



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Bielak-Jomaa

Warszawa, dnia 12 maja 2016 r.

DOLiS-033-133/16

**Podsekretarz Stanu
w Ministerstwie Spraw Wewnętrznych
i Administracji**

w związku z zamieszczeniem na stronie internetowej <http://legislacja.rcl.gov.pl/docs//2/12284561/12348757/12348758/dokument220225.pdf> (Biuletyn Informacji Publicznej Rządowego Centrum Legislacji) projektu **ustawy o działaniach antyterrorystycznych** (wersja z dnia 09.05.2016 r.), który to projekt nie został przedłożony do zaopiniowania przez Generalnego Inspektora Ochrony Danych Osobowych, uprzejmie informuję, że organ do spraw ochrony danych osobowych zdecydował się przedstawić do tego projektu następujące uwagi.

I – Podzielając opinię Projektodawcy co do potrzeby koordynacji i intensyfikacji działań mających na celu przeciwdziałanie i zwalczanie przestępczości o charakterze terrorystycznym, Generalny Inspektor Ochrony Danych Osobowych z aprobatą przyjmuje fakt zamieszczenia w przepisach ustawowych [art. 6 projektu **ustawy o działaniach antyterrorystycznych** (wersja z dnia 09.05.2016 r.), powoływanego dalej z zastosowaniem skrótu „projekt z 09.05.2016”] unormowań określających katalog osób, o których informacje mają znaleźć się w wykazie: 1) osób podejmujących działalność na rzecz organizacji terrorystycznych lub organizacji związanych z działalnością terrorystyczną lub członków tych organizacji, 2) poszukiwanych osób prowadzących działalność terrorystyczną lub osób podejrzewanych o popełnienie przestępstw o charakterze terrorystycznym, wobec których w Rzeczypospolitej Polskiej wydane zostało zarządzenie o zatrzymaniu, poszukiwaniu oraz postanowienie o poszukiwaniu listem gończym, a także poszukiwanych na podstawie europejskiego nakazu aresztowania, 3) osób wobec których istnieje uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa o charakterze terrorystycznym, w tym osób

stanowiących zagrożenie bezpieczeństwa lotnictwa cywilnego, 4) osób uczestniczących w szkoleniach terrorystycznych albo podejmujących podróże w celu popełnienia przestępstwa o charakterze terrorystycznym, zwanym dalej „wykazem”. Uwadze Generalnego Inspektora Ochrony Danych Osobowych nie umyka wszakże, iż – w myśl art. 93 ust. 1 i 2 Konstytucji Rzeczypospolitej Polskiej – akt prawny o charakterze wewnętrznym, jakim jest zarządzenie, nie może stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów. Tym samym – w świetle uwarunkowań konstytucyjnych – za wysoce kontrowersyjną uznać trzeba konstrukcję prawną zaproponowaną w art. 6 ust. 4 projektu z 09.05.2016, zgodnie z którą podstawowe regulacje dotyczące wykazu (zakres informacji w nim gromadzonych, tryb udostępniania z niego informacji etc.) znajdują się w zarządzeniu (niejawnym) Szefa Agencji Bezpieczeństwa Wewnętrznego. Z jednej strony trudno bowiem przecież racjonalnie przyjąć, że fakt umieszczenia informacji o danej osobie w wykazie nie będzie skutkowało podejmowaniem wobec tej osoby określonych decyzji przez polskie organy władzy publicznej, z drugiej – akt prawny powszechnie obowiązujący, jakim jest rozporządzenie (art. 87 ust. 1 Konstytucji Rzeczypospolitej Polskiej), nie może być dokumentem niejawnym, a organ do spraw ochrony danych osobowych zdaje sobie sprawę z konieczności zachowania w tajemnicy działań prowadzonych wobec osób, o których informacje (których dane) znajdują się w wykazie.

Generalny Inspektor Ochrony Danych Osobowych jedynie sygnalizuje powyższy dylemat pozostawiając jego rozwiązanie Projektodawcy, a w dalszej kolejności Parlamentowi.

II – W odniesieniu do – przewidzianych w art. 39 projektu z 09.05.2016 – zmian ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.) zauważyć należy, iż:

a. Obowiązujący art. 60 a ust. 1 a ustawy – Prawo telekomunikacyjne normujący zakres danych, które abonent niebędący stroną zawartej na piśmie umowy o świadczenie usług telekomunikacyjnych może udostępnić dostawcy publicznie dostępnych usług telekomunikacyjnych, przewiduje zamknięty katalog takich danych (w przypadku abonenta będącego osobą fizyczną – imię, nazwisko, numer ewidencyjny PESEL, adres korespondencyjny, a przypadku osoby nieposiadającej numeru ewidencyjnego PESEL – nazwa i numer dokumentu stwierdzającego tożsamość). Tymczasem w – dodawanym przez art. 39 pkt 1 projektu z 09.05.2016 – art. 60 b ust. 1 ustawy – Prawo telekomunikacyjne katalog danych abonenta (z wyłączeniem abonenta

korzystającego z publicznie dostępnych usług telefonicznych świadczonych za pomocą aparatu publicznego lub przez wybranie numeru dostępu do sieci dostawcy publicznie dostępnych usług telekomunikacyjnych) podlegających obligatoryjnemu przekazaniu dostawcy publicznie dostępnych usług telekomunikacyjnych poprzedzony został sformułowaniem „co najmniej” i zyskał w ten sposób charakter otwarty. Przyjęcie zaproponowanego brzmienia art. 60 b ust. 1 ustawy – Prawo telekomunikacyjne prowadziłoby do sytuacji, w której obowiązek abonenta przekazania danych dostawcy publicznie dostępnych usług telekomunikacyjnych mógłby obejmować wszelkie (dowolne) dane tego abonenta. Taka konstrukcja, nakładająca obowiązki na abonentów, (projektowanego) przepisu ustawy – Prawo telekomunikacyjne pozostaje w sprzeczności ze – statuowaną w art. 26 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.) – zasadą adekwatności przetwarzanych danych w stosunku do celów, w jakich są przetwarzane,

- b. W art. 60 b ust. 2 in fine ustawy – Prawo telekomunikacyjne, dodawanym przez art. 39 pkt 1 projektu z 09.05.2016, Projektodawca zadekretował swobodę dostawcy publicznie dostępnych usług telekomunikacyjnych w zakresie określania sposobu, w jaki abonent ma mu przekazać swoje dane, o których mowa w – powołanym wyżej – art. 60 b ust. 1 ustawy – Prawo telekomunikacyjne. Taki kształt komentowanego przepisu ustawy – Prawo telekomunikacyjne rodzić może niebezpieczeństwo naruszenia praw abonenta. Zgodnie z art. 60 b ust. 1 ustawy – Prawo telekomunikacyjne (dodawany przez art. 39 pkt 1 projektu z 09.05.2016) będzie on bowiem zobligowany do przekazania („podania” według terminologii przyjętej w przepisie) swoich danych dostawcy publicznie dostępnych usług telekomunikacyjnych, zaś – pozostając w zgodzie z brzmieniem (proponowanego) art. 60 b ust. 2 ustawy – Prawo telekomunikacyjne – dostawca publicznie dostępnych usług telekomunikacyjnych może mu nakazać przekazanie tych danych w dowolny, wygodny dla siebie, sposób, w tym również taki, który nie zapewni ich bezpieczeństwa,
- c. W myśl art. 60 b ust. 3 pkt 1 lit. a ustawy – Prawo telekomunikacyjne, dodawanego przez art. 39 pkt 1 projektu z 09.05.2016, dostawca publicznie dostępnych usług telekomunikacyjnych może rozpocząć świadczenie usługi telekomunikacyjnej abonentowi dopiero po potwierdzeniu zgodności podanych przez niego danych z danymi zawartymi w dokumencie potwierdzającym tożsamość abonenta będącego osobą fizyczną. W projektowanych przepisach ustawy –

Prawo telekomunikacyjne pominięto wszakże całkowitym milczeniem kwestię zasadniczą z punktu widzenia oceny prawidłowości procesu przetwarzania danych, to jest zagadnienie sposobu, w jaki przedmiotowe potwierdzenie zgodności ma się odbywać. Projektodawca ograniczył się jedynie do stwierdzenia, iż potwierdzenia, o którym mowa w art. 60 b ust. 3 pkt 1 lit. a ustawy – Prawo telekomunikacyjne (dodawanym przez art. 39 pkt 1 projektu z 09.05.2016) dostawca publicznie dostępnych usług telekomunikacyjnych może dokonać również za pośrednictwem osoby trzeciej działającej w jego imieniu (art. 60 b ust. 4 ustawy – Prawo telekomunikacyjne, dodawany przez art. 39 pkt 1 projektu z 09.05.2016). Tym samym – w oparciu o projektowane przepisy ustawy – Prawo telekomunikacyjne nie tylko nie można ustalić jak będzie się odbywać proces potwierdzania zgodności danych abonenta i jak w związku z tym procesem będą przetwarzane jego dane, lecz także – kto tego potwierdzenia może dokonywać. Nie może zaś umknąć uwadze, że – zgodnie z art. 159 ust. 1 pkt 1 ustawy – Prawo telekomunikacyjne – dane użytkownika usługi telekomunikacyjnej są objęte tajemnicą telekomunikacyjną. Użyte w art. 60 b ust. 4 ustawy – Prawo telekomunikacyjne, dodawanym przez art. 39 pkt 1 projektu z 09.05.2016, nieostre sformułowanie „osoba trzecia działająca w imieniu dostawcy usług” nie pozwala na skonkretyzowanie kręgu osób, które w ramach procedury potwierdzania zgodności danych abonenta uzyskają dostęp do – objętych tajemnicą telekomunikacyjną – danych tych abonentów,

- d. Stosownie do dyspozycji art. 60 b ust. 3 pkt 2 lit. a ustawy – Prawo telekomunikacyjne, dodawanego przez art. 39 pkt 1 projektu z 09.05.2016, potwierdzenie podanych przez abonenta danych, o których mowa w art. 60 b ust. 1 ustawy – Prawo telekomunikacyjne (dodawanym przez art. 39 pkt 1 projektu z 09.05.2016), może nastąpić drogą elektroniczną: „przy wykorzystaniu środków identyfikacji elektronicznej służących do uwierzytelniania w systemie teleinformatycznym banku krajowego”. Jak było to już podnoszone w pkt II lit. c dane użytkownika usługi telekomunikacyjnej są objęte tajemnicą telekomunikacyjną (art. 159 ust. 1 pkt 1 ustawy – Prawo telekomunikacyjne). Organ do spraw ochrony danych osobowych wyraża zatem wątpliwość na jakiej podstawie prawnej bank będący „stroną trzecią” w stosunku prawnym abonent – dostawca publicznie dostępnych usług telekomunikacyjnych ma – w związku z procesem potwierdzania zgodności danych abonenta drogą elektroniczną – uzyskać informację, iż dana osoba fizyczna jest użytkownikiem usługi telekomunikacyjnej oferowanej przez danego dostawcę publicznie dostępnych

usług telekomunikacyjnych. Informacja taka jest przecież objęta tajemnicą telekomunikacyjną także wobec banku niebędącego uczestnikiem stosunku prawnego między abonentem a dostawcą publicznie dostępnych usług telekomunikacyjnych. Marginesowo zauważyć również należy, że komentowany przepis – art. 60 b ust. 3 pkt 2 lit. a ustawy – Prawo telekomunikacyjne (dodawany przez art. 39 pkt 1 projektu z 09.05.2016) – nie reguluje kwestii zasad przetwarzania przez bank informacji pozyskanych w ramach procedury potwierdzania zgodności danych abonenta drogą elektroniczną.