



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 23 lutego 2010 r.

DIS/DEC-188/7688/10

Dot. [...]

D E C Y Z J A

Na podstawie art. 104 § 1 i art. 105 § 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 oraz art. 22 w związku z art. 26 ust. 1 pkt 4, art. 31 ust. 2, art. 36 ust. 1, art. 38, art. 41 ust. 2, art. 46 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 7 ust. 1 pkt 2, § 7 ust. 3 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 częścią C pkt XIII załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Prezydenta Miasta T.,

I. Nakazuję Prezydentowi Miasta T., usunięcie uchybień w procesie przetwarzania danych poprzez:

- 1. Określenie w umowie dotyczącej powierzenia przetwarzania danych osobowych użytkowników karty [...], zawartej przez Prezydenta Miasta T. z Z. Sp. z o.o., zakresu i celu przetwarzania powierzonych danych osobowych, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zapewnienie kryptograficznej ochrony danych przesyłanych w sieci publicznej, wykorzystywanych do uwierzytelniania w systemie informatycznym o nazwie „A”, służącym do przetwarzania danych osobowych użytkowników karty [...], w terminie [...] miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

3. Zapewnienie, aby system informatyczny o nazwie „A” zapewniał odnotowanie identyfikatora użytkownika wprowadzającego dane do ww. systemu, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.
4. Zapewnienie, aby system informatyczny o nazwie „A” zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące identyfikatora użytkownika wprowadzającego dane do ww. systemu, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili u Prezydenta Miasta T., kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. [...], 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 Miejskiego w T. ustne wyjaśnienia, skontrolowano system informatyczny oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Prezydenta Miasta T.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Prezydent Miasta T., jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Nieokreśleniu po jakim czasie, w przypadku ustania celu ich przetwarzania, usuwane będą ze zbioru dane pozyskiwane w związku z funkcjonowaniem karty [...] (art. 26 ust. 1 pkt 4 ustawy).
2. Niezawarciu w umowach dotyczących powierzenia przetwarzania danych osobowych zawartych z Z. Sp. z o.o. i E. Sp. z o.o., zakresu i celu przetwarzania powierzonych danych osobowych (art. 31 ust.2 ustawy).
3. Niezgłoszeniu Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizacji zbioru danych osobowych o nazwie „K” - zgłoszenie nr [...] (art. 41 ust. 2 ustawy).

4. Przetwarzaniu w zbiorze danych osobowych o nazwie „K” danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy, pomimo niezarejestrowania przez Generalnego Inspektora Ochrony Danych Osobowych ww. zbioru (art. 46 ust. 2 ustawy).
5. Niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia w systemie informatycznym o nazwie „A” 36 ust. 1 ustawy w związku z częścią C pkt XIII załącznika do rozporządzenia).
6. Niezapewnieniu, aby system informatyczny o nazwie „A” umożliwiał odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu (art. 38 ustawy w związku z § 7 ust. 1 pkt 2 rozporządzenia).
7. Niezapewnieniu, aby system informatyczny o nazwie „A” umożliwiał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje dotyczące identyfikatora użytkownika wprowadzającego dane do systemu (art. 38 ustawy w związku z § 7 ust. 3 rozporządzenia).

W związku z powyższym, w dniu [...] listopada 2009 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy sygn. [...].

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezydent Miasta T. w pismach z dnia [...] grudnia 2009 r., nr [...], [...] stycznia 2010 r., nr [...] i [...], [...] stycznia 2010 r., nr [...] i [...] stycznia 2010 r., nr [...], złożył wyjaśnienia, w których poinformował między innymi, że:

1. Od [...] października 2009 r. zaprzestano pozyskiwania, od osób ubiegających się o wydanie karty [...], kserokopii dowodów osobistych oraz kserokopii dokumentów potwierdzających prawo do ulgi, w tym dokumentów zawierających dane szczególnie chronione, o których mowa w art. 27 ust. 1 ustawy. Dokumentacja w tym zakresie, która dotychczas była pozyskiwana, została zniszczona przez komisję powołaną do tego celu przez Prezydenta Miasta T. Pozyskiwanie kopii dokumentów potwierdzających prawo do ulgi zostało zastąpione potwierdzeniem ww. uprawnienia na podstawie okazanych do wglądu dokumentów. Potwierdzenia prawa do ulgi dokonuje, na wniosku o wydanie karty [...], pracownik Urzędu Miejskiego w T. przyjmujący ww. wnioski.
2. Dane osobowe przetwarzane w zbiorze danych osobowych o nazwie „K” będą usuwane z ww. zbioru w terminie 14 dni od pozyskania informacji o rezygnacji przez użytkownika z karty [...]. Ponadto, dane z ww. zbioru usuwane będą w przypadku nieładowania i nieużywania karty przez 5 lat.

3. Umowa zawarta z E. Sp. z o.o., dotycząca drukowania kart [...], obowiązywała do dnia [...] grudnia 2009 r. Od [...] stycznia 2010 r. karty [...] drukowane są w Urzędzie Miejskim w T.
4. Dnia [...] stycznia 2010 r. zawarto nową umowę operatorską z E. Sp. z o.o., na podstawie której ww. podmiotowi powierzono przetwarzanie danych osobowych pozyskiwanych w związku z funkcjonowaniem karty [...]. W ww. umowie określono zakres i cel przetwarzania powierzonych danych.
5. Zgłoszono aktualizację zbioru danych osobowych o nazwie „K”.
4. Umowa, na podstawie której Prezydent Miasta T. powierzył przetwarzanie danych osobowych związanych z funkcjonowaniem karty [...]. Z. Sp. z o.o., wskazuje w sposób dostateczny zakres i cel powierzenia przetwarzania ww. danych. Wskazano, iż zakres i cel powierzenia przetwarzania danych określony został w § 5 porozumienia z dnia [...] grudnia 2008 r. zawartego z ww. podmiotem. Powołano również wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 6 lutego 2007 r. (9 II SA/Wa 1786/06) zgodnie z uzasadnieniem którego „przepisy ustawy o ochronie danych osobowych nie nakładają na strony umowy cywilnoprawnej obowiązku wprowadzania do ich treści zapisów dotyczących ochrony danych osobowych”. Jednocześnie, Prezydent Miasta T. zobowiązał się do wystąpienia do Z. Sp. z o.o., z inicjatywą uzupełnienia i doprecyzowania zakresu i celu powierzenia przetwarzania danych osobowych.
5. Zwrócono się do E. Sp. z o.o., tj. do dostawcy systemu informatycznego o nazwie „A”, z żądaniem dostosowania ww. systemu do wymogów ustawy o ochronie danych osobowych.

Do ww. pism załączono między innymi: kserokopię zarządzenia [...] Prezydenta Miasta T. z dnia [...] grudnia 2009 r. w sprawie powołania komisji do zniszczenia dokumentacji gromadzonej przy wnioskach o wydanie karty [...] w mieście T.; kserokopie protokołów zniszczenia kopii dokumentów potwierdzających prawo do ulgi; kserokopię pisma z dnia [...] grudnia 2009 r. do E. Sp. z o.o. wraz z załącznikiem; kserokopię pisma z dnia [...] grudnia 2009 r. otrzymanego z M. Sp. z o.o.; wzór wniosku o wydanie karty [...]; kserokopie zgłoszeń aktualizacji zbioru danych osobowych o nazwie „K”; kserokopię umowy operatorskiej zawartej z E. Sp. z o.o., wraz z załącznikami; kserokopię faktury i protokołu zdawczo – odbiorczego dotyczących zakupu zestawu do personalizacji kart miejskich.

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

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Natomiast zgodnie z art. 31 ust. 2

ustawy, podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

W toku kontroli ustalono, że Prezydent Miasta T., jako administrator danych, na podstawie umowy zawartej w dniu [...] grudnia 2008 r., powierzył Z. Sp. z o.o., przetwarzanie danych osobowych w związku z funkcjonowaniem karty [...]. Ww. umowa stanowi umowę powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ust. 1 ustawy. Nie można zgodzić się ze stanowiskiem administratora danych, zgodnie z którym powołana umowa wskazuje w sposób dostateczny w jakim zakresie i celu powierzył on przetwarzanie danych osobowych. W wyjaśnieniach z dnia [...] grudnia 2009 r. wskazano, które z postanowień ww. umowy według administratora danych określają zakres i cel powierzenia przetwarzania danych. Należy zauważyć, iż na podstawie wskazanych postanowień, nie można określić zakresu i celu, w jakim podmiot, któremu powierzono przetwarzanie danych, może te dane przetwarzać. Ponadto, mając na uwadze powołany w piśmie z dnia [...] grudnia 2009 r. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie (9 II SA/Wa 1786/06) należy wskazać, iż ww. orzeczenie, którego fragment uzasadnienia został przytoczony w wyjaśnieniach administratora danych, wydane zostało w wyniku rozpatrzenia skargi na decyzję Generalnego Inspektora Ochrony Danych Osobowych, dotyczącej innego stanu faktycznego, nie powiązanego z postępowaniem w sprawie przetwarzania danych osobowych przez Prezydenta Miasta T. Należy zauważyć, iż zgodnie z art. 31 ust. 2 ustawy, podmiot, któremu administrator danych powierzył przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Z użytego przez ustawodawcę sformułowania powołanego przepisu w sposób jednoznaczny wynika, iż zakres i cel powierzenia powinien zostać określony w ww. umowie.

Zgodnie z art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Natomiast zgodnie z częścią C pkt XIII załącznika do rozporządzenia, administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej.

W toku czynności kontrolnych ustalono, że dane przesyłane w sieci publicznej, wykorzystywane do uwierzytelniania w systemie informatycznym o nazwie „A” nie są szyfrowane. Należy wskazać, iż zwrócenie się administratora danych do dostawcy systemu „A” z żądaniem zapewnienia, aby ww. system informatyczny spełniał wymogi wskazane w przepisach o ochronie danych osobowych, nie może być uznane jako przywrócenie stanu zgodnego z prawem.

Zgodnie z art. 38 ustawy administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W myśl § 7 ust. 1 pkt 2 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba. Natomiast zgodnie z § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

W toku czynności kontrolnych ustalono, że dane z wniosków o wydanie karty [...] wprowadzane są do systemu informatycznego o nazwie „A” przez upoważnionych pracowników Urzędu Miejskiego w T. Jak ustalono ww. system informatyczny nie zapewnia odnotowania identyfikatora użytkownika wprowadzającego dane do systemu. Ponadto ustalono, że ww. system informatyczny nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji o identyfikatorze użytkownika wprowadzającego dane do systemu. Należy wskazać, iż również w przypadku powyższych uchybień w procesie przetwarzania danych osobowych, zwrócenie się administratora danych do dostawcy systemu „A” z żądaniem zapewnienia aby ww. system spełniał wymogi wskazane w przepisach o ochronie danych osobowych, nie może być uznane jako przywrócenie stanu zgodnego z prawem.

Jednocześnie, na podstawie przedstawionych przez Prezydenta Miasta T. dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych stanowiące przedmiot postępowania zostały usunięte, tj.:

1. Określono termin, po jakim usuwane będą dane osobowe ze zbioru danych o nazwie „K”, w przypadku ustania celu ich przetwarzania.
2. W umowie operatorskiej, na podstawie której Prezydent Miasta T. powierzył M. Sp. z o.o., przetwarzanie danych osobowych w związku z funkcjonowaniem karty [...], określono zakres i cel przetwarzania powierzonych danych.
3. Zaprzeszono przekazywania do E. Sp. z o.o., danych osobowych w celu wykonywania kart [...].
4. Zaprzeszono przetwarzania danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy.
5. Zgłoszono Generalnemu Inspektorowi Ochrony Danych Osobowych aktualizację zbioru danych osobowych o nazwie „K” (zgłoszenie nr [...]).

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Przesłanką umorzenia postępowania na podstawie art. 105 § 1 k.p.a jest bezprzedmiotowość postępowania „z jakiegokolwiek przyczyny”, czyli z każdej przyczyny powodującej brak jednego z elementów materialnoprawnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej (wyrok NSA z 21 stycznia 1999 r. SA/Sz1029/97).

Z uwagi na to, iż pozostałe uchybienia będące przedmiotem niniejszego postępowania administracyjnego zostały usunięte, postępowanie należało w tym zakresie umorzyć.

Wobec powyższego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja jest ostateczna. 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.