



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

DRZDO/DEC-31/09/1056

dot. DRZDO-401/003200/07

DECYZJA

z dnia 14 stycznia 2009 r.

Na podstawie art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 5, art. 44 ust. 2 pkt 1 i 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.) oraz 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.), §§ 3, 4 i 5 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 rejestracji zbioru danych o nazwie „X” zgłoszonego do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych w dniu 7 września 2007 r. przez firmę Y.

- 1) odmawiam Y rejestracji zbioru danych osobowych o nazwie „X”**
- 2) nakazuję Y ograniczenie przetwarzania danych osobowych zgromadzonych w zbiorze o nazwie „X” wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po**

jego ponownym zgłoszeniu, stosownie do art. 44 ust. 4 ustawy o ochronie danych osobowych.

Uzasadnienie

W dniu 7 września 2007 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło zgłoszenie do rejestracji zbioru danych o nazwie „X złożone przez Y zwaną dalej „Wnioskodawcą”. Zgłoszenie nie spełniało wymogów niezbędnych do zarejestrowania ww. zbioru danych, nie zawierało bowiem wyczerpującego 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 „ustawą”.

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 zwalniających go z tego obowiązku, 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 naruszałoby zasady określone w art. 23-30 ustawy,
- 3) 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.

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 (art. 36 ust. 3 ustawy), nadzorującego przestrzeganie zasad ochrony danych osobowych (chyba że administrator danych sam wykonuje te czynności), 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 zgłoszonego zbioru danych, określoną w art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 5 ustawy.

Z tych względów i wobec nieuzupełnienia przez Wnioskodawcę zgłoszenia o informacje dotyczące opracowania i wdrożenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych, wyznaczenia administratora bezpieczeństwa informacji, nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych, a także prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, Generalny Inspektor Ochrony Danych Osobowych był zobligowany do wydania decyzji odmawiającej rejestracji zbioru danych osobowych o nazwie „X

Odmawiając rejestracji zbioru danych, Generalny Inspektor Ochrony Danych Osobowych nakazał Wnioskodawcy ograniczenie przetwarzania wszystkich danych zgromadzonych w tym zbiorze wyłącznie do ich przechowywania, do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu.

Należy podkreślić, iż Wnioskodawca, stosownie do treści art. 44 ust. 4 ustawy, może ponownie zgłosić zbiór o nazwie „X do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych na obowiązującym wzorze zgłoszenia, po usunięciu wad, które były powodem odmowy rejestracji tego zbioru, tj. po uzupełnieniu ponownego zgłoszenia o informacje dotyczące:

- opracowania i wdrożenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych,
- wyznaczenia administratora bezpieczeństwa informacji,

- nadania upoważnień osobom dopuszczonym do przetwarzania danych osobowych,
- prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Informuję ponadto, że Generalnemu Inspektorowi Ochrony Danych Osobowych na każdym etapie prowadzonego postępowania, a także po jego zakończeniu, przysługuje prawo i obowiązek realizacji zadań, w które został wyposażony mocą przepisów ustawy o ochronie danych osobowych i ustawy – Kodeks postępowania administracyjnego, 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 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).