



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 3 lutego 2012 r.

DIS/DEC- 103/12/7510

dot. [...]

D E C Y Z J A

Na podstawie art. 138 § 1 pkt 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071 z późn. zm.) oraz art. 12 pkt 2, art. 18 ust. 1 pkt 1 i art. 22 w związku z art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), po przeprowadzeniu postępowania administracyjnego w sprawie wniosku Pana X. K. z Kancelarii Prawnej T. sp.j., pełnomocnika G. w S., o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora Ochrony Danych Osobowych z dnia 1 grudnia 2011 r., nr DIS/DEC-1020/58246/11, nakazującą usunięcie uchybień w procesie przetwarzania danych osobowych przez G. w S.,

utrzymuję w mocy zaskarżoną decyzję.

Uzasadnienie

W dniu 1 grudnia 2011 r. Generalny Inspektor Ochrony Danych Osobowych wydał decyzję nr DIS/DEC-1020/58246/11, nakazującą G. w S. (dalej G.), usunięcie uchybień w procesie przetwarzania danych osobowych poprzez wyznaczenie administratora bezpieczeństwa informacji.

W dniu [...] grudnia 2011 r. do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął, złożony w terminie, wniosek pełnomocnika G. o ponowne rozpatrzenie sprawy zakończonej decyzją Generalnego Inspektora nr DIS/DEC-1020/58246/11, uchylenie zaskarżonej decyzji w całości i umorzenie postępowania w sprawie.

We wniosku o ponowne rozpatrzenie sprawy pełnomocnik podniósł, że:

1. Art. 36 ust. 3 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, przewiduje dwie odrębne sytuacje sprawowania nadzoru nad przestrzeganiem zasad ochrony danych osobowych, tj. poprzez wyznaczenie administratora bezpieczeństwa informacji oraz poprzez samodzielne wykonywanie przez administratora danych czynności nadzorczych. Na odrębność tych dwóch sytuacji wskazuje literalne brzmienie przepisu, w tym przede wszystkim zawarty w nim spójnik „chyba, że”.
2. W odniesieniu do drugiej sytuacji przepis art. 36 ust. 3 ustawy nie zawiera jakichkolwiek ograniczeń podmiotowych wskazujących, że może ona mieć zastosowanie wyłącznie do określonej kategorii administratorów danych, np. wyłącznie do osób fizycznych prowadzących działalność gospodarczą. W przepisie tym jest mowa wyłącznie o „administratorze danych” wykonującym czynności w nim wskazane, którym jest zgodnie z art. 7 pkt 4 ustawy każdy podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych, a więc także osoba prawna. Brak jest zatem jakichkolwiek podstaw do przyjmowania na gruncie art. 36 ust. 3 ustawy innego rozumienia pojęcia administratora danych niż to wynika z jego definicji ustawowej.
3. Z brzmienia powołanego przepisu ustawy wynika, że ustawodawca przyjął regułę wyznaczenia administratora bezpieczeństwa informacji i powierzenie mu czynności nadzoru. Równocześnie jednak administratorowi danych pozostawiono możliwość samodzielnego nadzorowania tych zasad, wówczas gdy nie wyznaczy on administratora bezpieczeństwa informacji – w tej bowiem sytuacji administrator danych „sam wykonuje te [nadzoru] czynności”. Administrator danych nie staje się administratorem bezpieczeństwa informacji ani też nie „przejmuje” jego funkcji.
4. Z istoty czynności nadzoru w żadnym razie nie wynika, że czynności te mogą być wykonywane wyłącznie przez osobę fizyczną. Należy zauważyć, że już na gruncie samej ustawy na administratorze danych ciąży obowiązek wykonania wielu czynności związanych z dbałością o przestrzeganie przepisów o ochronie danych osobowych. Z przepisów tych wynika obowiązek sprawowania przez administratora danych bieżącej kontroli nad przestrzeganiem stosownych zasad danych osobowych w trakcie ich przetwarzania. Nie powinno ulegać wątpliwości, że w ramach struktury organizacyjnej administratora danych będącego osobą prawną sam administrator danych (a konkretnie osoby kierujące daną jednostką organizacyjną, zgodnie z mającą zastosowanie regulacją prawną) jest władny do podejmowania działań np. w postaci wyciągania określonych konsekwencji wobec pracowników upoważnionych do przetwarzania danych osobowych. Co więcej, w praktyce działania te okazują się o wiele bardziej skuteczne,

zapewniające wyższy poziom ochrony danych osobowych, niż określone działania podejmowane przez administratora bezpieczeństwa informacji.

5. Na mocy samej ustawy o ochronie danych osobowych na każdym administratorze danych ciąży obowiązek kontroli i nadzoru, w tym na administratorze danych będącym osobą prawną. Rozwiązanie to zgodne jest z przyjmowanym na gruncie polskich przepisów prawa modelem sprawowania nadzoru, zgodnie z którym dopuszczalne jest wykonywanie czynności nadzoru przez jednostki organizacyjne, nie zaś wyłącznie przez osoby fizyczne. Potwierdza to również orzecznictwo (por. wyrok Sądu Najwyższego z dnia 10 września 1971 r., sygn. I CR 260/71), a także literatura przedmiotu (por. m.in. P. Fajgielski, Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno – prawne. Lublin 2008, str. 183).
6. Uznaje się, że art. 36 ust. 3 ustawy jest w istocie przejawem możliwości delegowania przez administratora danych części obowiązków z zakresu kontroli przetwarzania danych na inną osobę w drodze wyznaczenia administratora bezpieczeństwa informacji. Akceptacja stanowiska Generalnego Inspektora oznaczałaby wręcz, że „w większości przypadków nie ma możliwości sprawowania nadzoru przez administratora danych z uwagi na to, że status administratora danych przysługuje często jednostce organizacyjnej (np. spółce), a nie konkretnej osobie fizycznej”. Należy raczej przyjąć, że to administrator bezpieczeństwa informacji przejmuje obowiązki administratora danych dotyczące sprawowania nadzoru, a nie odwrotnie.
7. Nietrafne jest powołanie się przez Generalnego Inspektora Ochrony Danych Osobowych na brzmienie przepisów dyrektywy odnoszących się do „urzędnika do spraw ochrony danych osobowych”. Instytucja ta „wykazuje immanentny związek z obowiązkiem rejestracji zbiorów danych osobowych”. Administrator bezpieczeństwa informacji nie jest takim urzędnikiem, ani też jego odpowiednikiem.
8. Wskazywane przez Generalnego Inspektora na stronie [...] uzasadnienie poglądu, zgodnie z którym administratorem bezpieczeństwa informacji może być wyłącznie osoba fizyczna, całkowicie nie przystaje do sytuacji, w której wskazane w art. 36 ust. 3 ustawy funkcje nadzorcze sprawuje samodzielnie administrator danych. Organ wskazał, że art. 37 ustawy wymaga udzielenia konkretnej osobie fizycznej przez administratora danych upoważnienia do podejmowania czynności związanych z przetwarzaniem danych osobowych, którym musi dysponować także administrator bezpieczeństwa informacji. Argument ten nie może być w żaden sposób zastosowany w odniesieniu do administratora danych, który dla legalnego przetwarzania danych osobowych nie udziela przecież sam sobie upoważnienia, lecz musi dysponować jedną z materialno – prawnych przesłanej wynikających z art. 23 (lub art. 27) ustawy.

9. G. jest członkiem programu [...] i podlega regularnemu, corocznemu procesowi badania zgodności z certyfikatem [...]. Daje to m.in. gwarancje przetwarzania danych osobowych zgodnie z zasadami wynikającymi z dyrektywy 95/46/WE, a więc i z polską ustawą o ochronie danych osobowych. Powyższe oznacza także, iż wdrożone przez G. procedury związane z ochroną danych osobowych są zgodne z zasadami określonymi w przywołanej dyrektywie.

Generalny Inspektor Ochrony Danych Osobowych zważył co następuje:

W uzasadnieniu wniosku o ponowne rozpatrzenie sprawy pełnomocnik G. przedstawił argumenty mające w jego opinii przemawiać za tym, że administratorem bezpieczeństwa informacji może być osoba prawna. Z tymi argumentami nie można się jednak zgodzić. Przede wszystkim nieprawdziwe jest twierdzenie pełnomocnika, że Generalny Inspektor Ochrony Danych Osobowych wydając zaskarżoną decyzję pominął brzmienie art. 36 ust. 3 ustawy, z którego wynikają dwie możliwe sytuacje sprawowania nadzoru nad przestrzeganiem zasad ochrony danych osobowych, tj. poprzez wyznaczenie administratora bezpieczeństwa informacji oraz poprzez samodzielne wykonywanie przez administratora danych czynności nadzorczych. Z treści decyzji w sposób jednoznaczny takie rozróżnienie wynika. Różnica natomiast sprowadza się do tego, że zdaniem Generalnego Inspektora, administrator danych sam może wykonywać zadania administratora bezpieczeństwa informacji jedynie wówczas, gdy jest osobą fizyczną prowadzącą działalność gospodarczą, gdy tymczasem w opinii pełnomocnika G. każdy administrator danych może te czynności wykonywać, niezależnie od tego, czy jest on osobą fizyczną prowadzącą działalność gospodarczą, czy też osobą prawną.

Choć można zgodzić się z pełnomocnikiem G., że ustawa o ochronie danych osobowych nie stanowi wyraźnie, że administratorem bezpieczeństwa informacji może być wyłącznie osoba fizyczna, to należy jednocześnie wskazać, że w literaturze przedmiotu przyjmuje się, że administrator bezpieczeństwa informacji musi być osobą fizyczną (por. A. Drozd, „Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy”, wydanie 4, str. 264-265; P. Barta i P. Litwiński, „Ustawa o ochronie danych osobowych. Komentarz.”, Warszawa 2009, str. 372, G. Sibiga, „Administrator bezpieczeństwa informacji (uwagi *de lege lata*)” w „Ochrona informacji niejawnych, biznesowych i danych osobowych” pod redakcją M. Gajos, Katowice 2010 r., str. 168). Wskazuje się również, że „przepis ten [art. 36 ust. 3 ustawy] ma umożliwić wykonywanie obowiązków administratora bezpieczeństwa informacji samodzielnie przez administratorów danych będących osobami fizycznymi prowadzącymi działalność gospodarczą. Jednocześnie wydaje się, że z uwagi na konstrukcję osób prawnych, administrator danych

osobowych będący osobą prawną ze swej istoty nie może korzystać z komentowanej instytucji i samodzielnie wykonywać obowiązków administratora bezpieczeństwa informacji” (P. Barta i P. Litwiński, „Ustawa o ochronie danych osobowych. Komentarz.”, Warszawa 2009, str. 372). Generalny Inspektor podziela w pełni zaprezentowane wyżej stanowisko doktryny.

Wbrew twierdzeniu pełnomocnika G. treść art. 37 ustawy jest istotna dla wykazania, że administrator bezpieczeństwa informacji musi być osobą fizyczną. Oczywiście w przypadku administratorów danych będących osobami fizycznymi prowadzącymi działalność gospodarczą, którzy samodzielnie wykonują czynności nadzoru nad przestrzeganiem zasad ochrony danych osobowych, nie ma mowy o tym, by nadawali oni sami sobie upoważnienia do przetwarzania danych, ale też nie dla takich sytuacji przepis ten został powołany w uzasadnieniu stanowiska Generalnego Inspektora zamieszczonego na stronie internetowej o adresie [...]. Powołanie się na ten przepis miało na celu wykazanie, że administrator danych niebędący osobą fizyczną prowadzącą działalność gospodarczą, jest zobowiązany wyznaczyć na administratora bezpieczeństwa informacji konkretną osobę fizyczną, gdyż tylko taka osoba w świetle art. 37 ustawy może zostać upoważniona do przetwarzania danych osobowych, a takie upoważnienie jest niezbędne do prawidłowego wykonywania czynności nadzorczych przez administratora bezpieczeństwa informacji.

Natomiast przywołany przez pełnomocnika G. art. 7 pkt 4 ustawy wskazuje wyłącznie, jakie podmioty podlegają przepisom ustawy i są zobowiązane do spełnienia wynikających z niej wymagań. Jednym z takich wymagań jest obowiązek wyznaczenia administratora bezpieczeństwa informacji, czego, co należy jeszcze raz podkreślić, G. nie uczyniła. Wskazać również należy, że Generalny Inspektor Ochrony Danych Osobowych, wbrew twierdzeniu pełnomocnika G., w żadnym miejscu zaskarżonej decyzji nie stwierdził, że administrator danych sam wykonujący czynności nadzoru nad przestrzeganiem zasad ochrony staje się administratorem bezpieczeństwa informacji lub też „przejmuje” jego funkcje.

Pełnomocnik G. w uzasadnieniu wniosku o ponowne rozpatrzenie sprawy skupił się także na przedstawieniu modelu sprawowania kontroli i nadzoru oraz na rozważaniach, kto od kogo przejmuje obowiązki z zakresu nadzoru nad przestrzeganiem zasad ochrony danych osobowych w związku z wyznaczaniem administratora bezpieczeństwa informacji. Nie kwestionując wynikających z tych rozważań wniosków wskazać należy, że można je odnieść bezpośrednio jedynie do tych sytuacji, w których przepisy o ochronie danych osobowych nakładają wprost na administratora danych obowiązki w tym zakresie. Przykładem takim jest, przywołany zresztą przez pełnomocnika, art. 38 ustawy, z którego wynika obowiązek dla administratora danych zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz

komu są przekazywane. Odmienne należy jednak podejść do obowiązku określonego w art. 36 ust. 3 ustawy, co wbrew twierdzeniu pełnomocnika G. nie oznacza nieuwzględnienia istoty i celu wykonywania funkcji nadzoru. Z powołanego przepisu ustawy wynika bowiem, że nadzór nad przestrzeganiem zasad ochrony danych ma być sprawowany przez administratora bezpieczeństwa informacji i który tylko ewentualnie może być wykonywany przez administratora danych (gdy jest on osobą fizyczną prowadzącą działalność gospodarczą). Do tej sytuacji nie można zatem odnieść przytoczonego przez pełnomocnika G. wyroku Sądu Najwyższego z dnia 10 września 1971 r. (I CR 260/71, SNOSNC 1972/4/71), tym bardziej, że dotyczy on stanu prawnego sprzed wejścia w życie przepisów o ochronie danych osobowych.

Tezy pełnomocnika G., że administratorem bezpieczeństwa informacji może być również osoba prawna, nie potwierdza także powołana przez niego literatura przedmiotu (P. Fajgielski, Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno – prawne. Lublin 2008). W żadnym z zamieszczonych w uzasadnieniu wniosku o ponowne rozpatrzenie sprawy cytatów z ww. opracowania nie padło bowiem takie stwierdzenie. Co więcej, jeden z tych cytatów (ze str. 214) przemawia raczej za stanowiskiem Generalnego Inspektora. Wynika z niego bowiem, że sam administrator danych będący osobą prawną może nie mieć możliwości skutecznego sprawowania nadzoru nad przestrzeganiem zasad ochrony danych osobowych. Potwierdzeniem tego jest zresztą kontrola G., która wykazała szereg uchybień w procesie przetwarzania danych osobowych, pomimo tego, że G. zobowiązana była wyłącznie do dopełnienia obowiązków wynikających z przepisów rozdziału 5 ustawy o ochronie danych osobowych. Być może nie doszłoby do powstania tych nieprawidłowości, gdyby został wyznaczony administrator bezpieczeństwa informacji.

Wbrew twierdzeniu pełnomocnika G., uzasadnienia dla twierdzenia, że zadania administratora bezpieczeństwa informacji może wykonywać administrator danych będący osobą prawną, nie stanowi możliwość podejmowania działań np. w postaci wyciągania określonych konsekwencji wobec pracowników upoważnionych do przetwarzania danych osobowych. Do zadań administratora bezpieczeństwa informacji nie należy bowiem wyciąganie konsekwencji służbowych wobec osób naruszających zasady ochrony danych osobowych.

Nie można się również zgodzić ze stanowiskiem pełnomocnika, że administratora bezpieczeństwa informacji nie można odnosić do urzędnika do spraw ochrony danych osobowych, o którym mowa w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UEL Nr 281, poz. 31). W literaturze przedmiotu wskazuje się bowiem, że „pierwowzorem dla funkcji administratora bezpieczeństwa informacji jest

urzędnik ds. ochrony danych osobowych (data protection official), o którym mowa w dyrektywie 95/46” (G. Sibiga, „Administrator bezpieczeństwa informacji (uwagi *de lege lata*)” w „Ochrona informacji niejawnych, biznesowych i danych osobowych” pod redakcją M. Gajos, Katowice 2010 r., str. 165). Co więcej, wbrew twierdzeniu pełnomocnika G., zadania urzędnika do spraw ochrony danych osobowych związane z prowadzeniem rejestru operacji przetwarzania danych wykonywanych przez administratora danych nie są jego jedynymi zadaniami. Jest on także odpowiedzialny za zapewnienie, w niezależny sposób, wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy dyrektywy, w czym mieści się sprawowanie nadzoru przestrzegania zasad ochrony danych osobowych. Trudno jednocześnie uznać, że takim urzędnikiem może być osoba prawna.

Pełnomocnik G. podkreśla w uzasadnieniu wniosku o ponowne rozpatrzenie sprawy, że G. jest członkiem programu [...], co ma gwarantować zgodność przetwarzania danych osobowych z przepisami dyrektywy 95/46/WE z dnia 24 października 1995 r. i przepisami ustawy o ochronie danych osobowych. Przeprowadzona kontrola przetwarzania danych osobowych w związku z usługą [...] wykazała jednak, o czym już wcześniej wspomniano, uchybienia w procesie ich przetwarzania. Co prawda, większość stwierdzonych nieprawidłowości zostało usuniętych, ale nastąpiło to po kilkumiesięcznej wymianie korespondencji, pomimo szeroko deklarowanej przy każdej okazji przez G. chęci współdziałania z Generalnym Inspektorem Ochrony Danych Osobowych.

Należy ponadto wskazać, że przedstawiciel G. w rozmowie telefonicznej przeprowadzonej z Generalnym Inspektorem oświadczył, że G. wyznaczy osobę do kontaktów w sprawach bezpieczeństwa danych osobowych w ramach usługi G. Do Biura Generalnego Inspektora Ochrony Danych Osobowych nie wpłynęło jednak żadne pismo, z którego wynikałoby, że taka osoba została w G. wyznaczona oraz jakie nałożone zostały na nią obowiązki w zakresie ochrony danych osobowych przetwarzanych w związku z realizacją usługi G.

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

Decyzja jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych w związku z art. 53 § 1 i art. 54 § 1 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed

sądami administracyjnymi (Dz. U. Nr 153, poz. 1270 z późn. zm.), od niniejszej decyzji stronie przysługuje prawo wniesienia skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie, w terminie 30 dni od dnia doręczenia niniejszej decyzji, za pośrednictwem Generalnego Inspektora Ochrony Danych Osobowych (na adres: ul. Stawki 2, 00-193 Warszawa).

W razie niewykonania decyzji w terminie zostanie wobec podmiotu zobowiązanego do jej wykonania wszczęte postępowanie egzekucyjne na podstawie przepisów ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r., Nr 229, poz. 1954 z późn. zm.).