



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia *14* lutego 2017 r.

DOLiS-027-331/17/KK /*14251*

Pan dr Adam Bodnar
Rzecznik Praw Obywatelskich
Aleja Solidarności 77
00 – 090 Warszawa
e-mail: biurorzecznika@brpo.gov.pl

Szanowny Panie Rzeczniku,

w odpowiedzi na pismo z dnia 7 lutego 2017 roku – znak: VII.520.11.2017.AG – (data wpływu do Biura Generalnego Inspektora Ochrony Danych Osobowych 13 lutego 2017 r.) uprzejmie dziękuję za przesłanie wystąpienia do Ministra Cyfryzacji w sprawie problemu zgodności przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489), w zakresie dotyczącym obowiązku tzw. retencji danych nałożonego na operatorów telekomunikacyjnych, z prawem Unii Europejskiej.

W załączeniu przekazuję stanowisko organu ds. ochrony danych osobowych z dnia 25 stycznia br. dotyczące skutków wyroku dla polskiego porządku prawnego, które powstało w odpowiedzi na prośbę Ministra Spraw Zagranicznych (także w załączeniu). Obok Ministra Cyfryzacji także w/w Minister może udzielić Wielce Szanownemu Panu Rzecznikowi informacji o planowanych działaniach podejmowanych w celu dostosowania polskiego prawa do przepisów Karty Praw Podstawowych po wyroku TSUE w sprawie Tele2. W przypadku uzyskania nowych informacji uprzejmie proszę o ich przekazanie do Biura GODO.

Z wyrazami szacunku
GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH
Edyta
dr Edyta Bielak-Jomaa

ZALĄCZNIKI:

1. Kopia pisma MSZ z dnia 3 stycznia br. (sygn. DPUE.9323.492.2016/1/kw) – kart 2,
2. Kopia odpowiedzi GODO z dnia 25 stycznia br. (sygn. DESiWM-070-2/17/6388/17) – kart 4.



**20-LECIE PRAWA DO OCHRONY
DANYCH OSOBOWYCH W POLSCE**

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-03-00
fax 22 531-03-01
www.godo.gov.pl



Ministerstwo
Spraw Zagranicznych

Podsekretarz Stanu

Renata Szczęch

Warszawa, dnia 03 stycznia 2017 r.

DPUE.9323. 492 .2016/1 /kw
dot.: spraw C-203/15 i C-698/15 Tele2 Sverige i in.

Wg rozdzielnika

Szanowni Państwo,

niniejszym informuję, że w dniu 21 grudnia 2016 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie prejudycjalnej C-203/15 i C-698/15 Tele2 Sverige i in. (ochrona danych osobowych w sektorze łączności elektronicznej – skutki wyroku Digital Rights Ireland i in. w prawie krajowym – art. 7 i 8 Karty Praw Podstawowych UE).

Wyrok ten dotyczy wykładni art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).

Pełnomocnik Polski przedstawił uwagi na piśmie w sprawie C-203/15 i C-698/15. Pełnomocnik zaprezentował stanowisko, zgodnie z którym zatrzymywanie i przechowywanie danych o ruchu i lokalizacji w sieciach łączności elektronicznej w celu zapewnienia ich dostępności dla celów dochodzenia, wykrywania i ścigania przestępstw pozostaje poza zakresem regulacji prawa Unii. Oznacza to, że wyrok *Digital Rights Ireland Ltd*¹, stwierdzający nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetworzonych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE, nie ustanawia bezwzględnych wymogów mających zastosowanie do prawa wewnętrznego państw członkowskich normującego dostęp do takich danych.

Trybunał Sprawiedliwości nie podzielił powyższego stanowiska, uznając że przepisy umożliwiające organom państwowym dostęp do danych zatrzymywanych przez dostawców usług łączności elektronicznej dotyczą przetwarzania danych osobowych przez tych

¹ Wyrok *Digital Rights Ireland Ltd* C-369/11, EU:C:2014:238.
Al. J. Ch. Szucha 21
00-580 Warszawa

dostawców, w związku z czym wchodzi w zakres dyrektywy o prywatności i łączności elektronicznej.

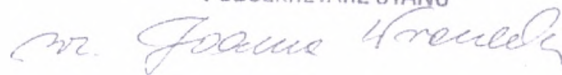
Zgodnie z sentencją wyroku art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej należy interpretować w ten sposób, że stoi on na przeszkodzie przepisom krajowym, które w celu zwalczania przestępczości umożliwiają ogólne i niedyskryminacyjne przechowywanie wszystkich danych o ruchu i lokalizacji abonentów i zarejestrowanych użytkowników usług łączności elektronicznej. Ponadto w ocenie Trybunału ogólny cel, jakim jest zwalczanie przestępczości, nie uzasadnia dostępu odpowiednich organów państwa do zatrzymywanych danych. Trybunał zwrócił również uwagę na konieczność dokonywania uprzedniej kontroli dostępu do tych danych przez niezależne organy oraz wymóg ich przechowywania na obszarze Unii Europejskiej.

Wobec powyższego, po dokonaniu wstępnej analizy wyroku, w opinii MSZ należy rozważyć konieczność zmiany polskiego prawa, w szczególności w zakresie, w jakim przewiduje ono ogólny obowiązek zatrzymywania i przechowywania wszystkich danych dotyczących ruchu w sieci i lokalizacji użytkowników przez przedsiębiorców telekomunikacyjnych (art. 180a ustawy Prawo telekomunikacyjne Dz.U. z 2016 r. poz. 1489, z późn. zm.).

Uprzejmie proszę o przedstawienie, w terminie 1 miesiąca od dnia otrzymania niniejszego zawiadomienia, uzasadnionego stanowiska dotyczącego skutków wyroku w polskim porządku prawnym. W szczególności proszę o informację, czy wyrok będzie powodował konieczność zmiany obowiązującego w Polsce prawa lub praktyki jego stosowania. W przypadku stwierdzenia konieczności zmian legislacyjnych, proszę o dołączenie harmonogramu ich realizacji.

Z poważaniem

PODSEKRETARZ STANU



Joanna Wronecka

Wyrok jest dostępny na stronie internetowej <http://curia.europa.eu>.

Otrzymują:

- 1) Pan Jakub Skiba
Sekretarz Stanu, Ministerstwo Spraw Wewnętrznych i Administracji
- 2) Pan Karol Okoński
Podsekretarz Stanu, Ministerstwo Cyfryzacji
- 3) Pan Łukasz Piebiak
Podsekretarz Stanu, Ministerstwo Sprawiedliwości
- 4) Pani Edyta Bielak-Jomaa
Generalny Inspektor Ochrony Danych Osobowych
- 5) Pan Marcin Cichy
Prezes Urzędu Komunikacji Elektronicznej

Sporządziła: Katarzyna Wilimborek, główny specjalista DPUE

Akceptował: Bogusław Majczyna, zastępca dyrektora DPUE



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

DESiWM-070-2/17/6388/17

Warszawa, dnia 25 stycznia 2017 r.

**Pani
Renata Szczęch
Podsekretarz Stanu
Ministerstwo Spraw
Zagranicznych
Al. J. Ch. Szucha 23
00 – 580 Warszawa**

Szanowne Pani Minister,

w odpowiedzi na pismo z dnia 3 stycznia 2017 r., sygn. DPUE.9323.492.2016/1/kw, dotyczące przedstawienia uzasadnionego stanowiska dotyczącego skutków wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-203/15 i C-698/15 Tele2 Sverige i In., przedstawiam poniżej stanowisko GIODO:

Trybunał Sprawiedliwości Unii Europejskiej wyrokiem z dnia 21 grudnia 2016 r. w sprawach połączonych C-203/15 Tele2 Sverige AB/ Post-ochtelestyrelsen i C-698/15 Secretary of State for the Home Department/Tom Watson i in., stwierdził, że państwa członkowskie nie mogą nakładać na operatorów telekomunikacyjnych ogólnego obowiązku zatrzymywania danych. W wyroku TSUE wskazał, że prawo UE zabrania masowego zatrzymywania wszystkich danych dotyczących ruchu w sieci i lokalizacji. Jednak państwa członkowskie mają możliwość wprowadzenia przepisów prawa, które pozwalają na retencję niektórych danych w celu zwalczania poważnej przestępczości. Dodatkowo prawo krajowe musi przewidywać warunki dostępu organów krajowych do zatrzymanych danych, w tym uprzednią kontrolę dostępu przez niezależny organ oraz obowiązek przechowywania danych na terytorium UE.

Należy wskazać, że wyrokiem TSUE w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland Ltd. stwierdzona została nieważność dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniającej dyrektywę 2002/58/WE. W związku z powyższym, co do zasady w chwili obecnej kwestia retencji danych nie jest regulowana na poziomie Unii Europejskiej, a państwa członkowskie mogą samodzielnie regulować zasady retencji danych w krajowych porządkach prawnych. W następstwie wydania wyroku Digital Rights Ireland do TSUE wpłynęły dwie sprawy dotyczące nałożonego w Szwecji i w Zjednoczonym Królestwie na podmioty świadczące usługi telekomunikacyjne ogólnego obowiązku zatrzymywania danych dotyczących łączności elektronicznej, który to obowiązek został ustanowiony w unieważnionej dyrektywie retencyjnej. W wyniku złożenia ww. spraw Trybunał wydał przedmiotowy wyrok.

Należy również mieć na uwadze, iż w podobne stanowisko zajął Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. K 23/11). Niniejszym wyrokiem TK uznał część krajowych przepisów upoważniających służby do sięgania po dane telekomunikacyjne za niekonstytucyjne. Zasygnalizował również ustawodawcy krajowemu dopuszczalność niejawnego pozyskiwania informacji o jednostkach jedynie w celu zapobiegania poważnym przestępstwom, konieczność stosowania zasady proporcjonalności oraz konieczność kontroli dostępu do danych, zarówno uprzedniej, jak i zastępczej.

Uprzejmie informuję, że w opinii Generalnego Inspektora Ochrony Danych Osobowych wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 21 grudnia 2016 r. w sprawach połączonych C-203/15 i C-698/15 będzie miał wpływ na przepisy krajowe dotyczące retencji danych. Ponadto, mając na uwadze zawarte w wyroku Digital Rights Ireland wytyczne dotyczące zasady proporcjonalności, wyrok Trybunału Konstytucyjnego K 23/11 oraz najnowsze orzeczenie TSUE, ustawodawca powinien pod tym kątem ocenić polskie prawo telekomunikacyjne oraz ustawy kompetencyjne poszczególnych służb w zakresie przepisów dotyczących retencji danych i dokonać odpowiednich zmiany ww. przepisów prawa.

Obowiązujące w Polsce przepisy dotyczące zatrzymywania danych powinny być zgodne z następującymi wytycznymi zawartymi w niniejszym wyroku TSUE:

1. **uprawnione organy mogą mieć dostęp do danych wyłącznie w celu zwalczania poważnych przestępstw**- Trybunał stoi na stanowisku, że wszystkie przepisy dotyczące

zatrzymywania danych muszą być jednoznaczne i szczegółowe. Przepisy te powinny wskazywać okoliczności i warunki, w których środek w zakresie zatrzymywania danych może zostać zastosowany tytułem prewencji w taki sposób, który gwarantuje, aby jego zakres w praktyce ograniczał się do tego, co jest absolutnie konieczne.

2. **możliwość zatrzymania danych musi być ograniczona tylko do tego, co jest bezwzględnie konieczne**- dotychczasowe orzecznictwo Trybunału wskazuje, że ochrona prawa podstawowego do poszanowania prywatności wymaga, aby odstępstwa od ochrony danych osobowych pozostawały w granicach tego, co jest „absolutnie konieczne”. Odnosi się to zarówno do norm regulujących zatrzymywanie danych, jak i tych regulujących dostęp do przechowywanych danych;
3. **prawo krajowe musi przewidywać warunki dostępu organów krajowych do zatrzymanych danych** - Trybunał w swoim wyroku wskazał, że przepisy krajowe nie mogą ograniczać się jedynie do ustanowienia wymogu, by dostęp do zatrzymanych danych był uzasadniony prowadzeniem walki z poważną przestępczością. Dodatkowo muszą one ustanawiać materialne i proceduralne warunki regulujące dostęp organów krajowych do danych;
4. **przepisy muszą regulować uprzednią kontrolę dostępu przez sąd lub niezależny organ administracyjny**- TSUE odnosząc się do treści systemów krajowych wskazał, że każdy ustawodawca musi uregulować uprzednią kontrolę dostępu do danych przez niezależny organ. Wyjątkiem od tej kontroli mogą być jedynie pilne przypadki żądania dostępu do danych;
5. **przepisy muszą regulować kwestię informowania osób, których dane zostały udostępnione** – TSUE po raz kolejny potwierdził, iż poinformowanie osób powinno mieć miejsce w sytuacji, gdy nie zagrazi to prowadzonym przez upoważnione organy i służby postępowaniom;
6. **przepisy muszą nakładać obowiązek przechowywania danych przez operatorów i dostawców na terytorium Unii Europejskiej**- w wyroku TSUE dodatkowo wprowadził wymóg przechowywania danych na terytorium UE. Wprowadzenie regulacji zobowiązujących operatorów i dostawców do przechowywania danych na terytorium UE niewątpliwie wpłynie na poszanowanie wymogów ochrony i bezpieczeństwa zatrzymanych danych;
7. **przepisy powinny precyzyjnie wskazywać usługodawcom i administratorom, jak zabezpieczyć dane przed nieuprawnionym dostępem albo nadużyciem ich wykorzystania** – obecnie kwestie te regulowane są na poziomie porozumień pomiędzy

podmiotami zobowiązanymi do przechowywania danych a uprawnionymi do dostępu za pośrednictwem sieci telekomunikacyjnej służbami.

Reasumując, niniejszy wyrok Trybunału Sprawiedliwości Unii Europejskiej powoduje konieczność zmiany prawa telekomunikacyjnego oraz ustaw kompetencyjnych poszczególnych służb w zakresie przepisów dotyczących retencji danych i zdalnego do nich dostępu oraz dostosowania ich do wytycznych wskazanych w wyroku. Ewentualny harmonogram zmian legislacyjnych powinien zostać przedstawiony przez ministra właściwego do spraw informatyzacji - w zakresie zmiany prawa telekomunikacyjnego, ministra właściwego do spraw wewnętrznych oraz ministra właściwego do spraw obrony narodowej - w zakresie zmian ustaw kompetencyjnych właściwych służb.

Z wyrazami szacunku

NY DAN
sfemoe
Edyta Bielak-Jomau