



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 18 sierpnia 2009 r.

DIS/DEC – 826/30202/09

dot. DIS-K-421/98/09

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 (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), art. 12 pkt 2 i art. 22 w związku z art. 36 ust. 2 i art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 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. z 2004 r., Nr 100, poz. 1024), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez XYZ Otwarty Fundusz Emerytalny reprezentowany przez XYZ Powszechne Towarzystwo Emerytalne S. A. z siedzibą w (...),

I. Nakazuję XYZ Otwartemu Funduszowi Emerytalnemu reprezentowanemu przez XYZ Powszechne Towarzystwo Emerytalne S. A. z siedzibą w (...), jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez nadanie osobom dopuszczonym do przetwarzania danych osobowych upoważnień do przetwarzania danych osobowych, w terminie miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.

II. W pozostałym zakresie postępowania umarzam.

Uzasadnienie

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę (sygn. akt GI-DIS-K-411/98/09) w XYZ Powszechne Towarzystwo Emerytalne S. A. z siedzibą w (...) (dalej: Towarzystwo), 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. Zakresem kontroli objęto zabezpieczenie danych osobowych członków XYZ Otwartego Funduszu Emerytalnego, które są przesyłane w sieci publicznej. W toku kontroli odebrano od pracowników Towarzystwa ustne wyjaśnienia, skontrolowano systemy informatyczne służące do przetwarzania danych osobowych oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez dwóch członków Zarządu Towarzystwa.

Na podstawie zgromadzonego w toku kontroli materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych, XYZ Otwarty Fundusz Emerytalny reprezentowany przez XYZ Powszechne Towarzystwo Emerytalne S. A. jako administrator danych osobowych naruszył przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Postanowienia „Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zasady zapobiegania ujawnianiu danych osobowych oraz sposób postępowania w sytuacji naruszenia ochrony danych osobowych” wprowadzonej uchwałą Nr 4 Zarządu Spółki z dnia 24 stycznia 2000 r. dotyczące tworzenia kopii zapasowych są niezgodne z faktycznie stosowanymi procedurami ich tworzenia (art. 36 ust. 2 ustawy, § 3 ust. 1 rozporządzenia).
2. Zarówno w „Polityce bezpieczeństwa informacji” wprowadzonej uchwałą Zarządu Towarzystwa z dnia 24 sierpnia 2005 r. Nr PTE/1/2/8/2005 oraz w „Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zasady zapobiegania ujawnianiu danych osobowych oraz sposób postępowania w sytuacji naruszenia ochrony danych osobowych” nie wskazano, aby postanowienia ww. dokumentacji odnosiły się do przetwarzania danych osobowych przez XYZ Otwarty Fundusz Emerytalny jako administratora danych osobowych członków tego funduszu (art. 36 ust. 2 ustawy, § 3 ust. 1 rozporządzenia).
3. Administrator danych nie nadał osobom dopuszczonym do przetwarzania danych osobowych upoważnień do przetwarzania danych osobowych (art. 37 ustawy).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w celu wyjaśnienia okoliczności sprawy (pismo sygn. DIS-K-421/98/09/26286).

W toku postępowania administracyjnego XYZ Powszechne Towarzystwo Emerytalne S. A. reprezentujące XYZ Otwarty Fundusz Emerytalny złożyło w piśmie z dnia 31 lipca 2009 r. (sygn. PTE/GI/2009/7/1) wyjaśnienia, w których poinformowano że:

1. Uchwałą Zarządu Towarzystwa z dnia 29 lipca 2009 r. nr PTE/ob/1/7/2009 przyjęto zmienioną procedurę wewnętrzną „Zarządzanie systemem informatycznym w celu ochrony danych osobowych w XYZ PTES.A.” likwidując tym samym rozbieżności pomiędzy przepisami wewnętrznymi a istniejącą praktyką w zakresie procedur tworzenia kopii zapasowych.
2. W zmienionej procedurze wewnętrznej „Zarządzanie systemem informatycznym w celu ochrony danych osobowych w XYZ PTE S.A.” uzupełniono brak w postaci wskazania, iż administratorem danych członków XYZ Otwartego Funduszu Emerytalnego jest ten fundusz. Jednocześnie w uchwale Zarządu Towarzystwa z dnia 29 lipca 2009 r. nr PTE/ob/1/7/2009 zmieniającą procedurę wewnętrzną „Zarządzanie systemem informatycznym w celu ochrony danych osobowych w XYZ PTES.A.” zawarto dodatkowy zapis, że postanowienia „Polityki bezpieczeństwa informacji” mają również zastosowanie do przetwarzania danych osobowych członków XYZ Otwartego Funduszu Emerytalnego przez ten fundusz, który jest ich administratorem.
3. Uchwałą Zarządu Towarzystwa z dnia 2 lipca 2009 r. Nr PTE/1/1/7/2009 osoba pełniąca funkcję Administratora Bezpieczeństwa Informacji została upoważniona do nadawania pracownikom upoważnień do przetwarzania danych osobowych. W ślad za powołaną uchwałą został opracowany wzór takiego upoważnienia, który będzie nadawany pracownikom dopuszczonym do przetwarzania danych osobowych poczynając od dnia 1 sierpnia 2009 r. Pracownicy zatrudnieni we wcześniejszym okresie będą otrzymywali takie upoważnienia sukcesywnie do dnia 20 września 2009 r.

Jednocześnie załączono dowody potwierdzające usunięcie uchybień, tj. kopię „Zarządzania systemem informatycznym w celu ochrony danych osobowych w XYZ PTE S.A.” wraz z uchwałą Zarządu Towarzystwa z dnia 29 lipca 2009 r. nr PTE/ob/1/7/2009 zmieniającą procedurę wewnętrzną „Zarządzanie systemem informatycznym w celu ochrony danych osobowych w Generali PTE S.A.”, a także kopię uchwały Zarządu Towarzystwa z dnia 2 lipca 2009 r. Nr PTE/1/1/7/2009, wzór upoważnienia do przetwarzania danych osobowych.

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

Zgodnie z art. 37 ustawy, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

W toku kontroli ustalono, iż od każdej osoby dopuszczonej do przetwarzania danych osobowych odbierane jest obligatoryjne oświadczenie, m.in. o zobowiązaniu do zachowania w tajemnicy danych osobowych, które nie spełnia wymogów upoważnienia do przetwarzania danych osobowych. Wobec powyższego należy uznać, że administrator danych nie nadał osobom

dopuszczonym do przetwarzania danych osobowych upoważnień, o których mowa w art. 37 ustawy. W piśmie z dnia 31 lipca 2009 r. (sygn. PTE/GI/2009/7/1) stanowiącym odpowiedź na zawiadomienie o wszczęciu postępowania poinformowano, że uchwałą Zarządu Towarzystwa z dnia 2 lipca 2009 r. Nr PTE/1/1/7/2009 osoba pełniącą funkcję Administratora Bezpieczeństwa Informacji została upoważniona do nadawania pracownikom upoważnień do przetwarzania danych osobowych. W ślad za powołaną uchwałą został opracowany wzór takiego upoważnienia, który będzie nadawany pracownikom dopuszczonym do przetwarzania danych osobowych poczynając od dnia 1 sierpnia 2009 r. Pracownicy zatrudnieni we wcześniejszym okresie będą otrzymywali takie upoważnienia sukcesywnie do dnia 20 września 2009 r. Należy jednak podkreślić, iż samo podjęcie działań w celu usunięcia uchybień nie stanowi podstawy do uznania, że został przywrócony stan zgodny z prawem. Powyższe okoliczności uwzględniono natomiast przy określaniu terminu na wydanie osobom dopuszczonym do przetwarzania danych osobowych upoważnień do przetwarzania danych osobowych.

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

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).

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.