

Izba pozytywnie ocenia kierunek zmian zaproponowanych w tym artykule w odniesieniu do usług ratunkowych.

Art. 14

Zgodnie z projektem zakłada się nałożenie na dostawców bliżej nieokreślonego, generalnego obowiązku „*to deploy state of the art measures to limit the reception of malicious or nuisance calls by end-users*", oprócz którego (… and shall also provide …) dostawcy muszą również zapewnić możliwość założenia blokad, o których mowa w tym artykule. Należy zwrócić uwagę, iż Rozporządzenie ePrivacy ma formę bezpośrednio stosowanego rozporządzenia, tym samym niedopuszczalne jest nakładanie obowiązków (zagrożonych groźbą kary) bez jednoczesnego sprecyzowania, co konkretnie jest przedmiotem takiego obowiązku. Jakie bowiem rozwiązania – inne niż wskazane w art. 14 w lit (a) – (c) (w wersji dokumentu z 5

grudnia 2017 brakuje wskazania liter (a) i (b), jest natomiast dodana litera (c), zakładamy że brakujące litery wynikają z pomyłki redakcyjnej) mają wdrożyć dostawcy usług, aby spełnić wymóg zapewnienia *"state of the art measures to limit the reception of malicious or nuisance calls by end-users"*? Izba proponuje następujące brzmienie tego postanowienia: *"Providers of publicly available number-based interpersonal communications services shall provide the called end-user with the following possibilities, free of charge: ....."*

Art.15 ust. 2

W ocenie Izby konieczność uzyskiwania dodatkowej zgody użytkownika na objęcie jego danych funkcjonalnością „szukaj" jest nadmiarowa. Jeżeli użytkownik wyraża zgodę na ujawnienie jego danych w spisie abonentów, zgoda ta powinna być równoznaczna ze zgodą na funkcję „szukaj", w przeciwnym razie przydatność spisów abonentów dla wszystkich użytkowników byłaby bardzo ograniczona. Z praktycznego punktu widzenia obecność w spisie abonentów danych, których nie można wyszukać, jest nielogiczna i nieprzydatna.

Art. 16

W ocenie Izby rozwiązanie, zgodnie z którym stosowanie marketingu bezpośredniego przy pomocy połączeń głosowych jest możliwe o ile odbiorca nie sprzeciwił się takiemu rozwiązaniu, powinno być zasadą obowiązującą jednolicie wszystkie Państwa Członkowskie. Kwestia marketingu jest na tyle istotna, że nie powinna być pozostawiana do ewentualnego odmiennego uregulowania na poziomie poszczególnych krajów. Jednocześnie w ocenie Izby samo oparcie takiego rodzaju marketingu na zasadzie opt-out jest rozwiązaniem słusznym.

Ponadto, Izba sprzeciwia się umożliwieniu Państwom Członkowskim nakładania na dostawców dodatkowego obowiązku w postaci konieczności stosowania specjalnego kodu/prefiksu identyfikującego bezpośrednie komunikaty marketingowe. Wdrożenie spójnego systemu kodów/prefiksów nie jest proste i budzi sprzeciw niektórych Państw Członkowskich, a zakres obowiązków wynikających z tej regulacji powinien być zharmonizowany w całej UE. Innymi słowy, obowiązek taki powinien dotyczyć wszystkich Państw Członkowskich albo żadnego. Proponowane rozwiązanie kłóci się z założeniem jednolitego rynku i może spowodować stworzenie różnych warunków dla prowadzenia takiej samej działalności. Dodatkowo:

W zakresie art. 16 ust. 1 i 2 wnosimy o usunięcie z tekstu słów zaznaczonych wykreśleniem: *"....for the purposes of [sending* ~~*or presenting*~~*] direct marketing communications to end-users...."; "...The right to object shall be given at the time of collection and each time a message* ***such direct marketing communication*** *is [sent* ~~***or presented***~~*]"* zgodnie z argumentacją przytoczoną w uwagach do art. 1 ust. 1 (cc) i art. 4 ust. 3 (f).

Art. 16 ust. 4

Ww. przepis powinien dotyczyć zarówno osób fizycznych, jak i prawnych. Obecnie dotyczy tylko osób fizycznych, a więc powstaje pytanie, czy można go zastosować do osób prawnych, a to właśnie osoby prawne wymagają mniejszej niż osoby fizyczne ochrony.

Art. 16 ust. 5 i 6

Zgodnie z argumentacją przytoczoną w uwadze do art. 1 ust. 1 (cc), art. 4 ust. 3 (f) oraz art. 16 ust. 1 i 2, wnosimy o usunięcie z tekstu słów zaznaczonych wykreśleniem: *„...**direct***

marketing *communications [sent* ~~***or presented***~~*] by means set forth under paragraph 1 are sufficiently protected."; "Any natural or legal person using electronic communications services to transmit [send* ***or present]*** *direct marketing communications shall inform..."*

Art. 23

Izba stoi na stanowisku, że podstawą do obliczenia nakładanych kar pieniężnych powinien być przychód związany z tą działalnością, której dotyczy naruszenie. W dobie oferowania przez przedsiębiorców telekomunikacyjnych również innych usług (finansowych, sprzedaży energii etc.) inne rozwiązanie naruszałoby zasadę proporcjonalności.

Ponadto, w ocenie Izby należy rozważyć zmniejszenie proponowanych maksymalnych pułapów nakładanych kar pieniężnych. Zwracamy uwagę na coraz mniejszą marżowość usług łączności elektronicznej, co oznacza, że takie wysokości kar mogą prowadzić do upadłości/likwidacji przedsiębiorstw.

Ostatnim elementem związanym z sankcjami za naruszenia Rozporządzenia ePrivacy jest konieczność uwzględnienia okresu przedawnienia dla możliwości nakładania kar umownych. Rozwijający się rynek oraz nie zawsze precyzyjnie sformułowane normy prawne wymagają wprowadzenia pewnych gwarancji dla przedsiębiorców aby uniknąć sytuacji, w której będą oni karani za naruszenia, które zostały już dawno wyeliminowane.

Prezes Zarządu

Stefan Kamiński