



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

Michał Serzycki

Warszawa, dnia 22 grudnia 2009 r.

DESiWM/DEC-1292/48027/09

Dotyczy sprawy: DESiWM-41-30/09

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. 12 pkt 2 i 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 S, z siedzibą w Warszawie, danych osobowych do S, z siedzibą w Indiach, na podstawie zastosowanych standardowych klauzul umownych stanowiących załącznik do decyzji Komisji Europejskiej 2002/16/WE z dnia 27 grudnia 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania przetwarzającym dane mającym siedzibę w państwach trzecich, na mocy dyrektywy 95/46/WE (Dz. Urz. UE L 006, z 10.01.2002),

**wyrażam zgodę na przekazanie danych osobowych do wyżej wymienionego odbiorcy danych
w Indiach.**

Uzasadnienie

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

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

- 1) Wnioskodawca jest administratorem danych przetwarzanych w prowadzonym przez niego zbiorze danych „...”, który został zarejestrowany w ogólnokrajowym, jawnym rejestrze zbiorów danych osobowych prowadzonym przez Generalnego Inspektora;
- 2) Spółka zobowiązała się zawrzeć umowę o przekazaniu danych osobowych do Indii (projekt umowy w załączniku do wniosku) po uzyskaniu zgody Generalnego Inspektora, której treść odpowiadać będzie standardowym klauzulom umownym stanowiącym załącznik do decyzji Komisji Europejskiej 2002/16/WE z dnia 27 grudnia 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych przetwarzającym dane mającym siedzibę w państwach trzecich, na mocy dyrektywy 95/46/WE (Dz. Urz. UE L 006, z 10.01.2002), zwanej dalej decyzją Komisji;
- 3) przekazanie danych będzie się odbywało na zasadach ich powierzenia w rozumieniu art. 31 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;
- 4) celem przekazania danych jest zapewnienie tzw. „...” świadczonych przez Odbiorcę na rzecz Wnioskodawcy; ww. usługi zostały szczegółowo opisane w „Umowie o Świadczenie Usług zawartej z... (ang. ...)”; są to następujące usługi:
 - a. „...”,
 - b. „...”,
 - c. „...”,
 - d. „...”,
 - e. „...”,
 - f. „...”(czynności przetwarzania danych w ramach ww. usług zostały określone w Załączniku nr 1 do umowy o przekazaniu danych);
- 5) przekazywane dane dotyczą następujących kategorii osób:
 - a. pracownicy Wnioskodawcy lub jego podmiotów powiązanych,
 - b. zleceńbiorecy (np. zewnętrzni konsultanci) Wnioskodawcy lub jego podmiotów powiązanych,
 - c. klienci Wnioskodawcy lub jego podmiotów powiązanych;
- 6) przekazywane dane dotyczą następujących kategorii danych:
 - a. dane kontaktowe osoby, której dane dotyczą (np. nazwisko, numer służbowego telefonu komórkowego lub służbowy adres poczty elektronicznej),
 - b. główne dane służbowe pracowników (np. numer identyfikacyjny pracownika (Employee ID lub identyfikator grupowy... (GID)),

- c. szczegółowy podział kategorii danych na poszczególne kategorie osób został wymienione w piśmie Wnioskodawcy z dnia 30 października 2009 r.;
- 7) nie będą przekazywane dane szczególnie chronione w rozumieniu ustawy;
 - 8) wykorzystywane systemy informatyczne zasadniczo 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 częstotliwości zmiany haseł, bowiem w przedstawionej dokumentacji brakuje zapisu dotyczącego faktycznych interwałów zmian haseł, co świadczy o tym, że nie zostały spełnione wymogi zawarte w 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; w przedstawionej dokumentacji jest bowiem napisane, że: „zmiana hasła następować będzie zgodnie z wytycznymi administratora systemu, lub nie rzadziej, niż co 90 dni; 30 dni w przypadku danych szczególnie chronionych/kont użytkowników uprzywilejowanych (np. administratora systemu)”; zapis ten nie precyzuje faktycznych interwałów dotyczących zmian haseł w przypadku danych osobowych, a określa ogólne zasady stosowane do wszystkich danych w Spółce;
 - 9) dane osobowe będą przekazywane w czasie trwania umowy z Odbiorcą tj. do momentu rozwiązania umowy.
 - 10) pismem z dnia 30 października 2009 r. Wnioskodawca oświadczył, że Odbiorca złoży oświadczenie o zobowiązaniu się do przestrzegania „Wytycznych dla podmiotów zależnych (w państwach trzecich) w zakresie ochrony danych osobowych” razem z podpisaniem umowy o przekazywaniu danych osobowych i przed rozpoczęciem wykonywania czynności objętych umową o przekazaniu danych;
 - 11) pismem z dnia 26 listopada 2009 r. Wnioskodawca oświadczył, że adres siedziby Odbiorcy uległ zmianie w trakcie trwania postępowania:

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 Indiach zasługuje na uwzględnienie. Należy wskazać, że zgodnie z art. 47 ust. 1 ustawy, 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 Indie, z racji braku wystarczających uregulowań prawnych dotyczących ochrony danych osobowych, nie może być uznane za państwo zapewniające odpowiedni poziom ochrony danych osobowych, jak również w świetle zebranych materiałów dowodowych 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), 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. Taki charakter ma również powołana przez Spółkę decyzja Komisji.

Zadeklarowane przez Spółkę zastosowanie standardowych klauzul umownych, określonych decyzją Komisji, powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez Spółkę klauzul ze standardowymi klauzulami umownymi. Analiza ta wykazała, że przedstawiony przez Spółkę projekt klauzul jest zgodny ze standardowymi klauzulami umownymi. Ponadto, Spółka zobowiązała się do zawarcia umowy o przekazaniu danych osobowych do Indii (zgodnej z przedstawionym projektem załączonym do wniosku) po uzyskaniu zgody Generalnego Inspektora.

Analizie również zostały poddane przedstawione przez Spółkę środki organizacyjno-techniczne mające na celu zabezpieczenie przetwarzanych danych osobowych. Wykładnia art. 48 wskazuje, że zastosowane przez Odbiorcę środki organizacyjno-techniczne muszą być „odpowiednie”. Środki te nie muszą być identyczne do tych, które są wymagane na terytorium Rzeczypospolitej Polskiej tzn. powinny one adekwatnie zabezpieczać prywatność oraz prawa i wolności osób, których dane dotyczą. W związku z tym, pomimo faktu, że zastosowane zasady częstotliwości zmiany haseł są niezgodne z rozporządzeniem, uwzględniając całość przyjętych 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.

Spółka przekazując dane Odbiorcy nie traci przymiotu ich administratora. W przedmiotowej sprawie dochodzi jedynie do powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy. Pomimo tego, że podmiotowi, któremu powierzono przetwarzanie danych osobowych nie przysługuje status administratora danych, to ustawa nakłada na niego pewne obowiązki. Zgodnie z art. 31 ust. 2 ustawy, może on przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Natomiast odpowiedzialność za przestrzeganie przepisów ustawy z zasady spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. W konsekwencji, pomimo przekazania danych osobowych Odbiorcy, Spółka nadal będzie ponosiła odpowiedzialność za zgodność z prawem przetwarzania powierzonych danych osobowych.

Wspomnienia wymaga także fakt, że 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.

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 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 Indii jedynie na warunkach określonych w złożonym wniosku oraz po podpisaniu umowy o przekazaniu danych z Odbiorcą.

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).