



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Wojciech R. Wiewiórowski

Warszawa, dnia 20 sierpnia 2014 r.

DESIWM/DEC-826/14

Dotyczy sprawy: [...]

DECYZJA

Na podstawie art. 104 § 1 i art. 105 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2013 poz. 267) 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.), zwanej dalej ustawą, po przeprowadzeniu postępowania administracyjnego w sprawie wyrażenia zgody na przekazanie przez L. sp. z o.o., z siedzibą w W., danych osobowych do:

- 1) Australii:
 - do R. Ltd, z siedzibą pod adresem: C.;
 - do R2. Ltd, z siedzibą pod adresem: C.;
- 2) Austrii:
 - do L., z siedzibą pod adresem: W
- 3) Brazylii:
 - do E., z siedzibą pod adresem: R;
- 4) Chińskiej Republiki Ludowej:
 - do R., z siedzibą pod adresem: B;
- 5) Danii:
 - do A., z siedzibą pod adresem: A.;
- 6) Francji:
 - do E., z siedzibą pod adresem: P.;
 - do L., z siedzibą pod adresem: P.;
 - do E2., z siedzibą pod adresem: B.;
 - do G., z siedzibą pod adresem: P.;
 - do L2., z siedzibą pod adresem: P.;
 - do L3., z siedzibą pod adresem: N. Nimes;
- 7) Hiszpanii:
 - do E., z siedzibą pod adresem: M.;
- 8) Holandii:
 - do R., z siedzibą pod adresem: A.;
 - do E., z siedzibą pod adresem A.;
 - do L., z siedzibą pod adresem: R.;
 - do L2., z siedzibą pod adresem: A.,

- do R2., z siedzibą pod adresem: A.;
 - do R3., z siedzibą pod adresem: Z.;
 - do K., z siedzibą pod adresem: Z.;
- 9) Indii:
- do R., z siedzibą pod adresem: D.;
- 10) Irlandii:
- do E., z siedzibą pod adresem: C.;
 - do B., z siedzibą pod adresem: D.;
- 11) Japonii:
- do E., z siedzibą pod adresem: T.;
 - do L., z siedzibą pod adresem: T.;
- 12) Kanady:
- do R., z siedzibą pod adresem: T.;
 - do L., z siedzibą pod adresem: M.;
- 13) Korei Południowej:
- do E., z siedzibą pod adresem: S.;
- 14) Malezji:
- do L., z siedzibą pod adresem: K.;
- 15) Meksyku:
- do M., z siedzibą pod adresem: M.;
- 16) Niemiec:
- do E., z siedzibą pod adresem: M.;
 - do E2., z siedzibą pod adresem: F.;
 - do C., z siedzibą pod adresem: K.;
 - do L., z siedzibą pod adresem: M.;
- 17) Nowej Zelandii:
- do L., z siedzibą pod adresem: W.;
- 18) Rzeczypospolitej Polskiej:
- do E. Sp. z o.o., z siedzibą pod adresem: W.
- 19) Republiki Południowej Afryki
- do L., z siedzibą pod adresem: D.;
- 20) Rosji:
- do R., z siedzibą pod adresem: M.;
- 21) Singapuru:
- do E., z siedzibą pod adresem: W.;
 - do R., z siedzibą pod adresem: S.;
 - do R2., z siedzibą pod adresem: S.;
- 22) Stanów Zjednoczonych Ameryki:
- do E., z siedzibą pod adresem: N.;
 - do R., z siedzibą pod adresem: N.;
- 23) Tajwanu:
- do E., z siedzibą pod adresem: T.;
- 24) Wielkiej Brytanii:
- do R., z siedzibą pod adresem: L.;
 - do R2., z siedzibą pod adresem: L.;
 - do E., z siedzibą pod adresem: O.;
 - do B., z siedzibą pod adresem: L.;
 - do R3., z siedzibą pod adresem: S.;
- 25) Włoch:
- do E., z siedzibą pod adresem: M.;

- do I. z siedzibą pod adresem: M..

na podstawie zastosowanych standardowych klauzul umownych stanowiących załącznik do decyzji Komisji Europejskiej 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach 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 39, z 12.02.2010),

- 1) umarzam postępowanie w zakresie przekazania danych osobowych do podmiotów z siedzibą w Austrii, Danii, Francji, Niemczech, Irlandii, Włoszech, Holandii, Rzeczypospolitej Polskiej, Hiszpanii oraz Wielkiej Brytanii;**
- 2) umarzam postępowanie w zakresie przekazania danych osobowych do podmiotów:**
 - z siedzibą w Kanadzie, do których zastosowanie znajduje decyzja Komisji z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz.U. L 2 z 4.1.2002, str. 13—16),**
 - z siedzibą w Nowej Zelandii, do których zastosowanie znajduje decyzja wykonawcza Komisji z dnia 19 grudnia 2012 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych w Nowej Zelandii (Dz.U. L 28 z 30.1.2013, str. 12—14);**
- 3) w pozostałym zakresie wyrażam zgodę na przekazanie danych.**

Uzasadnienie

Do Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem”, wpłynął wniosek złożony przez L. sp. z o.o., z siedzibą w W., zwaną dalej Wnioskodawcą lub Spółką, o wyrażenie zgody na przekazanie danych osobowych do wyżej wymienionych podmiotów, mających siedziby zarówno na terytorium Europejskiego Obszaru Gospodarczego, jak i poza nim, zwanych dalej Odbiorcami.

Po zapoznaniu się z przedstawionymi przez Wnioskodawcę dokumentami, Generalny Inspektor ustalił, co następuje:

- 1) Wnioskodawca jest spółką posiadającą siedzibę na terytorium Rzeczypospolitej Polskiej;

- 2) Wnioskodawca zawarł umowę z Odbiorcami dotyczącą przekazania danych osobowych, wzorowaną na standardowych klauzulach umownych stanowiących załącznik do decyzji Komisji Europejskiej 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach 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 39, z 12.02.2010);
- 3) przekazanie będzie się odbywało na zasadzie powierzenia przetwarzania zgodnie z art. 31 ustawy;
- 4) przekazane będą dane pracowników spółek Grupy R. na całym świecie, dla celów ułatwienia zarządzania zasobami kadrowymi, rozwoju i zatrzymania pracowników spółek Grupy R. na całym świecie, w tym: rocznych ocen pracowników, planowania przekazywania obowiązków między pracownikami oraz rozwoju zarządzania;
- 5) przekazane zostaną następującego kategorii danych: spis pracowników i dane dotyczące pracy: historia kariery poza i w organizacji (dostarczane przez pracownika), zadania specjalne/projekty (dostarczane przez pracownika), edukacja i akredytacja/certyfikaty (dostarczane przez pracownika), nagrody/wyróżnienia/uznanie (dostarczane przez pracownika), udział w kursach dot. kierowania zespołem oraz w specjalistycznych kursach technicznych, ocena planu rozwoju osobistego (gdzie ma zastosowanie) w okresie ostatnich 3 lat, rezultaty związane z pełnieniem bieżącej funkcji (dostarczane przez pracownika), ocena mocnych stron (dostarczane przez pracownika), ocena obszarów wymagających dalszego rozwoju (dostarczane przez pracownika); dane dotyczące wykształcenia, szkolenia i certyfikatów pracowników a także dane dotyczące przebiegu kariery pracowników i planowania przekazywania obowiązków między pracownikami: wskaźnik ryzyka utrzymania (prawdopodobieństwo odejścia), wpływ/efekt utraty, czy nowe wyzwanie jest potrzebne, potencjał pracownika i prawdopodobieństwo jego awansu (dostarczane przez menadżera), ocena ścieżki kariery, możliwe role w przyszłości, możliwi następcy do zatrudnienia (dostarczane przez menadżera), rok uczestnictwa w lokalnym przeglądzie talentów/Przeгляд talentów w grupie/program zarządzania (jeżeli ma zastosowanie), pole dla ogólnych komentarzy (dostarczane przez osobę zajmującą się zarządzaniem predyspozycjami – talent manager); pożądana ścieżka kariery, rozwój celów i działań (dostarczane przez pracownika);
- 6) nie będą przekazane dane szczególnie chronione w rozumieniu ustawy;

7) wykorzystywane przez Odbiorcę 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 urzędnicy i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024), zwanego dalej rozporządzeniem.

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

1. Stosownie do art. 104 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2013 r., poz. 267.), zwanej dalej kpa, organ administracji publicznej załatwia sprawę przez wydanie decyzji, chyba że przepisy kodeksu stanowią inaczej. Zgodnie zaś z art. 105 § 1 kpa, gdy postępowanie z jakiegokolwiek przyczyny stało się bezprzedmiotowe, organ administracji publicznej wydaje decyzję o umorzeniu postępowania. Bezprzedmiotowość postępowania w rozumieniu powołanego przepisu oznacza, iż brak jest któregoś z elementów materialnego stosunku prawnego, a wobec tego nie można wydać decyzji załatwiającej sprawę przez rozstrzygnięcie jej co do istoty. Przyczyny bezprzedmiotowości mogą powstać na skutek faktów naturalnych lub na skutek zdarzeń prawnych. Klasyczna postać bezprzedmiotowości postępowania ujawni się wtedy, gdy przedmiot rozstrzygnięcia w sprawie faktycznie i prawnie nie istnieje.

Należy wskazać, że art. 47 oraz 48 ustawy, dotyczą przekazania danych do państwa trzeciego, którym zgodnie z art. 7 pkt. 7 ustawy, jest państwo nienależące do Europejskiego Obszaru Gospodarczego. Biorąc pod uwagę, że Spółka objęła swoim wnioskiem Odbiorców, z siedzibą w Austrii, Danii, Francji, Niemczech, Irlandii, Włoszech, Holandii, Rzeczypospolitej Polskiej, Hiszpanii oraz Wielkiej Brytanii, tj. w państwach należących do EOG, postępowanie w tym zakresie jako bezprzedmiotowe należało umorzyć.

2. Należy wskazać, że zgodnie z art. 47 ust. 1 ustawy, przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Odpowiedni poziom ochrony danych osobowych, o którym mowa powyżej, jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter danych, cel i czas

trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe (art. 47 ust. 1a ustawy).

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 istnieją na terytorium Rzeczypospolitej Polskiej. Tym samym spełniona jest przesłanka określona w art. 47 ust. 1 ustawy.

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.

W dniu 20 grudnia 2001 r. Komisja Europejska wydała decyzję na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych (Dz.U. L 2 z 4.1.2002, str. 13—16). 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 prowincjami, należy uznać, że taka sytuacja będzie miała miejsce w niniejszej sprawie.

W dniu 19 grudnia 2012 r. Komisja Europejska wydała decyzję wykonawczą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych

osobowych w Nowej Zelandii (Dz.U. L 28 z 30.1.2013, str. 12—14) w której uznała, że Nowa Zelandia zapewnia właściwy poziom ochrony danych osobowych przekazywanych ze Wspólnoty.

W konsekwencji, w zakresie objętym ww. decyzjami Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych toczące się postępowania należało umorzyć.

4. Przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego 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 przekazanie danych osobowych 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, które obejmuje punkt 3 sentencji, 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 uzyskanie zgody Generalnego Inspektora.

Generalny Inspektor, rozpatrując wniosek o wyrażenie zgody na przekazanie danych do państwa trzeciego, jest zobowiązany ustalić, czy administrator danych zapewnił odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Ze względu na to, że zapewnienie odpowiednich zabezpieczeń 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 odpowiednie gwarancje ochrony prywatności oraz podstawowych praw i wolności osób fizycznych oraz wykonywania odpowiednich praw zgodnie wymogami art. 26 ust. 2 dyrektywy. Nie wyłącza to jednak obowiązku spełnienia pozostałych

wymogów nałożonych przez właściwe przepisy krajowe. Taki charakter ma również przywołana przez Spółkę decyzja Komisji 2010/87/UE.

Zadeklarowane przez Spółkę zastosowanie standardowych klauzul umownych określonych decyzją Komisji 2010/87/UE 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.

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 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 osoby, której 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. Po dokonaniu ich analizy Generalny Inspektor stwierdził, że przedstawione przez Spółkę środki zapewniają odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.

Spółka przekazując dane w ramach powierzenia nie traci przymiotu ich administratora. Przedmiotowa sprawa dotyczy 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 planowanego przekazania danych osobowych na zasadach ich powierzenia, Spółka nadal będzie ponosić odpowiedzialność za zgodność przetwarzania danych osobowych z prawem. Jednakże należy podkreślić, że w sytuacji powierzenia przetwarzania danych osobowych musi mieć możliwość sprawowania kontroli nad operacjami przetwarzania danych osobowych.

Wspomnienia wymaga także fakt, że ustawa wprowadzając w swym rozdziale 7 (art. 47 i 48) szczególny reżim dotyczący przekazania 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 przekazać

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 przekazanie danych osobowych do państwa trzeciego nie legalizuje wcześniejszego przekazania danych osobowych do państwa trzeciego, które ewentualnie miałyby miejsce przed datą wydania decyzji w sprawie. W konsekwencji, rozpoczęcie operacji przekazania danych osobowych do państwa trzeciego może nastąpić dopiero po wydaniu stosownej decyzji przez Generalnego Inspektora. Niniejsza decyzja upoważnia Spółkę do przekazania danych osobowych do państw trzecich, 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.

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, 00-193 Warszawa).