GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 27 kwietnia 2012 r.

DIS/DEC- 381/12/27622/12

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 i art. 22 w związku z art. 39 ust. 1 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 pkt 1 i pkt 2 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 części A pkt IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Bank w W. S.A.,

I. Nakazuję Bankowi S.A. w W. usunięcie uchybień w procesie przetwarzania danych osobowych w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna, poprzez uzupełnienie dokumentacji stanowiącej politykę bezpieczeństwa o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

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 kontrolę w Banku S.A. z siedzibą w W., zwanym dalej Bankiem, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. akt […], 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 Wiceprezesa Zarządu Banku.

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

1. Niezawarciu w ewidencji osób upoważnionych do przetwarzania danych osobowych daty nadania i ustania upoważnienia do przetwarzania danych osobowych (art. 39 ust. 1 ustawy).
2. Niezgłoszeniu zbioru danych [X] do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ustawy).
3. Braku odniesienia w dokumentacji stanowiącej politykę bezpieczeństwa do planu ochrony, w którym określony został obszar przetwarzania danych osobowych oraz na niezawarciu w niej zbioru danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […] wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (§ 4 pkt 1 i pkt 2 rozporządzenia).
4. Używaniu do uwierzytelniania użytkowników, podczas dostępu do danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […], hasła zmienianego co 90 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).

W związku z powyższym, w dniu […] lutego 2012 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy sygn. pisma ….].

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego inspektor ochrony danych osobowych w Banku pismem z dnia […] marca 2012 r. złożył wyjaśnienia, w których poinformowano, że:

1. Na ewidencję osób upoważnionych do przetwarzania danych osobowych składa się rejestr osób zatrudnionych w Banku oraz rejestr osób uprawnionych do dostępu do określonej opcji systemu informatycznego, które zawierają wszystkie wymagane informacje. W związku z wnioskami pokontrolnymi sformułowanymi w zawiadomieniu o wszczęciu postępowania administracyjnego Bank podjął decyzję o wprowadzeniu do zarządzenia nr […] „Zasady Ochrony Danych Osobowych w Banku S.A. w W." zapisu doprecyzowującego informację na temat prowadzonej przez Bank ewidencji osób upoważnionych do przetwarzania danych osobowych.
2. Zbiór danych osobowych, w ramach którego przetwarzane są dane pracowników podmiotów współpracujących z Bankiem w zakresie […] został zgłoszony przez Bank do rejestracji Generalnemu Inspektorowi pod nazwą [X] w dniu […] marca 2011 r. Zbiór ten został umieszczony w dokumencie o nazwie „Zbiory danych osobowych przetwarzanych przez Bank w W. S.A.".
3. Przygotowana została zmiana zarządzenia nr […] „Zasady Ochrony Danych Osobowych w Banku S.A. w W. polegająca na dodaniu zapisu doprecyzowującego informację na temat obszaru przetwarzania danych osobowych. Jednocześnie Bank uzupełnił wykaz zbiorów danych osobowych o informację wskazującą, jakie programy zastosowano do przetwarzania danych.
4. Decyzja o zastosowaniu częstotliwości zmiany hasła dostępu do danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […] co 90 dni została podjęta z uwzględnieniem decyzji Generalnego Inspektora Ochrony Danych Osobowych nr […] z dnia […] maja 2009 r. oraz nr […] z dnia […] maja 2009 r. W ww. decyzjach Generalny Inspektor wyraził stanowisko, iż mimo że używane systemy informatyczne przetwarzające dane osobowe wymuszają zmianę haseł dostępu co 90 dni, co nie spełnia wymogu części A pkt IV ust. 2 załącznika do rozporządzenia (który stanowi, że w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana powinna następować nie rzadziej niż co 30 dni), to należy uznać, iż systemy te zapewniają wystarczający poziom ochrony osobowych i że adresaci tych decyzji zapewnili odpowiedni poziom zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. W dalszej części ww. decyzji Generalny Inspektor zalecił (a nie nakazał) dostosowanie systemów informatycznych do wymogu wynikającego z części A pkt IV ust. 2 załącznika do rozporządzenia, tak by zapewniały zmianę hasła co 30 dni. Systemy używane przez adresatów ww. decyzji służyły do przekazywania danych osobowych do państw trzecich nie zapewniających gwarancji ochrony danych co najmniej takich , jakie

obowiązują w Polsce. W przypadku Banku badany proces przetwarzania danych w plikach Excell ma miejsce w ramach Polski i nie obejmuje udostępniania danych innym podmiotom, co również ogranicza ryzyko ewentualnego naruszenia ochrony informacji. Zgodnie z gwarantowaną przez art. 32 Konstytucji zasadą równości podmiotów gospodarczych oraz orzecznictwem Trybunału Konstytucyjnego (np. orzeczenie TK z dnia 13 września 1990 r., U 4/90, OTK 1990, nr 10), podmioty prawa (adresaci norm prawnych) charakteryzujące się daną cechą istotną w równym stopniu, mają być traktowane równo przez organy państwowe. Bank mając przekonanie, że ta zasada jest respektowana oraz zważywszy na ww. decyzje administracyjne GIODO, nie znalazł powodu, dla którego w badanym procesie musiałby stosować odmienne rozwiązanie informatyczne, które jest mniej korzystne dla użytkowników niż te formalnie zaakceptowane przez GIODO i wprowadził zasadę zmiany hasła co 90 dni z zachowaniem innych warunków technicznych i organizacyjnych gwarantujących ochronę danych. Zdaniem Banku wymuszanie zmiany hasła dostępu do ww. danych co 30 dni nie zapewnia większego poziomu bezpieczeństwa przetwarzanym danym osobowym. Bank jednak podjął decyzję o zmianie ww. praktyki i dostosowaniu procesu postępowania z danymi osobowymi pracowników podmiotów współpracujących z nim w zakresie […], wprowadzając proces polegający na zmianie haseł dostępu do tych danych co 30 dni.

Ponadto, do pisma z dnia […] marca 2012 r. inspektor ochrony danych osobowych w Banku przedstawił dowody mające potwierdzić usunięcie uchybień stwierdzonych w toku kontroli.

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

Zgodnie z § 4 pkt 1 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.

W toku kontroli ustalono, że w Banku na dokumentację stanowiącą politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych składają się dokumenty o nazwach: „Zbiory danych osobowych przetwarzanych przez Bank S.A. w W.”, „Zasady ochrony danych osobowych w Banku S.A. w W.”, stanowiące załącznik nr […] do zarządzenia nr […] Prezesa Zarządu Banku z dnia […] marca 2008 r., „Zasady bezpieczeństwa informacji”, stanowiące załącznik nr […] do zarządzenia nr […] Prezesa Zarządu Banku z dnia […] kwietnia 2010 r., zarządzenie nr […] Prezesa Zarządu Banku z dnia […] października 2007 r. „Zasady i standardy zapewnienia ciągłości działalności biznesowej w Banku S.A. w W.”, „Procedura tworzenia i zarządzania kontami użytkowników w domenie […]), „Procedura zapobiegania zagrożeniom wirusami komputerowymi i reakcji na występujące infekcje wirusowe”,

„Ochrona antywirusowa stacji roboczych zarządzanych przez […]", „Dokumentacja procesu przeglądu uprawnień na zasobach sieciowych", „Dokumentacja procesu zarządzania kopiami bezpieczeństwa". Jednocześnie w toku kontroli ustalono, że obszar przetwarzania danych osobowych określony został w planie ochrony. Informacji o tym nie wpisano jednak do dokumentacji stanowiącej politykę bezpieczeństwa, co stanowi naruszenie powołanego przepisu rozporządzenia.

W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego wskazano, że przygotowana została zmiana zarządzenia nr […] „Zasady Ochrony Danych Osobowych w Banku S.A. w W." polegająca na dodaniu zapisu doprecyzowującego informację na temat obszaru przetwarzania danych osobowych. Z zapisu tego wynika m.in., że wykaz budynków i pomieszczeń Banku składających się na obszar przetwarzania danych osobowych prowadzi Departament Nieruchomości. Nie przedstawiono jednak żadnego dokumentu, z którego wynikałoby, że wskazany departament rzeczywiście taki wykaz prowadzi. Ponadto, w powołanym zapisie zarządzenia nr […] nadal brak jest odniesienia do planu ochrony, w którym, jak ustalono w toku kontroli, został określony obszar przetwarzania danych osobowych. W konsekwencji nie można uznać, że w tym zakresie przywrócony został stan zgodny z prawem.

Jednocześnie, na podstawie złożonych przez inspektora ochrony danych osobowych w Banku pisemnych wyjaśnień oraz przedstawionych dowodów, należy stwierdzić, że pozostałe uchybienia w procesie przetwarzania danych osobowych, stanowiące przedmiot postępowania, zostały usunięte, tj.:

1. Na ewidencję osób upoważnionych do przetwarzania danych osobowych składa się rejestr osób zatrudnionych w Banku oraz rejestr osób uprawnionych do dostępu do określonej opcji systemu informatycznego, które zawierają wszystkie określone w art. 39 ust. 1 ustawy informacje.
2. Dane osobowe pracowników podmiotów współpracujących z Bankiem w zakresie […] przetwarzane są w ramach zbioru danych osobowych o nazwie „X", który został zgłoszony przez Bank do rejestracji Generalnemu Inspektorowi.
3. Zbiór danych osobowych o nazwie „X" został umieszczony w dokumencie o nazwie „Zbiory danych osobowych przetwarzanych przez Bank S.A. w W.". Ww. dokument został uzupełniony o programy zastosowane do przetwarzania danych w tym zbiorze.
4. Wprowadzony został proces polegający na zmianie haseł dostępu do danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […] co 30 dni.

Ustosunkowując się do wymienionych w odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego powodów, dla których w Banku częstotliwość zmiany hasła

dostępu do danych osobowych pracowników podmiotów współpracujących z nim w zakresie […] określona została na 90 dni, a w szczególności do powołanych w niej decyzji Generalnego Inspektora Ochrony Danych Osobowych, wskazać należy, że decyzje nr […] z dnia […] maja 2009 r. oraz nr […] z dnia […] maja 2009 r. zostały wydane w sprawach dotyczących przekazywania danych osobowych do państw trzecich. Należy w tym miejscu wskazać, że art. 48 ustawy wymaga dla przekazania danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, zapewnienia przez administratora danych odpowiedniego zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, oraz uzyskania zgody Generalnego Inspektora Ochrony Danych Osobowych. Odpowiedniość zabezpieczeń, o których mowa w ww. przepisie ustawy, nie jest jednak równoznaczna z koniecznością wdrożenia rozwiązań tożsamych z wymogami określonymi w ustawie o ochronie danych osobowych, w szczególności w odniesieniu do środków technicznych i organizacyjnych. Istotne jest natomiast to, aby zastosowane środki zabezpieczały prywatność oraz prawa i wolności osoby, której dane dotyczą. I to właśnie jest przedmiotem oceny Generalnego Inspektora. W konsekwencji, może on uznać, że zastosowane środki zabezpieczają prywatność oraz prawa i wolności osoby, której dane dotyczą, nawet wówczas gdy nie są one identyczne z tymi, które obowiązują na terytorium Rzeczypospolitej Polskiej. Natomiast w przypadku Banku obowiązek zmiany hasła wynika z części A pkt IV ust. 2 załącznika do rozporządzenia, który nie pozwala na dokonywanie żadnych ocen pod kątem odpowiedniości zabezpieczenia (tak jak jest to w przypadku art. 48 ustawy) – hasło jest zmieniane co 30 dni albo nie jest zmieniane z taką częstotliwością. Z uwagi na to, że w opisanej sytuacji znajdują zastosowanie różne przepisy o ochronie danych osobowych, nie można mówić o naruszeniu wynikającej z art. 32 Konstytucji zasady równości.

Bank, pomimo zawarcia w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego uwag na temat zasadności zmiany hasła co 30 dni, wprowadził jednak wymóg zmiany hasła dostępu do danych osobowych pracowników podmiotów współpracujących z nim w zakresie […] z częstotliwością wymaganą przez przepis części A pkt IV ust. 2 załącznika do rozporządzenia, przywracając tym samym stan zgodny z prawem w tym zakresie. Na marginesie należy jedynie zauważyć, że z załączonych do ww. pisma Banku procedur dotyczących zmiany hasła wynika, że hasło to „musi być co najmniej 6 znakowe". Tymczasem z ustaleń kontroli wynika, że przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […], połączone jest z siecią publiczną. Oznacza to wymóg stosowania hasła składającego się z co najmniej 8 znaków (część B pkt VIII załącznika do rozporządzenia).

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

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

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

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.

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.).