GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Edyta Bielak-Jomaa

Warszawa, dnia 28 lipca 2015 r.

DOLiS-035- 2498 /15

Pani
Teresa Piotrowska
Minister Spraw Wewnętrznych
ul. Stefana Batorego 5
02-591 Warszawa

WYSTĄPIENIE

na podstawie art. 19a ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.), zgodnie z którym Generalny Inspektor Ochrony Danych Osobowych może kierować do osób prawnych wystąpienie zmierzające do zapewnienia skutecznej ochrony danych osobowych, zwracam się o podjęcie działań legislacyjnych zmierzających do znowelizowania przepisów ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (t.j. Dz. U. 2013 r., poz. 1383), prowadzącego do zapewnienia strażom gminnym dostępu do danych objętych tajemnicą telekomunikacyjną w zakresie, w jakim jest im to niezbędne do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych - zgodnie z art. 12 ust. 1 pkt 5 ustawy o strażach gminnych (t.j. Dz. U. 2013 r., poz. 1383), i art. 17 § 3 i 54 - 57 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2013 r., poz. 395, z późn. zm.).

Praktyka działalności organu do spraw ochrony danych osobowych dowodzi, iż przedsiębiorcy telekomunikacyjni w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. Prawo

telekomunikacyjne (t.j. Dz. U. 2014 r. poz. 243 ze zm.) zwanej dalej Prawem telekomunikacyjnym, odmawiają udostępnienia informacji stanowiących tajemnicę telekomunikacyjną - powołując się na uregulowania ww. ustawy. W takich przypadkach, straże miejskie składają skargi do Generalnego Inspektora Ochrony Danych Osobowych, aby ten, korzystając ze swych – przewidzianych przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze. zm.) zwanej dalej także ustawą – uprawnień, nakazał określonemu przedsiębiorcy telekomunikacyjnemu udostępnienie straży miejskiej danych osobowych. Taki stan rzeczy powoduje w wielu przypadkach wydłużanie postępowań prowadzonych przez straże miejskie, a przede wszystkim prowadzenie postępowań, których można by uniknąć, w przypadku organu do spraw ochrony danych osobowych. W konsekwencji dochodzić może do podważania zasad określonych w przepisach ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t. j. Dz. U. z 2013 r., poz. 267, ze. zm.), chociażby jej art. 12 § 1 stanowiącego, iż organy administracji publicznej powinny działać w sprawie wnikliwie i szybko, posługując się możliwie najprostszymi środkami prowadzącymi do jej załatwienia, czy art. 8 stanowiącego, że organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej.

Istniejące przepisy w obecnym brzmieniu i zakresie utrudniają ich rozumienie przedsiębiorcom telekomunikacyjnym i powodują rozbieżności interpretacyjne utrudniające realizowanie przez właściwe organy obowiązków wynikających z przepisów prawa. Dotyczy to zwłaszcza straży gminnych strzegących przecież porządku publicznego i egzekwujących postanowienia przepisów prawa w granicach przyznanych im kompetencji. Celem egzekwowania prawa jest nałożenie sankcji karnej na osobę, która łamie przepisy, ku czemu niezbędne jest efektywne zebranie niezbędnych informacji zmierzających do ukarania sprawcy.

Straż gminna, zdaniem organu do spraw ochrony danych osobowych, posiada podstawę prawną do pozyskania danych osobowych na mocy ww. przepisów prawa.

Zgodnie z art. 10 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (t.j. Dz. U. 2013 r., poz. 1383), zwanej dalej ustawą o strażach gminnych, straż wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ustaw i aktów prawa miejscowego. W celu realizacji tych zadań straż może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą uzyskane w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia (art. 10a pkt 1 ustawy o strażach gminnych). Stosownie do brzmienia art. 12 ust. 1 pkt 5 ustawy o strażach gminnych, strażnik wykonując zadania, o których mowa w art. 10 i 11, ma prawo do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych – w trybie i zakresie określonych w Kodeksie postępowania w sprawach o wykroczenia.

Ponadto, straż gminna jest jednym z oskarżycieli publicznych w myśl art. 17 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (t.j. Dz. U. 2013 r., poz. 395, z

późn. zm.), któremu przysługuje prawo do przeprowadzenia czynności wyjaśniających w celu ustalenia, czy istnieją podstawy do wystąpienia z wnioskiem o ukaranie oraz zebrania danych niezbędnych do sporządzenia wniosku o ukaranie (art. 54 – 56 ustawy Kodeks postępowania w sprawach o wykroczenia). Zwrócić należy uwagę, iż w myśl art. 54 ust. 1 in fine ustawy Kodeks postępowania w sprawach o wykroczenia, czynności te [tu: czynności wyjaśniające] w miarę możności należy podjąć w miejscu popełnienia czynu bezpośrednio po jego ujawnieniu i zakończyć w ciągu miesiąca.

Realizacja przez straż gminną zadań nałożonych na nią ustawowo wymaga wykorzystywania informacji o osobach, których działania te dotyczą. Przepisy ustawy o strażach gminnych wprost stanowią o prawie straży gminnej do przetwarzania danych w związku z realizacją określonych prawem zadań, bez konieczności uzyskania na to zgody osoby, której dane dotyczą. Oznacza to, iż straż gminna, na mocy stosownych przepisów rangi ustawowej, ma prawo zwrócić się do operatora telekomunikacyjnego o udostępnienie niezbędnych jej danych osobowych, zaś operator ten winien – mając na względzie fakt realizacji obowiązku czuwania przez straż gminną nad przestrzeganiem prawa przez obywateli – udostępnić informacje w zakresie wnioskowanym przez straż (i adekwatnym do potrzeb prowadzonego przez straż postępowania). W takiej sytuacji dochodzi bowiem do realizacji dyspozycji z przepisu art. 161 ust. 1 in fine ustawy Prawo telekomunikacyjne.

Problem wydaje się jednak być związany z interpretacją wynikających z ww. przepisów norm prawnych, co jednakże może oznaczać, iż niedopełniają one zasad techniki prawodawczej. Ustawa powinna wyczerpująco regulować daną dziedzinę spraw, nie pozostawiając poza zakresem swego unormowania istotnych fragmentów tej dziedziny, zaś przepis prawa materialnego powinien możliwie bezpośrednio i wyraźnie wskazywać kto, w jakich okolicznościach i jak powinien się zachować, natomiast wyjątkowo wskazywać tylko zachowanie nakazywane albo zakazywane jego adresatowi, jeżeli adresat lub okoliczności tego nakazu albo zakazu są wskazane w sposób niewątpliwy w innej ustawie (§ 3 i 25 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" [Dz. U. Nr 100, poz. 908]).

Problem ten wydaje się dotyczyć w szczególności braku unormowań przepisów ustawy o strażach gminnych podobnych do postanowień art. 20c ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity: Dz. U. 2015 r. poz. 355 ze zm.), czy art. 10b ustawy z dnia 12 października 1990 r. o Straży Granicznej (tekst jednolity: Dz. U. 2014 r. poz. 1402 ze zm.), które to przepisy określają zasady i tryb udostępniania danych, przy czym, pożądane zmiany przepisów ustawy o strażach gminnych powinny uwzględnić potrzebę przetwarzania przez straże gminne ograniczonego katalogu danych objętych tajemnicą telekomunikacyjną. Katalog ten mógłby obejmować dane identyfikujące użytkownika sieci telekomunikacyjnej w zakresie jego imienia i nazwiska, adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania, ewentualnie nazwy firmy i siedziby prowadzenia działalności.

Zgodnie z brzmieniem art. 1 ust. 1 ustawy o ochronie danych osobowych, każdy ma prawo do ochrony dotyczących go danych osobowych. W myśl zaś art. 1 ust 2 ustawy, przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane

dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą. Oznacza to, iż w przypadku zaistnienia uzasadnionej okoliczności (przesłanki legalności), racjonalny ustawodawca dopuszcza przetwarzanie danych osobowych, także objętych tajemnicą prawnie chronioną, w celu innym, niż zostały zebrane. Przetwarzaniem danych osobowych – w myśl art. 7 pkt 2 ustawy o ochronie danych osobowych – jest m.in. ich zbieranie. W doktrynie podkreśla się, iż cyt.: „(...) wytyczając reguły ochrony danych osobowych, należy uważać, aby nie przekroczyć granicy, za którą trafne i szlachetne zamiary oraz założenia zaczynają już wywoływać negatywne skutki. Ma to miejsce na przykład wówczas, gdy zbyt rygorystyczne ograniczenia w pozyskiwaniu i gromadzeniu informacji (danych osobowych) przeszkadzają w należytym zapewnieniu porządku i bezpieczeństwa" (tak: J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych Komentarz, 4 wydanie, Kraków 2007, str. 303-304).

Przytoczyć należy w tym miejscu także wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 12 maja 2008 r. (sygn. II SA/Wa 229/2008), w którym WSA orzekł, iż cyt.: „Z art. 1 ust. 2 ustawy o ochronie danych osobowych wynika, iż przysługujące każdemu prawo do ochrony dotyczących go danych osobowych nie ma charakteru absolutnego, bowiem przetwarzanie danych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą lub dobro osób trzecich w zakresie i trybie określonym ustawą". Z powyższego wyroku wynika, iż prawo do ochrony danych osobowych nie może pozostawać w oderwaniu od innych przepisów prawa, i czynników, które należy mieć na względzie bez zakładania a priori, iż prawo do ochrony danych osobowych, będzie zawsze prawem nadrzędnym.

Uwzględniając powyższe, zasadnym jest zasygnalizowanie celowości podjęcia procesu legislacyjnego w tej sprawie.

Stosownie do art. 19a ust. 3 ustawy o ochronie danych osobowych uprzejmie proszę o ustosunkowanie się do niniejszego wystąpienia **w terminie 30** dni od dnia jego otrzymania.

Informuję przy tym, że treść niniejszego wystąpienia wraz z udzieloną odpowiedzią opublikowana będzie na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.