



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

DRZDO/DEC-556/10/18978

dot. DRZDO-401/005358/08

DECYZJA

z dnia 6 maja 2010 r.

Na podstawie art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 5 i 6, art. 44 ust. 1 pkt 2 w związku z art. 26 ust. 1 pkt 3, art. 44 ust. 2 pkt 1 i 2 w związku z art. 18 ust. 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 i 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 „Rejestr osób, którym administrator danych zamierza zaoferować produkty będące w jego ofercie oraz nabywców produktów oferowanych przez administratora”, dokonany przez „E” Sp. z o.o. z siedzibą w (...):

- 1) odmawiam „E” Sp. z o.o. z siedzibą w (..) rejestracji zbioru danych osobowych o nazwie „Rejestr osób, którym administrator danych zamierza zaoferować produkty będące w jego ofercie oraz nabywców produktów oferowanych przez administratora”,**
- 2) nakazuję „E” Sp. z o.o. z siedzibą w (...):**
 - a) usunięcie ze zbioru danych o nazwie „Rejestr osób, którym administrator danych zamierza zaoferować produkty będące w jego ofercie oraz nabywców produktów oferowanych przez administratora” danych nieadekwatnych do celu ich przetwarzania tj. numeru ewidencyjnego PESEL oraz serii i numeru dowodu osobistego,**

b) ograniczenie przetwarzania w zbiorze o nazwie „Rejestr osób, którym administrator danych zamierza zaoferować produkty będące w jego ofercie oraz nabywców produktów oferowanych przez administratora” innych niż wymienione w pkt 2a) danych osobowych, wyłącznie do ich przechowywania do czasu zarejestrowania tego zbioru po jego ponownym zgłoszeniu, stosownie do art. 44 ust. 4 ustawy o ochronie danych osobowych.

U z a s a d n i e

W dniu 4 grudnia 2008 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło zgłoszenie do rejestracji zbioru danych o nazwie „Rejestr osób, którym administrator danych zamierza zaoferować produkty będące w jego ofercie oraz nabywców produktów oferowanych przez administratora”, złożone przez administratora danych, tj.: „E” Sp. z o.o. z siedzibą w (...). Zgłoszenie nie zawiera informacji dotyczących:

- opracowania i wdrożenia polityki bezpieczeństwa,
- opracowania i wdrożenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych,
- prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych,
- poziomu zastosowanych środków bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

Ponadto z treści zgłoszenia wynika, iż administrator danych pozyskuje do przedmiotowego zbioru dane w postaci numeru ewidencyjnego PESEL oraz serii i numeru dowodu osobistego w celu „marketingowym, reklamowym, pozyskiwania nowych klientów”.

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 również „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 1 ustawy, Generalny Inspektor Ochrony Danych Osobowych odmawia, w drodze decyzji administracyjnej, rejestracji zgłoszonego zbioru danych, jeżeli nie zostały spełnione wymogi określone w art. 41 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 zgłoszenie zbioru danych do rejestracji powinno zawierać opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39 ustawy. Stosownie do art. 36 ustawy administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych

odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Jednakże każdy administrator danych, bez względu na kategorię przetwarzanych danych oraz zagrożenia, ma obowiązek spełnić wymogi wskazane wprost w przepisach art. 36-39 ustawy, tj.: wyznaczyć administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony danych osobowych - chyba że administrator danych sam wykonuje te czynności (art. 36 ust. 3 ustawy), nadać upoważnienia osobom dopuszczonym do przetwarzania danych osobowych (art. 37 ustawy), prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych (art. 39 ust. 1 ustawy), a także prowadzić dokumentację opisującą sposób przetwarzania danych osobowych oraz środki ich ochrony (art. 36 ust. 2 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), zwanego dalej „rozporządzeniem”, składa się polityka bezpieczeństwa (§ 4 rozporządzenia), a w przypadku przetwarzania danych w systemie informatycznym również instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (§ 5 rozporządzenia).

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

Natomiast zgodnie z art. 41 ust. 1 pkt 6 ustawy zgłoszenie zbioru danych do rejestracji powinno zawierać informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a ustawy. Na mocy przepisu § 6 ust. 1 rozporządzenia, wydanego na podstawie art. 39a ustawy, wprowadzone zostały trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym: podstawowy, podwyższony oraz wysoki.

Brak informacji o zastosowanym poziomie bezpieczeństwa, zgodnie z przepisami rozporządzenia, stanowi przesłankę odmowy rejestracji zgłoszonego zbioru danych, o której mowa w art. 44 ust. 1 pkt 1 w związku z art. 41 ust. 1 pkt 6 ustawy.

Ponadto w myśl art. 26 ust. 1 pkt 3 ustawy, administrator danych powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby były one merytorycznie poprawne i adekwatne w stosunku do celów, dla których są przetwarzane. Adekwatność powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi osobowymi, a interesem administratora danych. Równowaga jest zachowana wówczas, gdy administrator przetwarza dane tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim te dane są przez niego przetwarzane. W przypadku gdy administratorzy danych pozyskują dane ponad rzeczywiste potrzeby naruszają zasadę adekwatności. Naruszenie zasady adekwatności, stanowi przesłankę wydania decyzji o odmowie rejestracji zbioru danych, określoną w art. 44 ust. 1 pkt 2 w związku z art. 26 ust. 1 pkt 3 ustawy.

Zatem należy uznać, iż przedmiotowe zgłoszenie nie spełnia wymogów określonych w art. 41 ust. 1 ustawy, a przetwarzanie w przedmiotowym zbiorze danych w postaci numeru ewidencyjnego PESEL oraz serii i numeru dowodu osobistego w celu „marketingowym, reklamowym, pozyskiwania nowych klientów” narusza zasadę adekwatności.

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).