



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 21 maja 2008 r.

DIS/DEC-306/12915/08

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. 23 ust. 1 pkt 1 i art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Bank S.A.,

I. Nakazuję Bankowi S.A., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

- 1) przetwarzanie danych osobowych użytkowników imiennych przedpłaconych kart płatniczych na podstawie zgody wyrażonej przez użytkowników ww. kart, w terminie trzech miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna,**
- 2) realizację obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), wobec użytkowników imiennych przedpłaconych kart płatniczych, w terminie trzech 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 (sygn. akt [...]) w Banku S.A., zwanym dalej Bankiem, w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, 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. z 2004 r., Nr 100, poz. 1024) zwanym dalej rozporządzeniem.

W toku kontroli odebrano od pracowników Banku ustne wyjaśnienia skontrolowano systemy informatyczne, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Wiceprezesa Zarządu Banku S.A.

Na podstawie zgromadzonego w toku kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, Bank S.A., jako administrator danych osobowych naruszyła przepisy o ochronie danych osobowych poprzez:

- 1) przetwarzanie bez podstawy prawnej danych osobowych użytkowników imiennych przedpłaconych kart płatniczych (art. 26 ust. 1 pkt 1 ustawy),
- 2) nierealizowanie wobec użytkowników imiennych przedpłaconych kart płatniczych obowiązku informacyjnego, o którym mowa w art. 25 ust. 1 ustawy,
- 3) przetwarzanie bez podstawy prawnej danych osobowych użytkowników bezimiennych przebieganych kart płatniczych, gdyż oświadczenie składane telefonicznie przez użytkowników ww. kart nie stanowi zgody na przetwarzanie danych osobowych przez Bank w rozumieniu art. 7 pkt 5 ustawy; zgoda wyrażana przez te osoby dotyczy bowiem aktywowania karty, a nie przetwarzania danych osobowych.

W odpowiedzi na zawiadomienie o wszczęciu postępowania Inspektor Ochrony Danych Osobowych w Banku umocowany na podstawie pełnomocnictwa z dnia [...] września 2007 r. do składania oświadczeń woli oraz innych oświadczeń i wykonywania wszelkich innych czynności w toku postępowań prowadzonych przed Generalnym Inspektorem, złożył m. in. następujące wyjaśnienia:

- 1) umowy o wydanie przedpłaconych kart płatniczych oraz obsługę operacji dokonywanych przy ich użyciu są typowymi umowami o świadczenie usług, do których stosuje się odpowiednio przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 1964 r. Nr 16, poz. 93 z późn. zm.) dotyczące umów zlecenie oraz ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. Nr 169, poz. 1385 z późn. zm.); zleceniodawcą usługi jest podmiot gospodarczy, który zleca Bankowi, jako zleceniobiorcy, wydanie i obsługę kart płatniczych w celu określonym przez ten podmiot,
- 2) Bank działa według dyspozycji, instrukcji posiadacza rachunku (zleceniodawcy), posiadacz jako administrator danych osobowych użytkowników kart imiennych i jedyny ich dysponent przekazuje je w celach określonych w załączniku do umowy o wydanie przedpłaconych kart płatniczych,

- 3) władcza pozycja posiadacza rachunku, jako zlecniodawcy i administratora danych osobowych, polega na tym, iż jest on jedynym gestorem i zarządcą praw do środków, którymi rozporządza, przekazując je użytkownikom i używając do tego przekazu Banku oraz infrastruktury technicznej; tylko posiadacz rachunku może decydować o przyznaniu bądź odebraniu karty użytkownikowi,
- 4) wszelkie spory związane z przyznaniem oraz zwrotem środków w ramach przedpłaconych kart płatniczych, rozstrzygnięte zostaną bezpośrednio z użytkownikiem karty przez posiadacza, bez jakiegokolwiek zaangażowania ze strony Banku,
- 5) Bank i użytkownik są związani instrukcjami posiadacza od początku zlecenia do jego wykonania, zgodnie z wolą posiadacza; określenie celów przetwarzania danych jest niezbywalnym prawem przynależnym posiadaczowi rachunku, który powierza ich przetwarzanie Bankowi w celu ściśle określonym w umowie,
- 6) Bank pełni rolę wyłącznie wykonawcy zlecenia, a do wykonania tego zlecenia są mu niezbędne dane, którymi dysponuje zlecniodawca; dane osobowe nie mogą być zebrane przez Bank, a wyłącznie przez posiadacza rachunku,
- 7) Bank decyduje o środkach technicznych czyli o zastosowaniu określonych aplikacji informatycznych niezbędnych do obsługi kart przedpłaconych; infrastruktura techniczna, którą dysponuje Bank, jako zlecniobiorca, stanowi narzędzie techniczne niezbędne do realizacji celów określonych przez zlecniodawcę; w przypadku imiennych kart przedpłaconych Bank uzyskuje od posiadacza tylko taki zakres danych, jaki jest niezbędny do bezpiecznej obsługi transakcji dokonywanych za pomocą tych kart, zatem zakres danych wynika wprost, bezpośrednio z celu, który określa posiadacz – administrator tych danych,
- 8) decydowanie przez Bank o zastosowanych środkach technicznych, bez jednoczesnej możliwości decydowania przez Bank o celach przetwarzania, nie stanowi przesłanki do uznania Banku za administratora danych osobowych przetwarzanych w procesie imiennych kart przedpłaconych,
- 9) umowa o wydanie przedpłaconych kart płatniczych oraz obsługę operacji dokonywanych przy ich użyciu zawarta pomiędzy Bankiem a posiadaczem rachunku jest klasyczną umową zlecenia zawierającą wszystkie wymagane prawem elementy charakterystyczne dla umowy powierzenia; cel powierzenia przetwarzania danych został sformułowany w § 2 ust. 8 wskazanej umowy, a jego zakres w stanowiących jej integralną część załącznikach,
- 10) ze względu na brak podstaw do uznania Banku za administratora danych osobowych użytkowników kart imiennych, Bank nie powinien spełniać obowiązków nałożonych na administratorów danych wynikających z art. 25 ustawy; obowiązki te są realizowane przez administratorów danych osobowych,
- 11) oświadczenie składane przez użytkownika podczas aktywowania karty bezimiennnej nie stanowi domniemanej bądź dorozumianej zgody lecz klauzula zgody jasno informuje iż aktywowanie karty jest równoznaczne ze zgodą na przetwarzanie danych osobowych,

12) odmiennie, niż w przypadku imiennych kart przedpłaconych, Bank występuje w roli administratora danych bezimiennych kart przedpłaconych, gdyż posiadacz nie powierza Bankowi przetwarzania danych osobowych, dane te Bank zbiera w momencie, kiedy zgłosi się do niego telefonicznie użytkownik, któremu posiadacz przekazał nieaktywną kartę; zbieranie danych, a następnie inne formy ich przetwarzania odbywają się na podstawie utrwalanej w systemie informatycznym zgody osoby, która zgłasza się telefonicznie.

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

W toku kontroli ustalono, iż Bank S.A. oferuje dwa rodzaje przedpłaconych kart płatniczych: imienne i bezimienne. Produkty są skierowane do podmiotów z sektora prywatnego oraz publicznego, natomiast nie są przeznaczone dla osób indywidualnych. Umowa o wydanie przedpłaconych kart płatniczych oraz obsługę operacji dokonywanych przy ich użyciu zawierana jest z podmiotem, który staje się posiadaczem karty i może ją przekazać do użytkowania wybranym przez siebie osobom fizycznym. Wyłącznie posiadacz karty decyduje o przyznaniu bądź o odebraniu karty użytkownikowi.

Celem zbierania przez Bank danych użytkowników imiennych i bezimiennych przedpłaconych kart płatniczych jest obsługa tych kart, tzn. możliwość zastrzeżenia karty w chwili jej utraty, przyjęcia reklamacji od użytkownika, sprawdzenia przez użytkownika stanu transakcji na karcie, możliwość weryfikacji z danymi podanymi przez posiadacza w przypadku aktywacji kart imiennych.

W przypadku wydawania kart imiennych posiadacz wskazuje użytkowników kart przekazując Bankowi ich dane osobowe obejmujące: imię i nazwisko, nr PESEL, datę urodzenia, adres. Dane przekazywane są elektronicznie za pośrednictwem udostępnionego przez Bank systemu o nazwie „A” lub na nośniku CD. Z treści umowy o wydanie przedpłaconej imiennej karty płatniczej wynika, że „Posiadacz, jako administrator danych zbioru danych osobowych Użytkowników Kart, zobowiązuje się do uzyskania zgody każdego Użytkownika karty na przetwarzanie jego danych osobowych objętych ochroną danych osobowych oraz tajemnicą bankową, w tym na ich udostępnianie przez Bank stronom trzecim w kraju i za granicą w zakresie niezbędnym do wydawania i należytej obsługi Kart. Ryzyko związane z uzyskaniem zgody leży po stronie Posiadacza. Posiadacz uzyska od Użytkowników oświadczenie następującej treści: Potwierdzam, iż zostałem poinformowany o tym, że moje dane osobowe zostaną udostępnione Bankowi S.A. w celu wykonywania przez niego czynności bankowych niezbędnych do obsługi Karty Płatniczej [...]”

Dane osobowe użytkowników bezimiennych kart płatniczych w następującym zakresie: imię i nazwisko, nr PESEL, data urodzenia, adres, są udostępniane Bankowi bezpośrednio przez

użytkownika w chwili telefonicznego aktywowania karty. Zgoda na przetwarzanie danych osobowych wyrażana telefonicznie przez użytkownika jest nagrywana na nośnik magnetyczny w celach dowodowych. Wyrażenie zgody nie jest potwierdzane pisemnie. W trakcie połączenia telefonicznego odtwarzane jest nagranie zawierające następującą informację: „Bank S.A. informuje, iż Pani/Pana dane osobowe będą przetwarzane przez Bank i podmioty z nim współpracujące, w celu obsługi karty, ma Pani/Pan prawo do dostępu do swoich danych oraz ich poprawiania. Aktywowanie karty jest równoznaczne ze zgodą na przetwarzanie Pani/Pana danych, w tym w zagranicznych ośrodkach obliczeniowych [...], której Bank jest członkiem. Czy chce Pani/Pan aktywować kartę?”

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Umowa powierzenia przetwarzania danych osobowych jest najczęściej umową o świadczenie usług, do której stosuje się przepisy dotyczące umowy zlecenia. Za niepoprawne należy uznać jednak przedstawione przez Bank rozumowanie, zgodnie z którym fakt, iż umowa o wydanie przedpłaconej imiennej karty płatniczej jest umową zlecenia decyduje o uznaniu jej za umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ust. 1 ustawy. Mimo, iż w większości do umów powierzenia przetwarzania danych osobowych będą miały zastosowanie przepisy dotyczące umów zlecenia, to nieuprawnione jest twierdzenie, iż każda umowa zlecenie, której przedmiotem jest, m. in. przetwarzanie danych osobowych, należy traktować jako umowę powierzenia przetwarzania tych danych. Zasadniczą kwestią decydującą o uznaniu, czy podmiot przetwarzający dane osobowe jest ich administratorem jest stwierdzenie, czy decyduje on o celach i środkach przetwarzania tych danych. Nie można zgodzić się ze stanowiskiem Banku, jakoby nie decydował on o celach i środkach przetwarzania danych, tylko dokonywał operacji na danych w wykonaniu umowy powierzenia. Wykładania przepisów ustawy o ochronie danych osobowych nie sprzeciwia się możliwości przyznania przymiotu administratora danych obu stronom umowy, jeżeli każda z nich w swoim zakresie decyduje o ww. okolicznościach. Należy zgodzić się ze stwierdzeniem strony postępowania, iż podmiot zlecający obsługę przedpłaconych kart imiennych jest administratorem danych użytkowników tych kart. Nie wyklucza to jednak uznania Banku za administratora danych przekazanych przez podmiot zlecający. Ze zgromadzonego materiału dowodowego jednoznacznie wynika, że podmiot zlecający nie decyduje o zakresie danych zbieranych na potrzeby obsługi ww. kart. W gestii Banku pozostaje natomiast określenie zakresu i celu przetwarzania danych niezbędnych do obsługi stworzonego przez Bank produktu.

Jednocześnie należy wykazać brak konsekwencji w argumentacji przedstawionej przez Bank, zgodnie z którą sposób zebrania danych (bezpośrednio od osób, których dane dotyczą – w przypadku kart bezimiennych lub za pośrednictwem posiadacza karty – w przypadku kart imiennych) przesądza o uznaniu za administratora danych, bądź za podmiot, o którym mowa w art.

31 ust. 1 ustawy. W ocenie Generalnego Inspektora, sposób zbierania danych pozostaje bez wpływu na uznanie, czy Bankowi przysługuje przymiot administratora danych użytkowników zarówno jednych jak i drugich z wymienionych wyżej kart, czy też wyłącznie użytkowników kart bezimiennych. W szczególności, należy powołać § 1, który został sformułowany w identyczny sposób zarówno umowach o wydanie przedpłaconych kart płatniczych oraz operacji dokonywanych przy ich użyciu odnoszących się do kart imiennych jak i bezimiennych, który brzmi: Bank działając według dyspozycji Posiadacza wyda Karty w celu ich przekazania zaakceptowanym przez Posiadacza Użytkownikom oraz zobowiązuje się wobec Posiadacza do rozliczania Operacji dokonanych przy użyciu Karty”.

Wobec powyższych ustaleń należy uznać, że Bank jest administratorem danych osobowych użytkowników imiennych przedpłaconych kart płatniczych, a zatem powinien legitymować się przynajmniej jedną przesłanką wskazaną w art. 23 ust. 1 ustawy. W przedmiotowej sytuacji podstawę prawną przetwarzania danych ww. osób powinna stanowić zgoda na przetwarzania danych osobowych, czyli przesłanka, o której mowa w art. 23 ust. 1 pkt 1 ustawy.

Zgodnie z art. 25 ust. 1 ustawy, w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych, o : 1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku; 2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych; 3) źródle danych; 4) prawie dostępu do treści swoich danych oraz ich poprawiania; 5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 ustawy.

Konsekwencją uznania Banku za administratora danych osobowych użytkowników imiennych przedpłaconych kart płatniczych jest konieczność stwierdzenia, iż Bank powinien spełniać ustawowe obowiązki nałożone na administratorów danych, w tym jest zobligowany do informowania osób, których dane dotyczą, o okolicznościach wskazanych w art. 25 ust. 1 ustawy o ochronie danych osobowych. Bank nie realizuje ww. obowiązku.

Jednocześnie należy podkreślić, że sposób wykonania nakazu pozyskiwania przez Bank jako administratora danych osobowych zgody na przetwarzanie danych osobowych użytkowników imiennych przedpłaconych kart płatniczych oraz nakazu spełnienia wobec tych osób obowiązku informacyjnego jest pozostawiony adresatowi niniejszej decyzji. Nie jest zatem wymagane, aby Bank bezpośrednio dopełniał ww. obowiązków, może to uczynić również za pośrednictwem podmiotu, który zleca obsługę imiennych przedpłaconych kart płatniczych (posiadacza).

Stosowanie 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). Należy uznać argumentację strony, w której wykazano, iż treść oświadczenia składanego telefonicznie podczas aktywowania bezimiennej przedpłaconej karty płatniczej wskazuje jednoznacznie na wyrażenie zgody na przetwarzanie przez Bank danych osobowych użytkownika ww. karty.

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.