



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 20 maja 2009 r.

DESiWM/DEC-406/18293/09

Dotyczy sprawy: DESiWM-41-1/08

DECYZJA

Na podstawie art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 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 C, z siedzibą w Warszawie, danych osobowych do C, z siedzibą w Stanach Zjednoczonych Ameryki, na podstawie zastosowanych standardowych klauzul umownych stanowiących załącznik do decyzji Komisji Europejskiej 2004/915/WE z dnia 27 grudnia 2004 r. zmieniającej decyzję Komisji Europejskiej 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz.Urz. WE L 385/19 z 29.12.2004),

**wyrażam zgodę na przekazanie danych osobowych do wyżej wymienionego odbiorcy danych
w Stanach Zjednoczonych Ameryki.**

Uzasadnienie

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

Po przeprowadzeniu postępowania wyjaśniającego, w toku którego zwrócono się do Wnioskodawcy o złożenie wyjaśnień, Generalny Inspektor ustalił, co następuje:

- 1) Spółka zawarła z Odbiorcą umowę, zwanej dalej Umową, której treść odpowiada standardowym klauzulom umownym stanowiącym załącznik do decyzji Komisji Europejskiej 2004/915/WE z dnia 27 grudnia 2004 r. zmieniającej decyzję Komisji Europejskiej 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz.Urz. WE L 385/19 z 29.12.2004), zwanej dalej decyzją Komisji;
- 2) przekazywane dane dotyczą następujących kategorii osób:
 - a. pracowników Wnioskodawcy,
 - b. pracowników firm zależnych od Wnioskodawcy;
- 3) przekazywane dane dotyczą m.in. następujących kategorii danych:
 - a. informacji z zakresu pracy pracownika;
 - b. uprawnień, udziałów i/lub pobieranych świadczeń pracowniczych; podań o pracę, weryfikacji i wypowiedzeń umów;
 - c. oznaczenia pracownika;
 - d. adresu w sieci LAN;
 - e. kompletnego nazwiska i imienia; tytułu;
 - f. daty urodzenia; płci; stanu cywilnego;
 - g. rodzaju państwowego dowodu tożsamości oraz dowodu tożsamości;
 - h. adresu zamieszkania;
 - i. numeru domowego/telefonu komórkowego; służbowego adresu poczty elektronicznej;
 - j. statusu pracownika; ostatniej daty zatrudnienia; daty wygaśnięcia umowy;
 - k. oraz innych danych wymienionych w Załączniku B do Umowy – „Opis przekazywania danych”;
- 4) Odbiorca będzie przetwarzać dane w związku z zapewnieniem centralnego repozytorium wszystkich danych pracowniczych firmy C i jej spółek zależnych;
- 5) z wyłączeniem byłych pracowników, którzy nadal posiadają udziały w ramach planu pracowniczego udziału, przechowywane dane pracownicze będą obejmować tylko aktualnych, aktywnych pracowników;
- 6) nie będą przekazywane dane szczególnie chronione;
- 7) 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), zwanego dalej rozporządzeniem, z wyłączeniem zasad zmiany hasła, ponieważ hasła automatycznie tracą ważność po upływie 90 dni;

- 8) dane osobowe będą przekazywane w czasie trwania Umowy z Odbiorcą, tj. do momentu rozwiązania Umowy.

Po zapoznaniu się z całością zgromadzonego w sprawie materiału dowodowego Generalny Inspektor 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 Ameryki zasługuje na uwzględnienie. Należy 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. 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).

W związku z powyższym, należy stwierdzić, że Stany Zjednoczone Ameryki, z racji braku wystarczających uregulowań prawnych dotyczących ochrony danych osobowych, nie mogą być uznane za państwo zapewniające odpowiedni poziom ochrony danych osobowych, jak również w świetle zebranego materiału dowodowego nie zachodzi żadna z przesłanek określonych w art. 47 ust. 2 lub 3 ustawy. W konsekwencji konieczne jest wyrażenie zgody przez 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.

Biorąc pod uwagę możliwość zastosowania takiego rozwiązania przez Wnioskodawcę i Odbiorcę danych należy wskazać na kompetencję Komisji Europejskiej, która na mocy art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz. Urz. WE L 281, z 23.11.1995), zwanej dalej dyrektywą, jest uprawniona do uznania w drodze decyzji, że określone standardowe klauzule umowne zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek. Decyzje te wymagają, aby państwa członkowskie nie odmawiały uznania zabezpieczeń ustanowionych w standardowych klauzulach umownych określonych w decyzjach za zapewniające odpowiedni poziom ochrony danych osobowych. Nie wyłącza to jednak obowiązku spełnienia pozostałych wymogów nałożonych przez właściwe przepisy krajowe.

Zadeklarowane przez Spółkę zastosowanie alternatywnych standardowych klauzul umownych, określonych decyzją Komisji, powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez Spółkę klauzul ze standardowymi klauzulami umownymi. Analiza ta wykazała, że przedstawione przez Spółkę klauzule są zgodne z alternatywnymi standardowymi klauzulami umownymi.

Analizie również zostały poddane przedstawione przez Spółkę środki organizacyjno-techniczne mające na celu zabezpieczenie przetwarzanych danych osobowych. 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. Nie mniej jednak, zalecane byłoby dostosowanie systemu uwierzytelniania w taki sposób, aby zmiana hasła następowała nie rzadziej, niż co 30 dni.

Generalny Inspektor wyjaśnia, że niniejsza decyzja upoważnia Spółkę do przekazywania danych osobowych do Stanów Zjednoczonych Ameryki jedynie na warunkach określonych złożonym wnioskiem. Jednocześnie, poza zakresem niniejszego rozstrzygnięcia jest kwestia spełnienia przez Spółkę pozostałych przepisów ustawy. Podkreślenia również wymaga konieczność poinformowania osób, których dane dotyczą, o fakcie przekazywania ich danych osobowych do państwa trzeciego oraz o Odbiorcy danych w tym państwie. Należy wyraźnie stwierdzić, że wypełnienie powyższego obowiązku przez Spółkę ma kluczowe znaczenie dla zapewnienia realizacji uprawnień przez osoby, których dane dotyczą.

Wspomnienia wymaga także fakt, 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. W szczególności, co do zasady, przekazywanie danych osobowych pracowników przez pracodawcę innemu podmiotowi wymaga uprzedniego wyrażenia zgody przez pracowników.

W tym miejscu należy podkreślić, że decyzja Generalnego Inspektora w przedmiocie wyrażenia zgody na przekazywanie danych osobowych do państwa trzeciego nie legalizuje wcześniejszego przekazywania danych osobowych, które ewentualnie miałyby miejsce 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 Stanów Zjednoczonych Ameryki jedynie na warunkach określonych w złożonym wniosku.

Niezależnie od powyższego należy wskazać, że w przypadku zastosowania alternatywnego zestawu klauzul umownych decyzja Komisji wprowadza możliwość zastosowania dalej idących sankcji niż było to przewidziane w decyzji 2001/497/WE Komisji Europejskiej z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich na podstawie dyrektywy (Dz.Urz. WE L 181/19, z 4.07.2001).

Należy jedynie zaznaczyć, że w celu zapobieżenia nadużyciom mogącym wynikać ze zwiększenia elastyczności alternatywnego zestawu klauzul umownych, organy ochrony danych osobowych mają szerszą możliwość zakazania lub zawieszenia transferu danych w przypadku, gdy przekazujący dane odmówi podjęcia stosownych kroków w celu realizacji zobowiązań umownych dotyczących odpowiedzialności odbiorcy danych lub odbiorca odmówi współpracy w dobrej wierze z właściwymi organami ochrony danych osobowych w zakresie ochrony danych osobowych.

Z uwagi na powyższe Generalny Inspektor Ochrony Danych Osobowych rozstrzygnął jak w sentencji.

Decyzja niniejsza jest ostateczna. Na podstawie art. 21 ust. 1 ustawy o ochronie danych osobowych 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, 00-93 Warszawa).