



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 24 listopada 2010 r.

DESiWM/DEC-1296/46437/10

Dotyczy sprawy: [...]

DECYZJA

Na podstawie art. 104 ust. 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 **H. Sp. z o.o.**, danych osobowych do spółek należących do międzynarodowej grupy H., tj. do **H. Ltd.**, z siedzibą w Republice Indii, **H. Ltda.**, z siedzibą w Republice Kostaryki, oraz **H. S. de R.L. de C.V.**, Meksykańskich Stanach Zjednoczonych, na podstawie umowy o przekazywaniu danych wewnątrz grupy H. z dnia [...] czerwca 2009 r. (ang. *Amended and Restated Global Personal Data Transfer Agreement*), zawierającej w swym załączniku nr 2 zestaw 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 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. UE L 6, z 10.01.2002),

wyrażam zgodę na przekazanie danych osobowych do wyżej wymienionych odbiorców danych w Republice Indii, Republice Kostaryki oraz Meksykańskich Stanach Zjednoczonych.

Uzasadnienie

Do Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem”, wpłynęły dwa wnioski o wyrażenie zgody na przekazanie danych osobowych do ww. spółek należących do międzynarodowej grupy H., zwanej dalej „Grupą H.”, złożone przez:

- 1) **H. Sp. z o.o.**, o sygn. [...], zwaną dalej Wnioskodawcą lub Spółką, oraz
- 2) **G. Sp. z o.o.**, o sygn. [...].

Po zapoznaniu się z przedstawionymi przez Wnioskodawcę dokumentami oraz przeprowadzeniu postępowania wyjaśniającego, w toku którego zwrócono się do Wnioskodawcy o złożenie wyjaśnień, Generalny Inspektor ustalił, co następuje:

H. F. Sp. z o.o., nie składała wniosku o wyrażenie zgody na przekazanie danych do państw trzecich ze względu na to, iż osoby świadczące usługi na jej rzecz zatrudnione są przez spółkę G. Sp. z o.o. i dane jej pracowników przekazywane będą na podstawie decyzji wydanej względem G. Sp. z o.o.

Wymienione wyżej spółki Grupy H. mające siedziby w Rzeczypospolitej Polskiej zbierają od osób, których dane dotyczą, pisemną zgodę na przekazywanie danych osobowych, która ze względu na swoją treść nie może być uznana za przesłankę z art. 47 ust. 3 pkt 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, na przekazywanie danych osobowych do Republiki Indii, Republiki Kostaryki oraz Meksykańskich Stanów Zjednoczonych.

- 1) w dniu [...] kwietnia 2004 r. podmioty należące do Grupy H. zawarły umowę o przekazywaniu danych, tym danych osobowych, wewnątrz grupy, która została zmieniona aneksem do umowy z dnia [...] czerwca 2009 r. (ang. *Amended and Restated Global Personal Data Transfer Agreement*, zwana dalej „Umową GPDTA”); Umowa GPDTA zawiera:

- a. listę definicji (część I),
- b. opis obowiązków wewnątrz Grupy H. (część II),
- c. system ochrony danych (część III),
- d. Procedury egzekucyjne oraz prawa (osób, których dane dotyczą) (część IV),

oraz trzy załączniki zawierające:

- e. listę spółek z Grupy H. będących stroną Umowy GPDPA (załącznik nr 1, ang. *Exhibit A*),
 - f. postanowienia umowne odpowiadające swą treścią standardowym klauzulom umownym 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 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. UE L 6, z 10.01.2002), zwanej dalej „decyzją Komisji 2002/16/WE” (załącznik nr 2, ang. *Exhibit B*),
 - g. postanowienia umowne odpowiadające swą treścią standardowym klauzulom umownym 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, z 29.12.2004), zwanej dalej „decyzją Komisji 2004/915/WE” (załącznik nr 3, ang. *Exhibit C*);
- 2) wniosek o wyrażenie zgody na przekazanie danych do państw trzecich dotyczy trzech podmiotów wymienionych w załączniku nr 1 do Umowy GPDPA, których siedziby mieszczą się w Republice Indii, Republice Kostaryki oraz Meksykańskich Stanach Zjednoczonych i ogranicza się wyłącznie do powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy; w związku z ewentualnymi zmianami w procesach przepływu danych Wnioskodawca oświadczył, że w przyszłości może dochodzić do zmian podmiotów z listy wskazanej w załączniku nr 1, na rzecz których następować będzie powierzenie przetwarzania danych;
- 3) przekazane będą następujące kategorie osób:
- a. pracowników Wnioskodawcy,
 - b. kandydatów do pracy;
- 4) przekazane kategorie danych zostały przedstawione w załączniku nr 9 do wniosku o wyrażenie zgody na przekazanie danych, oraz w piśmie Wnioskodawcy z dnia 19 lipca br.;

- 5) w ramach Grupy H. przewiduje się przekazywanie danych szczególnie chronionych w rozumieniu ustawy; nie będą natomiast takie dane zbierane w państwach Europejskiego Obszaru Gospodarczego i przekazywane do państw trzecich;
- 6) celem planowanych operacji przekazywania danych są zmiany w zakresie wewnętrznych procedur związanych z przetwarzaniem danych osób w związku z zatrudnieniem lub procesem rekrutacyjnym; wykorzystywana będzie w tym celu infrastruktura sprzętowa zlokalizowana w Republice Indii, Republice Kostaryki i Meksyku;
- 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 wyjątkiem częstotliwości zmiany hasła wykorzystywanego do uwierzytelniania użytkowników systemów informatycznych, bowiem wymuszanie jego zmiany następuje maksymalnie, co 365 dni, co jest niezgodne z wymogami Części A pkt IV ust. 2 załącznika do rozporządzenia, który stanowi, że jego zmiana następować będzie nie rzadziej, niż co 30 dni; nadmienić należy, że systemy odbiorców danych spełniają zasady wynikające z polityki haseł stosowanej w podmiotach należących do Grupy H., która przewiduje wykorzystanie haseł o długości, co najmniej 12 znaków, ustawianego przez użytkownika; w przypadku pierwszego logowania generowane jest hasło tymczasowe, które musi zostać zmienione na hasło wybrane przez użytkownika; hasło musi posiadać 3 z 5 typów znaków tj. duże litery, małe litery, symbole, cyfry lub symbole Unicode; wdrożony jest również mechanizm zabezpieczający przed wykorzystaniem dotychczasowych haseł, który zapamiętuje 6 ostatnich haseł; istnieje także możliwość wykorzystania do autoryzacji użytkowników, zamiast identyfikatora i hasła, urządzenia [...] lub karty [...] zawierający certyfikat (PKI); autoryzacja odbywa się po podaniu kodu PIN; ponadto, wszystkie laptopy użytkowane w Grupie H. posiadają zaszyfrowane dyski twarde zabezpieczone oprogramowaniem [...]; dostęp do zbiorów danych osobowych objętych przedmiotowym wnioskiem wymaga, aby użytkownik:
 - a. podał hasło (PIN) w celu odszyfrowania dysku,
 - b. zalogował się do domeny H. i systemu operacyjnego (zgodnie z powyższą procedurą dotyczącą haseł lub z wykorzystaniem tokena USB lub karty).

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

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

W aktualnym stanie faktycznym i prawnym wniosek Spółki w zakresie przekazywania danych osobowych do wyżej wymienionych odbiorców danych w Republice Indii, Republice Kostaryki oraz Meksykańskich Stanach Zjednoczonych 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 Republika Indii, Republika Kostaryki oraz Meksykańskie Stany Zjednoczone z racji braku wystarczających uregulowań prawnych dotyczących ochrony danych osobowych, nie mogą być uznane za państwa 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 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. Taki charakter ma również powołana przez Spółkę decyzja Komisji 2002/16/WE.

Zgodnie z art. 7 decyzji Komisji Europejskiej 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy (Dz. Urz. UE L 39, z 12.02.2010), zwanej dalej „decyzją Komisji 2010/87/UE”, decyzja Komisji 2002/16/WE utraciła moc obowiązywania z dniem 15 maja 2010 r. Umowa powierzenia przetwarzania danych zawarte zgodnie z decyzją Komisji 2002/16/WE przed dniem 15 maja 2010 r. pozostają w mocy i obowiązują dopóty, dopóki czynności przekazywania i przetwarzania danych, które są przedmiotem danej umowy, pozostają niezmienione, a dane osobowe objęte decyzją Komisji 2002/16/WE są nadal przekazywane między stronami. Jeżeli umawiające się strony zdecydują o dokonaniu zmian w tym zakresie lub podzleceniu (podpowierzeniu) wykonania czynności przetwarzania danych, które są przedmiotem umowy, wymagać to będzie zawarcia nowej umowy zgodnej ze standardowymi klauzulami umownymi określonymi w decyzji Komisji 2010/87/UE.

Zadeklarowane przez Spółkę zastosowanie standardowych klauzul umownych, określonych decyzją Komisji 2002/16/WE, powoduje konieczność porównania przez Generalnego Inspektora przyjętych przez Spółkę klauzul ze standardowymi klauzulami umownymi. Analiza ta wykazała, że przedstawione przez Spółkę klauzule są zgodne ze standardowymi klauzulami umownymi. Przedstawione zastosowane klauzule umowne zostały zawarte przed datą wygaśnięcia decyzji 2002/16/WE tj. przed dniem 15 maja 2010 r.

Analizie również zostały poddane przedstawione przez Spółkę środki organizacyjno-techniczne mające na celu zabezpieczenie przetwarzanych danych osobowych. Art. 48 ustawy wskazuje, że zastosowane przez Odbiorcę środki organizacyjno-techniczne muszą być „odpowiednie” (adekwatne). Środki te nie muszą być identyczne do tych, które są wymagane na terytorium Rzeczypospolitej Polskiej – powinny one adekwatnie zabezpieczać prywatność oraz prawa i wolności osób, których dane dotyczą.

Podkreślenia wymaga, że nie ma wątpliwości, co do adekwatności przyjętych środków organizacyjno-technicznych w przypadku, gdy środki te spełniają minimalne wymagania określone

w rozporządzeniu. Jeżeli natomiast środki te różnią się od rozwiązań przyjętych w rozporządzeniu, podlegają one każdorazowo ocenie Generalnego Inspektora. Pomimo faktu, że zmiana hasła następować będzie maksymalnie, co 365 dni, co jest niezgodne z wymogami Części A pkt IV ust. 2 załącznika do rozporządzenia, który stanowi, że jego zmiana następować będzie nie rzadziej, niż co 30 dni, uwzględniając całość przyjętych środków organizacyjno-technicznych można uznać, iż prowadzone przez odbiorców danych systemy informatyczne zapewniają wystarczający poziom ochrony danych osobowych. W konsekwencji można stwierdzić, że Spółka zapewniła odpowiedni poziom zabezpieczeń w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Niemniej, Wnioskodawca zobowiązany jest dostosować system uwierzytelniania w taki sposób, aby zmiana hasła następowała nie rzadziej, niż co 30 dni.

Spółka przekazując dane 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, 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 Republiki Indii, Republiki Kostaryki oraz Meksykańskich Stanów Zjednoczonych jedynie na warunkach określonych w złożonym wniosku.

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 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).