GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH

dr Wojciech R. Wiewiórowski

Warszawa, dnia 27 marca 2012 r.

DIS/DEC-264/12/20327

dot. […]

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 pkt 6 oraz art. 22 w związku z art. 26 ust. 1 pkt 3 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.) oraz § 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Bank S.A.,

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

1. **Zaprzestanie pozyskiwania danych pracowników podmiotów współpracujących z Bankiem S.A. w zakresie […], dotyczących ich niekaralności za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę ich rzetelności i wiarygodności oraz prowadzonych wobec nich postępowań karnych, w terminie 2 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**
2. **Usunięcie zebranych danych pracowników podmiotów współpracujących z Bankiem S.A. w zakresie […], dotyczących ich niekaralności za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę ich rzetelności i**

wiarygodności oraz prowadzonych wobec nich postępowań karnych, w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

3. **Zgłoszenie prowadzonego zbioru danych osobowych pracowników podmiotów współpracujących z Bankiem S.A. w zakresie […] do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Modyfikację systemu informatycznego o nazwie „A", tak aby system ten zapewniał 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 oraz 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 6 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

U z a s a d n i e n i e

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili w Banku S.A., zwanym dalej Bankiem, kontrolę 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, i 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 pełnomocnika 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. Zbieraniu od pracowników podmiotów współpracujących z Bankiem w zakresie […] oświadczeń o karalności zawierających dane dotyczące ich niekaralności za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę ich rzetelności i wiarygodności oraz prowadzonych wobec nich postępowań karnych (art. 26 ust. 1 pkt 3 ustawy).
2. Niezgłoszeniu prowadzonego zbioru danych osobowych pracowników podmiotów współpracujących z Bankiem w zakresie […] do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (art. 40 ustawy).
3. Niezapewnianiu przez system informatyczny o nazwie „A" dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu oraz sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia (§ 7 ust. pkt 1 i 2 oraz § 7 ust. 3 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 pełnomocnik Banku pismem z dnia […] lutego 2012 r., nr […], złożył wyjaśnienia, w których poinformował, że:

1. Bank zaprzestaje przetwarzania informacji o niekaralności pracowników przedsiębiorców, z którymi zawarł umowę o współpracy na podstawie art. 6a ust. 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r. Nr 72, poz. 665 z późn. zm.).
2. Administratorem danych osobowych pracowników przedsiębiorcy, z którym Bank zawarł umowę o współpracy na podstawie art. 6a ust. 1 Prawa bankowego, jest ten przedsiębiorca jako pracodawca. To pracodawca decyduje o celach i środkach przetwarzania danych osobowych swoich pracowników, w tym jest uprawniony do ujawnienia danych osobowych pracowników w celu realizacji zadań służbowych. Generalny Inspektor Ochrony Danych Osobowych w decyzji nr […] stwierdził, że pracodawca może się posługiwać danymi służbowymi pracownika w ramach prowadzonej przez siebie działalności, jeżeli zakres przetwarzanych danych nie wkracza w sferę prywatności pracownika (sprawozdanie za 2002 r., str. 120). Bank otrzymuje dane pracowników przedsiębiorców, z którymi zawarł umowę o współpracy na podstawie art. 6a ust. 1 Prawa bankowego, w celu realizacji tej umowy. Bank nie decyduje o

celu i środkach przetwarzania danych osobowych. Bank należy w tym przypadku traktować jako odbiorcę danych, a nie administratora danych.

3. System „A", w którym przechowywane są udostępnione dane, nie umożliwia wyszukania pracowników według określonego kryterium. Przeszukiwanie bazy poprzez NIP i nazwę oraz adres siedziby […] umożliwia odnalezienie informacji o przedsiębiorcy, w tym o jego pracownikach.
4. Udostępnienie danych osobowych wymaga spełnienia chociaż jednej z przesłanek legalizujących przetwarzanie danych osobowych. Udostępnienie przez pracodawcę – podmiot współpracujący, z którym Bank zawarł umowę o współpracy w zakresie […], niezbędnych danych osobowych pracownika jest dopuszczalne, kiedy jest usprawiedliwione celem działania pracodawcy i nie narusza praw i wolności pracownika, a zatem spełnia przesłankę, o której mowa w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych.
5. Z uwagi na to, że Bank nie jest administratorem danych pracowników podmiotu, z którym zawarł umowę o współpracy na podstawie art. 6a ust. 1 Prawa bankowego, nie ciążą na nim określone w ustawie o ochronie danych osobowych i rozporządzeniach wykonawczych do tej ustawy obowiązki, w tym wynikające z treści art. 40 i rozdziału 5 ww. ustawy.

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.

Przeprowadzona kontrola wykazała, że jednym z wymogów wynikającym z powołanych wyżej wewnętrznych przepisów Banku, który musi spełnić podmiot zamierzający współpracować z Bankiem w zakresie […], jest przekazanie danych osobowych swoich pracowników, którzy mają wykonywać czynności powierzone przez Bank. Przekazanie tych danych związane jest ze składanym przez te osoby „oświadczeniem o niekaralności oraz o wyrażeniu zgody na przetwarzanie danych osobowych przez […]". Wzór tego oświadczenia został wprowadzony decyzją nr […] Dyrektora Zarządzającego kierującego Pionem […] z dnia […] lipca 2010 r. i zmieniony na mocy wytycznych wprowadzonych w dniu […] czerwca 2011 r. Pracownik podmiotu, który ma współpracować z Bankiem w zakresie […], wypełniając ww. oświadczenie podaje swoje imię, nazwisko, nr PESEL, serię i nr dowodu osobistego oraz oświadcza w szczególności, że nie był karany prawomocnym wyrokiem sądu za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę ich rzetelności i wiarygodności oraz, że nie jest

prowadzone wobec niego postępowanie karne. Uzasadnieniem dla żądania przez Bank danych o niekaralności od ww. osób jest konieczność zapewnienia należytego poziomu bezpieczeństwa działalności Banku, w tym przede wszystkim interesów klientów Banku w związku z powierzaniem wykonywania czynności z zakresu […] osobom niebędącym pracownikami Banku. Szczegółowe uzasadnienie pozyskiwania tego typu danych zostało zawarte w opinii prawnej przygotowanej przez radcę prawnego Banku.

Podany przez Bank powód, dla którego są zbierane od pracowników podmiotów współpracujących z Bankiem w zakresie […] oświadczenia o niekaralności, nie może zostać jednak uznany za uzasadnienie przetwarzania tych danych. Wskazać bowiem należy, że warunki, na jakich Bank może powierzyć innemu przedsiębiorcy wykonywanie czynności faktycznych związanych z działalnością bankową, zostały określone w art. 6a – 6c Prawa bankowego. Żaden z tych przepisów (jak również żaden inny przepis Prawa bankowego) nie formułuje jednakże wymogów, jakie mają spełniać pracownicy tych podmiotów, a w szczególności nie wskazuje, że mają oni składać oświadczenia, że nie byli karani prawomocnym wyrokiem sądu za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę ich rzetelności i wiarygodności oraz, że nie jest prowadzone wobec nich postępowanie karne. Należałoby tymczasem uznać, że racjonalny ustawodawca przy określaniu ww. warunków wprowadziłby do tych przepisów obowiązek wykonywania powierzonych czynności przez osoby, które nie były karane, gdyby uznał, że w ten sposób rzeczywiście zostanie zapewniony należyty poziom bezpieczeństwa działalności banków, w tym interesów klientów banków, w związku z powierzaniem wykonywania czynności z zakresu […] osobom niebędącym pracownikami banku.

Należy także zauważyć, że zbieranie oświadczeń o niekaralności od pracowników podmiotów współpracujących z Bankiem w zakresie […] prowadzi do konieczności naruszenia przez te podmioty przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r., Nr 21, poz. 94 z późn. zm.), które w art. 22^1 określiły dopuszczalny zakres danych osobowych, które pracodawca może zbierać od osób, które zatrudnia. Jednocześnie żaden przepis prawa, a w szczególności Prawa bankowego, o czym wyżej wspomniano, nie pozwala na rozszerzenie określonego w art. 22^1 Kodeksu Pracy katalogu danych, które mogą być zbierane od pracowników przez pracodawców.

Przeciwko zbieraniu przedmiotowych oświadczeń przemawia również zakres czynności, do wykonywania których w świetle zawartych umów o współpracy są uprawnieni pracownicy podmiotów współpracujących z Bankiem w zakresie […]. Z przedłożonych w toku kontroli przykładowych umów wynika, że […] jest uprawniony jedynie do przyjęcia wniosku o kredyt / pożyczkę wraz z dokumentacją, co oznacza, że ostateczną decyzję w tych sprawach podejmuje Bank. Takie rozwiązanie jest bez wątpienia rozwiązaniem zapewniającym należyty poziom

bezpieczeństwa działalności Banku, w tym interesów klientów Banku, w związku z powierzaniem wykonywania czynności z zakresu […] osobom niebędącym pracownikami banku. Konsekwencją przyjętego rozwiązania w ww. zakresie jest jednak również konieczność uznania, że zbieranie oświadczeń o karalności od pracowników podmiotów współpracujących z Bankiem w zakresie […] prowadzi do nadmiernego pozyskiwania danych od ww. osób, co jest niezgodne z art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych.

W piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego pełnomocnik Banku poinformował, że Bank zaprzestaje przetwarzania informacji o niekaralności pracowników przedsiębiorców, z którymi zawarł umowę o współpracy na podstawie art. 6a ust. 1 Prawa bankowego. Z ww. pisma nie wynika jednak, jakie działania Bank podjął w celu usunięcia stwierdzonego w toku kontroli uchybienia, a w szczególności, czy zmienione zostały postanowienia umów o współpracy zobowiązujące podmioty współpracujące za Bankiem w zakresie […] do przekazywaniu mu oświadczeń o karalności zawierających dane o niekaralności za przestępstwa przeciwko mieniu, dokumentom oraz innym, których charakter może mieć wpływ na ocenę rzetelności i wiarygodności oraz prowadzonych postępowaniach karnych wobec pracowników ww. podmiotów, a także, czy dane już zebrane zostały usunięte. Sama zatem deklaracja pełnomocnika Banku o zaprzestaniu przetwarzania przez Bank kwestionowanych danych nie może stanowić podstawy do uznania, że w ww. zakresie przywrócony został stan zgodny z prawem.

Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

W toku kontroli ustalono, że dane osobowe pracowników podmiotu współpracującego z Bankiem w zakresie […] (obejmujące w szczególności imię, nazwisko, nr PESEL, nazwę i adres miejsca pracy, zajmowane stanowisko oraz służbowy adres poczty elektronicznej i numery telefonów służbowych) są wprowadzane do systemu informatycznego o nazwie „A”. Wskazany system umożliwia przeszukiwanie bazy poprzez NIP i nazwę oraz adres siedziby […]. Istnienie tego kryterium dostępu do danych przesądza o tym, że dane przetwarzane przy użyciu ww. systemu informatycznego tworzą zbiór danych osobowych w rozumieniu art. 7 pkt 1 ustawy. Jednocześnie nie zachodzi żadna z przesłanek wyłączających omawiany obowiązek, wymienionych w art. 43 ust. 1 ustawy. Zbiór ten nie został jednak zgłoszony przez Bank do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Zgodnie z § 7 ust. 1 pkt 1 i pkt 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.

W toku kontroli ustalono, że system informatyczny o nazwie „A" nie zapewnia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, odnotowania daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu, co stanowi naruszenie powołanego przepisu rozporządzenia.

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.

Przeprowadzona kontrola wykazała, że system informatyczny o nazwie „A" nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia, co stanowi naruszenie ww. przepisu rozporządzenia.

Ustosunkowując się do zawartego w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego twierdzenia pełnomocnika Banku, że na Banku nie ciążą obowiązki wynikające z art. 40 i rozdziału 5 ustawy o ochronie danych osobowych oraz rozporządzenia, wskazać należy, że przedsiębiorca, z którym Bank zawarł umowę o współpracy na podstawie art. 6a ust. 1 Prawa bankowego jest administratorem danych swoich pracowników jako pracodawca przetwarzający dane tych osób w celu realizacji obowiązków wynikających z prawa pracy. Administratorem danych ww. osób, w zakresie przekazanym przez przedsiębiorców dla realizacji zawartej umowy współpracy, jest, wbrew twierdzeniu pełnomocnika, jednak również Bank S.A. Bank przetwarza bowiem dane wskazanych osób dla realizacji swoich własnych celów, do których należy w szczególności przeprowadzanie weryfikacji tych osób, tj. sprawdzenie ich, czy w stosunku do nich nie było zastrzeżeń w związku z naruszeniem przez nich procedur bankowych lub przepisów prawa. Bank decyduje również o środkach tego przetwarzania, wprowadzając dane do własnego systemu informatycznego (systemu o nazwie „A") oraz określając procedury dotyczące przetwarzania tych danych. Co więcej, to Bank opracował wzór umowy o współpracy nakładając na przedsiębiorców chcących z nim współpracować w zakresie […] określone obowiązki. Jeden z tych obowiązków dotyczy przekazania danych osobowych tych pracowników, którzy mają wykonywać czynności powierzone przez Bank. Przekazane Bankowi na podstawie umów o współpracy dane osobowe pracowników ww. przedsiębiorców są włączane do prowadzonego zbioru danych osobowych (są w szczególności wprowadzane, o czym już wyżej wspomniano, do systemu informatycznego o nazwie „A"). Bank określając cele i środki przetwarzania danych wskazanych osób jest zatem nie tylko odbiorcą tych danych, ale także, wbrew twierdzeniu pełnomocnika Banku, staje się jednocześnie ich administratorem. Jak bowiem podnosi się w literaturze przedmiotu, „pojęciem <odbiorcy danych> są objęci administratorzy

danych, którym dane zostały udostępnione w celu włączenia do zbioru (…)" (P. Barta, P. Litwiński „Ustawa o ochronie danych osobowych. Komentarz", Warszawa 2009 r., str.147 – 148). W konsekwencji na Banku, jako administratorze danych pracowników podmiotów współpracujących z nim w zakresie […], przekazanych mu przez te podmioty w związku z zawartą umową współpracy, ciążą obowiązki wynikające z przepisów o ochronie danych osobowych, w tym obowiązki określone w art. 40 ustawy o ochronie danych osobowych i jej rozdziale 5 oraz w rozporządzeniu.

Przywołany przez pełnomocnika Banku w piśmie stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania administracyjnego fragment sprawozdania z działalności Generalnego Inspektora Ochrony Danych Osobowych za 2002 r. odnosi się do istnienia podstawy prawnej udostępniania przez pracodawcę danych służbowych swoich pracowników innym podmiotom, a nie do istnienia bądź nie istnienia obowiązku zgłoszenia przez podmiot, któremu te dane zostały udostępniane, powstałego w ten sposób zbioru danych osobowych. Na marginesie należy jedynie zwrócić uwagę na to, że w przywołanym fragmencie sprawozdania jest mowa o danych służbowych pracownika, do których nie zalicza się nr PESEL, a który to jest pozyskiwany przez Bank od pracowników podmiotów współpracujących z nim w zakresie […]. Należy także podkreślić, że Generalny Inspektor Ochrony Danych Osobowych nie kwestionuje podstawy prawnej przetwarzania przez Bank danych osobowych pracowników ww. podmiotów (kwestionowany jest jedynie zakres pozyskiwanych danych, co zostało już wyżej wykazane).

Pełnomocnik wskazuje ponadto, że przeszukiwanie bazy systemu informatycznego o nazwie „A", w którym przechowywane są udostępnione Bankowi dane, poprzez NIP i nazwę oraz adres siedziby […] umożliwia odnalezienie informacji o przedsiębiorcy, w tym o jego pracownikach. Możliwe jest zatem wyszukanie danych przy użyciu określonego kryterium, co oznacza w konsekwencji, że spełnione zostały warunki niezbędne do uznania, że określony zestaw danych jest zbiorem danych osobowych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych.

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

Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i 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.).