GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

Warszawa, dnia 1 grudnia 2010 r.

DIS/DEC – 1321/47592/10
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 art. 22 w związku z art. 36 ust. 2 i art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), oraz § 4 pkt 2, pkt 3 i pkt 4, § 7 ust. 1 pkt 1 i pkt 2 oraz § 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 Dyrektora Urzędu Kontroli Skarbowej,

nakazuję

Dyrektorowi Urzędu Kontroli Skarbowej jako administratorowi danych, usunięcie uchybień w procesie przetwarzania danych osobowych poprzez:

1. Zmodyfikowanie systemu informatycznego o nazwie „A" (w którym przetwarzane są dane osobowe […]) w taki sposób, aby umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie:

- **odnotowanie daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego te dane do systemu, w terminie 4 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna;**
- **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 4 miesięcy od dnia, w którym niniejsza decyzja stanie się ostateczna.**

2. Uzupełnienie „Polityki Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]" o następujące elementy:

- **wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,**
- **opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązań między nimi,**
- **sposób przepływu danych pomiędzy poszczególnymi systemami**

oraz uwzględnienie w niej systemu informatycznego o nazwie „B", systemu informatycznego o nazwie „D" i systemu informatycznego o nazwie „C", z których korzystają pracownicy Urzędu Kontroli Skarbowej w ramach wykonywania swoich obowiązków służbowych, w terminie 30 dni 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 kontrolę w Urzędzie Kontroli Skarbowej, zwanym dalej również Urzędem, 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 m.in. odebrano od pracowników ustne wyjaśnienia, skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których

odbywa się przetwarzanie danych osobowych. Stan faktyczny został szczegółowo opisany w protokole kontroli (sygn. kontroli […]), który został podpisany przez Dyrektora Urzędu. Na podstawie całokształtu materiału dowodowego zgromadzonego w sprawie ustalono, że Dyrektor Urzędu Kontroli Skarbowej, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Stwierdzone uchybienia polegały na:

1. Niezapewnieniu, aby system informatyczny o nazwie „A" (w którym przetwarzane są dane osobowe […]) umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie odnotowanie daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego te dane do systemu (§ 7 ust. 1 pkt 1 i pkt 2 rozporządzenia).
2. Niezapewnieniu, aby system informatyczny o nazwie „A" (w którym przetwarzane są dane osobowe […]) umożliwiał dla każdej osoby, której dane osobowe są przetwarzane w tym systemie sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 rozporządzenia.
3. Niezapewnieniu, aby „Polityka Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]" spełniała następujące wymagania: 1) zawierała w swej treści: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami; 2) uwzględniała systemy informatyczne wykorzystywane do przetwarzania danych osobowych takie jak: system informatyczny o nazwie „B", system informatyczny o nazwie „D" oraz system informatyczny o nazwie „C", z których korzystają pracownicy Urzędu Kontroli Skarbowej w ramach wykonywania swoich obowiązków służbowych (§ 4 pkt 2, pkt 3 i pkt 4 rozporządzenia).

W związku z powyższym Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy. Pismem zawiadamiającym o wszczęciu postępowania administracyjnego w przedmiotowej sprawie (nr […]), administrator danych został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań.

W odpowiedzi na zawiadomienie o wszczęciu postępowania pismem z dnia […] października 2010 r. (znak: […]) administrator danych przesłał wyjaśnienia w sprawie stwierdzonych uchybień, w których wskazał że:

1. Przetwarzanie danych osobowych w systemie informatycznym o nazwie „A” odbywa się na zlecenie jednostki nadrzędnej jaką jest Ministerstwo Finansów. Jest to narzędzie pozwalające na gromadzenie i przekazywanie informacji w wymaganym formacie sprawozdań. Wskazana nieprawidłowość w postaci braku możliwości automatycznego odnotowania daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego te dane do systemu zostanie usunięta wraz z wprowadzeniem do pełnej eksploatacji systemu informatycznego o nazwie „B”, który zapewnia zachowanie wszelkich standardów ochrony danych.
2. Dążąc do zapewnienia zgodności z przepisami prawa prowadzonej dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych podjęto działania zmierzające do zawarcia w „Polityce Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]” brakujących elementów w postaci: wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami.

Ponadto, dnia […] października 2010 r. Generalny Inspektor Ochrony Danych Osobowych skierował do Ministra Finansów, jako podmiotu odpowiedzialnego za opracowanie i udostępnienie Urzędom Kontroli Skarbowej systemu informatycznego o nazwie „A”, pismo informujące o stwierdzonych uchybieniach dotyczących systemu informatycznego o nazwie „A”. Powołane pismo zawierało również prośbę o podjęcie działań zmierzających do dostosowania systemu „A” do wymogów określonych w przepisach o ochronie danych osobowych.

W odpowiedzi na ww. pismo Generalny Inspektor Kontroli Skarbowej w piśmie z dnia […] listopada 2010 r. (znak: […]) wskazał między innymi, iż system „A” zostanie dostosowany do wymogów określonych w przepisach o ochronie danych osobowych w ciągu trzech miesięcy. W okresie przejściowym, tj. do czasu wdrożenia wymaganych rozwiązań informatycznych, wszyscy dyrektorzy Urzędów Kontroli Skarbowej zostali zobowiązani do prowadzenia, w formie papierowej, rejestru umożliwiającego odnotowywanie daty pierwszego wprowadzenia danych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu.

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

Zgodnie z art. 38 ustawy administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

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; identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.

Natomiast 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.

W toku czynności kontrolnych ustalono, iż system informatyczny o nazwie „A" (w którym przetwarzane są dane osobowe […]) nie umożliwia dla każdej osoby, której dane osobowe są przetwarzane w tym systemie informatycznym odnotowania daty pierwszego wprowadzenia danych osobowych do systemu oraz identyfikatora użytkownika wprowadzającego dane osobowe do systemu. Wyżej wskazany system informatyczny nie umożliwia także sporządzenia i wydrukowania raportu, o którym mowa w § 7 ust. 3 rozporządzenia.

W toku niniejszego postępowania strona podniosła m.in., iż przetwarzanie danych osobowych w systemie informatycznym o nazwie „A" odbywa się na zlecenie jednostki nadrzędnej jaką jest Ministerstwo Finansów. Jak wynika z wyjaśnień przedstawionych przez Generalnego Inspektora Kontroli Skarbowej w piśmie z dnia […] listopada 2010 r. dostosowanie systemu informatycznego o nazwie „A" do wymogów określonych w § 7 ust. 1 pkt 1 i pkt 2 oraz § 7 ust. 3 rozporządzenia nastąpi w ciągu trzech miesięcy. W oparciu o powyższe wyjaśnienia nie można jednak uznać, iż na chwilę obecną w przedmiotowym zakresie został przywrócony stan zgodny z prawem. Niemniej jednak wyjaśnienia złożone przez stronę oraz Generalnego Inspektora Kontroli Skarbowej w toku niniejszego postępowania zostały uwzględnione poprzez wyznaczenie odpowiedniego terminu na usunięcie wskazanych powyżej uchybień.

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".

Jak stanowi § 4 pkt 2, pkt 3 i pkt 4 rozporządzenia, polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

W toku czynności kontrolnych ustalono, że administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych m.in. w postaci „Polityki Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]". Powołana dokumentacja nie spełnia wymagań, o których mowa w § 4 pkt 2, pkt 3 i pkt 4 rozporządzenia z uwagi na to, iż nie zawarto w niej następujących elementów: wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opisu struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposobu przepływu danych pomiędzy poszczególnymi systemami. Ponadto ustalono, iż w „Polityce Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]" nie zostały uwzględnione systemy informatyczne wykorzystywane do przetwarzania danych osobowych takie jak: system informatyczny o nazwie „B", system informatyczny o nazwie „D" oraz system informatyczny o nazwie „C", z których korzystają pracownicy kontrolowanego podmiotu w ramach wykonywania swoich obowiązków służbowych.

Z wyjaśnień przedstawionych przez Wicedyrektora Urzędu pismem z dnia […] października 2010 r. wynika, iż podjęto działania zmierzające do uzupełnienia „Polityki Bezpieczeństwa Danych Osobowych Systemów Teleinformatycznych Przetwarzających Dane Osobowe w Urzędzie Kontroli Skarbowej […]" o brakujące elementy, takie jak: wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; opis struktury zbiorów danych wskazującego zawartość poszczególnych pól informacyjnych i powiązań między nimi; sposób przepływu danych pomiędzy poszczególnymi systemami. Należy jednak zauważyć, iż z powyższych wyjaśnień nie wynika, iż proces ten został zakończony. Samo podjęcie działań zmierzających do usunięcia uchybień nie stanowi natomiast wystarczającej podstawy do uznania, iż został przywrócony stan zgodny z prawem.

W świetle dokonanych ustaleń, 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.