



Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 15.07.2019 r.

KIGEiT/2283/07/2019

Sz. P. Marek Zagórski
Minister
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dotyczy: 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 kolejnej wersji projektu rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (dalej „*Rozporządzenie E-privacy*” - dokument 1101/19, z dn. 17 lipca 2019 zaproponowany przez Prezydencję fińską na grupę TELE), Izba przedstawia następujące stanowisko.

Podtrzymując uwagi przekazane wcześniej podczas prac nad projektem rozporządzenia *E-privacy*, Izba pragnie odnieść się do ostatnio wprowadzonych zmian w dokumencie oraz przypomnieć i poszerzyć zgłaszane wcześniej uwagi do art.13 i 14.

- **Motyw 32 i art. 4**

Popieramy wprowadzone zmiany i wynikające z nich doprecyzowanie.

- **Art.13**

Postulujemy usunięcie **art. 13 ust. 3** z projektu rozporządzenia *E-privacy*, ewentualnie zwracamy się do Ministerstwa Cyfryzacji z prośbą o podjęcie próby wyjaśnienia na poziomie UE i przekazania informacji na temat intencji i istoty projektowanego przepisu, które stanowi:

“Notwithstanding Article 8(1), Regardless of whether the end-user has prevented access to the terminal equipment’s Global Navigation Satellite Systems (GNSS) capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such settings may not prevent access to GNSS such location data to determine and provide the caller calling end-user’s

location to emergency services an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.”

Zwracamy uwagę, że przepis odnosi się do będącego wciąż w budowie, koncepcyjnego systemu GNSS. Niemniej jednak ważniejsze jest, iż w świetle krajowych przepisów (Prawo telekomunikacyjne wraz z rozporządzeniami wykonawczymi i dokumentacją PLI CBD) lokalizacja abonenta usług mobilnych dzwoniącego na numer alarmowy jest ustalana i przekazywana do PLI CBD na podstawie danych z sieci operatora (w szczególności na podstawie danych lokalizacyjnych ze stacji bazowych - BTS), a nie na podstawie danych z systemów nawigacji satelitarnej, z której może korzystać urządzenie końcowe abonenta. Tym samym polski operator nie ma żadnego wpływu na to, czy telefon użytkownika jest wyposażony w GPS i czy użytkownik z GPS korzysta, operator nie ma również dostępu do informacji z GPS telefonu użytkownika. Na dzień dzisiejszy obowiązki, o których mowa w art. 13 ust. 3 projektu rozporządzenia, są realizowane w oparciu o dane z sieci operatora, w tym w szczególności BTS.

Biorąc powyższe pod uwagę, projektowany art. 13 ust. 3 wydaje się „przejrzysty” dla polskich dostawców mobilnych usług telekomunikacyjnych. Jednocześnie, w obawie przed ewentualnymi zmianami brzmienia tego przepisu, które w sposób niezrozumiały mogłyby prowadzić do uznania, że dostawcy usług telekomunikacyjnych muszą stosować systemy nawigacji satelitarnej do ustalania lokalizacji abonenta na potrzeby połączeń alarmowych, postulujemy usunięcie tego przepisu, a przynajmniej wyjaśnienie i potwierdzenie, że w przypadku realizacji ww. obowiązku w oparciu o dane z sieci ruchomej (np. BTS) dostawca usług telekomunikacyjnych wypełnia obowiązki wynikające z projektowanych przepisów. Zwracamy uwagę, że przy takiej niekorzystnej interpretacji art. 13 ust. 3 (tj. w przypadku uznania, że dostawcy usług telekomunikacyjnych muszą stosować systemy nawigacji satelitarnej do ustalania lokalizacji abonenta na potrzeby połączeń alarmowych) dostawcy usług telekomunikacyjnych stanęliby przed koniecznością wprowadzenia kosztownych, daleko idących zmian systemowych i sieciowych, które nie mają żadnego uzasadnienia biorąc pod uwagę sprawne funkcjonowanie systemu opartego na lokalizacji sieciowej. Co więcej, koszty takiej zmiany dotknęłyby również administracji publicznej, w szczególności Prezesa Urzędu Komunikacji Elektronicznej, gdyż najprawdopodobniej taka interpretacja art. 13 ust. 3 projektu rozporządzenia oznaczałaby konieczność przebudowania istniejącej platformy PLI CBD, zarządzanej przez Prezesa UKE.

Jeśli usunięcie art. 13 ust. 3 projektu rozporządzenia jest z jakichkolwiek powodów niemożliwe (np. przepis jest potrzebny tym Państwom Członkowskim UE, w których lokalizacja na potrzeby ratunkowe opiera się na danych lokalizacyjnych z systemów satelitarnych), zwracamy uwagę na potrzebę takiego przeformułowania projektowanego przepisu, aby jasno z niego wynikało, że przepis ten nie znajduje zastosowania w tych Państwach Członkowskich UE, w których lokalizacja użytkownika na potrzeby systemów powiadamiania ratunkowego opiera się na danych z sieci telekomunikacyjnej, a nie na danych z systemów satelitarnych albo innych podobnych. Taka zmiana mogłaby przybrać następującą postać:

“Where end-user location is based on terminal equipment based location data for the purpose of emergency communications, notwithstanding Article 8(1), ~~R~~egardless of whether the end-user has prevented access to the terminal equipment’s Global Navigation Satellite Systems

(GNSS) capabilities—capabilities or other types of terminal equipment based location data through the terminal equipment settings, when a call is made to emergency services, such settings may not prevent access to GNSS such location data to determine and provide the caller calling end-user's location to emergency services an organisation dealing with emergency communications, including public safety answering points, for the purpose of responding to such calls.”

- **Art. 14**

Przeniesienie tekstu z art.13.ust.2. do art. **14.ust.1a** – zmiana redakcyjna, brak uwag.

Art.14.1

Przepis art. 14.1 nakłada na dostawców bliżej nieokreślony, generalny obowiązek „*shall deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end-users*”. Jednocześnie projektowany art. 14 ust. 2 rozporządzenia stanowi, że dostawca usług telekomunikacyjnych powinien „również” („*also*”), jeśli to technicznie wykonalne, na żądanie użytkownika końcowego blokować połączenia przychodzące z określonych numerów albo numerów z określonymi prefiksami (art. 14 ust. 2 lit. a) oraz blokować automatyczne przekierowania (art. 14 ust. 2 lit. b).

Należy zwrócić uwagę, iż *E-privacy* ma formę bezpośrednio stosowanego rozporządzenia, tym samym niedopuszczalne jest nakładanie obowiązków (zagrożonych groźbą kary) bez jednoczesnego sprecyzowania, co konkretnie jest przedmiotem takiego obowiązku. Jakież bowiem rozwiązania – inne niż wskazane w art. 14 ust. 2 w lit (a) – (b) mają wdrożyć dostawcy usług, aby spełnić wymóg zapewnienia “*state of the art measures to limit the reception of unwanted, malicious or nuisance calls by end-users*”?

W ocenie członków Izby, biorąc pod uwagę, że art. 14 ust. 2 projektu rozporządzenia kompleksowo określa obowiązki dostawcy usług telekomunikacyjnych w zakresie zwalczania niechcianych lub uciążliwych połączeń, a art. 14 ust. 1 w obecnym brzmieniu nie jest możliwy do praktycznego stosowania:

- art. 14 ust. 1 powinien zostać usunięty z projektu rozporządzenia;
- w art. 14 ust. 2 należy usunąć słowo „*also*”.

Alternatywnie, należy połączyć obecne przepisy art. 14 ust. 1 i 2 w jedną jednostkę redakcyjną, której można nadać następujące brzmienie:

“Providers of publicly available number-based interpersonal communications services shall deploy state of the art measures to limit the reception of unwanted, malicious or nuisance calls by providing called end-users with the following possibilities, free of charge:

- (a) to block, where technically feasible, incoming calls from specific numbers or from anonymous sources or from numbers using a specific code or prefix referred to in Article 16(3a); and*
- (b) to stop automatic call forwarding by a third party to the end-user's terminal equipment.*

• Art.16

Proponujemy pozostawienie poprzedniej wersji tytuł tego artykułu, tj. „*Direct marketing communications*”, jako że przepisy w nim zawarte dotyczą de facto przypadków “*unsolicited marketing*”(przy braku zgody użytkownika końcowego) oraz “*solicited marketing*” (w sytuacji gdy marketing bezpośredni dot. podobnych produktów i usług przedsiębiorcy i użytkownik ma prawo zgłoszenia sprzeciwu wobec takich działań – bezpłatnie i w prosty sposób).

z powstania

Prezes Zarządu



Stefan Kamiński