GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 18 lutego 2013 r.

DOLiS/DEC-168/13
dot. […]

DECYZJA

Na podstawie art. 104 § l ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2, art. 18 ust. 1 pkt 2, art. 22, art. 23 ust. 1 pkt 2 i 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze późn. zm.), art. 56 ust. 2 w zw. z art. 54 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2008 r. Nr 133, poz. 848 z późn. zm.), art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 1997 r. Nr 123, poz. 779 z późn. zm.) oraz art. 161 w zw. z art. 159 ust. 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie odmowy udostępnienia Komendantowi Straży Miejskiej w R., z siedzibą w […], przez T. S. A., z siedzibą […], danych osobowych abonenta usług telekomunikacyjnych świadczonych na jego rzecz przez T. S. A., tj. użytkownika numeru telefonu: […], w zakresie jego imienia, nazwiska oraz adresu zamieszkania,

nakazuję T. S. A., z siedzibą w […], udostępnienie Komendantowi Straży Miejskiej w R., z siedzibą w […], danych osobowych użytkownika numeru telefonu: […], w zakresie jego imienia, nazwiska oraz adresu siedziby prowadzonej przez niego działalności gospodarczej.

Uzasadnienie

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek Komendanta Straży Miejskiej w R., z siedzibą w […], o nakazanie T. S. A., z siedzibą w […], udostępnienia danych osobowych abonenta usług telekomunikacyjnych świadczonych przez Spółkę, tj. użytkownika numeru telefonu: […] w zakresie jego imienia, nazwiska oraz adresu zamieszkania.

W treści skargi podniesiono, iż do Straży Miejskiej skierowany został wniosek […] Spółdzielni Mieszkaniowej […] z siedzibą w […], o ściganie osób rozklejających ogłoszenia o treści cyt.: „Chwilówki

Kredyty Płatne natychmiast....., tel. […]" na klatkach schodowych w administrowanych przez ww. spółdzielnię budynkach, położonych w […], bez zgody ich administratora.

Wobec okoliczności, iż podjęte przez Straż Miejską czynności nie doprowadziły do ustalenia osób odpowiedzialnych za powyższe działanie, Komendant Straży Miejskiej zwrócił się do Spółki o cyt.: „udzielenie informacji o danych osobowych (imię, nazwisko, adres zamieszkania) abonenta telefonu nr […]. Uzyskanie danych osobowych abonenta ww. nr telefonu jest niezbędne do ustalenia sprawcy wykroczenia z art. 63a kw, dokonanego na terenie miasta R., a polegającego na umieszczaniu ogłoszeń reklamowych w miejscach do tego nie przeznaczonych, bez zgody zarządzającego tymi miejscami. Czynności te są niezbędne do wykonania określonych prawem zadań realizowanych przez Straż Miejską".

W odpowiedzi na ww. wniosek Spółka w piśmie z dnia […] kwietnia 2012 r. odmówiła udzielenia Komendantowi Straży Miejskiej przedmiotowych informacji wskazując, iż cyt.: „(...) dane dotyczące użytkownika sieci telekomunikacyjnej stanowią tajemnicę telekomunikacyjną (art. 159 ust. 1 pkt 1 ustawy Prawo Telekomunikacyjne), a jej ujawnienie (art. 159 ust 3) narusza obowiązek zachowania tajemnicy telekomunikacyjnej. W myśl art. 159 ust 4 dane objęte tajemnicą telekomunikacyjną mogą być ujawnione na podstawie postanowienia sądu, prokuratury lub innych służb uprawnionych na podstawie odrębnych przepisów". W rzeczonym piśmie Spółka nie wyjaśniła Komendantowi Straży Miejskiej, że abonentem ww. numeru telefonu nie jest osoba fizyczna tylko przedsiębiorca, informując natomiast, iż cyt.: „ (...) dane klienta (imię, nazwisko, adres zamieszkania itp...) są chronione nie tylko Ustawą o Ochronie Danych Osobowych, ale są enumeratywnie wymienione w rozdziale VII Prawa telekomunikacyjnego, który to bezwzględnie zabrania ujawniania tych danych w inny sposób niż zapisany w Prawie telekomunikacyjnym (Art. 159 pkt 3)".

W toku przeprowadzonego w niniejszej sprawie postępowania administracyjnego Generalny Inspektor Ochrony Danych Osobowych otrzymał pisemne wyjaśnienia Spółki, w których podniesiono, iż Spółka przetwarza dane osobowe użytkownika numeru telefonu […] w zakresie cyt.: nazwa przedsiębiorcy, adres siedziby przedsiębiorcy, adres do korespondencji, numer telefonu, numer telefonu kontaktowego, numer identyfikacji podatkowej NIP, REGON przedsiębiorcy". Spółka wyjaśniła ponadto, że odmówiła udostępnienia żądanych przez Straż Miejską informacji na podstawie art. 159 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800 z późn. zm.), zwanej dalej Prawem telekomunikacyjnym.

Wobec powyższego Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje.

Przedmiotem niniejszego postępowania Komendant Straży Miejskiej uczynił zarzut nieudostępnienia przez Spółkę informacji identyfikujących abonenta numeru telefonu […]. Rzeczone informacje, jak wskazał Komendant Straży Miejskiej we wniosku do Spółki, jak i w skardze inicjującej niniejsze postępowanie, są niezbędne dla zrealizowania przez ten podmiot uprawnień i obowiązków nałożonych przepisami prawa.

Wobec powyższego wskazać należy, że zgodnie z brzmieniem art. 1 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), każdy ma prawo do ochrony dotyczących go danych osobowych. W myśl zaś art. 1 ustęp 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. Przepis ten wskazuje, iż od generalnej zasady prawa do ochrony danych osobowych istnieją wyjątki. Oznacza to, iż w przypadku zaistnienia uzasadnionej okoliczności (przesłanki) racjonalny ustawodawca dopuszcza przetwarzanie danych osobowych. 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). Nie jest dopuszczalne działanie, które zmierza do utrudniania realizowania przez właściwe organy obowiązków wynikających z przepisów prawa, zwłaszcza, gdy organy te strzegą porządku publicznego i egzekwują postanowienia przepisów prawa w granicach przyznanych im kompetencji. Celem egzekwowania prawa jest nałożenie sankcji karnej na osobę, która łamie przepisy, poprzez efektywne zebranie niezbędnych informacji zmierzających do ukarania sprawcy.

Przytoczyć należy w tym miejscu 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.

Wprawdzie z art. 5 ustawy o ochronie danych osobowych wynika, iż jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw, zaś zadaniem Generalnego Inspektora Ochrony Danych Osobowych jest czuwanie nad prawidłowym przestrzeganiem przepisów z zakresu ochrony danych osobowych, czyli nad ochroną i zabezpieczeniem danych osobowych, to jednak wskazać należy, iż ww. przepis nie stanowi absolutnie wykluczenia stosowania przepisów ustawy o ochronie danych osobowych, zaś działania organu do spraw ochrony danych osobowych nie mogą zmierzać do ochrony osób (podmiotów), które nie przestrzegają przepisów prawa i porządku publicznego. Powyższe jest tym bardziej zasadne, gdy organ powołany do strzeżenia porządku publicznego legitymuje się przesłanką dla przetwarzania danych osobowych. Podstawę do zgodnego z prawem przetwarzania danych osobowych daje spełnienie jednej z przesłanek określonych w art. 23 ust. 1 pkt 1 – 5 ustawy o ochronie danych osobowych. Udostępnienie danych osobowych przez administratora tych danych jest dopuszczalne m.in. gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych), bądź gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego (art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych).

Zgodnie z art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego, zakazane jest zapoznawanie się, utrwalanie, przechowywanie, przekazywanie lub inne wykorzystywanie treści lub danych objętych tajemnicą telekomunikacyjną przez osoby inne niż nadawca i odbiorca komunikatu, chyba że będzie to konieczne z innych powodów przewidzianych ustawą lub przepisami odrębnymi. Art. 159 ust. 4 Prawa telekomunikacyjnego stanowi, iż przepisów ust. 2 i 3 nie stosuje się do komunikatów i danych ze swojej istoty jawnych, z przeznaczenia publicznych lub ujawnionych postanowieniem sądu, postanowieniem prokuratora lub na podstawie odrębnych przepisów. W myśl art. 161 ust. 1 ustawy Prawo telekomunikacyjne, z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem", dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.

Powyższe przepisy prawa wskazują na możliwość udostępnienia danych objętych tajemnicą telekomunikacyjną, gdy stanowią tak przepisy odrębne, bądź – co nie budzi wątpliwości – gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego, o czym stanowi art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

Zgodnie z art. 10 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z1997 r. Nr 123, poz. 779 z późn. zm.), 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.

Straż Miejska jest jednym z oskarżycieli publicznych w myśl art. 17 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2008 r. Nr 133, poz. 848 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 Miejską zadań nałożonych na nią ustawowo wymaga wykorzystywania informacji o osobach, których działania te dotyczą. Przepisy ustawy o strażach gminnych wprost stanowią o prawie Straży Miejskiej do przetwarzania danych w związku z realizacją określonych prawem zadań, bez konieczności uzyskania na to zgody osoby, której dane dotyczą. Oznacza to, iż Straż Miejska, 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 Miejską nad przestrzeganiem prawa przez obywateli – udostępnić informacje w zakresie wnioskowanym przez Straż Miejską. W takiej sytuacji dochodzi bowiem do realizacji dyspozycji

z przepisu art. 161 ust. 1 in fine ustawy Prawo telekomunikacyjne. Spółka odrzuciła wniosek Straży Miejskiej, wskazując na fakt, iż żądane dane objęte są tajemnicą telekomunikacyjną (art. 159 ustawy Prawo telekomunikacyjne). Spółka nie podjęła zatem działań zmierzających do rozważenia zasadności wniosku Straży Miejskiej, w kontekście art. 161 ust. 2 ustawy Prawo telekomunikacyjne oraz art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, odrzucając jej wniosek a priori.

Straż Miejska posiada podstawę prawną do pozyskania danych osobowych na mocy ww. przepisów prawa, tj. art. 161 ust. 2 Prawa telekomunikacyjnego, art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, jak również na mocy art. 23 ust. 1 pkt 4 ustawy o ochronie danych osobowych.

W przedmiotowej sprawie Straż Miejska wykonuje zadania w zakresie ochrony porządku publicznego. Do wypełnienia zadania realizowanego dla dobra publicznego niezbędne jest ustalenie sprawcy wykroczenia,

a następnie skierowania do sądu wniosku o ukaranie. Dobro publiczne jest wartością, którą Spółka powinna wziąć pod uwagę w kontekście realizacji obowiązku ochrony danych abonenta na gruncie przepisów ustawy Prawo telekomunikacyjne i wyważyć wyższość dobra publicznego nad prawem jednostki do decydowania o sposobie przetwarzania jej danych osobowych. Pogląd taki zaprezentował także Naczelny Sąd Administracyjny, który w wyroku z dnia 28 stycznia 2003 r. (sygn. akt: II SA 2210/01) orzekł, iż cyt.: „system ochrony danych osobowych tworzą powiązane ze sobą rozwiązania w sposób uwzględniający hierarchię chronionych dóbr i wartości. Wyrazem tego jest m.in. art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych, dopuszczający przetwarzanie danych, gdy na to zezwalają przepisy prawa i gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Podobnie art. 69 ust. 1 Prawa telekomunikacyjnego [obecnie art. 161 ust. 1 ustawy Prawo telekomunikacyjne] zezwala na przetwarzanie danych objętych tajemnicą telekomunikacyjną również w innych celach niż świadczenie usług abonenckich, gdy jest dopuszczalne na podstawie przepisów ustawowych. Łącznie z (...) treścią art. 10 ust. 1 ustawy o strażach gminnych i art. 19 § 1 kpw [obecnie art. 54 ust. 1 oraz art. 56 ust 2 ustawy Kodeks postępowania w sprawach o wykroczenia] powstaje z tych przepisów uprawnienie straży do żądania udostępnienia jej danych osobowych pozostających w dyspozycji ich administratora, gdy jest stosownie uzasadnione okolicznościami sprawy”.

W tym stanie faktycznym i prawnym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), art. 129 § 2 w zw. z art. 127 § 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.), strona niezadowolona z niniejszej decyzji, w terminie 14 dni od dnia jej doręczenia, może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy.