



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

DRZDO-DEC/707/10/23872

dot. DRZDO-401/002084/08

DECYZJA

z dnia 11 czerwca 2010 r.

Na podstawie art. 44 ust. 1 pkt 3, art. 44 ust. 2 w związku z art. 18 ust. 1 pkt 3, art. 22 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), 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.), § 6 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 związku ze zgłoszeniem do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych o nazwie „ZBIÓR DANYCH OSOBOWYCH KLIENTÓW”, dokonany przez Kancelarię Finansową XX Sp. z o.o. z siedzibą w (...):

1) odmawiam Kancelarii Finansowej XX Sp. z o.o. z siedzibą w (...) rejestracji zbioru danych osobowych o nazwie „ZBIÓR DANYCH OSOBOWYCH KLIENTÓW”;

2) nakazuję Kancelarii Finansowej XX Sp. z o.o. z siedzibą w (...):

ograniczenie przetwarzania danych osobowych zgromadzonych w zbiorze o nazwie „ZBIÓR DANYCH OSOBOWYCH KLIENTÓW” wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu, stosownie do art. 44 ust. 4 ustawy o ochronie danych osobowych;

a) wprowadzenie dodatkowych środków zabezpieczających zgromadzone w zbiorze dane na poziomie wysokim, zgodnie z § 6 ust. 4 ww. rozporządzenia.

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

W dniu 23 maja 2008 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło zgłoszenie do rejestracji zbioru danych osobowych o nazwie „ZBIÓR DANYCH OSOBOWYCH KLIENTÓW” złożone przez administratora danych, tj. Kancelarię Finansową XX Sp. z o.o. z siedzibą w (...).

Z informacji zawartych w zgłoszeniu wynika, iż administrator danych zastosował środki bezpieczeństwa na poziomie podwyższonym oraz że co najmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną.

Po przeanalizowaniu zgromadzonego w sprawie materiału dowodowego, Generalny Inspektor Ochrony Danych Osobowych zważył, co następuje.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwana dalej „ustawą”, w art. 40 wprowadziła dla administratora danych obowiązek zgłoszenia Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych do rejestracji, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1 ustawy. Stosownie do treści art. 44 ust. 1 pkt 3 ustawy, Generalny Inspektor Ochrony Danych Osobowych odmawia, w drodze decyzji administracyjnej, rejestracji zgłoszonego zbioru danych, jeżeli urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy.

Stosownie do treści przepisu § 6 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), zwanego dalej „rozporządzeniem”, wprowadzone zostały trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony oraz wysoki. Poziom środków bezpieczeństwa należy dostosować do zagrożeń oraz kategorii danych osobowych przetwarzanych w systemie informatycznym. Poziom co najmniej podstawowy stosuje się, gdy w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną (ust. 2). Poziom co najmniej podwyższony stosuje się, gdy w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną (ust. 3). Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną (ust. 4).

Niezastosowanie odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym oznacza, że urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w rozporządzeniu, co

stanowi przesłankę odmowy rejestracji zgłoszonego zbioru danych, o której mowa w art. 44 ust. 1 pkt 3 ustawy.

W związku z tym należy uznać, iż urządzenia i systemy informatyczne służące do przetwarzania danych w przedmiotowym zbiorze nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w rozporządzeniu.

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

Zgodnie z art. 44 ust. 4 ustawy administrator danych może ponownie zgłosić przedmiotowy zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, po usunięciu wad, które były powodem odmowy rejestracji tego zbioru. Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępnego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.

Stronie, na podstawie art. 21 ust. 1 ustawy oraz art. 127 § 3 Kpa, przysługuje prawo do złożenia wniosku o ponowne rozpatrzenie sprawy do Generalnego Inspektora Ochrony Danych Osobowych w terminie 14 dni od daty otrzymania decyzji (adres: Generalny Inspektor Ochrony Danych Osobowych ulica Stawki 2, 00-193 Warszawa).