



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 26 maja 2009 r.

DESiWM/DEC-440/19191/09

Dotyczy sprawy: DESiWM-430/20/07

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. 2000 r., Nr 98, poz. 1071 ze zm.) oraz art. 48 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 ze zm.) po przeprowadzeniu postępowania administracyjnego w sprawie wyrażenia zgody na przekazanie przez A, z siedzibą w Warszawie, danych osobowych do spółki A, z siedzibą w Stanach Zjednoczonych Ameryki, na podstawie zastosowanych rozwiązań umownych,

wyrażam zgodę na przekazanie danych osobowych do A, z siedzibą w Stanach Zjednoczonych Ameryki.

Uzasadnienie

Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynął wniosek złożony przez A, z siedzibą w Warszawie, zwaną dalej Wnioskodawcą lub Spółką, o udzielenie zgody na przekazanie danych osobowych do spółki A, z siedzibą w Stanach Zjednoczonych Ameryki, zwanej dalej Odbiorcą.

Po przeprowadzeniu postępowania wyjaśniającego Generalny Inspektor ustalił, co następuje:

- 1) Wnioskodawca z Odbiorcą zawarli „Umowę w sprawie przekazywania danych”, która została opracowana na podstawie alternatywnego zestawu standardowych klauzul umownych przyjętego decyzją Komisji Europejskiej nr 2004/915/WE z dnia 27 grudnia 2004 zmieniającą decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do

państw trzecich (Dz. Urz. UE L 385/74 z dnia 29 grudnia 2004 r.), zwaną dalej decyzją Komisji;

- 2) planowane przekazanie danych osobowych będzie się odbywało pomiędzy ich administratorami;
- 3) przekazywane będą dane osobowe w zakresie: nazwisko, imię, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, (dane te dotyczyć mogą również małżonków), adres zamieszkania lub pobytu, narodowość, adres stałego zameldowania, kraj zamieszkania lub pobytu, numery identyfikacyjne (PESEL, NIP, numer i seria dowodu osobistego oraz organ wydający dowód osobisty), miejsce pracy, zawód, wykształcenie, numer telefonu stacjonarnego oraz komórkowego, numer faksu oraz adres poczty elektronicznej;
- 4) dane będą wykorzystywane do obsługi infolinii ds. etyki działającej na terenie Stanów Zjednoczonych w celu umożliwienia wszystkim pracownikom oraz osobom współpracującym z podmiotami należącymi do grupy A poufnego zgłaszania wszelkich działań handlowych, które niosą w sobie ryzyko naruszenia etyki, przepisów prawa bądź są niezgodne z Kodeksem Postępowania, Kodeksem Etycznym bądź z innymi zasadami obowiązującymi w grupie A;
- 5) korporacja A opracowała procedury infolinii ds. etyki działającej na obszarze Unii Europejskiej i w krajach o podobnym poziomie ochrony danych osobowych;
- 6) w ramach linii ds. etyki będą przetwarzane dane osobowe zbierane w związku z następującymi zagadnieniami: rachunkowość, audyt wewnętrzny, kontrola finansowa lub oszustwa; ochrona konkurencji; pytania dotyczące polityki zgodności z przepisami; konflikt interesów; bezprawne wręczanie i przyjmowanie upominków; ujawnienie poufnych informacji - prywatność; dyskryminacja i prześladowanie; fałszowanie umów, sprawozdań i dokumentacji; kadry; przekupstwo lub bezprawne przekazywanie pieniędzy, w tym przekazywanie pieniędzy urzędnikom państwowym; wykorzystanie w obrocie papierami wartościowymi informacji wewnętrznych i inne przypadki naruszenia regulacji prawnych dotyczących obrotu papierami wartościowymi; wprowadzanie w błąd, nieuczciwe lub oszukańcze praktyki handlowe; niewłaściwe wykorzystywanie majątku firmy; usługi i kradzież; działania odwetowe; sankcje handlowe, Biuro Kontroli Aktywów Zagranicznych (OFAC), przypadki naruszenia polityki firmy i prawa, ogólne/różne;
- 7) zgodnie z oświadczeniem Wnioskodawcy strony umowy w sprawie przekazywania danych przyjęły procedury przetwarzania danych osobowych, które zapewniają zgodność z wytycznymi wynikającymi z opinii 1/2006 Grupy roboczej art. 29 w sprawie ochrony danych osobowych z dnia 1 lutego 2006 r. w sprawie zastosowania unijnych zasad ochrony

danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych (WP 117), zwanej dalej opinią 1/2006, a także zobowiązały się do ich przestrzegania;

- 8) Odbiorca będzie korzystał z oprogramowania i usług S, z siedzibą w Stanach Zjednoczonych Ameryki, która będzie przetwarzała dane na zasadzie powierzenia;
- 9) Wnioskodawca wyjaśnił, że osoba zgłaszająca nieprawidłowości będzie przekazywać dane do E, która jest autoryzowanym dostawcą usług w Stanach Zjednoczonych Ameryki zapewniającym bezpieczeństwo; następnie E przesyła zgłoszenie do Regionalnego Komitetu ds. Etyki w...; Regionalny Komitet ds. Etyki podejmuje decyzję, gdzie zgłoszenie powinno być skierowane: czy przekazać je lokalnemu zarządowi w celu rozpatrzenia, rozpatrzyć samodzielnie lub, w sytuacji zgłoszenia przestępstwa przeciwko ustawie Sarbanes Oxley, wysłać do Centralnego Komitetu ds. Etyki w... (siedziba Odbiorcy); przekazywane mogą być nie tylko zgłoszenia, ale również wszelkie informacje dotyczące przedmiotu dochodzenia, które mogą być niezbędne aby prawidłowo rozpatrzyć zgłoszenie;

10) w systemach informatycznych:

- a. zapewnione zostanie automatyczne odnotowanie daty pierwszego wprowadzenia danych,
- b. nie będzie automatycznego odnotowywania identyfikatora użytkownika wprowadzającego dane do systemu - system zezwala na anonimowe zgłoszenia,
- c. będzie zapewnione odnotowanie źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą, chyba że informacja jest przekazywana anonimowo,
- d. będzie zapewnione odnotowanie informacji o odbiorcach i zakresie przekazanych danych oraz o fakcie zgłoszenia sprzeciwu przez osobę, której dane dotyczą,
- e. będzie zapewnione wydrukowanie raportu dotyczącego wszystkich opisanych odnotowań;

11) zmiana haseł dostępu do systemu informatycznego następuje co 90 dni;

12) w pozostałym zakresie wykorzystywane systemy informatyczne spełniają wymogi 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. z 2004 r., Nr 100, poz. 1024 ze zm.).

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

Stosownie do art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071 ze zm.), zwanej dalej k.p.a., organ administracji publicznej załatwia sprawę przez wydanie decyzji, chyba że przepisy kodeksu stanowią inaczej.

W aktualnym stanie prawnym i faktycznym wniosek Spółki w zakresie przekazywania danych osobowych do wyżej wymienionego odbiorcy w Stanach Zjednoczonych zasługuje na uwzględnienie. Należy jednak wskazać, że zgodnie z art. 47 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 ze zm.), zwanej dalej ustawą, przekazywanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium, przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. Podkreślić należy, że powołany przepis ustawy odzwierciedla treść art. 25 ust. 1 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281/31, z 23.11.1995), zgodnie z którym państwa członkowskie zapewnią, że przekazywanie do kraju trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas, gdy - niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych postanowień niniejszej dyrektywy - dany kraj trzeci zapewni odpowiedni stopień ochrony.

Przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia takiego poziomu ochrony z zasady może nastąpić tylko wtedy gdy zostaną spełnione dodatkowe przesłanki określone w art. 47 ust. 2 lub 3 ustawy. Natomiast jeżeli w danym przypadku one nie zachodzą, to przekazywanie danych może mieć miejsce tylko po uzyskaniu zgody Generalnego Inspektora, pod warunkiem, że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą (art. 48 ustawy).

Ze względu na brak w Stanach Zjednoczonych Ameryki wystarczających regulacji z zakresu ochrony danych osobowych oraz fakt, że w świetle okoliczności przedmiotowej sprawy nie zachodzi żadna z przesłanek, o których mowa w art. 47 ust. 2 lub 3 ustawy, wymagane jest uzyskanie zgody Generalnego Inspektora.

Generalny Inspektor, rozpatrując wniosek o wyrażenie zgody na przekazywanie danych do państwa trzeciego, jest zobowiązany ustalić, czy administrator danych zapewnił odpowiedni poziom zabezpieczeń w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Ze

względu na to, że zapewnienie odpowiedniego poziomu ochrony może wiązać się z przyjęciem odpowiednich zobowiązań umownych, Generalny Inspektor musi również przeanalizować odpowiednie postanowienia umowne.

Przedłożona przez Spółkę umowa w sprawie przekazywania danych jest dokumentem, który zawiera postanowienia odpowiadające określonej decyzją Komisji alternatywnemu zestawowi standardowych klauzul umownych i czyni zadość wymogom określonym w art. 48 ustawy. Należy również stwierdzić, że przedstawione przez Spółkę środki organizacyjno - techniczne mające na celu zabezpieczenie danych osobowych, pomimo pewnych braków, stwarzają odpowiednie gwarancje ochrony przetwarzanych danych. W toku postępowania stwierdzono odstępstwa od przepisów rozporządzenia polegające na dopuszczeniu wprowadzania danych anonimowo, co jest związane z istotą funkcjonowania linii ds. etyki, w ramach których dopuszcza się anonimowe zgłaszanie nieprawidłowości. Ponadto pomimo faktu, że hasła automatycznie tracą ważność po upływie 90 dni, co nie spełnia wymogu części A pkt IV ust. 2 załącznika do rozporządzenia, który stanowi, że w przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana powinna następować nie rzadziej, niż co 30 dni, uwzględniając całość środków organizacyjno-technicznych można uznać, iż prowadzone przez Odbiorcę systemy informatyczne zapewniają wystarczający poziom ochrony danych osobowych. W konsekwencji należy stwierdzić, że Spółka zapewniła odpowiedni poziom zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Niemniej jednak, zalecane byłoby dostosowanie systemu uwierzytelniania w taki sposób, aby zmiana hasła następowała nie rzadziej, niż co 30 dni.

W tym miejscu podkreślić należy, że decyzja Generalnego Inspektora w przedmiocie wyrażenia zgody na przekazywanie danych osobowych do państwa trzeciego nie legalizuje wcześniejszego przekazywania danych osobowych do państwa trzeciego, które nastąpiłoby przed datą wydania decyzji w sprawie. W konsekwencji, rozpoczęcie operacji przekazywania danych osobowych do państwa trzeciego może nastąpić dopiero po wydaniu stosownej decyzji przez Generalnego Inspektora.

Niniejsza decyzja upoważnia Spółkę do przekazywania danych osobowych do Odbiorcy z siedzibą w Stanach Zjednoczonych Ameryki jedynie na warunkach określonych w złożonym wniosku dotyczącym przekazywania danych w ramach systemu linii ds. etyki i nie może stanowić podstawy dla przekazywania danych w innych celach. Jednocześnie poza zakresem niniejszego rozstrzygnięcia jest kwestia wypełnienia przez Spółkę pozostałych wymogów zawartych w ustawie o ochronie danych osobowych np. takich jak wykazanie się odpowiednią przesłanką legalności przetwarzania danych, czy spełnienie obowiązku informacyjnego.

Niezależnie od powyższego podkreślenia wymaga, że w przypadku kwalifikowanej formy przetwarzania danych, jaką jest przekazanie danych do państwa trzeciego, zachodzi także konieczność spełnienia jednej z przesłanek legalności przetwarzania danych, wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy. Ustawa wprowadzając w swym rozdziale 7 (art. 47 i 48) szczególny reżim dotyczący przekazywania danych osobowych do państw trzecich, nie wyłączyła zastosowania w takich wypadkach pozostałych przepisów ustawy. Przepisy art. 47 i 48 ustawy wprowadzają bowiem jedynie dodatkowe wymogi, które należy spełnić, gdy zamierza się przekazywać dane osobowe do państwa trzeciego. Konieczność ich wypełnienia nie zwalnia administratora danych z pozostałych obowiązków nałożonych na niego przepisami ustawy. A zatem w przypadku kwalifikowanej formy przetwarzania danych, jaką jest przekazanie danych do innego administratora danych, który ma siedzibę w państwie trzecim, zachodzi konieczność spełnienia jednej z przesłanek legalności przetwarzania danych, wymienionych w art. 23 ust. 1 lub art. 27 ust. 2 ustawy. Należy więc zauważyć, że zgodnie z art. 23 ust. 1 pkt 5 ustawy, przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Co do zasady powołana przesłanka może znaleźć zastosowanie w przypadku przetwarzania danych osobowych w systemach informowania o nieprawidłowościach, czy też liniach ds. etyki. Takie operacje nie mogą jednak w żaden sposób naruszać praw i wolności osób, których dane dotyczą, co jednocześnie wiąże się z koniecznością zapewnienia przez administratorów, że będą przestrzegane podstawowe zasady opisane w powołanej opinii 1/2006. Odrębnie należałoby też oceniać przekazywanie danych w związku z naruszeniami poza systemami linii ds. etyki.

W odniesieniu do kwestii dotyczącej sposobu spełnienia obowiązku informacyjnego należy odwołać się do treści art. 25 ust. 1 ustawy, zgodnie z którym w przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych obowiązany jest poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych o: adresie swojej siedziby i pełnej nazwie, a w przypadku kiedy administratorem jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku, celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych, źródle danych, prawie dostępu do treści swoich danych oraz ich poprawiania, uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8. Cytowany przepis implementuje art. 11 ust. 1 dyrektywy, w myśl którego w przypadku, gdy dane nie zostały uzyskane od osoby, której dane dotyczą, państwa członkowskie zapewniają, aby administrator danych bądź jego przedstawiciel był zobowiązany, w chwili przystąpienia do rejestracji danych osobowych lub w przypadku planowania ujawnienia danych osobie trzeciej, ale nie później gdy te dane są ujawniane

po raz pierwszy, dostarczyć osobie, której dane dotyczą, z wyjątkiem przypadku, gdy uzyskał je już wcześniej, określone informacje.

Wobec obecnego brzmienia art. 25 ustawy uznać należy, że nie daje on możliwości odstępstwa od zasady, że osoba, której dane dotyczą, powinna pozyskać wiadomość o gromadzeniu na jej temat określonych informacji bezpośrednio po ich utrwaleniu, jak i modyfikacji zakresu informacji, jakie powinny być przez administratora danych przekazane osobie, której dane dotyczą.

Z uwagi na powyższe, wobec zaistnienia odpowiednich przesłanek rozstrzygnięcia niniejszego postępowania administracyjnego, Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja niniejsza jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych oraz art. 129 § 1 i § 2 w zw. z art. 127 § 3 Kodeksu postępowania administracyjnego stronie niezadowolonej z niniejszej decyzji przysługuje, w terminie 14 dni od dnia jej doręczenia, prawo złożenia do Generalnego Inspektora Ochrony Danych Osobowych wniosku o ponowne rozpatrzenie sprawy (adres: Biuro Generalnego Inspektora Ochrony Danych Osobowych, ul. Stawki 2,00-193 Warszawa).