



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

DRZDO/DEC-491/08/21607

dot. DRZDO-401/001087/08

DECYZJA

z dnia 20 sierpnia 2008 r.

Na podstawie art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 5, 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 ust. 4 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 w sprawie zgłoszenia do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych zbioru danych osobowych o nazwie „Płace Z” złożonego przez Gminę,

1) odmawiam Gminie , rejestracji zbioru danych osobowych o nazwie „Z”,

2) nakazuję Gminie

a. wprowadzenie dodatkowych środków zabezpieczających zgromadzone w zbiorze dane na poziomie wysokim,

b. ograniczenie przetwarzania danych osobowych zgromadzonych w zbiorze o nazwie „Płace Z” wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu.

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

W dniu 17 marca 2008 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło zgłoszenie do rejestracji zbioru danych osobowych o nazwie „Płace Z” dokonane przez Gminę, zwaną dalej „Wnioskodawcą”.

Zgłoszenie zbioru danych osobowych nie spełniało wymogów niezbędnych do zarejestrowania ww. zbioru, gdyż nie zawierało pełnego opisu środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36 – 39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zwanej dalej także „ustawą”. Z treści zgłoszenia wynikało również, że Wnioskodawca nie spełnił wymogów z § 6 ust. 4 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”, tj. pomimo połączenia urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, z siecią publiczną nie wprowadził środków bezpieczeństwa na poziomie wysokim.

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

Ustawa o ochronie danych osobowych 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 ustawy, Generalny Inspektor Ochrony Danych Osobowych odmawia, w drodze decyzji administracyjnej, rejestracji zgłoszonego zbioru danych, jeżeli:

- 1) nie zostały spełnione wymogi określone w art. 41 ust. 1 ustawy,
- 2) przetwarzanie danych naruszałoby zasady określone w art. 23-30 ustawy,
- 3) urządzenia i systemy informatyczne służące do przetwarzania danych w zbiorze zgłoszonym do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy.

Zgodnie z art. 41 ust. 1 pkt 5 ustawy w zgłoszeniu powinien znajdować się opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy. Powołane przepisy, zawarte w Rozdziale 5 ustawy – Zabezpieczenie danych osobowych, obligują administratora danych do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Stosownie do ich treści, na administratorze danych ciąży w szczególności obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki ich ochrony (art. 36 ust. 2 ustawy), wyznaczenia administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony danych osobowych (chyba że administrator danych sam wykonuje te czynności) (art. 36 ust. 3 ustawy), nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych (art. 37 ustawy), a także prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy). Na ww. dokumentację, stosownie do treści § 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), składa się polityka bezpieczeństwa (§ 4 rozporządzenia) i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (§ 5 rozporządzenia).

Brak w zgłoszeniu ww. informacji, stanowi przesłankę odmowy rejestracji zbioru danych, określoną w art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 5 ustawy.

Ponadto, na mocy przepisu § 6 rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, wydanego na podstawie art. 39a ustawy, 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, określone 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,

określone 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).

Brak odpowiedniego poziomu bezpieczeństwa, zgodnie z przepisami rozporządzenia stanowi przesłankę odmowy rejestracji zgłoszonego zbioru danych, o której mowa w art. 44 ust. 1 pkt 3 ustawy.

Z informacji zawartych w zgłoszeniu wynika, iż urządzenia systemu informatycznego służącego do przetwarzania danych w zbiorze o nazwie „Płace Z” połączone są z siecią publiczną, co zgodnie z ww. przepisami wymaga zastosowania wysokiego poziomu bezpieczeństwa. Zastosowane przez Wnioskodawcę środki bezpieczeństwa na poziomie podwyższonym są zatem niewystarczające. Ponadto Wnioskodawca w toku postępowania wyjaśniającego nie uzupełnił zgłoszenia o informacje dotyczące wyznaczenia administratora bezpieczeństwa informacji.

Mając na uwadze powyższy stan faktyczny oraz przytoczone uregulowania prawne Generalny Inspektor Ochrony Danych Osobowych był zobligowany do wydania decyzji odmawiającej rejestracji zbioru danych o nazwie „Płace Z”.

Stosownie do art. 44 ust. 2 ustawy Generalny Inspektor Ochrony Danych Osobowych odmawiając rejestracji zbioru danych, nakazał Wnioskodawcy ograniczenie przetwarzania wszystkich danych zgromadzonych w tym zbiorze wyłącznie do ich przechowywania, do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu oraz wprowadzenia dodatkowych środków zabezpieczających zgromadzone dane na poziomie wysokim.

Należy podkreślić, że wnioskodawca, zgodnie z art. 44 ust. 4 ustawy, może ponownie zgłosić zbiór o nazwie „Płace Z” do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych na obowiązującym wzorze zgłoszenia, po usunięciu wad, które były powodem odmowy rejestracji tego zbioru, tj. po wprowadzeniu środków zabezpieczających zgromadzone w zbiorze dane na poziomie wysokim oraz uzupełnieniu zgłoszenia o informacje dotyczące wyznaczenia administratora bezpieczeństwa informacji.

Informuję ponadto, że Generalnemu Inspektorowi Ochrony Danych Osobowych na każdym etapie prowadzonego postępowania, jak również po jego zakończeniu, przysługuje prawo oraz obowiązek realizacji zadań, w które wyposażony został na mocy przepisów ustawy o ochronie danych osobowych, a także ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.), w tym kontrola wykonania nakazów nałożonych na administratorów danych w decyzji.

W tym stanie prawnym i faktycznym, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął, jak w sentencji.

Decyzja jest ostateczna. Stronie, na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 127 § 3 ustawy Kodeks postępowania administracyjnego, 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, ul. Stawki 2, 00-193 Warszawa).