GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 16 grudnia 2011 r.

DIS/DEC- 1065/61961/11
dot. […]

D E C Y Z J A

Na podstawie art. 104 § 1 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 1, art. 22 w związku z art. 36 ust. 2 i art. 39 ust. 1 pkt 4 i art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz pkt II ust. 2a) i pkt IV ust. 2 części A załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Prezydenta Miasta L.,

nakazuję Prezydentowi Miasta L., usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. Zgłoszenie do rejestracji zbioru danych osobowych przetwarzanych w systemie informatycznym o nazwie „A", w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Uzupełnienie polityki bezpieczeństwa o następujące informacje dotyczące przetwarzania danych osobowych w systemie informatycznym o nazwie „A": wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych

pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych; **w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna**

3. Uzupełnienie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych o następujące informacje dotyczące przetwarzania danych osobowych w systemie informatycznym o nazwie „A": procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych, o których mowa powyżej; sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; sposób realizacji wymogu odnotowania przez systemy informatyczne informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępniania; procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

4. Zawarcie w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatorów użytkowników systemu informatycznego o nazwie „A", w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

5. Zapewnienie, aby w systemie informatycznym o nazwie „A" był rejestrowany odrębny identyfikator dla każdego użytkownika tego systemu, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

6. Zapewnienie, aby hasło użytkownika oraz administratora systemu informatycznego o nazwie „A" było zmieniane co 30 dni, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili u Prezydenta Miasta L. - Urzędzie Miasta L., zwanym dalej Urzędem, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych […], tj. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926

z późn. zm.), zwaną dalej ustawą, i rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), zwanym dalej rozporządzeniem. W toku kontroli odebrano od pracowników Urzędu ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Zastępcę Prezydenta Miasta L.

Na podstawie zgromadzonego podczas ww. kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Prezydent Miasta L., jako administrator danych, naruszył przepisy o ochronie danych osobowych, polegające na:

1. Niezgłoszeniu do rejestracji zbioru danych osobowych przetwarzanych w systemie informatycznym o nazwie „A" (art. 40 ustawy).
2. Niezawarciu w polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych informacji dotyczących przetwarzania danych w systemie informatycznym o nazwie „A", określonych w § 4 i § 5 rozporządzenia.
3. Niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatorów użytkowników systemu informatycznego o nazwie „A" (art. 39 ust. 1 pkt 4 ustawy).
4. Nierejestrowaniu w systemie informatycznym o nazwie „A" odrębnego identyfikatora dla każdego użytkownika tego systemu (częścią A pkt II ust. 2 załącznika do rozporządzenia).
5. Niezmienianiu hasła użytkownika oraz administratora systemu informatycznego o nazwie „A" (częścią A pkt IV ust. 2 załącznika do rozporządzenia).

W związku z powyższym, w dniu […] października 2011 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy.

W piśmie z dnia […] października 2011, sygn. […], stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Prezydent Miasta L. został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych w toku kontroli dowodów i materiałów oraz zgłoszonych żądań.

Pismem z dnia […] października 2011 r. (znak: […]) Prezydent Miasta L. zwrócił się z wnioskiem o przedłużenie terminu na złożenie wyjaśnień do dnia […] października 2011 r.

Pismem z dnia […] października 2011 r. (znak: […]) Prezydent Miasta L. wyjaśnił, iż w jego ocenie system informatyczny o nazwie „A" nie dokonuje identyfikacji osób fizycznych i nie przetwarza danych osobowych w rozumieniu art. 6 ustawy. Strona podnosi w szczególności, iż taką

daną osobową nie jest numer rejestracyjny pojazdu. W związku z tym, iż dostęp do danych zdaniem strony jest możliwy tylko według jednego kryterium, to jest kryterium czasu nagrania, dane zawarte w systemie informatycznym o nazwie „A" nie tworzą zbioru danych osobowych w rozumieniu art. 7 pkt 1 ustawy. Ponadto, jak twierdzi strona, nawet gdyby uznać, iż dane przetwarzane w tym systemie tworzą zbiór danych osobowych, to nie podlegałby on zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych na podstawie art. 43 ust. 1 pkt 2 ustawy, to jest dane w tym zbiorze są przetwarzane dla potrzeb postępowania sądowego.

Ponadto strona poinformowała, iż jeszcze w bieżącym roku w systemie informatycznym o nazwie „A" zostaną wprowadzone dla każdego użytkownika identyfikatory oraz hasła o długości minimum 6 znaków oraz że zmiana tych haseł będzie wymuszana co 30 dni. Wskazano również, iż operatorzy systemu logują się na jedno konto, jednakże ich identyfikacja następuje poprzez dokonanie zapisu w „Książce […]", przypisanej do stanowiska, prowadzonej przez każdego operatora oraz przez […] wewnętrzny pracy operatorów. Odnośnie uchybień dotyczących ewidencji osób upoważnionych do przetwarzania danych strona wskazała, iż spis identyfikatorów jest prowadzony w systemie informatycznym oraz załączono do pisma wydruk z ewidencji zawierających identyfikatory użytkowników.

Strona nie odniosła się natomiast do braku w dokumentacji dotyczącej przetwarzania danych osobowych, tj. polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych informacji dotyczących przetwarzania danych osobowych w systemie informatycznym o nazwie „A".

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy.

W myśl art. 6 ust. 1 ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zgodnie z ww. definicją dane osobowe mogą przybrać różną formę. Mogą to być np.: zdjęcia, filmy, zarejestrowane głosy pod warunkiem spełnienia dalszych wymogów zawartych w definicji z art. 6 ustawy. Każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu widzenia pojęcia danych osobowych i każda informacja może zostać uznana za informację o charakterze osobowym. Natomiast zgodnie z art. 6 ust. 2 ustawy, osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe,

ekonomiczne, kulturowe lub społeczne. Jednocześnie w myśl art. 6 ust. 3 ustawy, informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Biorąc pod uwagę powyższe, danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia. Poza zakresem przedmiotowej definicji znajdzie się zatem taka informacja, na podstawie której identyfikacja osoby wymagać będzie nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań.

Nie można zgodzić się z twierdzeniem strony, iż danymi osobowymi nie są informacje, których powiązanie z oznaczoną osobą nie jest łatwo osiągalne, w szczególności że numer rejestracyjny pojazdu nie jest taką daną.

Należy zauważyć, iż to, czy określona informacja stanowi daną osobową zależy od tego, czy podmiot dysponujący tą informacją (w przypadku uznania tej informacji za daną osobową, będący administratorem danych) jest w stanie zidentyfikować osobę, której dotyczy ta informacja, bez ponoszenia nadmiernych kosztów, czasu, działań. Tak więc będzie to zależeć od możliwości, jakimi dysponuje dany podmiot, w tym dostępem do innych informacji dotyczących danej osoby.

Należy wskazać, iż Straż Miejska w L. dysponując uprawnieniami wynikającymi z ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 ze zm.), w tym posiadając dostęp do Centralnej Ewidencji Pojazdów i Kierowców, będzie mogła ustalić tożsamość osoby, np. właściciela pojazdu, posiadając zarejestrowany wizerunek czy też numer rejestracyjny pojazdu, bez nadzwyczajnego wysiłku i nakładów.

Mając na uwadze powyższe należy uznać, iż na podstawie zarejestrowanych przez system informatyczny o nazwie „A" informacji w postaci wizerunku osób oraz numerów rejestracyjnych pojazdów, Straż Miejska Miasta L. będzie mogła identyfikować osoby, których dotyczą te informacje, a zatem informacje te należy uznać za dane osobowe w rozumieniu art. 6 ustawy.

Zgodnie natomiast z art. 7 pkt 1 ustawy zbiór danych jest to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

W toku kontroli ustalono, iż nagrania z […] zapisywane są na dyskach serwera […]. Wyszukiwanie określonego zdarzenia zarejestrowanego w systemie informatycznym o nazwie „A" odbywa się według czasu oraz miejsca zaistnienia tego zdarzenia. Należy podnieść, iż sposób zapisu danych na nośniku komputerowym oraz wbudowane w system procedury ich przetwarzania umożliwiają prawidłowe zestawienie ich struktury wtedy, kiedy to jest

potrzebne w czasie ich przetwarzania (np. wizerunek osoby naruszającej porządek publiczny). Innymi słowy kamery cyfrowe zlokalizowane w L. zostały połączone z systemem informatycznym umożliwiającym dokonanie analizy zarejestrowanych danych według określonych kryteriów.

Nie można zatem zgodzić się ze stanowiskiem strony, iż wyłącznym kryterium dostępu do obrazów zdarzeń zarejestrowanych w systemie informatycznym o nazwie „A." jest jedno kryterium, to jest kryterium czasu zarejestrowania obrazu.

Nie ma również podstaw, by zakładać, że dane osobowe mają być dostępne według kryteriów osobowych rozumianych jako zapewniające dostęp do danych identyfikujących (np. imię, nazwisko, adres, numery PESEL i NIP), gdyż ustawa o ochronie danych osobowych nie posługuje się takim pojęciem. W piśmiennictwie wskazuje się ponadto, że przyjęcie założenia o „osobowym charakterze kryteriów" umożliwiałoby obchodzenie ustawy i unikanie rejestracji zbiorów danych (por. G. Szpor: *Publicznoprawna ochrona danych osobowych*, PUG 1999, nr 12, s. 12).

Jak wskazał Naczelny Sąd Administracyjny w wyroku z dnia 7 maja 2011 r., sygn. akt I OSK 983/07, „z art. 7 ust. 1 ustawy nie wynika, że dane osobowe mają być w definiowanym tam „zbiorze danych" danymi podstawowymi. Nie wynika również, że kryterium dostępu do tych danych mają być dane identyfikacyjne (inne nazwisko, adres, PESEL). Byłoby sprzeczne z intencją ustawodawcy i gwarancjami konstytucyjnymi przyjęcie, że dane osobowe prowadzone i przechowywane w zbiorach tworzonych dla realizowania celów gospodarczych czy ochrony bezpieczeństwa, mają nie podlegać ochronie tylko dlatego, że nie są w tych zbiorach danymi podstawowymi".

Wobec powyższego uznać należy, iż system ten zawiera zestaw danych osobowych dostępnych według określonych kryteriów będący zbiorem danych osobowych w rozumieniu art. 7 pkt 1 ustawy.

Odnośnie natomiast stanowiska strony, iż niezbędne jest występowanie co najmniej dwóch kryteriów dostępu do danych, aby można było mówić o danych osobowych, to należy wskazać, że jest to pogląd dyskusyjny. Zasadnym jest zastosowanie w tym przypadku wykładni celowościowej. Pogląd taki znalazł również potwierdzenie w doktrynie: „Biorąc pod uwagę stanowisko Generalnego Inspektora, interpretacje przyjęte w polskiej doktrynie (...), a także cel i funkcje przepisów o ochronie danych osobowych przychylamy się do stanowiska, według którego wystarczy występowanie jednego kryterium wyszukiwawczego w zestawieniu danych, aby zaklasyfikować go jako zbiór danych w rozumieniu art. 7 pkt 1 ustawy" (J. Barta, R. Markiewicz, Ochrona danych osobowych. Komentarz, Zakamycze 2004, s. 399).

Nie zasługuje również na uwzględnienie twierdzenie strony, iż zbiór danych osobowych przetwarzanych w systemie informatycznym o nazwie „A" podlega zwolnieniu z obowiązku rejestracji na podstawie art. 43 ust. 1 pkt 2 ustawy, zgodnie z którym z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych przetwarzanych dla potrzeb postępowania sądowego, gdyż zgodnie z art. 11 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.) straży gminnej (miejskiej) przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych m.in. dla utrwalenia dowodów popełnienia wykroczenia. Zgodnie natomiast z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 2003 r. w sprawie wykroczeń, za które strażnicy straży gminnych są uprawnieni do nakładania grzywien w drodze mandatu karnego (Dz. U. Nr 208, poz. 2026 z późn. zm.), strażnicy Straży Miejskiej Miasta L. mogą nakładać, w przypadku stwierdzenia popełnienia określonych wykroczeń, grzywnę w formie mandatu karnego.

Stosownie do treści art. 97 § 1 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.), uprawniony funkcjonariusz publiczny może nałożyć grzywnę w drodze mandatu karnego m.in. wtedy, gdy stwierdzi popełnienie wykroczenia za pomocą przyrządu kontrolno-pomiarowego lub urządzenia rejestrującego, a sprawca nie został schwytany na gorącym uczynku lub bezpośrednio potem, i nie zachodzi wątpliwość co do sprawcy czynu - w tym także, w razie potrzeby, po przeprowadzeniu w niezbędnym zakresie czynności wyjaśniających, podjętych niezwłocznie po ujawnieniu wykroczenia.

Jak z powyższego wynika, w przypadku gdy w wyniku prowadzenia […] zostanie stwierdzone popełnienie wykroczenia, strażnik miejski może nałożyć grzywnę w drodze mandatu karnego. W przypadku, gdy sprawca wykroczenia przyjmie mandat, nie dojdzie do postępowania przed sądem. Tym samym należy uznać, iż w takich przypadkach dane nie są przetwarzane dla potrzeb postępowania sądowego, a więc nie ma tutaj zastosowania przesłanka określona w art. 43 ust. 1 pkt 2 ustawy. Na podstawie zebranego w toku niniejszego postępowania materiału dowodowego nie można również uznać, aby jakakolwiek inna przesłanka, określona w art. 43 ust. 1 ustawy, zwalniała stronę z obowiązku zgłoszenia zbioru danych osobowych przetwarzanych w systemie informatycznym o nazwie „A".

Reasumując, w systemie informatycznym o nazwie „A" przetwarzane są dane osobowe tworzące zestaw danych dostępnych według określonych kryteriów, a więc będący zbiorem danych osobowych podlegającym zgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Zgodnie z art. 36 ust. 2 ustawy, administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1. W myśl § 3 ust. 1 rozporządzenia, na dokumentację, o której mowa w § 1 pkt 1, składa się polityka

bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

Zgodnie z § 4 rozporządzenia polityka bezpieczeństwa zawiera: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zgodnie z § 5 rozporządzenia zawiera natomiast: procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych, o których mowa powyżej, sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia; sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W toku czynności kontrolnych ustalono, iż Zarządzeniem nr […] Prezydenta Miasta L. z dnia […] sierpnia 2010 r. w sprawie zasad przetwarzania danych osobowych w Urzędzie Miasta L. wprowadzono „Politykę bezpieczeństwa przetwarzania danych osobowych systemu informatycznego Urzędu Miasta L.”, „Instrukcję zarządzania systemem informatycznym Urzędu Miasta L.” oraz „Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych”.

Dokumenty, o których mowa powyżej nie zawierają informacji dotyczących przetwarzania danych osobowych w systemie informatycznym o nazwie „A”, określonych w § 4 i § 5 rozporządzenia.

Zgodnie z art. 39 ust. 1 pkt 3 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku kontroli jako ewidencję osób upoważnionych do przetwarzania danych osobowych podmiot kontrolowany przedstawił „Rejestr upoważnień wydanych pracownikom Urzędu Miejskiego w L. dot. ochrony danych osobowych" (prowadzony w latach od 1999 r. do 2003 r.) oraz prowadzony od 2004 r. „Rejestr użytkowników i uprawnień w systemie informatycznym". Oba rejestry są prowadzone w formie papierowej i nie zawierają identyfikatorów użytkowników.

W piśmie z dnia […] października 2011 r. Prezydenta Miasta L. (znak: […]) strona oświadczyła, iż ewidencję użytkowników zawierającą m.in. ich identyfikatory prowadzi w systemie informatycznym. Zaznaczyć należy, że skoro operatorzy systemu informatycznego o nazwie „A" logują się na jedno konto operatora to nie posiadają indywidualnych identyfikatorów, a co za tym idzie identyfikatory te nie mogą być do czasu ich nadania wpisane do prowadzonej ewidencji. W związku z tym należy uznać, iż ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona przez stronę nie zawiera identyfikatorów użytkowników systemu informatycznego o nazwie „A", a więc został naruszony art. 39 ust. 1 ustawy.

Zgodnie z częścią A pkt II ust. 2a) załącznika do rozporządzenia, jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.

W toku kontroli ustalono, że po uruchomieniu stacji roboczej systemu informatycznego o nazwie „A" automatycznie jest logowane konto operatora. Operatorzy logują się na jedno konto użytkownika. Również administratorzy systemu logują się na jedno konto administratora. Wobec tego uznać należy, że dla każdego z ww. użytkowników nie jest rejestrowany w tym systemie odrębny identyfikator. Z treści pisma z dnia […] października 2011 r. Prezydenta Miasta L. (znak: […]) wynika, iż uchybienie to zostanie usunięte w bieżącym roku, jednakże do dnia wydania niniejszej decyzji Generalny Inspektor nie został poinformowany, iż uchybienie to zostało usunięte.

Zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni.

W toku czynności kontrolnych ustalono, że hasła użytkownika oraz administratora systemu informatycznego o nazwie „A" nie są zmieniane. Z treści pisma z dnia […] października 2011 r. wynika, iż uchybienie to zostanie usunięte w bieżącym roku, jednakże do dnia wydania niniejszej decyzji Generalny Inspektor nie został poinformowany, iż uchybienie to zostało usunięte.

Mając powyższe na uwadze, w tym stanie faktycznym i prawnym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 2 Kodeksu postępowania administracyjnego, strona niezadowolona z niniejszej decyzji może zwrócić się do Generalnego Inspektora Ochrony Danych Osobowych (adres: ul. Stawki 2, 00-193 Warszawa) z wnioskiem o ponowne rozpatrzenie sprawy, w terminie 14 dni od dnia doręczenia niniejszej decyzji. W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954 z późn. zm.).