



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 20 grudnia 2010 r.

DESiWM/DEC-1385/50319/10

Dotyczy sprawy: [...]

DECYZJA

Na podstawie art. 104 ust. 1 i art. 105 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 **I. Sp. z o.o.**, danych osobowych do następujących spółek mających siedziby:

- 1) w Republice Argentyńskiej:
 - a. I. S.A.
 - b. In. S.A.,
- 2) w Kanadzie:
 - a. I., Ltd.
 - b. L., Inc.
- 3) w Stanach Zjednoczonych Ameryki:
 - a. I. Corp.,
 - b. U. LLC.
 - c. U. Corp.,
 - d. US. Corp.,
- 4) w Związku Australijskim:
 - a. I. Ltd.,
 - b. I. Pty. Ltd.,
 - c. I. A. Ltd.,
- 5) we Wspólnocie Bahamów: I. Ltd.,
- 6) na Barbadosie: I. Corp. (Barbados),
- 7) w Federacyjnej Republice Brazylii: I. Ltda.,
- 8) w Republice Chile:

- a. I. SAC,
 - b. S. Ltda.,
- 9) w Chińskiej Republice Ludowej:
- a. I. (Shanghai) Co, Ltd.,
 - b. I. (China) Co. Ltd.,
 - c. I. Ltd.,
 - d. I. (Shenzhen) Co. Ltd.,
 - e. I. Co. Ltd.,
 - f. IB. Co. Ltd.,
- 10) w Specjalnym Regionie Administracyjnym Hongkongu Chińskiej Republice Ludowej:
- I. Ltd.,
- 11) na Tajwanie: I. Corp.,
- 12) w Republice Kolumbii:
- a. In. S.A.,
 - b. IB.,
- 13) w Republice Kostaryki: I. S.R.L.,
- 14) w Republice Chorwacji: I. Ltd.
- 15) w Republice Ekwadoru:
- a. I. CA.,
 - b. S. S.A.,
- 16) w Arabskiej Republice Egiptu: I. Co.,
- 17) w Republice Indii:
- a. I. Ltd.,
 - b. IB. Ltd.,
 - c. N. Ltd.,
- 18) w Republice Indonezji:
- a. P.,
 - b. PT.,
- 19) w Państwie Izrael:
- a. I. Ltd.,
 - b. I.T. Ltd.,
 - c. I.P. Ltd.,
 - d. I.I. Ltd.,
 - e. I.S. Ltd.,

20) na Jamajce: I. Co.,

21) w Japonii:

- a. I. Co.,
- b. I. Co. Ltd.,
- c. I. S. Co. Ltd.,
- d. I. Se. Co. Ltd.,
- e. IB. Se. Co. Ltd.,
- f. I. So. Co. Ltd.,
- g. IB. So. Co. Ltd.,
- h. I. Ser. Co. Ltd.,
- i. I. C. Co.,
- j. IB. C. Co. Ltd.,
- k. I. E. Co. Ltd.,
- l. IB. Ser. Co. Ltd.,
- m. IB. S. Co.,
- n. IB. Sol. Co. Ltd.,
- o. D. Inc.,
- p. R. Co. Ltd.,
- q. IS Co., Ltd.,
- r. Re. Co. Ltd.,
- s. D. Co. Ltd.,
- t. E. Corp.,
- u. J. Co. Ltd.,
- v. K. Corp.,
- w. N. Co. Ltd.,
- x. I. Ltd.,
- y. M. Inc.,

22) w Republice Korei: I. Inc.,

23) w Malezji: I. Bhd.,

24) w Meksykańskich Stanach Zjednoczonych:

- a. I. de CV.,
- b. I. S. de R.L.,
- c. I. S. de R.L. de CV.,

25) w Królestwie Marokańskim: I.,

- 26) na Curaçao: I. Corp.,
- 27) w Nowej Zelandii: I.,
- 28) w Islamskiej Republice Pakistanu: I.,
- 29) w Republice Peru:
- a. I. SAC,
 - b. IB. SAC,
- 30) w Republice Filipin:
- a. I. Inc.,
 - b. IB. Inc.,
 - c. I. Incorporated,
 - d. I. D., Inc.,
- 31) w Federacji Rosyjskiej: I. Ltd.,
- 32) w Republice Serbii: I. d.o.o.,
- 33) w Republice Singapuru:
- a. I. Ltd.,
 - b. In. Ltd.,
- 34) w Republice Południowej Afryki: I. Ltd.,
- 35) w Republice Surinamu: I.
- 36) w Królestwie Tajlandii:
- a. I. Co. Ltd.,
 - b. IB. Co. Ltd.,
- 37) w Republice Trynidadu i Tobago: I.,
- 38) w Republice Tunezyjskiej:
- a. I.,
- 39) w Republice Turcji:
- a. T.,
 - b. P.,
 - c. S.,
 - d. So.,
 - e. I.,
 - f. B.,
- 40) na Ukrainie: I.,
- 41) w Państwie Zjednoczonych Emiratów Arabskich: I.,
- 42) we Wschodniej Republice Urugwaju: I.,

43) w Boliwariańskiej Republice Wenezueli:

a. I. S.A.,

b. e. S.A.,

44) w Socjalistycznej Republice Wietnamu: I.,

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 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),

1) umarzam postępowanie w zakresie przekazywania danych do:

a. podmiotów mających siedziby w Republice Argentyńskiej oraz w Kanadzie (pkt 1 i 2),

b. I. Corp., z siedzibą w Stanach Zjednoczonych Ameryki,

2) w pozostałym zakresie wyrażam zgodę na przekazanie danych osobowych do wyżej wymienionych odbiorców danych w państwach trzecich (pkt od 3b do 44).

Uzasadnienie

Do Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem”, wpłynął wniosek złożony przez **I. Sp. z o.o.**, zwaną dalej Wnioskodawcą lub Spółką, o udzielenie zgody na przekazanie danych osobowych do wyżej wymienionych odbiorców danych w państwach trzecich, zwanych dalej Odbiorcami.

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

- 1) spółki **I. Sp. z o.o.**, **I. S. Sp. z o.o.**, **I. B. Sp. z o.o.**, oraz **I. G. Sp. z o.o.**, należą do międzynarodowej grupy kapitałowej I., której główną spółką jest In. Corp., z siedzibą w Stanach Zjednoczonych Ameryki, zwana dalej „I. Corp.”;
- 2) zgodnie z powszechnie dostępnymi informacjami Departamentu Handlu Stanów Zjednoczonych Ameryki I. Corp. uczestniczy w programie „bezpiecznej przystani” od 15 sierpnia 2002 r.;
- 3) ww. polskie spółki należące do międzynarodowej grupy kapitałowej I. odbierają od pracowników związanych umową o pracę, pracowników czasowych oraz dorywczych 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 przekazanie danych osobowych do państw trzecich;
- 4) w dniu [...] grudnia 2009 r. spółki należące do międzynarodowej grupy kapitałowej I., mające siedziby na terytorium Europejskiego Obszaru Gospodarczego (EOG), w tym I. Sp. z o.o., I. S. Sp. z o.o. oraz I.B. Sp. z o.o., podpisały umowę, na czas nieokreślony, o powierzeniu przetwarzania danych ze spółkami należącymi do międzynarodowej grupy kapitałowej I., mającymi siedziby poza terytorium EOG, której treść odpowiada 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 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”;

- 5) w dniu [...] grudnia 2009 r. spółka I. G. Sp. z o.o. podpisała analogiczną umowę, na czas nieokreślony, o powierzeniu przetwarzania danych ze spółkami międzynarodowej grupy kapitałowej I., mającymi siedziby poza terytorium EOG, której treść odpowiada standardowym klauzulom umownym stanowiącym załącznik do decyzji Komisji 2002/16/WE;
- 6) ww. umowy powierzenia przetwarzania danych osobowych zostały zawarte przed dniem 15 maja 2010 r. tj. przed datą utraty mocy decyzji Komisji 2002/16/WE; przekazanie danych będzie się odbywało na zasadach ich powierzenia w rozumieniu art. 31 ustawy;
- 7) przekazywane będą dane dotyczące następujących kategorii osób:
 - a. *w odniesieniu do danych kadrowych*: pracowników związanych umową o pracę; pracowników czasowych; pracowników dorywczych; wolontariuszy; osób przydzielonych; pracowników oddelegowanych; kursantów; niezależnych wykonawców; emerytowanych pracowników; kandydatów do pracy; osób na utrzymaniu pracowników (ubezpieczeni współmałżonkowie i partnerzy, dzieci, rodzice); osób wskazanych do kontaktu w nagłych wypadkach,
 - b. *w odniesieniu do danych handlowych*: pracowników; członków kierownictwa; agentów; konsultantów i innych ekspertów aktualnych klientów; konsultantów i innych ekspertów potencjalnych klientów; partnerów biznesowych; sprzedawców; podwykonawców; dostawców,
 - c. *a także innych osób, których dane dotyczą* tj. użytkowników serwisów internetowych IBM, którzy podali swoje dane osobowe;
- 8) przekazywane będą następujące kategorie danych:
 - a. *w odniesieniu do danych kadrowych*:
 - i. podstawowe informacje, w tym również dane o osobach na utrzymaniu (wdowiec/wdowa, dzieci, opiekun prawny),
 - ii. wewnętrzne dane identyfikacyjne,
 - iii. dane kontaktowe,
 - iv. informacje dotyczące miejsce wykonywania pracy,
 - v. informacje dotyczące przydziałów i przeniesień,
 - vi. dane o zatrudnieniu oraz informacje administracyjne,
 - vii. informacje dotyczące zawodu,
 - viii. informacje dotyczące godzin pracy,

- ix. informacje bankowe,
 - x. historia zatrudnienia, wykształcenia i szkolenia,
 - xi. informacje o datach związanych z zatrudnieniem,
 - xii. dane o nieobecnościach w pracy,
 - xiii. informacje o przynależności do stowarzyszeń i organizacji branżowych oraz do Klubu I.,
 - xiv. informacje o wynagrodzeniu i świadczeniach,
 - xv. informacje o wydatkach,
 - xvi. dane dotyczące wydajności i rozwoju,
 - xvii. inne dane osobowe, w tym m.in. uprawnienia dostępu, fotografia,
- b. *w odniesieniu do danych handlowych:*
- i. pracowników, członków kierownictwa, agentów, konsultantów i innych ekspertów aktualnych lub potencjalnych klientów, partnerów biznesowych, sprzedawców, podwykonawców, dostawców: dane kontaktowe,
 - ii. klientów, partnerów biznesowych, sprzedawców, podwykonawców, dostawców: podstawowe informacje,
- c. *innych osób, których dane dotyczą* tj. użytkowników serwisów internetowych I.: kraj siedziby i preferowany język; identyfikacja użytkownika; imię i nazwisko; dane kontaktowe; dane o organizacji; obszar zainteresowań zawodowych; inne informacje (Biznes Partner, Deweloper),
- d. nie będą przekazywane dane szczególnie chronione w rozumieniu art. 27 ustawy z wyjątkiem danych o stanie zdrowia pracowników w zakresie wynikającym z obowiązków i praw Wnioskodawcy w związku z zatrudnieniem,
- e. kategorie danych zostały szczegółowo opisane w Załącznikach nr 1 do umów, o których mowa w pkt 4 oraz 5;
- 9) celem ogólnym przekazywania danych osobowych jest scentralizowanie przetwarzania informacji kadrowych i handlowych w ograniczonej liczbie współużytkowanych ośrodków oraz innych obiektów na potrzeby świadczenia na rzecz spółek należących do międzynarodowej korporacji I. mających siedziby na terytorium EOG usług wspomagających ich procesy biznesowe (w tym m.in. udostępnianie infrastruktury informatycznej oraz oprogramowania aplikacyjnego);
- 10) dane o osobach na utrzymaniu będą przetwarzane w celach związanych z realizacją świadczeń z ubezpieczenia społecznego pracowników oraz organizacją wyjazdów pracowników wraz z osobami na utrzymaniu w celu podjęcia pracy w innych spółkach I.,

- 11) cele szczegółowe zostały opisane w Załącznikach nr 1 do umów, o których mowa w pkt 4 oraz 5;
- 12) lokalizacja współużytkowanych ośrodków, w których będą przetwarzane dane, zależeć będzie od pojemności poszczególnych ośrodków i dostępności zasobów przydzielonych im w danym czasie; przekazywane dane osobowe, oraz wykorzystywane oprogramowanie mogą fizycznie znajdować się na różnych serwerach w różnych scentralizowanych ośrodkach (w tym na serwerach zapasowych) oraz korzystać ze wsparcia współużytkowanych ośrodków (np. ośrodków zintegrowanych usług technicznych lub ośrodków usług outsourcingu na potrzeby transformacji biznesu); niemniej wszystkie te operacje przetwarzania danych odbywać się będą odpowiedniego Odbiorcy;
- 13) 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 (90 dni), co jest niezgodne z wymogami rozporządzenia, które stanowi, że jego zmiana następować będzie nie rzadziej, niż co 30 dni.

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

I. Stwierdzić należy, że w myśl art. 6 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r., Nr 98, poz. 1071 ze zm.), zwanej dalej kpa, organy administracji publicznej działają na podstawie przepisów prawa. Zgodnie z art. 105 ust. 1 kpa, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o umorzeniu postępowania.

Przesłanką umorzenia postępowania w świetle powołanego przepisu jest bezprzedmiotowość postępowania „z jakiegokolwiek przyczyny”, czyli z każdej przyczyny powodującej brak jednego z elementów materialnego stosunku prawnego w odniesieniu do jego strony podmiotowej lub przedmiotowej. Sytuacja taka ma właśnie miejsce w rozpatrywanej sprawie.

W odniesieniu do postępowań toczących się na podstawie art. 48 ustawy, o ich bezprzedmiotowości można mówić w szczególności wtedy, gdy państwo trzecie, do którego mają

być przekazane dane osobowe zapewnia odpowiedni poziom ochrony. W takiej sytuacji Generalny Inspektor jest obowiązany umorzyć toczące się postępowanie.

Biorąc pod uwagę, że złożony przez Spółkę wniosek wśród Odbiorców wskazuje podmioty mające siedziby w Republice Argentyńskiej oraz Kanadzie, a także dotyczy przekazywania danych do I. uczestniczącego w programie „bezpiecznej przystani”, zauważyć należy, iż na mocy art. 25 ust. 6 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, zwanej dalej dyrektywą, Komisja Europejska uprawniona jest do stwierdzenia w drodze decyzji, że dane państwo trzecie zapewnia odpowiedni stopień ochrony, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji z Komisją Europejską, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych. Uznanie przez Komisję Europejską danego państwa za zapewniające odpowiednią ochronę jest równoznaczne z tym, iż zapewnia ono takie same gwarancje ochrony, jakie są na terytorium Rzeczypospolitej Polskiej. Tym samym spełniona jest przesłanka określona w art. 47 ust. 1 ustawy.

W dniu 30 czerwca 2003 r. Komisja Europejska wydała decyzję 2003/490/WE w sprawie właściwej ochrony danych osobowych w Argentynie (Dz. Urz. UE L 168, z 5. 07. 2003). Zgodnie z jej art. 1 dla celów art. 25 ust. 2 dyrektywy 95/46/WE, Argentyna jest traktowana jako państwo zapewniające odpowiedni poziom bezpieczeństwa w odniesieniu do danych osobowych przekazywanych ze Wspólnoty. W konsekwencji została spełniona przesłanka określona w art. 47 ust. 1 ustawy.

W dniu 20 grudnia 2001 r. Komisja Europejska wydała decyzję 2002/2/WE w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz. Urz. UE L 2, z 4.01.2002). Na mocy jej art. 1 Kanada uznawana jest za kraj zapewniający odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty do odbiorców objętych przepisami kanadyjskiej ustawy o ochronie informacji osobowych i dokumentów elektronicznych. Należy zauważyć, że ustawę tę stosuje się do organizacji sektora prywatnego, które zbierają wykorzystują lub ujawniają informacje osobowe w ramach działalności komercyjnej. Pewne wątpliwości może jedynie rodzić kwestia zastosowania przepisów powołanej ustawy kanadyjskiej do danych pracowniczych. Biorąc jednak pod uwagę, że dane pracownicze podlegają ochronie wynikającej z przepisów ustawy o ochronie informacji osobowych i dokumentów m.in. wtedy, gdy dana organizacja prowadzi działalność gospodarczą, która wiąże się bądź z międzynarodowym przepływem danych, bądź z przepływem danych między

provincjami, należy uznać, że taka sytuacja będzie miała miejsce w niniejszej sprawie. W konsekwencji została spełniona przesłanka określona w art. 47 ust. 1 ustawy.

W dniu 26 lipca 2000 r. Komisja Europejska wydała decyzję 2000/520/WE w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu Stanów Zjednoczonych Ameryki (Dz. Urz. WE 215, 25.8.2000). Zgodnie z jej art. 1 dla celów art. 25 ust. 2 dyrektywy, w odniesieniu do wszystkich działań wchodzących w zakres dyrektywy przyjmuje się, że zasady ochrony prywatności w ramach programu „bezpiecznej przystani” zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty do organizacji mających siedzibę w Stanach Zjednoczonych Ameryki. Oznacza to, że przekazywanie danych do spółki I., która przystąpiła do programu „bezpiecznej przystani”, odbywałoby się na podstawie przepisów art. 47 ust. 1 ustawy.

Z uwagi na powyższe, wobec zaistnienia odpowiednich przesłanek, Generalny Inspektor umorzył postępowanie w omawianym zakresie z powodu bezprzedmiotowości.

II. Stosownie do art. 104 ust. 1 kpa, 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 wymienionych Odbiorców, o których mowa w pkt od 3b do 44, 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 państwa trzecie, o których mowa w pkt od 3b do 44, 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 przez Wnioskodawcę 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. Umowy 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 klauzule umowne zostały zawarte przed datą wygaśnięcia decyzji Komisji 2002/16/WE tj. przed 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 danych w państwie trzecim 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 następuje po 90 dniach, 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 następować będzie nie rzadziej, niż co 30 dni, uwzględniając całość przyjętych środków organizacyjno-technicznych, uznać można, iż prowadzone przez Odbiorców 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 w ramach powierzenia nie traci przymiotu ich administratora. W przedmiotowej sprawie dochodzi 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 na zasadach ich powierzenia, Spółka nadal będzie ponosiła odpowiedzialność za zgodność przetwarzania danych osobowych z prawem.

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 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 Odbiorców, o których mowa w pkt od 3b do 44, 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).