



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Wojciech R. Wiewiórowski*

Warszawa, dnia 6 lutego 2012 r.

DIS/DEC- 112/12/7893

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, 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 wniosku Prezydenta Miasta L., o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 16 grudnia 2011 r., nr DIS/DEC-1065/61961/11,

**utrzymuję w mocy zaskarżoną decyzję.**

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

W dniu 16 grudnia 2011 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nr DIS/DEC-1065/61961/11, nakazującą 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”.
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.
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.
4. Zawarcie w ewidencji osób upoważnionych do przetwarzania danych osobowych identyfikatorów użytkowników systemu informatycznego o nazwie „A”.
5. Zapewnienie, aby w systemie informatycznym o nazwie „A” był rejestrowany odrębny identyfikator dla każdego użytkownika tego systemu.
6. Zapewnienie, aby hasło użytkownika oraz administratora systemu informatycznego o nazwie „A” było zmieniane co 30 dni.

W dniu [...] stycznia 2012 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął, złożony w terminie, wniosek Prezydenta Miasta L. z dnia [...] stycznia 2012 r. znak: [...] o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych

Osobowych z dnia 16 grudnia 2011 r., nr DIS/DEC-1065/61961/11 i umorzenie wszczętego postępowania administracyjnego.

We wniosku o ponowne rozpatrzenie sprawy strona wskazała, iż w systemie informatycznym o nazwie „A” nie są przetwarzane dane osobowe w rozumieniu art. 6 ust. 1 pkt 1, pkt 2 i pkt 3 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 ustawą, a dane w nim zawarte nie stanowią zbioru danych osobowych, o którym mowa w art. 7 pkt 1 ustawy, który to na podstawie art. 40 ustawy podlegałby obowiązkowi zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Strona podnosi, iż w systemie tym obserwowane są i czasowo/doraźnie rejestrowane wyłącznie obrazy zdarzeń w miejscach publicznych w celu ochrony bezpieczeństwa i porządku publicznego. Strona podnosi w szczególności, iż daną osobową nie jest numer rejestracyjny pojazdu. Ponadto, 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, z uwagi na to, iż dane w tym zbiorze są przetwarzane dla potrzeb postępowania sądowego, a także że jest to zbiór doraźny, o którym mowa w art. 2 ust. 3 ustawy, do którego mają zastosowanie jedynie przepisy rozdziału 5 ustawy.

Generalny Inspektor Ochrony Danych Osobowych po ponownym rozpatrzeniu sprawy i przeanalizowaniu całego zebranego w sprawie materiału dowodowego, zważył co następuje:

Argumenty podniesione we wniosku o ponowne rozpatrzenie sprawy nie zasługują na uwzględnienie.

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 zatem zgodzić się z twierdzeniem strony, iż daną osobową nie jest numer rejestracyjny pojazdu.

Generalny Inspektor podtrzymuje stanowisko wyrażone w uzasadnieniu decyzji z dnia 16 grudnia 2011 r., nr DIS/DEC-1065/61961/11, iż określona informacja stanowi daną, jeżeli podmiot dysponujący tą informacją 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.

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 nadmiernego 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 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.

Nie można się też zgodzić 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. Strona błędnie twierdzi, iż kryterium

dostępu do danych nie stanowi miejsce zdarzenia, albowiem kamery mają charakter stacjonarny i dlatego położenie kamery nie jest żadnym takim kryterium, a jedynie prostym uwarunkowaniem technicznym.

W toku kontroli ustalono, iż 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 zanalizowanie zarejestrowanych danych według określonych kryteriów.

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”.

Jak wskazano powyżej (a także w uzasadnieniu decyzji z dnia 16 grudnia 2011 r., nr DIS/DEC-1065/61961/11, wyszukanie danego zdarzenia jest realizowane według miejsca wystąpienia zdarzenia a nie miejsca położenia kamery. Tak więc dostęp do danych osobowych przetwarzanych w „A” jest możliwy według kryteriów, jakim są czas oraz miejsca zdarzenia.

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.

Strona podnosi ponadto, 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. Jak strona wyjaśniła w treści uzasadnienia, w sytuacjach, gdy dochodzi do wykorzystania zapisu obrazu zdarzeń z „A”, to w przypadku ustalenia danych osobowych potencjalnego sprawcy wykroczenia, sprawa taka najczęściej kończy się wnioskiem o ukaranie kierowanym do sądu, albowiem obwinieni nie godzą się w takiej sytuacji na przyjęcie mandatu.

Z powyższych wyjaśnień wynika, iż w zbiorze danych osobowych przetwarzanych w „A” są przetwarzane dane osobowe, które mogą być wykorzystane w toku postępowania sądowego oraz takie, które w takim postępowaniu nie będą wykorzystane (albowiem osoba ukarana przyjmie mandat). Do takich zbiorów danych osobowych, zgodnie z utrwaloną praktyką Generalnego Inspektora Ochrony Danych Osobowych, nie ma 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” do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Odnosząc się natomiast do szeregu cytatów z wystąpień Generalnego Inspektora Ochrony Danych Osobowych z dnia [...] marca 2010 r. i [...] sierpnia 2011 r., skierowanych do Ministra Spraw Wewnętrznych i Administracji, na które powołuje się strona we wniosku o ponowne rozpatrzenie sprawy, wskazać należy iż w powyższych wystąpieniach Generalny Inspektor sygnalizował, iż obowiązujące przepisy o ochronie danych osobowych w odniesieniu do [...] **mają zastosowanie** jedynie wtedy, gdy skutek stosowania [...] dochodzi do utworzenia zbioru danych osobowych. Jak wskazano powyżej, Generalny Inspektor Danych Osobowych stoi na stanowisku, iż informacje, które zawiera „A” stanowią zbiór danych osobowych i tym samym w tym przypadku mają zastosowanie przepisy o ochronie danych osobowych.

Ponadto, strona wielokrotnie powołuje się na dyrektywę Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, m.in. wskazując, iż w świetle art. 3 ust. 2 tej dyrektywy jej zakres przedmiotowy nie obejmuje operacji przetwarzania danych w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz przetwarzania związanego z bezpieczeństwem publicznym, obronnością, bezpieczeństwem państwa. Zauważyć należy, iż ww. przepis dyrektywy wyłącza stosowanie dyrektywy, natomiast nie ma zastosowania do przepisów ustawy o ochronie danych osobowych, której zakres przedmiotowy obejmuje również ww. przypadki przetwarzania danych osobowych.

Należy zauważyć, iż strona błędnie przyjmuje, iż w zbiorze danych osobowych muszą być przetwarzane dane osobowe będące informacjami dotyczącymi zidentyfikowanej osoby. Tymczasem z art. 6 w związku z art. 7 pkt 1 ustawy wynika, iż możliwy jest przypadek, gdy zbiór danych osobowych będzie zawierał wyłącznie takie dane osobowe, które są informacjami dotyczącymi osoby **możliwej do zidentyfikowania**, natomiast nie będzie

zawierał danych osobowych będących informacjami dotyczącymi zidentyfikowanej osoby, a za taki zbiór można uznać zbiór danych przetwarzanych w „A”.

Nie można zgodzić się z argumentem strony, iż zbiór danych osobowych przetwarzanych w „A” ma charakter doraźny. Argument strony, iż dane z tego zbioru są usuwane po trzydziestu dniach od ich wprowadzenia do zbioru nie zasługuje na uwzględnienie.

Zgodnie z art. 2 ust. 3 ustawy w odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5 ustawy.

Należy zauważyć, iż dane do zbioru danych przetwarzanych w „A” są wprowadzane stale i po okresie trzydziestu dni są z tego zbioru usuwane. Jednakże sam zbiór ma charakter stały, albowiem permanentnie są w nim przetwarzane dane osobowe. Tym samym nie można uznać, aby zbiór był utworzony doraźnie.

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.

Ponadto, z treści wniosku o ponowne rozpatrzenie sprawy wynika, iż pkt 5 i pkt 6 zaskarżonej decyzji zostały przez stronę wykonane, tj:

1. W systemie informatycznym o nazwie „A” jest rejestrowany odrębny identyfikator dla każdego użytkownika tego systemu.
2. Hasło użytkownika oraz administratora systemu informatycznego o nazwie „A” jest zmieniane co 30 dni.

Dlatego też oceniając ponownie materiał dowodowy zebrany w przedmiotowej sprawie Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. Na podstawie art. 21 ust. 2 ustawy o ochronie danych osobowych w związku z art. 53 § 1 i 54 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. Nr 153, poz. 1270), od niniejszej decyzji stronie przysługuje prawo wniesienia skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie, w terminie

30 dni od dnia doręczenia decyzji, za pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych (na adres: ul. Stawki 2, 00-193 Warszawa).

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.).