GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 12 lutego 2013 r.

DOLiS/DEC – 133/13
dot. […]

D E C Y Z J A

Na podstawie art. 138 § l pkt 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 ze 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 zm.), art. 56 § 2 w zw. z art. 54 § 1 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2008 r. Nr 133, poz. 848 ze zm.), art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 1997 r. Nr 123, poz. 779 ze zm.) oraz art. 161 ust. 1 w zw. z art. 159 ust. 2 pkt 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 r. Nr 171, poz. 1800 ze zm.), po przeprowadzeniu postępowania administracyjnego w sprawie z wniosku P. Sp. z o.o., z siedzibą w W., o ponowne rozpatrzenie sprawy dotyczącej odmowy udostępnienia Straży Miejskiej, z siedzibą w J., przez P. Sp. z o.o. danych osobowych abonenta telefonu komórkowego, użytkowanego w sieci P. Sp. z o.o. o numerze telefonu […], rozstrzygniętej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 25 października 2012 r. (znak: DOLiS/DEC – 1054/12/65245,65247),

1) **uchylam zaskarżoną decyzję w całości,**
2) **nakazuję P. Sp. z o.o., z siedzibą w W., udostępnienie Komendantowi Straży Miejskiej, z siedzibą w J., danych osobowych abonenta telefonu komórkowego o numerze telefonu […], użytkowanego w sieci P. Sp. z o.o. w zakresie jego imienia, nazwiska oraz adresu zamieszkania.**

Uzasadnienie

W dniu […] czerwca 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga Pana A. Z. – Komendanta Straży Miejskiej, z siedzibą w J., dalej jako Straż Miejska, na odmowę udostępnienia Straży Miejskiej przez P. S.A. (obecnie P. Sp. z o.o.), z siedzibą w W., dalej jako Spółka, danych osobowych abonenta telefonu komórkowego o numerze telefonu

[…]. Komendant w skardze wskazał, iż Straż Miejska cyt.: „(…) prowadzi postępowanie wyjaśniające w sprawie o wykroczenia z art. 63a § 1 kodeksu wykroczeń, przeciwko domniemanemu sprawcy, który w dniu […] stycznia 2012 r. w J. umieścił w miejscu publicznym do tego nieprzeznaczonym ogłoszenia (…)". Komendant podkreślił w skardze, iż udostępnienie danych osobowych abonenta telefonu komórkowego o numerze […] jest niezbędne dla zrealizowania obowiązków nałożonych na Straż Miejską przez przepisy ustawy o strażach gminnych oraz ustawy Kodeks postępowania w sprawach o wykroczenia oraz zwrócił uwagę, iż cyt.: „(…) operator jest jedynym podmiotem, od którego Straż Miejska może uzyskać pełne dane tej osoby (…)". Komendant zaznaczył w skardze, iż „Straż Miejska zwróciła się [do Spółki] z wnioskiem nr […] o udostępnienie danych osobowych w zakresie imienia i nazwiska oraz adresu zamieszkania abonenta telefonu powołując za podstawę prawną art. 161 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (...), art. 23 ust. 1 pkt 2 i 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (...) oraz art. 12 ust. 1 pkt 5 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (...)".

W odpowiedzi na wniosek Straży Miejskiej, Spółka w piśmie z dnia […] marca 2012 r. wskazała, iż cyt.: „(…) w świetle art. 159 ustawy (...) Prawo telekomunikacyjne (...) dane (...) są objęte tajemnicą telekomunikacyjną (…)". Ponadto, Spółka wskazała, że cyt.: „(…) przestrzeganie tajemnicy telekomunikacyjnej jest podyktowane troską o zapewnienie pełnej realizacji konstytucyjnego prawa wolności i ochrony tajemnicy komunikowania się, o czym stanowi art. 49 Konstytucji (…)". Spółka podkreśliła, iż cyt.: „(…) obowiązek zachowania tajemnicy telekomunikacyjnej wynika nie tylko z naszych przepisów krajowych, ale ma również swoje oparcie w postanowieniach prawa europejskiego, które z dniem akcesji Polski do Unii Europejskiej stało się częścią naszego systemu prawnego (…)". Spółka zaznaczyła, że cyt.: „(…) ujawnienie danych objętych tajemnicą telekomunikacyjną jest możliwe, ale jedynie przy ścisłym zachowaniu szczególnej procedury zwolnienia P. S.A. z ustawowego obowiązku zachowaniu [zachowania] tej tajemnicy (…)".

Wobec powyższego, Komendant wniósł do Generalnego Inspektora Ochrony Danych Osobowych o cyt.: „(…) nakazanie operatorowi telefonicznemu P. S.A. (...) udostępnienie Komendantowi Straży Miejskiej w J., danych osobowych abonenta telefonów [telefonu] komórkowych [komórkowego] o numerze […], w zakresie imienia, nazwiska oraz adresu zamieszkania, ze zbiorów danych abonentów operatora telefonicznego (…)".

W toku przeprowadzonego w niniejszej sprawie postępowania administracyjnego Generalny Inspektor Ochrony Danych Osobowych otrzymał pisemne wyjaśnienia Spółki (pismo z dnia […] lipca 2012 r. oraz pismo z dnia […] sierpnia 2012 r.), z których wynika, iż Spółka przetwarza dane osobowe użytkownika numeru telefonu komórkowego […] na podstawie umowy o świadczenie usług telekomunikacyjnych w sieci P. zawartej w dniu […] listopada 2010 r. m. in. w zakresie imienia i nazwiska, imion rodziców, daty urodzenia, adresu zamieszkania oraz numeru ewidencyjnego PESEL.

Na podstawie tak ustalonego stanu faktycznego Generalny Inspektor Ochrony Danych Osobowych w dniu 25 października 2012 r. wydał decyzję administracyjną (znak: DOLiS/DEC – 1054/12/65245,65247), mocą której nakazał P. S.A. udostępnienie Komendantowi Straży Miejskiej

danych osobowych abonenta telefonu komórkowego o numerze telefonu […], użytkowanego w sieci P. S.A., w zakresie jego imienia, nazwiska oraz adresu zamieszkania.

Następnie w dniu […] listopada 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych, w terminie, wpłynęło pismo Spółki z dnia […] listopada 2012 r. stanowiące wniosek o ponowne rozpatrzenie przedmiotowej sprawy. W treści ww. wniosku Spółka wniosła o cyt.: „(…) uchylenie zaskarżonej decyzji w całości oraz orzeczenie przez Generalnego Inspektora odmowy uwzględnienia wniosku Komendanta Straży Miejskiej w J., poprzez uchylenie decyzji i umorzenie postępowania (…)". W uzasadnieniu ww. wniosku Spółka podniosła w szczególności, iż cyt.: „(…) w przedmiotowej decyzji został wskazany podmiot, który już nie istnieje. Tę wadę można uznać za wadę, która w przyszłości może skutkować uznaniem decyzji za nieważną (…)". Jednocześnie Spółka wskazała cyt. „(…) w związku z postanowieniem Sądu Rejonowego w W. […] z dnia […] maja 2012 r. nastąpiło przekształcenie P. S.A. w P. Sp. z o.o., tym samym, zgodnie z art. 533 ksh P. Sp. z o.o. przysługują wszelkie dotychczasowe prawa i obowiązki P. S.A. W związku z powyższym P. S.A. zarówno w dacie składania skargi przez Komendanta Straży Miejskiej w J., jak i dacie wydawania decyzji, nie istniała (…) zatem nie mogła mieć zdolności bycia stroną przedmiotowego postępowania (…)". Ponadto Spółka podniosła, że stroną niniejszego postępowania powinna być również osoba, której dane są przedmiotem rozstrzygnięcia, tj. ww. abonent Spółki. W ocenie Spółki ww. decyzja narusza art. 159 ust. 2 pkt 4, art. 159 ust. 3, art. 159 ust. 4, art. 160 ust. 1, art. 161 ust. 1 i 2, art. 162 ust. 1, art. 180d ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 r. Nr 171, poz. 1800 ze zm.), bowiem z ww. przepisów wynika, iż dane pozostające w związku z porozumiewaniem się w ramach telekomunikacji (w tym dane osobowe użytkowników) są objęte tajemnicą telekomunikacyjną, a przedsiębiorca telekomunikacyjny oraz osoby działające w jego imieniu są obowiązani do przestrzegania tajemnicy telekomunikacyjnej pod sankcją kary pieniężnej, i co za tym idzie, jest w każdym przypadku udostępnienia treści i danych objętych ww. tajemnicą, zobowiązany do weryfikacji czy istnieje ustawowa podstawa prawna do jej ograniczenia. Ponadto Spółka podniosła, iż przepis art. 161 ust. 1 Prawa telekomunikacyjnego nie stanowi samoistnej podstawy udostępniania osobom trzecim danych osobowych. Wskazała również na przepis art. 159 ust. 3 Prawa telekomunikacyjnego, stwierdzając, że brak jest w nowym prawie telekomunikacyjnym przepisów, które wprost uchylałyby tajemnicę telekomunikacyjną, zezwalając na przekazywanie danych nią objętych służbom powołanym do ochrony porządku i bezpieczeństwa (do których zaliczyć należy straże gminne), tym bardziej brak jest przepisu, który nakazywałby przedsiębiorcy telekomunikacyjnemu tego rodzaju działanie. Spółka zarzuciła również, iż został przez organ całkowicie pominięty przepis art. 180d Prawa telekomunikacyjnego, który stanowi, iż obowiązek udostępniania ww. informacji dotyczy ograniczonego kręgu podmiotów, którymi są podmioty wskazane enumeratywnie w art. 179 ust. 3 pkt 1 Prawa telekomunikacyjnego, a samo udostępnianie danych realizowane jest na podstawie odrębnych procedur, których brak w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), zwanej dalej ustawą, i ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 1997 r. Nr 123, poz. 779 ze zm.). W związku z powyższym w ocenie Spółki Generalny Inspektor Ochrony Danych Osobowych naruszył tym samym art. 5 ustawy. Zdaniem Spółki w zakresie udostępniania danych objętych tajemnicą telekomunikacyjną powinny mieć zastosowanie wyżej powołane przepisy Prawa

telekomunikacyjnego jako przewidujące dalej idącą ochronę praw jednostki. Przepisy ustawy nie mogą być traktowane jako „przepisy odrębne", o których mowa w art. 159 ust. 4 Prawa telekomunikacyjnego, czy „przepisy ustawowe", o których mowa w art. 161 ust. 1 zd. 2 Prawa telekomunikacyjnego. Zdaniem Spółki art. 159 i n. oraz 180d Prawa telekomunikacyjnego wyłączają stosowanie ustawy w zakresie udostępniania informacji podmiotom wyraźnie w Prawie telekomunikacyjnym lub przepisach odrębnych niewskazanych, ponieważ przewidują dalej idącą ochronę, a tym samym wyłączają możliwość stosowania w tym zakresie art. 23 ust. 1 pkt 2 i 4 ustawy jako podstawy wydania decyzji. W tym miejscu Spółka powołała się na wyrok Naczelnego Sądu Administracyjnego z dnia 6 stycznia 2009 r. (sygn. akt I OSK 174/08), który dokonał takiej samej wykładni, a także na uzasadnienie postanowienia Naczelnego Sądu Administracyjnego z dnia 15 lipca 2010 r. (sygn. akt I OSK 1079/10). Ponadto Spółka zarzuciła Generalnemu Inspektorowi Ochrony Danych Osobowych naruszenie art. 10a ustawy o strażach gminnych oraz art. 54 § 1 w zw. z art. 56 § 2 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. 2008 r. Nr 133, poz. 848 ze zm.), bowiem przepisy te nie zawierają przepisów, które uchylałyby tajemnicę telekomunikacyjną i zezwalałyby przedsiębiorcy telekomunikacyjnemu na udostępnienie straży gminnej danych osobowych abonenta. Dlatego brak było podstaw, by w oparciu o powyższe przepisy ustalić, że przedsiębiorca telekomunikacyjny ma obowiązek przekazania straży gminnej informacji dotyczących abonenta. W ocenie Spółki nakaz podejmowania straży gminnej czynności wyjaśniających wynikający z tych przepisów jest skierowany do straży, natomiast brak jest przepisu, który nakazywałby podmiotom prywatnym współdziałanie ze strażą gminną w dokonywaniu czynności wyjaśniających. Z przepisu nakładającego na straż gminną obowiązek zebrania danych niezbędnych do sporządzenia wniosku o ukaranie nie można wywodzić wniosku o istnieniu obowiązku osób trzecich do przekazywania tych danych, bowiem żaden przepis prawa nie nakłada na podmiot prywatny obowiązku współdziałania ze strażami gminnymi w ustalaniu i wykrywaniu sprawców wykroczeń, a ponadto przepisy dotyczące przetwarzania danych osobowych przez straż gminną nie mogą być interpretowane jako źródło obowiązku osób trzecich do udostępniania danych osobowych tym strażom. Tym samym organ naruszył art. 1, 2, 23 ust. 1 pkt 2 i 4 ustawy, bowiem brak jest przepisu, który nakładałby na przedsiębiorcę telekomunikacyjnego obowiązek przekazania danych abonenta na rzecz straży gminnej, natomiast Spółka nie wykonuje zadań publicznych ani też nie jest zobowiązana do współdziałania ze służbami powołanymi do ochrony porządku i bezpieczeństwa. Dodatkowo Spółka podniosła, iż interpretacja przepisów dokonana przez organ prowadzi do wniosku, iż straż gminna, choć uprawniona jest jedynie do niektórych czynności w ramach postępowania w sprawach o wykroczenia, to uzyskuje – w sferze dostępu do danych objętych tajemnicą telekomunikacyjną – szersze uprawnienia aniżeli policja czy inne służby powołane do wykonywania czynności w postępowaniach dotyczących przestępstw. W tym miejscu Spółka powołała wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 10 października 2006 r. (sygn. akt II SA/Wa 642/05). Na koniec Spółka podniosła naruszenie przez organ art. 12 pkt 2 i art. 18 ust. 1 pkt 2 ustawy, gdyż w jej ocenie nie naruszyła przepisów ustawy, stąd brak było podstaw do wydania przez organ decyzji.

Po ponownym rozpatrzeniu niniejszej sprawy, Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje.

Na wstępie odnosząc się do zarzutów Spółki dotyczących tego, że w zaskarżonej ww. decyzji został wskazany podmiot, który już nie istnieje, wskazać należy, iż istotnie Spółka aktualnie działa jako spółka z ograniczoną odpowiedzialnością i powstała w wyniku przekształcenia „P." spółki akcyjnej z siedzibą w W. w spółkę z ograniczoną odpowiedzialnością, zgodnie z uchwałą nr […] Nadzwyczajnego Walnego Zgromadzenia spółki P. S.A. z dnia […] kwietnia 2012 r., zaprotokołowaną przez notariusza w W. - D. W. (Rep. A nr […]).

Jednakże wskazać należy, iż mimo że w ww. decyzji Spółka została oznaczona jako funkcjonująca pod poprzednią formą prawną i ww. decyzję skierowano do P. S.A., to jednak zauważyć należy, iż P. Sp. z o.o. w toku całego postępowania przeprowadzonego przez organ w niniejszej sprawie, począwszy od wystąpienia do niej przez organ z pismem o złożenie wyjaśnień, aż do momentu skierowania do niej przedmiotowej decyzji, nie zakwestionowała, że nie jest jej stroną niniejszego postępowania. Przeciwnie, Spółka ustosunkowała się do przesłanej jej ww. skargi Straży Miejskiej, złożyła wyjaśnienia, jak również przesłała pełnomocnictwo udzielone przez P. S.A. Panu Z. S., uznając tym samym kontynuację i ważność tego stosunku pełnomocnictwa, jak i przede wszystkim istnienie po jej stronie wszystkich praw i obowiązków, przysługujących uprzednio P. S.A. Poza tym zauważyć należy, iż w świetle art. 553 § 1 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (Nr 94, poz. 1037 ze zm.), zgodnie z którym spółce przekształconej przysługują wszystkie prawa i obowiązki spółki przekształcanej, P. Sp. o.o. stała się podmiotem praw i obowiązków przysługujących P. S.A., a zatem również powstałych na skutek skierowania do P. S.A. przez Straż Miejską ww. wniosku z dnia […] lutego 2012 r. o udostępnienie ww. danych osobowych ww. abonenta. Nie bez znaczenia pozostaje również fakt, iż Spółka nie zawiadomiła organu o dokonanym przekształceniu w spółkę z ograniczoną odpowiedzialnością, natomiast w toku postępowania wyjaśniającego, przez cały czas, konsekwentnie podejmowała korespondencję kierowaną do niej przez organ z użyciem poprzedniej formy prawnej i co więcej na nią odpowiadała, a zatem stwierdzić należy, iż Spółka poprzez te czynności sama uznawała się za jej adresata i stronę niniejszego postępowania. W kontekście powyższego tym bardziej niezrozumiałe są zarzuty Spółki w tym przedmiocie, zwłaszcza że sama z powołaniem się na wyżej wskazany art. 533 § 1 Kodeksu spółek handlowych, wskazała na kontynuację bytu prawnego P. S.A. wraz z jej prawami i obowiązkami.

W związku z powyższym, mimo iż w zaskarżonej decyzji użyto poprzedniej formy prawnej Spółki i uczyniono jej adresatem poprzednika prawnego Spółki, okoliczność ta w żadnym stopniu nie wpływa na ważność tejże decyzji. Jakkolwiek organ nie wiedząc, że doszło do przekształcenia strony, w treści decyzji nie uwzględnił tego, to jednak w wyniku przekształcenia nastąpiła sukcesja generalna i nie ma wątpliwości co do podmiotu będącego stroną postępowania. Nie ma zatem stanu niepewności co do sytuacji prawnej Spółki. Brak jest tym samym podstaw do stwierdzenia nieważności ww. decyzji, jak sugerowała Spółka. Podobny pogląd odnośnie ww. kwestii zaprezentował Naczelny Sąd Administracyjny w wyroku z dnia 23 kwietnia 2009 r. (sygn. akt I FSK 184/08).

Jednakże rację należy przyznać Spółce o tyle, iż istotnie nakaz sformułowany w zaskarżonej decyzji pod jej adresem, sformułowany został przy użyciu jej poprzedniej formy prawnej „spółka akcyjna", co może powodować trudności w jej wykonaniu, gdyż jak wskazano, podmiot P. S.A. został wykreślony z rejestru przedsiębiorców. Dlatego też zasadne jest uchylenie zaskarżonej decyzji w całości i sformułowanie nakazu z uwzględnieniem aktualnej formy prawnej Spółki.

Podkreślenia bowiem wymaga, iż w ocenie Generalnego Inspektora Ochrony Danych Osobowych wszelkie zarzuty Spółki dotyczące sformułowanego w ww. decyzji nakazu udostępnienia przez nią na rzecz Straży Miejskiej danych osobowych ww. abonenta, są bezzasadne. Tym samym organ podtrzymuje w całości stanowisko wyrażone w zaskarżonej ww. decyzji z dnia 25 października 2012 r. Wskazać jednocześnie należy, iż tożsame stanowisko do prezentowanego przez organ w niniejszym postępowaniu zostało zajęte przez Naczelny Sąd Administracyjny, w analogicznej sprawie, w wyroku z dnia 5 lutego 2008 r. (sygn. akt I OSK 37/07), mocą którego został uchylony wyrok Wojewódzkiego Sadu Administracyjnego (sygn. akt II SA/Wa 642/05), na który powołuje się Spółka.

W ww. wyroku Naczelny Sąd Administracyjny uznał, iż do udostępnienia Straży Miejskiej danych osobowych abonenta telefonu komórkowego powinny znaleźć zastosowanie przepisy art. 23 ust. 1 pkt 2 i 4 ustawy w zw. z art. 54 § 1 i art. 56 § 2 Kodeksu postępowania w sprawach o wykroczenia i art. 10a ustawy o strażach gminnych oraz art. 161 ust. 1 i art. 159 ust. 2 pkt 4 Prawa telekomunikacyjnego.

Powtórzyć zatem należy, iż zgodnie z brzmieniem art. 1 ust. 1 ustawy, każdy ma prawo do ochrony dotyczących go danych osobowych. Ustęp 2 stanowi zaś, iż 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 ponownie 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.

Należy ponadto wskazać, że organ powołany do strzeżenia porządku publicznego (jakim jest w niniejszym postępowaniu Straż Miejska) 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 ustawy Prawo telekomunikacyjne 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. 2 ustawy Prawo telekomunikacyjne, 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 ustawy Prawo telekomunikacyjne 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 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.

Straż Miejska jest jednym z oskarżycieli publicznych w myśl art. 17 Kodeksu postępowania w sprawach o wykroczenia, 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 Kodeksu postępowania w sprawach o wykroczenia). Zwrócić należy uwagę, iż w myśl art. 54 ust. 1 *in fine* Kodeksu 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. Przepisu 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. 2 *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) oraz podkreślając, iż ich ujawnienie jest możliwe jedynie przy zachowaniu procedury zwolnienia z tego obowiązku, wskazanej w treści art. 179 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*.

Wbrew zarzutom Spółki, Straż Miejska posiada podstawę prawną do pozyskania danych osobowych na mocy ww. przepisów, tj. art. 161 ust. 1 i art. 159 ust. 2 pkt 4 ustawy Prawo telekomunikacyjne, art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych w zw. z art. 54 § 1 i art. 56 § 2 Kodeksu postępowania w sprawach o wykroczenia.

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 winna 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 Administracyjnym 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 Kodeksu 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 (…)”.

Na koniec dodać należy, iż chybiony jest również zarzut pominięcia przez organ art. 180d Prawa telekomunikacyjnego, zgodnie z którym przedsiębiorcy telekomunikacyjni są obowiązani do

zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3-5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych. Jak wynika wprost z dyspozycji powyższego przepisu, przepis ten dotyczy zupełnie innej sytuacji niż mamy do czynienia w niniejszej sprawie, stąd też nie znajduje z oczywistych względów zastosowania w sprawie, więc odnoszenie się do niego byłoby niecelowe.

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

Decyzja jest ostateczna. Na podstawie art. 21 ust. 2 ustawy o ochronie danych osobowych i w zw. z art. 13 § 2, art. 53 § 1 i art. 54 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270 z późn. zm.), od niniejszej decyzji stronie przysługuje prawo wniesienia skargi do Wojewódzkiego Sądu Administracyjnego, w terminie 30 dni od dnia doręczenia niniejszej decyzji, za pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa).