

ZASADY PRZEKAZYWANIA DANYCH OSOBOWYCH DO PAŃSTW TRZECICH.

Wstęp

Postępująca globalizacja gospodarki światowej wpływa na wzrost transgranicznej wymiany danych osobowych. Przekazywanie danych osobowych do państw trzecich, w szczególności do takich, które nie zapewniają na swoim terytorium przynajmniej takich gwarancji ochrony danych osobowych, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, wiąże się z dużym ryzykiem naruszenia praw i wolności osób których dane dotyczą. Dlatego ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), zawiera szczególne wymogi dotyczące przekazywania danych osobowych do państw trzecich. Zostały one określone w rozdziale 7 ustawy o ochronie danych osobowych zatytułowanym „Przekazywanie danych osobowych do państwa trzeciego” (art. 47 i 48). Podkreślenia wymaga, że powyższe przepisy implementują odpowiednie postanowienia 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. Dlatego też mają one istotne znaczenie dla wykładni przepisów ustawy o ochronie danych osobowych.

Na jakich zasadach można przekazywać dane osobowe do państw należących do Europejskiego Obszaru Gospodarczego?

Ustawa o ochronie danych osobowych, w obowiązującym obecnie brzmieniu, nie zawiera szczególnych przepisów regulujących odrębnie przekazywanie danych osobowych do państw należących do Europejskiego Obszaru Gospodarczego, zwanych dalej państwami członkowskimi EOG. Należy bowiem podkreślić, że zgodnie z definicją legalną określoną w art. 7 pkt 7 ustawy o ochronie danych osobowych, przez państwo trzecie rozumie się państwo nienależące do Europejskiego Obszaru Gospodarczego. Oznacza to, że przepływ danych w obrębie Europejskiego Obszaru Gospodarczego jest traktowany tak samo, jak transfer danych na terytorium Polski. Zasada ta dotyczy wszystkich państw członkowskich Unii Europejskiej oraz

tych państw członkowskich Europejskiego Obszaru Gospodarczego, które nie są członkami UE (obecnie to: Norwegia, Islandia i Lichtenstein).

Swobodny przepływ danych w ramach Unii Europejskiej oraz szerzej w ramach Europejskiego Obszaru Gospodarczego jest koniecznym wymogiem członkostwa Polski w strukturach UE. Państwa te implementowały w swych wewnętrznych porządkach prawnych postanowienia Dyrektywy 95/46/WE. Do dwóch podstawowych celów Dyrektywy należy zaś:

- zapewnienie odpowiedniego poziomu ochrony danych osobowych
- zapewnienie swobody przepływu danych wewnątrz terytorium Unii Europejskiej. W

konsekwencji przyjętego przez ustawodawcę rozwiązania przekazywanie danych osobowych do państw należących do Europejskiego Obszaru Gospodarczego podlega ogólnym zasadom przetwarzania danych osobowych ustalonych przez ustawę o ochronie danych osobowych, z wyłączeniem rozdziału 7. Taki administrator danych, tak samo jak administrator danych przetwarzający dane tylko na terytorium Polski, jest zobowiązany m.in. do spełnienia jednej z przesłanek legalności przetwarzania danych osobowych, zasady celowości i jakości danych osobowych, jak również jest zobowiązany do zabezpieczenia danych.

Czy przekazywanie danych osobowych do państw trzecich wymaga spełnienia dodatkowych obowiązków?

Tak. W odróżnieniu do przekazywania danych osobowych do państwa członkowskiego EOG, w przypadku przekazywania danych osobowych do państwa trzeciego, oprócz konieczności spełnienia ogólnych wymogów przewidzianych przez ustawę o ochronie danych osobowych, należy również dodatkowo wypełnić obowiązki nałożone przepisami rozdziału 7 ustawy o ochronie danych osobowych.

Na jakich zasadach można przekazywać dane osobowe do państw trzecich?

Na podstawie art. 47 ust. 1 ustawy o ochronie danych osobowych, przekazanie 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.

Należy zaznaczyć, że cytowany przepis jest odzwierciedleniem treści art. 25 ust. 1 Dyrektywy 95/46/WE, zgodnie z którym państwa członkowskie zapewnią, że przekazywanie do

państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu może nastąpić tylko wówczas, gdy - niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych postanowień niniejszej Dyrektywy - dane państwo trzecie zapewni odpowiedni stopień ochrony.

W świetle postanowień ustawy o ochronie danych osobowych oraz prawa wspólnotowego przekazywanie danych osobowych do państwa trzeciego co do zasady jest możliwe tylko wtedy, gdy państwo to zapewnia odpowiedni stopień ochrony danych osobowych, co na gruncie ustawy o ochronie danych osobowych jest wyrażone jako zapewnienie gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Polski.

W jakich przypadkach państwo trzecie zapewnia odpowiednie gwarancje ochrony danych osobowych?

Ustawa o ochronie danych osobowych nie daje wprost wskazówek, jakie przesłanki decydują o ocenie, czy dane państwo trzecie zapewnia odpowiednią ochronę danych osobowych. Warto więc zwrócić uwagę na treść ust. 2 art. 25 Dyrektywy 95/46/WE, zgodnie z którym odpowiedniość stopnia ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zestawu takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, normy prawne, zarówno ogólne jak i branżowe, obowiązujące w państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym kraju.

Próbie ustalenia metodologii badania stopnia ochrony danych osobowych w państwie trzecim podjęła Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołanej na mocy art. 29 Dyrektywy 95/46/WE, zwana dalej Grupą Roboczą Art. 29.

Grupa Robocza Art. 29 w dokumencie roboczym z dnia 24 lipca 1998 r. nr WP 12 w sprawie przekazywania danych osobowych do państw trzecich: zastosowanie art. 25 i 26 Dyrektywy UE dotyczącej danych osobowych podkreśliła, że analiza pojęcia odpowiedniej ochrony musi uwzględniać dwa elementy: treść zasad dotyczących przetwarzania danych osobowych oraz środki zapewniające skuteczne zastosowanie tych zasad. Wśród podstawowych zasad przetwarzania danych osobowych, które powinny być zapewnione w państwie trzecim należy wymienić:

zasadę celowości – dane powinny być przetwarzane dla określonych celów; ich dalsze wykorzystywanie jest jedynie możliwe, jeżeli nie jest niezgodne z pierwotnym celem przekazywania danych.

zasadę jakości danych oraz ich adekwatności – dane powinny być dokładne i jeżeli jest to konieczne aktualne. Dane powinny być adekwatne do celu ich przekazywania.

zasadę zapewnienia obowiązku informacyjnego – osobom, których dane dotyczą powinna być zapewniona odpowiednia informacja o celu przetwarzania danych osobowych oraz o administratorze danych w państwie trzecim.

zasadę zapewnienia zabezpieczenia danych – powinny być podjęte odpowiednie do istniejącego ryzyka środki techniczne i organizacyjne mające na celu zabezpieczenie danych osobowych.

zasadę zapewnienia prawa dostępu do danych, poprawiania oraz prawa sprzeciwu – osoba, której dane dotyczą powinna mieć zapewnione prawo dostępu do informacji o przetwarzanych o niej danych, prawo do ich poprawiania, a także w określonych sytuacjach prawo sprzeciwu wobec ich przetwarzania.

zasadę ograniczenia dalszego przekazywania danych - co do zasady dalsze przekazywanie danych przez podmiot w państwie trzecim powinno być dopuszczalne jedynie w sytuacji, gdy następny podmiot otrzymujący dane jest również związany zasadami zapewniającymi odpowiednią ochronę danych osobowych.

Ze względu na duże zróżnicowanie krajowych systemów ochrony danych osobowych Grupa Robocza wskazała trzy cechy, które te systemy powinny spełniać w zakresie środków pozwalających na realizację zasad przetwarzania danych osobowych, a zatem system ten powinien zapewniać wysoki poziom zgodności z zasadami przetwarzania danych osobowych (powinien być on efektywny oraz zapewniać wysoki poziom świadomości swych obowiązków przez administratorów danych). System ten także powinien umożliwiać dochodzenie swoich praw przez poszczególne osoby, których dane dotyczą, co oznacza konieczność istnienia mechanizmów zapewniających niezależne rozpatrywanie skarg. System powinien również zapewniać możliwość dochodzenia odpowiedniego odszkodowania w razie naruszenia zasad przetwarzania danych osobowych.

Tekst dokumentu roboczego (m.in. w języku angielskim, francuskim i niemieckim jest dostępny na stronie internetowej:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/1998_en.htm .

Komisja Europejska na mocy art. 25 ust. 6 Dyrektywy 95/46/WE jest uprawniona 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. Komisja dotychczas wydała kilka decyzji o zróżnicowanym charakterze i zakresie zastosowania. Decyzje w sprawie przekazywania danych osobowych dotyczyły następujących państw:

Argentyna

Decyzja Komisji z dnia 30 czerwca 2003 r. w sprawie właściwej ochrony danych osobowych w Argentynie jest dostępna w wersji elektronicznej na :

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:31:32003D0490:PL:PDF>

Guernsey

Decyzja Komisji z dnia 21 listopada 2003 r. w sprawie właściwej ochrony danych osobowych w Guernsey jest dostępna w wersji elektronicznej na:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:16:01:32003D0821:PL:PDF>

Kanada

Decyzja Komisji z dnia 20 grudnia 2001 r. w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych jest dostępna w wersji elektronicznej na:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:27:32002D0002:PL:PDF>

Stany Zjednoczone Ameryki

Decyzja Komisji z dnia 26 lipca 2000 r. 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 USA jest dostępna w wersji elektronicznej na:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:16:01:32000D0520:PL:PDF>

Decyzja Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych jest dostępna w wersji elektronicznej na:

<http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:PL:HTML>

Szwajcaria

Decyzja Komisji z dnia 26 lipca 2000 r. w sprawie właściwej ochrony danych osobowych w Szwajcarii jest dostępna w wersji elektronicznej na:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:16:01:32000D0518:PL:PDF>

Wyspa Man

Decyzja Komisji z dnia 28 kwietnia 2004 r. w sprawie odpowiedniej ochrony danych osobowych na Wyspie Man jest dostępna w wersji elektronicznej na:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:34:32004D0411:PL:PDF>

Ocena, czy państwo docelowe zapewnia odpowiednie gwarancje ochrony należy do administratora danych, który musi we własnym zakresie ocenić, czy spełnione są przesłanki z art. 47 ust. 1. Generalny Inspektor nie wydaje w tym zakresie żadnych zaświadczeń. Należy zwrócić uwagę, iż w razie wątpliwości, co do odpowiedniego stopnia ochrony administrator danych zamierzający przekazywać dane do państwa trzeciego powinien legitymować się jedną z przesłanek określonych w art. 47 ust 2 i 3 lub art. 48 ustawy o ochronie danych osobowych.

Czy ustawa o ochronie danych zezwala na przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniej ochrony danych osobowych?

Tak, jednak przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniej ochrony danych osobowych jest możliwe pod warunkiem spełnienia jednej z przesłanek określonych w art. 47 ust. 2 i 3 ustawy.

W pierwszej kolejności należy wyjaśnić, że transfer danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniej ochrony danych osobowych jest dopuszczalne, gdy wynika on z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej (art. 47 ust. 2). Podkreślenia wymaga, iż powołana norma swym zakresem obejmuje jedynie przepisy prawa obowiązujące na terytorium Rzeczypospolitej Polskiej bądź ratyfikowane umowy międzynarodowe. Wykładnia gramatyczna art. 47 ust. 2 zaś wskazuje na konieczność istnienia wyraźnego obowiązku przekazywania danych osobowych.

Artykuł 47 ust. 3 ustawy, zawiera kolejne przesłanki upoważniające do przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiednich gwarancji ochrony. Mianowicie administrator danych może przekazać dane osobowe do państwa trzeciego, jeżeli:

1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie,

Omawiana przesłanka powinna być interpretowana w świetle definicji określonej w art. 7 pkt 5 ustawy. Zgodnie z nią przez zgodę osoby, której dane dotyczą rozumie się oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. W konsekwencji, osoba składająca takie oświadczenie woli powinna być świadoma braku odpowiedniego poziomu ochrony w państwie trzecim, do którego dane jej dotyczące mają być przekazane.

2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,

W ramach tej przesłanki można wyodrębnić dwie sytuacje, w których przekazanie danych jest dopuszczalne. Pierwsza ma zastosowanie w przypadku wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą. Druga zaś dotyczy sytuacji, gdy przekazanie danych jest podejmowane na życzenie osoby, której dane dotyczą. Jednocześnie należy uznać, że hipoteza powołanej normy obejmuje działania związane z wykonaniem umowy oraz działania przed zawarciem umowy - podejmowane na życzenie osoby, której dane dotyczą. Podkreślenia wymaga, że dane osobowe mogą być przekazane, jeżeli są niezbędne dla ww. celów. Nie wystarczy więc, aby dane były tylko użyteczne.

3) *przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,*

Ważne jest aby umowa pomiędzy administratorem danych a innym podmiotem była zawarta w interesie osoby, której dane dotyczą. Dla przykładu można wspomnieć o umowie reasekuracji.

4) *przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,*

Analizując możliwość przekazania danych osobowych do państwa trzeciego, gdy jest to niezbędne dla dobra publicznego, warto zauważyć, że zgodnie z pkt 58 preambuły do Dyrektywy 95/46/WE, przekazanie danych jest dopuszczalne, jeżeli wymagać tego będzie ochrona ważnego interesu publicznego, jak np. przesyłanie danych za granicę przez władze podatkowe i celne lub przez służby odpowiedzialne za sprawy ubezpieczeń społecznych. Należy więc ten przepis interpretować ściśle.

5) *przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,*

Żywotne interesy osoby, której dane dotyczą należy rozumieć jako interesy niezbędne dla życia tej osoby. Tym samym, co do zasady poza zakresem tego pojęcia znajdują się interesy ekonomiczne.

6) *dane są ogólnie dostępne.*

Należy zauważyć, że omawiana przesłanka nie znajdzie zastosowania w przypadku, gdy dane stały się ogólnie dostępne z naruszeniem prawa.

W jakich przypadkach Generalny Inspektor Ochrony Danych Osobowych może zezwolić na przekazanie danych do państwa trzeciego?

Jeżeli nie zostały spełnione wymagania określone w art. 47 ust. 2 lub 3 ustawy, a państwo docelowe nie zapewnia odpowiednich standardów ochrony, przekazanie 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).

Należy podkreślić, że rozpoczęcie przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiednich gwarancji ochrony danych osobowych jest możliwe dopiero po wydaniu pozytywnej decyzji przez Generalnego Inspektora. Decyzja ta nie legalizuje bowiem wcześniejszego przekazywania danych osobowych.

Generalny Inspektor, rozpatrując wniosek o wyrażenie zgody na przekazywanie danych, musi ocenić, czy administrator danych zapewnia odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą. Ocenę taką dokonuje się z uwzględnieniem tych samych przesłanek, które wykorzystuje się przy generalnej ocenie poziomu ochrony danych osobowych zapewnianej w państwie trzecim. Niemniej jednak, każdy wniosek należy oceniać indywidualnie, z uwzględnieniem wszystkich okoliczności sprawy.

Administrator danych może zapewnić odpowiedni poziom ochrony danych osobowych, które podlegają przekazaniu, przede wszystkim poprzez przyjęcie odpowiednich zobowiązań umownych, takich jak:

- wzorcowe klauzule umowne przyjęte przez Komisję Europejską,
- wzorcowe klauzule umowne z modyfikacjami wprowadzonymi przez administratora danych,
- klauzule umowne, które zostały w całości samodzielnie przygotowane przez administratora danych,
- wiążące reguły korporacyjne.

Czy administrator danych może zastosować wzorcowe klauzule umowne przyjęte przez Komisję Europejską?

Tak. Komisja Europejska na mocy art. 26 ust. 4 Dyrektywy jest uprawniona do uznania w drodze decyzji, że określone wzorcowe klauzule umowne zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek. Decyzje te wymagają, aby państwa członkowskie nie odmawiały uznania zabezpieczeń ustanowionych we wzorcowych 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. Komisja Europejska wydała trzy decyzje w tym zakresie.

Decyzja 2001/497/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych do państw trzecich na podstawie 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 181/19, z 4.07.2001) została wydana przez Komisję Europejską w dniu 15 czerwca 2001 r. Wprowadzone niniejszą decyzją klauzule umowne mają zastosowanie do przekazywania danych osobowych do administratora danych w państwie trzecim. Tekst decyzji w języku polskim jest dostępny na stronie internetowej:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:26:32001D0497:PL:PDF>

Decyzja 2004/915/WE zmieniająca decyzję 2001/497/WE w zakresie alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz. Urz. WE L 385/19, z 29.12.2004) została wydana przez Komisję Europejską w dniu 27 grudnia 2004 r. Powołana decyzja wprowadziła zestaw alternatywnych klauzul umownych, które administrator danych może wykorzystać w przypadku przekazywania danych do innego administratora danych w państwie trzecim. Administrator danych może więc wybrać jeden spośród dwóch zestawów wzorcowych klauzul umownych. Tekst decyzji w języku polskim jest dostępny na stronie internetowej:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:PL:PDF>

Decyzja 2002/16/WE w sprawie wzorcowych klauzul umownych w związku z przekazywaniem danych osobowych przetwarzającym w krajach trzecich na podstawie 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 006, z 10.01.2002) została wydana przez Komisję Europejską w dniu 27 grudnia 2001 r. Wprowadzone niniejszą decyzją wzorcowe klauzule umowne mają zastosowanie do przekazywania danych osobowych w przypadku powierzenia przetwarzania danych osobowych w rozumieniu art. 31 ustawy o ochronie danych osobowych.

Tekst decyzji w języku polskim jest dostępny na stronie internetowej:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:27:32002D0016:PL:PDF>

Zadeklarowanie przez wnioskodawcę zastosowania wzorcowych klauzul umownych określonych powołanymi decyzjami Komisji Europejskiej, w pierwszej kolejności powoduje

konieczność porównania przez Generalnego Inspektora przyjętych przez wnioskodawcę rozwiązań z treścią wzorcowych klauzul umownych. Ponadto, Generalny Inspektor bada również okoliczności planowanego transferu danych.

W jakiej formie mogą być wprowadzone wzorcowe klauzule umowne?

Należy podkreślić, że wzorcowe klauzule umowne mogą być zawarte w szerszej umowie zawartej między administratorem danych osobowych a odbiorcą danych w państwie trzecim. Mogą być też dodane do niej w formie aneksu. Możliwe jest również sporządzenie zupełnie odrębnego dokumentu.

Czy administrator danych może zastosować wiążące reguły korporacyjne?

Tak. Zastosowanie wzorcowych klauzul umownych określonych decyzjami Komisji Europejskiej nie jest jedynym rozwiązaniem pozwalającym na wydanie przez Generalnego Inspektora decyzji zezwalającej na przekazanie danych do państwa trzeciego. Możliwe jest zastosowanie zmodyfikowanych wzorcowych klauzul umownych, jak również klauzul, które w pełni zostały ukształtowane przez wnioskodawcę.

Odrębnym instrumentem są wiążące reguły korporacyjne, które szczególną rolę mogą odegrać w przypadku przekazywania danych osobowych w ramach międzynarodowych korporacji. Jest to stosunkowo nowy instrument, który z jednej strony może zapewnić większą elastyczność, z drugiej zaś zagwarantować w ramach korporacji jednolity, a zarazem wysoki poziom ochrony praw osób, których dane dotyczą, bez względu na poziom ochrony danych osobowych zapewniony na terytorium poszczególnych państw.

Grupa Robocza Art. 29 w dniu 3 czerwca 2003 r. wydała dokument roboczy WP 74 pt.: „Przekazywanie danych osobowych do krajów trzecich: zastosowanie Art. 26 ust. 2 dyrektywy UE w sprawie ochrony danych w odniesieniu do wiążących reguł korporacyjnych zobowiązujących przedsiębiorstwa do ich stosowania przy międzynarodowym przepływie danych”.

Tekst dokumentu roboczego (w językach: angielskim, francuskim i niemieckim) jest dostępny na stronie internetowej:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

Grupa Robocza Art. 29, dokonując analizy pojęcia wiążących reguł korporacyjnych, wskazała że są one:

- a) „wiązące” lub „możliwe do wyegzekwowania na drodze prawnej”, ponieważ tylko klauzule mające ten charakter mogą być uznane za „wystarczające gwarancje” w rozumieniu art. 26 ust. 2 Dyrektywy 95/46/WE;
- b) korporacyjne, ponieważ chodzi o reguły obowiązujące wewnątrz korporacji (koncernu) międzynarodowej, na ogół opracowane w siedzibie głównej;
- c) stosowane przy międzynarodowych transferach danych, ponieważ w tym tkwi sens istnienia tych reguł.

Grupa Robocza Art. 29 w dniu 14 kwietnia 2005, w dokumencie roboczym WP 108, przyjęła listę kontrolną ze wszystkimi niezbędnymi elementami, które powinny zawierać wiążące reguły korporacyjne.

Biorąc pod uwagę, że wiążące reguły korporacyjne w zamierzeniu mają mieć charakter powszechny, europejskie organy ochrony danych osobowych przyjęły procedurę współpracy, której celem jest wspólne rozpatrywanie wniosków o wyrażenie zgody na przekazywanie danych osobowych, na podstawie wiążących reguł korporacyjnych (dokument roboczy WP 107 przyjęty w dniu 14 kwietnia 2005 r.).

Oba dokumenty robocze (w języku angielskim, francuskim i niemieckim) dostępne są w wersji elektronicznej na stronie internetowej:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

Jakie informacje powinien zawierać wniosek o wydanie zgody na przekazanie danych do państwa trzeciego?

Jeżeli w ocenie wnioskodawcy zachodzi konieczność wyrażenia przez Generalnego Inspektora zgody na przekazywanie danych osobowych do państwa trzeciego, to powinien on przedstawić dowody pozwalające na potwierdzenie zapewnienia przez wnioskodawcę odpowiedniego zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osób, których dane dotyczą. Dlatego Generalny Inspektor wymaga wskazania:

- 1) stron takiego transferu danych osobowych,
- 2) kategorii danych,
- 3) ich zakresu,

- 4) celu oraz czasu trwania proponowanych operacji przekazywania danych,
- 5) środków podjętych w celu zagwarantowania przez strony zamierzające przekazywać dane osobowe, praw osób, których dane dotyczą, w tym np. przedstawić treść konkretnej umowy (np. zawierającej wzorcowe klauzule umowne) stanowiącej podstawę przekazania danych,
- 6) środków organizacyjno – technicznych, które odbiorca danych zapewni w celu zabezpieczenia przekazywanych danych (dokładny opis).

Generalny Inspektor w toku postępowania może zwrócić się do wnioskodawcy o udzielenie dodatkowych wyjaśnień lub przesłanie dokumentów.

Wniosek winien spełniać wymogi określone w art. 63 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071 z późn. zm.). Ponadto w myśl art. 1 pkt 1 ustawy z dnia 9 września 2000 r. o opłacie skarbowej (Dz. U. z 2004 r. Nr 253, poz. 2532 z późn. zm.), podanie (żądanie, wnioski, odwołania, zażalenia) i załączniki do podań podlegają opłacie skarbowej. Obowiązek zapłaty opłaty skarbowej powstaje z chwilą wniesienia podania lub załącznika (art. 6 pkt 1 ustawy o opłacie skarbowej). Od podania skierowanego do Generalnego Inspektora pobiera się opłatę skarbową w wysokości: 5,00 zł, a od każdego załącznika do podania opłatę w wysokości: 50 gr. Na podstawie art. 261 § 1 k.p.a., wnioskodawca powinien wnieść stosowną opłatę skarbową, w postaci znaków opłaty skarbowej, stanowiącą należność związaną z rozpoznaniem i załatwieniem sprawy.