GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
Michał Serzycki

Warszawa, dnia 18 stycznia 2010 r.

DIS/DEC- 54/1981/10
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 oraz art. 22 w związku z art. 26 ust. 1 pkt 4, art. 36 ust. 1, art. 36 ust. 2, art. 38 i art. 41 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.), oraz § 4 pkt 3 i pkt 4, § 7 ust. 1 pkt 1 i pkt 2 i § 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 Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o.,

I. Nakazuję Miejskiemu Przedsiębiorstwu Komunikacyjnemu Sp. z o.o., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. Zastosowanie środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, w terminie od dnia, w którym niniejsza decyzja stanie się ostateczna.

2. Spowodowanie, by system informatyczny o nazwie „A" (w którym przetwarzane są dane osobowe […]) dla każdej osoby, której dane osobowe są przetwarzane w tym systemie

informatycznym, zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu – w terminie dwóch miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w Miejskim Przedsiębiorstwie Komunikacyjnym Sp. z o.o., zwanej dalej także Spółką w celu ustalenia 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, 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 Spółki 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 Prezesa Zarządu Spółki.

Na podstawie materiału dowodowego zgromadzonego w toku kontroli ustalono, że w procesie przetwarzania danych Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o., jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1) nieokreśleniu procedur oraz terminów usuwania danych przetwarzanych w zbiorze danych o nazwie „B.”, w przypadku gdy cel ich przetwarzania zostanie osiągnięty (art. 26 ust. 1 pkt 4 ustawy),

2) niedokonaniu aktualizacji zbioru danych o nazwie „B.” (zgłoszenie nr R […]),

3) niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej (art. 36 ust. 1 ustawy w związku z częścią C pkt XIII załącznika do rozporządzenia),

4) niezawarciu w Polityce bezpieczeństwa opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt 3 rozporządzenia); sposobu przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia),

5) niezapewnieniu, by system informatyczny o nazwie „A” dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym, zapewniał sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o dacie pierwszego wprowadzenia danych do systemu oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu (art. 38 ustawy w związku z § 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).

W piśmie z dnia […] listopada 2009 r. (sygn. […]), stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Miejskie Przedsiębiorstwo Komunikacyjne Sp. z o.o. została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Prezes Zarządu Spółki, pismem z dnia […] grudnia 2009 r. złożył wyjaśnienia, w których poinformował, iż:

1) opracowano i wdrożono procedurę usuwania danych w zbiorze danych o nazwie „B.”,

2) dokonano aktualizacji zbioru danych o nazwie „B.” (zgłoszenie nr R […]),

3) podjęto działania w celu wyeliminowania uchybienia polegającego na niezastosowaniu środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej. Ww. środki zostaną zastosowane w terminie do dnia […] grudnia 2009 r.,

4) skierowano wystąpienie do P. Sp. z o.o. w przedmiocie dokonania zmian w systemie informatycznym o nazwie „A”.

Do wskazanych wyjaśnień załączono: kserokopię zarządzenia Nr […] Prezesa Zarządu Miejskiego Przedsiębiorstwa Komunikacyjnego Sp. z o.o. z dnia […] grudnia 2009 r. w sprawie: wprowadzenia procedury usuwania danych w zbiorze danych biletu elektronicznego, kserokopię zgłoszenia zmian w zbiorze danych o nazwie „K.” (zgłoszenie nr R: […]), wydruk struktury zależności plików baz danych w systemie informatycznym o nazwie „A”, kserokopię pisma z dnia […] grudnia 2009 r. skierowanego do P. Sp. z o.o., kserokopię zarządzenia nr […] Prezesa Zarządu Miejskiego Przedsiębiorstwa Komunikacyjnego Sp. z o.o. z dnia […] grudnia 2009 r. w sprawie: zmiany zarządzenia nr […] Prezesa Zarządu Miejskiego Przedsiębiorstwa Komunikacyjnego Sp. z o.o. z dnia [..] grudnia 2007 r. w sprawie wprowadzenia Regulaminu […].

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

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, zabraniem 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 uwierzytelnienia, które są przesyłane w sieci publicznej.

W toku czynności kontrolnych ustalono, że połączenie z bazą danych osobowych systemu informatycznego o nazwie „A" odbywa się przy pomocy łączy publicznych bez zastosowania środków kryptograficznej ochrony tych danych.

Wobec powyższego należy uznać, iż administrator danych nie stosuje środków kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

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.

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 czynności kontrolnych ustalono, że system informatyczny o nazwie „A" (w którym przetwarzane są dane osobowe […]) nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje o dacie pierwszego wprowadzenia danych do systemu (§ 7 ust. 1 pkt 1 rozporządzenia) oraz identyfikatorze użytkownika wprowadzającego dane osobowe do systemu (§ 7 ust. 1 pkt 2 rozporządzenia).

Prezes Zarządu Spółki w piśmie z dnia […] grudnia 2009 r. wskazał, iż zostały podjęte działania w celu przywrócenia stanu zgodnego z prawem. Ustosunkowując się do ww. wyjaśnień należy podkreślić, że samo podjęcie działań w celu usunięcia uchybienia nie stanowi podstawy do uznania, iż przywrócony został stan zgodny z prawem. Nie przedstawiono dowodów potwierdzających, iż powyższe uchybienia zostały usunięte. Jednak zważywszy na podjęte działania w tym zakresie, wyznaczono powołane w sentencji decyzji terminy na usunięcie przedmiotowych uchybień.

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

1) określono procedury oraz terminy usuwania danych przetwarzanych w zbiorze danych o nazwie „B.", w przypadku gdy cel ich przetwarzania zostanie osiągnięty,

2) dokonano aktualizacji zbioru danych o nazwie „B.” (zgłoszenie nr R […]),
3) uzupełniono Politykę bezpieczeństwa o opis struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Stosownie do art. 105 § 1 Kodeksu postępowania administracyjnego, gdy postępowanie z jakiejkolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o jego umorzeniu. Jak stwierdził Naczelny Sąd Administracyjny w uzasadnieniu wyroku z dnia 19 listopada 2001 r. (sygn. akt II SA 2702/00): „(...) skoro w toku prowadzonego (...) postępowania administracyjnego zniesiony został stan naruszenia prawa, którego miało dotyczyć rozstrzygnięcie, to postępowanie stało się bezprzedmiotowe”.

W związku z tym, że w toku postępowania usunięte zostały pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, w tym zakresie należało je umorzyć.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, 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.