



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 7 października 2009 r.

DIS/DEC- 990/36524/09

dot. DIS-K-421/56/09

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 (t.j. 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. 1 i 2 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 1, pkt 3 i pkt 4 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 B pkt VIII załącznika do powołanego wyżej rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Bank ,

nakazuję Bankowi usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

I. Opracowanie polityki bezpieczeństwa, która będzie zawierać kompletny wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposobu przepływu danych pomiędzy poszczególnymi systemami, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.

I. W pozostałym zakresie postępowanie umarzam.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili w Banku (dalej Bank) kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (sygn. DIS-K-421/56/09), 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 Banku 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 Banku.

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

1. Niezawarcia w polityce bezpieczeństwa informacji, o których mowa w § 4 pkt 1, pkt 3 oraz w pkt 4 rozporządzenia tj. wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami (art. 36 ust. 2 ustawy, § 4 pkt 1, pkt 3 oraz pkt 4 rozporządzenia).
2. Niezastosowaniu środków technicznych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. do uwierzytelniania użytkowników używaniu haseł, składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne (art. 36 ust. 1, część B pkt VIII załącznika do rozporządzenia).

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne (sygn. DIS-K-421/56/09/16148), w celu wyjaśnienia okoliczności sprawy.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Bank pismami: z dnia 18 maja 2009 r. z dnia 27 lipca 2009 r. (HBPL/CW/581/09) i z dnia 19 sierpnia 2009 r. złożył wyjaśnienia, w których poinformował, że:

1. Na podstawie wewnętrznej procedury obowiązującej w Banku, a wdrożonej uchwałą Zarządu Banku, wszyscy pracownicy zobowiązani zostali do stosowania haseł dostępu składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne. Bank podjął także działania w zakresie zmiany konfiguracji parametrów systemowych, tak aby hasła zabezpieczające dostęp do systemów, w których są przetwarzane dane osobowe składały się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Bank podjął działania w zakresie opracowania polityki bezpieczeństwa, która zawierać będzie wymogi wynikające z § 4 pkt 1, pkt 3 oraz pkt 4 rozporządzenia tj. kompletny wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami. Obecnie polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (Bank nie przedstawił dowodu potwierdzającego usunięcie przedmiotowego uchybienia). Dalej trwają prace nad sporządzeniem opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi i sposobu przepływu danych pomiędzy poszczególnymi systemami.

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

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, zwana dalej „instrukcją. 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 ust. 2, dokumentację, o której mowa § 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 pkt 1, pkt 3, pkt 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, opis struktury zbiorów danych

wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami.

W toku kontroli ustalono, iż w Banku prowadzona i wdrożona jest dokumentacja opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. Polityka bezpieczeństwa, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Jednakże opracowana przez Bank polityka bezpieczeństwa nie zawiera kompletnego wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar,

w którym przetwarzane są dane osobowe (tj. m.in. lokalizacji w Wielkiej Brytanii, gdzie znajdują się serwery Banku), opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi (opis struktury nie zawiera zawartości poszczególnych pól informacyjnych i powiązania między nimi), sposobu przepływu danych pomiędzy poszczególnymi systemami (w toku kontroli przedstawiono jedynie schemat wskazujący korelacje między poszczególnymi systemami, bez wskazania sposobu przepływu danych pomiędzy poszczególnymi systemami). Uznać zatem należy, iż Polityka bezpieczeństwa nie spełnia wymogów określonych w § 4 pkt 1, pkt 3, pkt 4 rozporządzenia.

Pismami: z dnia 18 maja 2009 r. z dnia 27 lipca 2009 r. i z dnia 19 sierpnia 2009 r. Bank wyjaśnił, iż podjął działania w zakresie opracowania polityki bezpieczeństwa, która zawierać będzie wymogi wynikające z § 4 pkt 1, pkt 3, pkt 4 rozporządzenia tj. kompletny wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami. Jak wskazał Bank w swych wyjaśnieniach, obecnie polityka bezpieczeństwa zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, jednakże nie przedstawił dowodu potwierdzającego usunięcie przedmiotowego uchybienia. Ponadto Bank wyjaśnił, iż nadal trwają prace nad sporządzeniem opisu struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi i sposobu przepływu danych pomiędzy poszczególnymi systemami.

Wobec powyższego nie można uznać, iż w przedmiotowym zakresie został przywrócony stan zgodny z prawem.

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 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. S.A./Sz 1029/97).

W toku postępowania Bank usunął uchybienie w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, poprzez zastosowanie środków technicznych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. Bank zobowiązał wszystkich pracowników (użytkowników) do używania haseł dostępu do systemów składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.

Podkreślenia wymaga, iż w celu zwiększenia bezpieczeństwa przetwarzanych danych osobowych wskazane i celowe jest zastosowanie środków technicznych, które automatycznie wymuszają zmianę hasła co 30 dni, jak i jego złożoność.

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.