

INSTRUKCJA
DLA PRZEDSTAWICIELA POLSKI
na posiedzenie grupy roboczej Rady UE ds. telekomunikacji i społeczeństwa
informacyjnego (H.05)
13 lipca 2020 r.

Dane przedstawiciela Polski:

Imię i nazwisko/stanowisko:	Aleksandra Chmielecka, I sekretarz
Institucja/komórka organizacyjna:	Stałe Przedstawicielstwo RP przy UE, Bruksela / Referat ds. Cyfryzacji
Numer telefonu:	+ 32 492 259 474
Adres poczty elektronicznej:	Aleksandra.chmielecka@msz.gov.pl

Rozpatrywany dokument:

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Presidency discussion paper (9243/20)

Stanowisko Polski do zaprezentowania:

1. Uwagi ogólne

- W ocenie Polski podstawy przetwarzania danych w art. 6 i 8 projektu ePrivacy powinny być, tam gdzie jest to możliwe i zasadne, maksymalnie zbliżone do podstaw z RODO. Należy przy tym równolegle zadbać aby podstawy te były możliwie precyzyjne i nie pozwalały na nadmierną swobodę w przetwarzaniu danych i unikaniu obowiązku uzyskiwania zgód użytkownika.

2. Art. 6b (1) (d) – ‘vital interest’

- Przedstawiciel Polski wskaże, że Polska popiera opcję 2, tj. zredagowanie brzmienia przepisu analogicznie do przesłanki zawartej w art. 6 ust. 1 (d)

RODO. Przepisy dotyczące przesłanek przetwarzania metadanych komunikacji elektronicznej, szczególnie na podstawie nieostrych kryteriów takich jak „żywotny interes osoby” powinny być jak najbardziej spójne z rozwiązaniami RODO.

[Należy zatem zastąpić obecne brzmienie:

“Art. 6b.1. Without prejudice to Article (6)(1), providers of electronic communications networks and services shall be permitted to process electronic communications metadata only if: (...)

(d) it is necessary to protect the vital interest of a natural person, in the case of emergency, in general upon request of a public authority, in accordance with Union or Member State law;”.

brzmieniem:

“(d) it is necessary in order to protect the vital interests of the end-user or of another natural person.”]

- W zakresie brzmienia motywu 17a odnoszącego się do przesłanki “vital interest”:
 - Wskazanie w motywie, na wzór RODO, iż przetwarzanie metadanych pochodzących z łączności elektronicznej w celu ochrony żywotnych interesów użytkownika końcowego może obejmować na przykład przetwarzanie konieczne do celów humanitarnych, w tym do monitorowania epidemii i ich rozprzestrzeniania się lub w nagłych przypadkach humanitarnych, w szczególności klęsk żywiołowych i katastrof spowodowanych przez człowieka — w świetle doświadczeń związanych z pandemią COVID-19 — jest słusznym kierunkiem.
 - Popieramy przeniesienie motywu 46 RODO do obecnego motywu 17a ePrivacy oraz proponujemy dodanie wskazania, iż *“Processing of electronic communications metadata of an end-user for the protection of the vital interest of an end-user who is a natural person should in principle take place where the protection of such interests cannot be ensured or ensuring is significantly impeded without that processing or in case of emergency requiring urgent action.”*
 - Istotne jest wskazanie, że przetwarzanie metadanych w oparciu o tę przesłankę powinno co do zasady odbywać się tylko wtedy, gdy nie można zapewnić (lub zapewnienie to jest znacznie utrudnione) ochrony takich interesów bez tego przetwarzania lub w nagłych przypadkach, które wymagają pilnego działania. Należy również podkreślić, że zgodnie z brzmieniem art. 6 ust. 2 „electronic communications data shall only be permitted to be processed (...) if the specified purpose or purposes cannot be fulfilled by processing information that is made anonymous.”
 - Proponujemy również rozważenie wpisania w motywie 17a jako przykładu

zastosowania przesłanki „vital interest”.

- Należy również zwrócić uwagę na kwestię akcji poszukiwawczych i ratowniczych prowadzonych przez służby. W opinii Polski, *istotne pozostaje zapewnienie służbom porządku publicznego państw członkowskich wysokiej efektywności realizacji zadań ustawowych, gwarantując prawo do pozyskiwania tzw. metadanych również w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Polska proponuje zatem rozważenie wpisania powyższych działań również do motywu 17b jako przykład przetwarzania danych ze względu na “vital interest”. Kwestia takich działań nie została dotychczas w rozporządzeniu ePrivacy zaadresowana – czy to w przepisach czy w motywach.*
 - Wyjaśnienie w motywach zaprezentowane w opcji nr 2. wydaje się w lepszy sposób zapewniać ochronę prywatności. Jednakże wymaga to jeszcze doprecyzowania. Nie wynika z powyższego choćby to, kto może przetwarzać te dane; czy dotyczy to tylko np. agencji rządowych czy może także podmiotów prywatnych m.in. w celu analiz rozprzestrzeniania się epidemii oraz również do celów biznesowych (processing necessary for humanitarian purposes, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters).
3. **Art. 6b(1) (e) oraz art. 6b(2) – ‘legitimate interest’/ ‘statistical counting’**
- Przedstawiciel Polski wskaże, że Polska kierunkowo popiera opcję 2, która odchodzi od zaproponowanej przez Prezydencję chorwacką propozycji przesłanki “uzasadnionego interesu”. Zawiera ona mniej klauzul generalnych i należy ją uznać za lepszą opcję i podstawę do dalszych dyskusji. W tym zakresie wyższy stopień precyzji przesłanek umożliwiających przetwarzanie 'electronic communications metadata' poprzez wskazanie wprost m.in. przesłanek bezpieczeństwa informacyjnego, przetwarzania danych do celów statystycznych oraz naliczenia opłat w miejsce uzasadnionego interesu jest rozwiązaniem korzystniejszym z punktu widzenia ochrony prywatności użytkowników końcowych. Jest to również spójne z Opinią 01/2017 Grupy Roboczej art. 29 na temat proponowanego rozporządzenia w sprawie prywatności i łączności elektronicznej (2002/58/WE). Grupa wskazała, że proponowane rozporządzenie ePrivacy – które zasadniczo powinno uwzględniać specyfikę danych przetwarzanych w tym sektorze – nie może wskazywać na rozwiązania, które obniżą stopień ochrony zapewniony przez RODO. A zatem, przepisy powinny uwzględniać podejście zakładające obowiązywanie zakazu przetwarzania danych pochodzących z łączności elektronicznej, a przetwarzanie tych danych powinno odbywać się w drodze wyjątku. Oznacza to, że podstawy przetwarzania tego typu danych powinny być precyzyjnie wskazane, a ich przetwarzanie powinno mieć miejsce tylko gdy jest to konieczne – np. gdy nie osiągnie się tego samego celu używając danych zanonimizowanych. Dodać przy tym należy, że precyzyjność formułowania podstaw przetwarzania danych powinna mieć również

odzwierciedlenie w posługiwaniu się pojęciami, które będą jednolicie interpretowane.

[W tym zakresie pozostają aktualne pisemne uwagi Polski zgłoszone do propozycji chorwackiej wprowadzenia przesłanki uzasadnionego interesu oraz dodatkowych warunków tej przesłanki – do ewentualnego wykorzystania załączone do niniejszej instrukcji]

- Tekst projektowanego rozporządzenia z 6 marca br. zakłada, jako konsekwencje wprowadzenia przesłanki “uzasadnionego interesu”, wykreślenie art. 6c dotyczącego dalszego zgodnego z pierwotnym celem, dla którego dane zostały zebrane, przetwarzania danych. Należy wskazać, że przesłanka uzasadnionego interesu nie zastępuje zasady dalszego zgodnego z pierwotnym celem przetwarzania (ang. further processing). Zasada ta oznacza dalsze przetwarzanie danych w nowych celach, jeśli te cele są zgodne z pierwotnymi. To nie jest podstawa prawna jako taka. Dlatego proponujemy rozważenie przywrócenia zasady dalszego zgodnego z pierwotnym celem przetwarzania, na wzór analogicznej regulacji zawartej w RODO, zamiast uzasadnionego interesu.
- W zakresie przesłanki “statistical counting” Polska kierunkowo popiera zmiany w lit. e) i f) w ramach wariantu 2, jednakże proponuje zastąpienie pojęcia “statistical counting” pojęciem “processing for statistical purposes”, aby w większym stopniu zapewnić spójność z RODO, a także w celu uniknięcia wprowadzenia nowego, niezdefiniowanego pojęcia, które sztucznie ograniczałoby analizy statystyczne. Alternatywnie proponuje wprowadzić następującą zmianę w brzmieniu lit. f:

“(f) it is necessary for statistical counting, other than based on electronic communications metadata that constitute location data or for other statistical purposes or scientific research, provided it is based on Union or Member State law which shall be proportionate to the aim pursued and provide for specific measures, including encryption and pseudonymisation, to protect fundamental rights and the interest of the end-users. Processing of electronic communications metadata under this point shall be done in accordance with paragraph 6 of Article 21 and paragraphs 1, 2 and 4 of Article 89 of Regulation (EU) 2016/679.”

Zmiana ta jest istotna, w szczególności z punktu widzenia organów statystyki publicznej. Chociaż wydaje się, że wcześniejsza wersja przepisu została przywrócona, istnieje niewielka różnica, która z punktu widzenia statystyki publicznej okazuje się mieć bardzo znaczący wpływ. Wyrażenie „statistical purposes” zastąpiono „statistical counting”, które zawęży znaczenie przepisu. Takie zrozumienie opiera się na tym, że:

- definicja “statistical counting” określona w motywie (25) odnosi się raczej do wewnętrznych działań usługodawcy, a nie do celów statystycznych w

rozumieniu rozporządzenia (WE) nr 223/2009 w sprawie statystyki europejskiej,

- wyjaśnienie, co uznaje się za „uzasadniony interes” przewidziany w motywie (17b) koncentruje się na uzasadnionych interesach sieci łączności elektronicznej lub dostawcy usług. Wykorzystanie takich metadanych przez władze publiczne jest raczej ograniczone (odpowiednie części motywu 17b: “Processing of electronic communication metadata for scientific research or statistical counting purposes should could also be considered as a legitimate interest of the provider, for instance for the provision of heat maps, a graphical representation of data using colours to indicate the presence of individuals. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure”).

Proponowana zmiana przepisu zapewni uwzględnienie zarówno “statistical counting” w rozumieniu rozporządzenia ePrivacy, jak i celów statystycznych w rozumieniu rozporządzenia nr 223/2009. Ponadto odniesienie do art. 89 rozporządzenia RODO byłoby w pełni właściwe.

4. Art. 8

- Polska wskazuje, iż jej stanowisko jest bliższe opcji 2, która odchodzi od chorwackiej propozycji „uzasadnionego interesu”. Polska widzi potrzebę dalszych analiz odnośnie do tej kwestii. Należy zwrócić uwagę, że poprzednie brzmienie art. 8 ust. 1 lit. da i lit. e – w którym wprost wskazano przesłanki bezpieczeństwa informacyjnego zarówno dostawcy jak i użytkownika końcowego; zapobiegania oszustwom czy wykrywaniu usterek technicznych – pozwalało w sposób bardziej jednoznaczny ocenić dopuszczalność przetwarzania danych użytkownika kiedy jego jednoznaczne działanie – zgoda – nie jest przesłanką legalności przetwarzania. Należy w tej kwestii wziąć pod uwagę trwające w EROD prace nad wytycznymi dot. art. 6 ust. 1 lit. f RODO – zakresu uzasadnionego interesu administratora do przetwarzania danych osobowych.

5. **Art. 6d – ‘detection of child abuse imagery’**

Kwestie zwalczania przestępczości, w szczególności tej dotyczącej terroryzmu oraz zwalczania pornografii dziecięcej powinny być uregulowane w innym akcie prawnym niż rozporządzenie ePrivacy. Temat ten wymaga szczegółowych analiz i nie powinien zdaniem Polski wpływać na przyjęcie innych ogólnych przepisów rozporządzenia.

6. **Pozostałe kwestie**

- Polska podtrzymuje konieczność wprowadzenia wielokrotnie dotychczas zgłaszanych wymienionych poniżej zmian, w szczególności:
- potwierdzenia, w kontekście zgody użytkownika, że chodzi o zgodę uprzednią,

- wskazania maksymalnego okresu wysyłki komunikatów w art. 16 ust. 2a projektu,
- określenia jakie decyzje mogą skarżyć poszkodowani naruszeniami,
- określenie jasnych zasad współpracy organów nadzoru,
- zapewnienia elastyczności państw członkowskich w wyborze organu nadzoru; dotychczasowy model, tj. kompetencje UKE w zakresie dyrektywy e-privacy docelowo powinny naszym zdaniem zostać niezmienione,
- **usunięcia domyślnego wyłączenia dla NGO i partii politycznych z pojęcia komunikacji marketingowej, co stanowi ogromne pole do potencjalnych nadużyć.**
- W kontekście art. 6 i n. Polska zwraca uwagę na kwestie prowadzonych przez służby postępowań. Niezasadny byłby obowiązek udzielania informacji końcowemu użytkownikowi w trakcie realizacji ustaleń na jego temat, o czynnościach realizowanych przez organy ścigania, bądź obowiązek zwracania się z prośbą do danej osoby o wyrażenie zgody na przetwarzanie jej danych, jeśli jest sprawcą przestępstwa.

Sporządziła: Agnieszka Chruszcz, główny specjalista Departamentu Telekomunikacji

Akceptował: Tomasz Proć, Zastępca Dyrektora Departamentu Telekomunikacji

Zatwierdziła: Agnieszka Krauzowicz, Dyrektor Departamentu Telekomunikacji