



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 5 marca 2010 r.

DEC/DIS-247/9383/10

dot. DIS-K-421/155/09

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, art. 22 w związku z art. 24 ust. 1, art. 36 ust. 2 i art. 38 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz § 7 ust. 1 pkt 1 i § 7 ust. 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), po przeprowadzeniu postępowania administracyjnego w sprawie przetwarzania danych osobowych przez Pana G prowadzącego serwis internetowy,

nakazuję Panu G prowadzącemu serwis internetowy, usunięcie, w terminie 30 dni od dnia, w którym niniejsza decyzja stanie się ostateczna, uchybień w procesie przetwarzania danych osobowych poprzez:

1. Dopełnianie wobec użytkowników serwisu internetowego obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.),

tj. poinformowanie ww. użytkowników o adresie swojej siedziby i pełnej nazwie; celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub

przewidywanych odbiorcach lub kategoriach odbiorców danych; prawie dostępu do treści swoich danych i ich poprawiania oraz dobrowolności podania danych.

2. Zapewnienie, aby system informatyczny zapewniał odnotowanie daty pierwszego wprowadzenia danych do systemu.

3. Zapewnienie, aby system informatyczny, umożliwiał dla każdej osoby, której dane są przetwarzane, sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w § 7 ust. 1 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).

4. Opracowanie i wdrożenie dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.).

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

Inspektorzy upoważnieni przez Generalnego Inspektora Ochrony Danych Osobowych, przeprowadzili u Pana G prowadzącego serwis internetowy, zwanego dalej Przedsiębiorcą, kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (DIS-K-421/155/09), 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, i 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 Przedsiębiorcy ustne wyjaśnienia, skontrolowano systemy informatyczne. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Przedsiębiorcę.

Na podstawie tak zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Przedsiębiorca, jako administrator danych, naruszył przepisy o ochronie danych osobowych, polegające na:

1. Niedopełnianiu wobec użytkowników serwisu internetowego obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy.
2. Niezapewnieniu przez system informatyczny odnotowania daty pierwszego wprowadzenia danych do systemu.

3. Niezapewnieniu przez system informatyczny sporządzenia i wydrukowania raportu zawierającego datę pierwszego wprowadzenia danych do systemu.
4. Nieopracowaniu i niewdrożeniu dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 ustawy.

W związku z powyższym, w dniu 25 stycznia 2010 r. Generalny Inspektor Ochrony Danych Osobowych wszczął z urzędu postępowanie administracyjne w niniejszej sprawie w celu wyjaśnienia okoliczności sprawy.

W piśmie z dnia 25 stycznia 2010 r., sygn. DIS-K-421/155/09/3199/10, stanowiącym zawiadomienie o wszczęciu postępowania administracyjnego w przedmiotowej sprawie, Przedsiębiorca został poinformowany o prawie czynnego udziału w każdym stadium postępowania, a przed wydaniem decyzji wypowiedzenia się, co do zebranych w toku kontroli dowodów i materiałów oraz zgłoszonych żądań, jednakże Przedsiębiorca nie skorzystał z ww. uprawnień.

Po zapoznaniu się z całością materiału dowodowego zebranego w sprawie Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

1. Zgodnie z art. 24 ust. 1 ustawy w przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku; celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych; prawie dostępu do treści swoich danych oraz ich poprawiania; dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W toku kontroli ustalono, iż Przedsiębiorca nie dopełniał wobec użytkowników serwisu internetowego obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy.

2. Zgodnie z art. 38 ustawy administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Zgodnie § 7 ust. 1 pkt 1 rozporządzenia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu.

W toku czynności kontrolnych ustalono, iż system informatyczny nie zapewnia odnotowania daty pierwszego wprowadzenia danych do systemu, a zatem nie został spełniony wymóg określony w § 7 ust. 1 pkt 1 rozporządzenia.

Zgodnie z § 7 ust. 3 rozporządzenia, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

Jak ustalono, system informatyczny nie zapewnia sporządzenia i wydrukowania raportu zawierającego w powszechnie zrozumiałej formie informacji, o której mowa w § 7 ust. 1 pkt 1 rozporządzenia, tj. datę pierwszego wprowadzenia danych do tego systemu.

3. 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, zwana dalej instrukcją. 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 toku czynności kontrolnych ustalono, że nie jest prowadzona dokumentacja opisująca sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, tj. polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

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

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych i 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.