GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa 26 kwietnia 2012 r.

DOLiS/DEC-373/12/27562,27570
dot. […]

D E C Y Z J A

Na podstawie art. 138 § 1 pkt 1 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, 18 ust. 1 pkt 2, art. 22 i 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 z 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.) oraz art. 161 ust. 1 w zw. z art. 159 ust. 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 odmowy udostępnienia Straży Miejskiej z siedzibą w J., przez A. S.A., danych osobowych abonenta telefonu komórkowego, użytkowanego w sieci A. S.A., o numerze telefonu […],

utrzymuję w mocy zaskarżoną decyzję.

Uzasadnienie

W dniu […] czerwca 2011 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęła skarga Komendanta Straży Miejskiej, zwanego dalej Komendantem, na odmowę udostępnienia Straży Miejskiej z siedzibą w J. przez A. S.A., zwana dalej Spółką, danych osobowych abonenta telefonu komórkowego o numerze telefonu […]. Komendant w skardze wskazał, iż Straż Miejska z siedzibą w J. „prowadzi postępowanie wyjaśniające w sprawie o wykroczenie z art. 63a ust. 1 kodeksu wykroczeń, przeciwko domniemanemu sprawcy, który w dniu […] lutego 2011 r. w J. umieścił w miejscu publicznym do tego nieprzeznaczonym ogłoszenie". Komendant podkreślił

w skardze, iż udostępnienie danych osobowych abonenta telefonu komórkowego o numerze […] jest niezbędne dla zrealizowania obowiązków nałożonych na Straż Miejską z siedzibą w J. przez przepisy ustawy o strażach gminnych oraz ustawy Kodeks postępowania w sprawach o wykroczenia oraz zwrócił uwagę, iż „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 […] kwietnia 2011 r. wskazała, iż „w świetle art. 159 ustawy (...) Prawo telekomunikacyjne (...) dane (...) są objęte tajemnicą telekomunikacyjną". Ponadto, Spółka wskazała, że „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 „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 „ujawnienie danych objętych tajemnicą telekomunikacyjną jest możliwe, ale jedynie przy ścisłym zachowaniu szczególnej procedury zwolnienia A. S.A. z ustawowego obowiązku zachowania tej tajemnicy".

Wobec powyższego, Komendant wniósł do Generalnego Inspektora Ochrony Danych Osobowych o „nakazanie operatorowi telekomunikacyjnemu A. S.A. (...) udostępnienie Komendantowi Straży Miejskiej w J. danych osobowych abonenta telefonu 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 dodatkowe pisemne wyjaśnienia od Pana P. W. – Administratora Bezpieczeństwa Informacji w Spółce (pismo z dnia […] sierpnia 2011 r.), z których wynika, iż Spółka przetwarza dane osobowe użytkownika numeru telefonu komórkowego [...] od dnia […] marca 2010 r. na skutek rejestracji przez użytkownika powołanego numeru telefonu karty prepaid za pośrednictwem eBOK. W wyniku tej czynności, za pośrednictwem formularza rejestracyjnego Spółka pozyskała dane osobowe w zakresie imienia i nazwiska, daty urodzenia, adresu zamieszkania, numeru dowodu osobistego. Z wyjaśnień Spółki wynika, iż dane osobowe są przetwarzane w celu świadczenia usług, sprzedaży produktów i usług oraz dla potrzeb działań marketingowych, na podstawie art. 23 ust. 1 pkt 1, 3 i 5 ustawy o ochronie danych osobowych.

W tym stanie faktycznym Generalny Inspektor Ochrony Danych Osobowych wydał decyzję administracyjną z dnia 23 grudnia 2011 r. (DOLiS/DEC-1088/11/63446,63448), mocą której nakazał A. S.A. udostępnienie Komendantowi Straży Miejskiej z siedzibą w J, danych osobowych abonenta

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

W ustawowym terminie A. S. A. złożyła wniosek o ponowne rozpatrzenie sprawy zakończonej ww. decyzją.

W uzasadnieniu wniosku Spółka wniosła o cyt.: „ponowne rozpatrzenie sprawy zakończonej wydaniem przez Generalnego Inspektora Ochrony Danych Osobowych decyzji z dnia 23 grudnia 2011 r., nakazującej A. S. A. udostępnienie Komendantowi Straży Miejskiej w J. danych osobowych abonenta A. S. A., w zakresie jego imienia, nazwiska oraz adresu zamieszkania".

Spółka zarzuciła Generalnemu Inspektorowi Ochrony Danych Osobowych naruszenie cyt.: „art. 159 ust. 3, art. 160 ust. 1, art. 161 ust. 1 oraz art. 162 ust. 1 w zw. z art. 180 d Prawa telekomunikacyjnego", „art. 10a ustawy o strażach gminnych oraz art. 54 § 1 w zw. z art. 56 § 2 kodeks psw" a także „art. 18 ust. 1 pkt 2 oraz art. 23 ust. 1 pkt 2 i 4 ustawy o ochronie danych osobowych w związku z naruszeniem przepisów Prawa telekomunikacyjnego i kodeksu psw". Uzasadniając ww. zarzuty Spółka wskazała w szczególności, iż w jej ocenie, z przepisów, na których oparł się Generalny Inspektor wydając zaskarżoną decyzję z dnia 23 grudnia 2011 r., nie można wywieźć podstawy do nakazania podmiotowi prywatnemu, jakim jest Spółka, udostępnienia na rzecz Straży Miejskiej informacji objętych tajemnicą telekomunikacyjną. W ocenie Spółki, okoliczność, iż Straż Miejska nie została wymieniona wśród podmiotów uprawnionych do udostępniania na ich rzecz tajemnicy telekomunikacyjnej, o których mowa w art. 179 ust 3 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 r. Nr 171, poz. 1800 ze zm.) przesądza o niemożności zobowiązania Spółki do udostępnienia na rzecz Straży Miejskiej wnioskowanych przez Straż danych.

Po powtórnym rozpatrzeniu zgromadzonego w sprawie materiału dowodowego i przeanalizowaniu wniosku o ponowne rozpatrzenie sprawy Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje.

Rozstrzygnięcie zawarte w zaskarżonej decyzji Generalnego Inspektora z dnia 23 grudnia 2011 r. (znak: DOLiS/DEC-1088/11/63446,63448) jest prawidłowe, a podnoszone we wniosku o ponowne rozpatrzenie sprawy zarzuty nie uzasadniają konieczności jego zmiany.

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.), zwanej dalej także ustawą, 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 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 (firm), które nie przestrzegają przepisów prawa i porządku publicznego. Przytoczyć w tym miejscu należy stanowisko Naczelnego Sądu Administracyjnego wyrażone w wyroku z dnia 5 lutego 2008 r. (I OSK 37/2007), w którym podkreślono, iż przepis art. 5 ustawy o ochronie danych osobowych cyt.: *„określa relacje między normami prawa wewnętrznego i statuuje zasadę rozstrzygania zbiegu norm na korzyść tych norm, które przewidują wyższy poziom ochrony. W polskim systemie prawa istnieje wiele przepisów odrębnych, które odnoszą się do szeroko rozumianego przetwarzania danych osobowych. Zaliczyć do nich w szczególności należy przepisy ustawy Prawo telekomunikacyjne, gdzie w art. 161 ust. 1 w zw. z art. 159 ust. 1 pkt 1 ustawodawca unormował problematykę przetwarzania danych osobowych użytkownika objętych tajemnicą telekomunikacyjną. Ustawa ta stanowi, że 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 (art. 161 ust. 1). Brzmienie zd. 2 ust. 1 art. 161 dowodzi, że przetwarzanie danych, stanowiących tajemnicę telekomunikacyjną, może się odbywać w oparciu o przesłanki określone w innych aktach prawnych rangi ustawowej. Odesłanie do przepisów*

ustawowych prowadzi, w ocenie Naczelnego Sądu Administracyjnego, do wniosku, iż w grę wchodzić tu będzie przede wszystkim regulacja przewidziana w ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych – art. 10a pkt 1 oraz w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych – art. 23 ust. 1 pkt 2 i 4. Istnienie w przepisach Prawa telekomunikacyjnego tego rodzaju odesłania, pozwala zatem podzielić pogląd Generalnego Inspektora Ochrony Danych Osobowych, że pomiędzy omawianymi tu ustawami nie zachodzi relacją wyłączania lecz uzupełniania".

W świetle powyższego wskazać należy, iż w niniejszej sprawie dla legalnego pozyskania ww. danych osobowych przez Straż Miejską od Spółki, koniecznym jest 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 ustawy Prawo telekomunikacyjne, 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.

Powtórzyć zatem należy argumentację zawartą w zaskarżonej decyzji z dnia 23 grudnia 2011 r., iż 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. Za niezasadny uznać zatem argument Spółki zaprezentowany we wniosku o ponowne rozpoznanie sprawy, iż nieuwzględnienie Straży Miejskiej w katalogu podmiotów określonych w przepisie art. 179 ust. 3 Prawa telekomunikacyjnego przesądza o niemożności zobowiązania Spółki do udostępnienia na rzecz Straży Miejskiej przedmiotowych danych.

Podkreślić należy, iż zgodnie z art. 10 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. 1997 r. Nr 123, poz. 779 ze 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.

Ponadto, 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. 2008 r. Nr 133, poz. 848 ze 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. 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 z siedzibą w J., 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 z siedzibą w J., 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*.

W ocenie organu ochrony danych osobowych Straż Miejska w J. posiada podstawę prawną do pozyskania danych osobowych na mocy ww. przepisów, tj. art. 161 ust. 2 ustawy Prawo telekomunikacyjne, 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 w J. 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 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 pt 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.

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 Warszawie, 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).