



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 11 sierpnia 2008 r.

DIS/DEC- 471/20697/08

dot. DIS-K-421/73/08

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 i art. 22 w związku z art. 26 ust. 1 pkt 3 i art. 41 ust. 1 pkt 3a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), § 4 pkt 3, § 6 ust. 4, § 7 ust. 1 pkt 1 i 2 oraz § 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) i częścią A pkt III ppkt 2, częścią A pkt IV ust. 2, częścią B pkt VIII oraz częścią C pkt XIV załącznika do rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Zakład Gospodarki Mieszkaniowej

Nakazuję Zakładowi Gospodarki Mieszkaniowej usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

- 1. Zaprzestanie pozyskiwania danych osobowych najemców lokali mieszkalnych stanowiących własność miasta i gminy w zakresie imion rodziców, daty i miejsca urodzenia oraz poprzedniego i kolejnego adresu zamieszkania, jako zbędnych do realizacji celu, dla którego dane tych osób są przetwarzane, od dnia, w którym niniejsza decyzja stanie się ostateczna.**
- 2. Zgłoszenie aktualizacji zbioru danych osobowych o nazwie „Najemcy i właściciele zasobów komunalnych” w zakresie kategorii osób, których dane przetwarzane są w ww. zbiorze, oraz zakresu danych osobowych w nim przetwarzanych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**

3. Uzupełnienie „Polityki bezpieczeństwa informacji” o opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
4. Zmodyfikowanie systemów informatycznych o nazwach „X” oraz „Y”, służących m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych tak, aby zapewniały dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.
5. Zmodyfikowanie systemu informatycznego o nazwie „K”, służącego do przetwarzania danych osobowych pracowników Zakładu Gospodarki Mieszkaniowej, oraz systemów informatycznych o nazwach „X” i „Y”, służących m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych tak, aby zapewniały dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 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), w terminie 3 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.
6. Zabezpieczenie systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, przed utratą danych spowodowaną awarią zasilania lub zakłócaniami w sieci zasilającej, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
7. Zapewnienie, aby hasło do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, było zmieniane nie rzadziej niż co 30 dni, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.
8. Zapewnienie, aby hasło do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, oraz hasło do systemu informatycznego o nazwie „K”, służącego do przetwarzania danych osobowych pracowników Zakładu Gospodarki Mieszkaniowej, składało się co najmniej z 8 znaków, zawierało małe i wielkie litery oraz cyfry lub znaki specjalne, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w Zakładzie Gospodarki Mieszkaniowej zwanym dalej ZGM, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. akt DIS-K-421/73/08), 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, oraz 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 ZGM 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 Dyrektora ZGM.

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

1. Pozyskiwaniu danych osobowych najemców lokali mieszkalnych stanowiących własność miasta i gminy w zakresie szerszym, niż jest to niezbędne do realizacji celu, dla którego dane tych osób są przetwarzane.
2. Niepodaniu w zgłoszeniu do rejestracji zbioru danych osobowych o nazwie „Najemcy i właściciele zasobów komunalnych” (zgłoszenie nr R 001370/2008) prawidłowej kategorii osób, których dane przetwarzane są w ww. zbiorze, oraz pełnego zakresu danych osobowych w nim przetwarzanych.
3. Niezawarcia w „Polityce bezpieczeństwa informacji” opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi.
4. Niezapewnianiu przez systemy informatyczne o nazwach „X” oraz „Y”, służące m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu.

5. Niezapewnianiu przez system informatyczny o nazwie „K”, służący do przetwarzania danych osobowych pracowników ZGM, oraz systemy informatyczne o nazwach „K” oraz „Y”, służące m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, dla każdej osoby, której dane osobowe są przetwarzane
w systemie informatycznym, sporządzenia i wydrukowania raportu zawierającego
w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.
6. Niezabezpieczeniu systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, przed utratą danych spowodowaną awarią zasilania lub zakłócaniami w sieci zasilającej.
7. Zmienianiu hasła do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, rzadziej niż co 30 dni.
8. Niestosowaniu hasła do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, oraz hasła do systemu informatycznego o nazwie „K”, służącego do przetwarzania danych osobowych pracowników ZGM, składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.

W związku z powyższym, w dniu 24 czerwca 2008 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy (sygn. pisma DIS-K-421/73/08/15779).

Zakład Gospodarki Mieszkaniowej nie ustosunkował się pisemnie do stwierdzonych uchybień w procesie przetwarzania danych osobowych, stanowiących przedmiot postępowania administracyjnego, wymienionych w zawiadomieniu o wszczęciu postępowania.

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

Zgodnie z art. 26 ust. 1 pkt 3 ustawy, administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

Kontrola wykazała, że zakres przetwarzanych danych osobowych najemców lokali mieszkalnych stanowiących własność miasta i gminy obejmuje imię, nazwisko, adres zamieszkania, imiona rodziców, datę i miejsce urodzenia, poprzedni i kolejny adres zamieszkania. Dane w zakresie imion rodziców, daty i miejsca urodzenia, poprzedniego i kolejnego adresu zamieszkania są pozyskiwane w związku z prowadzeniem książki meldunkowej, stanowiącej obecnie wykaz osób zamieszkujących w poszczególnych lokalach stanowiących własność miasta

i gminy (obowiązek prowadzenia przez administratorów mieszkań komunalnych ksiąg meldunkowych został zniesiony w 1998 r.). Jednocześnie ustalono, że dane, które wprowadzane są do książki meldunkowej, nie są obecnie wykorzystywane, a ich gromadzenie związane jest z istnieniem określonych rubryk w tej książce. Należy zatem uznać, że pozyskiwanie danych osobowych najemców lokali mieszkalnych stanowiących własność miasta i gminy w zakresie imion rodziców, daty i miejsca urodzenia, poprzedniego i kolejnego adresu zamieszkania, od momentu ustania w 1998 r. obowiązku prowadzenia książki meldunkowej, jest zbędne do realizacji celu, dla którego dane tych osób są przetwarzane, tj. zawarcia i realizacji umowy najmu lokalu mieszkalnego.

Zgodnie z art. 41 ust. 1 pkt 3a ustawy, zgłoszenie zbioru danych do rejestracji powinno zawierać opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych.

W zgłoszeniu do rejestracji Generalnemu Inspektorowi zbioru danych osobowych o nazwie „Najemcy i właściciele zasobów komunalnych” wskazano, że w jego ramach przetwarzane są dane osobowe najemców lokali mieszkalnych stanowiących własność miasta i gminy oraz dane osobowe właścicieli lokali mieszkalnych, którzy wykupili ten lokal od miasta i gminy, a zakres przetwarzanych danych ww. osób obejmuje imiona, nazwisko i adres zamieszkania lub pobytu. Tymczasem przeprowadzona kontrola wykazała, że ZGM nie jest administratorem danych osobowych właścicieli lokali mieszkalnych, którzy wykupili ten lokal od miasta i gminy – dane tych osób ZGM przetwarza jako podmiot, któremu administratorzy danych (wspólnoty mieszkaniowe) powierzyły przetwarzanie danych osobowych swoich członków w związku z zawarciem umów o zarządzaniu

i administrowaniu nieruchomością wspólną. W konsekwencji należy stwierdzić, że w ramach omawianego zbioru danych osobowych nie są przetwarzane dane osobowe właścicieli lokali mieszkalnych, którzy wykupili ten lokal od miasta i gminy. Ponadto, w toku kontroli ustalono, że w związku z istnieniem do 1998 r. obowiązku prowadzenia przez administratorów mieszkań komunalnych ksiąg meldunkowych ZGM przetwarza dane najemców lokali mieszkalnych w zakresie, który był niezbędny do realizacji tego obowiązku, tj. imion rodziców, daty i miejsca urodzenia, poprzedniego i kolejnego adresu zamieszkania. Powyższe dane nie zostały jednak wymienione w zgłoszeniu przedmiotowego zbioru do rejestracji Generalnemu Inspektorowi.

Zgodnie z § 4 pkt 3 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.

W toku czynności kontrolnych ustalono, że prowadzona w ZGM „Polityka bezpieczeństwa informacji” nie zawiera opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi.

Zgodnie z § 7 ust. 1 pkt 1 i 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 daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba, że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

Kontrola wykazała, że systemy informatyczne o nazwach „X” oraz „Y”, służące m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane do systemu.

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 ust. 1.

W toku kontroli ustalono, że system informatyczny o nazwie „K”, służący do przetwarzania danych osobowych pracowników ZGM, oraz systemy informatyczne o nazwach „X” oraz „Y”, służące m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, nie zapewniają dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.

Zgodnie z częścią A pkt III pkt 2 załącznika do rozporządzenia, system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

Przeprowadzona kontrola wykazała, że system informatyczny o nazwie „X”, służący m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, nie został zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

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. Hasło składa się co najmniej z 6 znaków.

W toku kontroli ustalono, że hasło do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, jest zmieniane rzadziej niż co 30 dni.

Zgodnie z § 6 ust. 4 rozporządzenia, poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną. Natomiast w myśl części C pkt XIV załącznika do rozporządzenia,

administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej. Z kolei zgodnie z częścią B pkt VIII załącznika do rozporządzenia, w przypadku gdy dla uwierzytelnienia użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

Z ustaleń kontroli wynika, że hasło do systemu informatycznego o nazwie „X”, służącego m.in. do przetwarzania danych osobowych najemców lokali mieszkalnych, oraz hasło do systemu informatycznego o nazwie „K”, służącego do przetwarzania danych osobowych pracowników ZGM, składa się z pięciu znaków, a jego złożoność nie spełnia wymogów, o których mowa w części B pkt VIII załącznika do rozporządzenia.

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.