

**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*Dr Wojciech R. Wiewiórowski*

Warszawa, dnia 28 marca 2011 r.

**DESiWM/DEC-244/11/13775**

Dotyczy sprawy: [...]

**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 **T. Sp. z o.o.**, danych osobowych do **T Inc.**, z siedzibą w Stanach Zjednoczonych Ameryki oraz **T1 Inc.**, 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),

1. **odmawiam wyrażenia zgody na przekazanie danych ujawniających pochodzenie etniczne pracownika;**
2. **w pozostałym zakresie wyrażam zgodę na przekazanie danych osobowych do wyżej wymienionych odbiorców danych w Stanach Zjednoczonych Ameryki;**

**Uzasadnienie**

Do Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej Generalnym Inspektorem, wpłynął wniosek złożony przez **T. Sp. z o.o.**, zwaną dalej Wnioskodawcą lub Spółką, o udzielenie zgody na

przekazanie danych osobowych do **T. Inc.** z siedzibą w Stanach Zjednoczonych Ameryki oraz **T1 Inc.** z siedzibą Stanach Zjednoczonych Ameryki, zwanych dalej Odbiorcami.

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:

1) Wnioskodawca jest administratorem danych osobowych i pozostaje częścią międzynarodowej grupy spółek T, w której wiodącą rolę odgrywają T. Inc. w Stanach Zjednoczonych Ameryki;

2) Wnioskodawca zawarł z Odbiorcami umowę transferu danych, zwaną dalej Umową, zgodną ze standardowymi klauzulami umownymi stanowiącymi 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;

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

4) przekazywane dane dotyczą pracowników Wnioskodawcy oraz osób zatrudnionych na innych podstawach prawnych niż stosunek pracy;

5) przekazywane będą następujące dane: imię i nazwisko, data urodzenia, stan cywilny, adres zamieszkania i numer telefonu, kraj zamieszkania, obywatelstwo, narodowość, poziom znajomości języków obcych, dane kontaktowe w sytuacjach awaryjnych, nazwa pracodawcy, stanowisko i kategoria wynagrodzenia, doświadczenie zawodowe, płaca podstawowa, dodatki i świadczenia, stawka podatku, program emerytalny i wysokość składki, data zatrudnienia bądź ponownego zatrudnienia, program zarządzania świadczeniami (np. osoby pozostające na utrzymaniu, beneficjenci), udzielone upomnienia, szkolenia, oceny pracowników i ich rozwoju, sposób rozwiązywania stosunku pracy, dane z wywiadu przy odejściu, informacja o nieobecnościach w pracy, dane współmałżonków: imię, nazwisko, adres, stopień pokrewieństwa oraz jeśli to konieczne, data urodzenia osób pozostających na utrzymaniu;

6) w ramach transferu mogą być również przekazywane dane wrażliwe, w tym dotyczące stanu zdrowia, tj.: o zakończeniu i czasie trwania zwolnienia chorobowego, urlopu macierzyńskiego (w stopniu koniecznym jedynie do ustalenia wysokości świadczeń) oraz informacje o stopniu niepełnosprawności. Zgodnie z oświadczeniem ewidencja stanu zdrowia pracownika nie będzie przechowywana w scentralizowanej bazie danych, lecz oddzielnie u Wnioskodawcy. Ponadto Wnioskodawca dopuszcza możliwość przekazywania danych o pochodzeniu etnicznym pracownika

w celu monitorowania i zapewnienia równych szans zgodnie z polityką grupy i przepisami obowiązującego prawa (dozwolone w USA jedynie w celu przechowywania bez możliwości analizowania lub wykorzystywania), jednocześnie w złożonych przez siebie wyjaśnieniach Wnioskodawca prezentował stanowisko, że podstawą prawną do przetwarzania danych o przynależności etnicznej w celu ochrony pracowników przed dyskryminacją jest art. 18<sup>3a</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r., Nr 21, poz. 94 ze zm.), zwanej dalej Kodeksem pracy, oraz Międzynarodowa Konwencja w sprawie Likwidacji Wszelkich Form Dyskryminacji Rasowej z dnia 7 marca 1966 r.;

7) dane mają być przetwarzane w celach zarządzania zasobami ludzkimi oraz wypłacania świadczeń pracownikom i ich rodzinom;

8) 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 urządzenia 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 2000 r. Nr 98, poz. 1071 ze zm.), organ administracji publicznej załatwia sprawę przez wydanie decyzji, chyba że przepisy kodeksu stanowią inaczej.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926), zwanej dalej ustawą, 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 przekazywać dane osobowe do państwa trzeciego. Konieczność ich wypełnienia nie zwalnia administratora danych z pozostałych obowiązków nałożonych na niego przepisami ustawy, a w szczególności z konieczności spełnienia zasady legalności, adekwatności, czy też celowości. Należy też wskazać, że administrator danych nie jest upoważniony do przekazania danych do państwa trzeciego w szerszym zakresie niż ten, w którym może przetwarzać dane osobowe na terytorium Rzeczypospolitej Polskiej.

Poprzedzając dalsze rozważania należy wyraźnie zaznaczyć, że legalność przetwarzania danych jest oceniana przy uwzględnieniu powszechnie obowiązujących na terytorium Rzeczypospolitej Polskiej źródeł prawa. I tak, zgodnie z art. 27 ust. 1 ustawy, zabrania się przetwarzania danych ujawniających pochodzenie

rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Na zasadzie wyjątku od powołanej zasady, przetwarzanie danych wrażliwych jest możliwe np. gdy przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie (art. 27 ust. 2 pkt 6 ustawy).

Zakres danych, które mogą być przetwarzane przez pracodawcę w związku z zatrudnieniem osoby został określony w art. 22<sup>1</sup> Kodeksu pracy, zgodnie z którym pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących; imię (imiona) i nazwisko; imiona rodziców; datę urodzenia; miejsce zamieszkania (adres do korespondencji); wykształcenie; przebieg dotychczasowego zatrudnienia (§ 1). Zgodnie z § 2 cytowanego przepisu, pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL). Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Ponadto, pracodawca może żądać podania innych danych osobowych niż określone w § 1 i 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów (§ 4). Jednakże w polskim systemie prawnym nie ma przepisów, które upoważniałyby do zbierania danych o takim charakterze, w szczególności nie stanowią takiej podstawy przepisy prawa pracy dotyczące równego traktowania w stosunkach pracy. Powyższe uwagi odnoszą się również do informacji o narodowości w zakresie wykraczającym poza pojęcie narodowości rozumianej jako obywatelstwo, taka informacja może również ujawniać pochodzenie etniczne.

Ze względu na powyższe, należało odmówić wyrażenia zgody na przekazanie danych ujawniających pochodzenie etniczne.

2. W aktualnym stanie prawnym i faktycznym, wniosek Spółki w pozostałym zakresie 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 Stany Zjednoczone Ameryki, z racji braku wystarczających uregulowań prawnych dotyczących ochrony danych osobowych, nie może być uznana 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 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 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. 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. Po dokonaniu ich analizy Generalny Inspektor

stwierdził, że przedstawione przez Spółkę środki stwarzają uzasadnione gwarancje ochrony przetwarzanych danych na poziomie nie gorszym niż na terytorium Rzeczypospolitej Polskiej.

Raz jeszcze podkreślenia wymaga 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. W szczególności, co do zasady, przekazywanie (udostępnianie) danych osobowych pracowników przez pracodawcę innemu administratorowi danych wymaga uprzedniego wyrażenia zgody przez pracowników w rozumieniu art. 23 ust. 1 pkt 1 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 Stanów Zjednoczonych jedynie na warunkach określonych w złożonym wniosku. Jednocześnie, poza zakresem niniejszego rozstrzygnięcia jest kwestia spełnienia przez Spółkę pozostałych przepisów ustawy.

W przypadku przekazania danych pomiędzy administratorami, podkreślenia również wymaga konieczność poinformowania osób, których dane dotyczą, o fakcie przekazania ich danych osobowych do państw trzecich oraz o odbiorcach danych w tych państwach. Należy wyraźnie stwierdzić, że wypełnienie powyższego obowiązku przez Spółkę ma kluczowe znaczenie dla zapewnienia realizacji uprawnień przez osoby, których dane dotyczą.

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 Komisji. 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 lub odbiorca odmówi współpracy w dobrej wierze z właściwymi organami ochrony danych osobowych w zakresie ochrony danych osobowych.

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 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).

