GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH
Michał Serzycki

Warszawa, dnia 29 stycznia 2009 r.

DIS/DEC-68/2867/09
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. 24 ust. 1 pkt 3 i pkt 4, art. 31 ust. 1 i ust. 2, art. 36 ust. 1 i ust. 2, art. 39 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.), § 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) oraz częścią A pkt IV ust. 2 załącznika do ww. rozporządzenia, po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez K. Sp. z o.o,

Nakazuję K. Sp. z o.o., usunięcie uchybień w procesie przetwarzania danych osobowych, poprzez:

1. **Dopełnianie obowiązku informacyjnego w zakresie informowania klientów Spółki o prawie dostępu do treści swoich danych oraz ich poprawiania, a także dobrowolności podania danych - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

2. **Uzupełnienie zawieranych umów agencyjnych o zapis określający zakres i cel przetwarzania danych osobowych klientów Spółki - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
3. **Zgłoszenie do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych klientów Spółki - w terminie 14 dni od dnia, w którym niniejsza decyzja stanie się ostateczna.**
4. **Zapewnienie, aby hasło do systemu informatycznego o nazwie „A", w którym przetwarzane są dane osobowe klientów Spółki oraz do systemów operacyjnych komputerów użytkowanych w Spółce było zmieniane nie rzadziej niż co 30 dni - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
5. **Opracowanie w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych – w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**
6. **Opracowanie ewidencji osób upoważnionych do przetwarzania danych osobowych - w terminie 1 miesiąca od dnia, w którym niniejsza decyzja stanie się ostateczna.**

Uzasadnienie

Inspektorzy, upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych przeprowadzili kontrolę w K. Sp. z o.o., w celu ustalenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych sygn. […], 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 Spółki 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 Spółki.

Na podstawie materiału dowodowego zgromadzonego w toku kontroli ustalono, że w procesie przetwarzania danych Spółka, jako administrator danych, naruszyła przepisy o ochronie danych osobowych. Uchybienia te polegały na:

1. Niedopełnieniu obowiązku informacyjnego (art. 24 ust. 1 pkt 3 i pkt 4 ustawy).
2. Nieuzupełnieniu umów agencyjnych o zapis określający zakres i cel przetwarzania danych osobowych klientów Spółki (art. 31 ust. 1 i ust. 2 ustawy).
3. Niezgłoszeniu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych klientów Spółki (art. 40 ustawy).
4. Niezapewnieniu, aby zmiana hasła do systemu informatycznego o nazwie „A", w którym przetwarzane są dane osobowe klientów Spółki oraz do systemów operacyjnych komputerów było zmieniane rzadziej niż co 30 dni (część A pkt IV ust. 2 załącznika do rozporządzenia).
5. Nieopracowaniu w formie pisemnej dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (art. 36 ust. 2 ustawy w związku z § 3 rozporządzenia).
6. Nieopracowaniu ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ustawy).

W piśmie z dnia […] grudnia 2008 r. sygn. […], stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Spółka została poinformowana o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się co do zebranych dowodów i materiałów oraz zgłoszonych żądań. Spółka nie skorzystała z prawa złożenia wyjaśnień oraz nie przesłała dowodów mogących 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 art. 24 ust. 1 pkt 3 i pkt 4 ustawy, w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o prawie dostępu do treści swoich danych oraz ich poprawiania oraz dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W toku kontroli ustalono, iż Spółka nie realizuje obowiązku informacyjnego wobec osób korzystających z imprez turystycznych, których jest organizatorem w zakresie art. 23 ust. 1 pkt 3 oraz pkt 4, tj. informacji o prawie dostępu do treści swoich danych oraz ich poprawiania, a także o dobrowolności podania danych.

Zgodnie z art. 31 ust. 1 ustawy, administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych, natomiast zgodnie z art. 31 ust. 2 ustawy, podmiot, któremu powierzono przetwarzanie danych może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie.

Jak ustalono w trakcie kontroli, Spółka organizuje we własnym imieniu imprezy turystyczne. W związku z powyższą działalnością Spółka sprzedaje imprezy turystyczne za pośrednictwem własnego biura oraz agentów, tj. biur turystycznych działających na podstawie ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2004 r. Nr 223, poz. 2268, z późn. zm.). Umowy agencyjne, zawierane przez Spółkę, dotyczące sprzedaży imprez turystycznych przez nią organizowanych są jednolite w swej treści. Z treści powołanych umów wynika, że zostały one zawarte w celu stałego pośrednictwa w sprzedaży usług turystycznych. W umowach nie został określony zakres, ani cel przetwarzania danych osobowych klientów Spółki (osób, które zamierzają zawrzeć lub zawarły umowę o świadczenie usług turystycznych na swoją rzecz lub rzecz innej osoby). A zatem ww. umowy nie spełniają wymogów, o których mowa w art. 31 ustawy.

Zgodnie z art. 40 ustawy, administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Jak ustalono w trakcie kontroli osoba zainteresowana zakupem imprezy turystycznej zawiera ze Spółką umowę zgłoszenie udziału w imprezie turystycznej. Zakres danych pozyskiwanych przez Spółkę wynika z ww. umowy. Dane przetwarzane są w systemie papierowym, tj. w umowach zgłoszenia udziału w imprezie turystycznej oraz w systemie informatycznym o nazwie „A” (moduł „B”). Podstawą prawną przetwarzania danych uczestników imprez turystycznych jest art. 23 ust. 1 pkt 3 ustawy, tj. umowa zawarta pomiędzy uczestnikiem imprezy turystycznej a Spółką. Dane zawarte w ww. systemie informatycznym dostępne są według określonych kryteriów, tj. w szczególności według imienia i nazwiska, numeru klienta.

W toku kontroli ustalono, iż w pomieszczeniu zlokalizowanym od ul. […], w części pomieszczenia oddzielonej biurkami od części, w której przyjmowani są interesanci w szafce zamykanej na klucz przechowywane są w skoroszytach umowy zgłoszenia na imprezy turystyczne, które Spółka organizuje jako organizator imprez turystycznych. Na pierwszych stronach ww. skoroszytów wpięte są wykazy z imionami i nazwiskami klientów Spółki. Ponadto ww. wykazy opisane są datą wyjazdu oraz datą przyjazdu z imprezy turystycznej. Umowy w skoroszytach ułożone są chronologicznie według daty uiszczenia należności na rzecz Spółki.

Stosownie do treści art. 7 pkt 1 ustawy, ilekroć w ustawie jest mowa o zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Mając powyższe na uwadze uznać należy, iż Spółka przetwarza dane osobowe swoich klientów zgromadzone w zbiorze danych. Nie zachodzi przy tym żadna z okoliczności wskazanych w art. 43 ust. 1 ustawy, zwalniających Spółkę z obowiązku zgłoszenia do rejestracji powyższego zbioru danych. Zatem Spółka zobowiązana jest do zgłoszenia zbioru danych klientów Spółki do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.

Zgodnie z art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Natomiast zgodnie z częścią A pkt IV ust. 2 załącznika do rozporządzenia, w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 30 dni.

W toku czynności kontrolnych ustalono, iż hasło do systemu informatycznego o nazwie „A", w którym przetwarzane są dane osobowe klientów Spółki oraz do systemów operacyjnych komputerów jest zmieniane rzadziej niż co 30 dni.

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. Zgodnie z ust. 2, dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej. Natomiast, zgodnie z ust. 3, dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

W czasie dokonywania czynności kontrolnych ustalono, iż w Spółce nie została opracowana i wdrożona polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym.

Zgodnie art. 39 ustawy, administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej, 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

W toku czynności kontrolnych ustalono, że w Spółce nie jest prowadzona ewidencja osób upoważnionych do przetwarzania danych, która spełnia wymagania określone w art. 39 ustawy.

Mając powyższe na uwadze, w tym stanie prawnym i faktycznym, 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.