

GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH

*dr Wojciech R. Wiewiórowski*

Warszawa, dnia 22 lutego 2013 r.

**DESiWM/DEC-215/13**

Dotyczy sprawy: [...]

**DECYZJA**

Na podstawie art. 105 § 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 **F. Sp. z o.o.**, danych osobowych na podstawie przyjętych rozwiązań umownych do następujących spółek:

- 1) S. Pty Ltd, z siedzibą w Australii;
  - 2) P. Ltd, z siedzibą w Australii;
  - 3) Su. Limitada, z siedzibą w Brazylii;
  - 4) Sh. Co. Ltd., z siedzibą w Chińskiej Republice Ludowej;
  - 5) B. Co. Ltd., z siedzibą w Chińskiej Republice Ludowej;
  - 6) S1. Limited, z siedzibą w Specjalnym Regionie Administracyjnym Hongkongu;
  - 7) S2. Limited, z siedzibą w Republice Indyjskiej;
  - 8) S3. z siedzibą w Japonii;
  - 9) S4. Ltd, z siedzibą w Korei;
  - 10) S5. z siedzibą w Meksyku;
  - 11) S6. Inc., z siedzibą na Filipinach;
  - 12) S7. Pte. Ltd, z siedzibą w Singapurze;
- zwanych dalej Odbiorcami,

**umarzam postępowanie w przedmiotowej sprawie.**

### **Uzasadnienie**

Do Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej „Generalnym Inspektorem”, wpłynął wniosek złożony przez F., zwaną dalej Wnioskodawcą lub Spółką, o udzielenie zgody na przekazanie danych osobowych do wyżej wymienionych Odbiorców w państwach trzecich.

Po zapoznaniu się z przedstawionymi przez Wnioskodawcę dokumentami oraz przeprowadzeniu postępowania wyjaśniającego Generalny Inspektor ustalił, co następuje:

- 1) Wnioskodawca jest administratorem danych z siedzibą na terytorium Rzeczypospolitej Polskiej;
- 2) Wnioskodawca powierzył F. Inc., z siedzibą w Stanach Zjednoczonych Ameryki, przetwarzanie danych w rozumieniu art. 31 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;
- 3) F. Inc. jest uczestnikiem programu „bezpiecznej przystani” w zakresie obejmującym cele i kategorie danych, które mają podlegać przekazaniu przez Wnioskodawcę;
- 4) pomiędzy Wnioskodawcą a F. Inc. została zawarta umowa, zwana dalej standardowymi klauzulami umownymi, której treść jest zgodna z klauzulami umownymi stanowiącymi załącznik do decyzji Komisji Europejskiej 2010/87/EU 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 95/46/WE Parlamentu Europejskiego i Rady (Dz. Urz UE L 39 z 12.02.2010 r.), zwanej dalej decyzją Komisji 2010/87/UE;

- 5) Wnioskodawca udzielił F. Inc. generalnej (blankietowej) zgody na dalsze podpowierzenie przetwarzania danych zgodnie z warunkami określonymi w standardowych klauzulach umownych (w związku z podwykonawstwem);
- 6) zgodnie z treścią klauzuli 11 ust. 4 standardowych klauzul umownych prowadzony będzie wykaz umów podwykonawstwa, jak również zgodnie z oświadczeniem Spółki złożonym w toku odrębnego postępowania (sygn. akt [...]) z podwykonawcami z Grupy kapitałowej F. oraz z podwykonawcami zewnętrznymi, zawierane są umowy o przetwarzanie danych osobowych w ramach podwykonawstwa, które mają na celu zapewnienie zgodności działań Odbiorców z obowiązkami nałożonymi na F. Inc. jako przetwarzającego dane osobowe na zlecenie;
- 7) F. Inc. jest spółką matką grupy kapitałowej F. i świadczy usługi na rzecz podmiotów z grupy, w tym utrzymuje i zarządza F. C. - centrum przetwarzania danych F.;
- 8) F. Inc. zamierza podpowierzyć przetwarzanie danych osobowych S. Inc. z siedzibą w Stanach Zjednoczonych Ameryki (w aktach sprawy uwierzytelnione tłumaczenie zawartej w tej sprawie umowy);
- 9) S. Inc. jest uczestnikiem programu „bezpiecznej przystani”;
- 10) ww. Odbiorcy pełnić będą rolę podwykonawców S. Inc., tj. będą oni przetwarzać dane przekazane przez Wnioskodawcę na zasadzie pod-podzlecenia;
- 11) S. Inc. zobowiązał się do zawarcia z Odbiorcami umowy odpowiadającej zmodyfikowanej treści standardowych klauzul umownych stanowiących załącznik do decyzji Komisji 2010/87/UE;
- 12) zgodnie z oświadczeniem Spółki Odbiorcy będą mieli dostęp do danych przetwarzanych w F. C. wyłącznie na potrzeby wykonania powierzonych im zadań;
- 13) zadania wykonywane przez Odbiorców mają dotyczyć stosowania i obsługi oprogramowania, obsługi informatycznej oraz zarządzania bazami danych, wsparcia w zakresie technicznym, w tym wsparcia dla użytkowników końcowych;
- 14) przekazaniu będą podlegać dane dotyczące pracowników i współpracowników Wnioskodawcy.

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

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 K.p.a., organy administracji publicznej działają na podstawie przepisów prawa. Stosownie do art. 104 ust. 1 K.p.a., organ administracji publicznej załatwia sprawę przez wydanie decyzji, chyba że przepisy kodeksu stanowią inaczej. 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 związku z powyższym 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. Przy czym odpowiedni poziom ochrony danych osobowych jest oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, w szczególności biorąc pod uwagę charakter pochodzenia i kraj ostatecznego przeznaczenia danych oraz przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe (ust. 1a). Podkreślić należy, że powołany przepis ustawy odzwierciedla treść art. 25 ust. 1 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 95/46/WE, zgodnie z którym państwa członkowskie zapewnią, że przekazywanie do kraju 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 - dany kraj trzeci zapewni odpowiedni stopień ochrony.

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 danych okolicznościach faktycznych i prawnych 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).

Kluczowe w przedmiotowej sprawie jest to, że Wnioskodawca pierwotnie przekazuje dane w ramach powierzenia do F. Inc., który uczestniczy w programie „bezpiecznej przystani”. Przedmiotowe dane będą następnie podpowierzone do S. Inc., który również przystąpił do programu „bezpiecznej przystani”. Zauważyć więc należy, iż na mocy art. 25 ust. 6 dyrektywy 95/46/WE, 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 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.

Jednocześnie należy zauważyć, że zgodnie z Zasadami ochrony prywatności w ramach „bezpiecznej przystani” wydanymi przez Departament Handlu USA dnia 21 lipca 2000 r., stanowiącymi Załącznik I do decyzji Komisji 2000/520/WE, uregulowane zostały kwestie dalszego przekazywania danych. I tak, w celu ujawnienia informacji stronie trzeciej, organizacje muszą stosować zasady ogłoszenia i wyboru. W przypadku gdy organizacja chce przesłać informację stronie trzeciej, będącej przedstawicielem, jak opisano w przypisie końcowym, może to zrobić pod warunkiem uprzedniego upewnienia się, iż strona trzecia przystąpiła do Zasad albo podlega dyrektywie 95/46/WE albo ustaleniom dotyczącym adekwatności lub zawrze z taką stroną trzecią pisemną umowę wymagającą, aby strona trzecia zapewniła, co najmniej taki sam poziom ochrony prywatności, jaki jest wymagany przez odnośne Zasady. Jeżeli organizacja będzie przestrzegać tych wymagań, to nie będzie ona ponosić odpowiedzialności (o ile organizacja nie postanowi inaczej) za to, że strona trzecia, do której przekazuje informacje, przetwarza je w sposób niezgodny z ograniczeniami albo oświadczeniami, chyba że organizacja ta wiedziała albo powinna była wiedzieć, że strona trzecia może przetwarzać dane w taki nieodpowiedni sposób i organizacja nie podjęła właściwych kroków, żeby zapobiec takiemu przetwarzaniu danych lub je powstrzymać.

Wydaje się więc, że dalsze przekazanie danych np. w ramach ich podpowierzenia powinno być oceniane w świetle zasad „bezpiecznej przystani”, które wprowadzają warunki, na których takie operacje mogą mieć miejsce, w szczególności gdy podmiot, któremu dane są przekazywane nie należy do programu „bezpiecznej przystani”. Jednocześnie należy zauważyć, że Zasady ochrony prywatności w ramach „bezpiecznej przystani” nie rozróżniają czy osoba trzecia znajduje się na terytorium Stanów Zjednoczonych Ameryki, czy też poza jej terytorium, wymagają m.in. zawarcia z taką osobą pisemnej umowy mającej na celu zapewnienie, co najmniej takiego samego poziomu ochrony danych osobowych, jaki jest wymagany przez Zasady. Powyższe należy również odnieść do sytuacji, w której dochodzi do podpowierzenia przetwarzania danych przez przetwarzającego uczestniczącego w programie „bezpiecznej przystani”.

Przyjęcie takiego stanowiska oznacza, że dalsze przekazywanie danych osobowych przez podmiot uczestniczący w programie „bezpiecznej przystani” do odbiorców pozostających poza tym programem odbywałoby się na podstawie przepisów art. 47 ust. 1 ustawy. Tym samym takie transfery nie wymagają wyrażenia przez Generalnego Inspektora zgody na podstawie art. 48 ustawy. W konsekwencji Generalny Inspektor w świetle okoliczności przedmiotowej sprawy odstępuje od wcześniejszej praktyki orzeczniczej w tym zakresie, przyjmując, że mechanizmy wymagane przez program „bezpiecznej przystani” zapewniają odpowiedni poziom ochrony danych osobowych.

Jednocześnie wyraźnego podkreślenia wymaga, 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.

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. Tym samym sam fakt przystąpienia przetwarzającego do programu „bezpiecznej przystani” nie jest wystarczający. Z

jednej strony administrator danych musi mieć pewność, że taki odbiorca danych w pełni wdrożył zasady zagwarantowane przez program „bezpiecznej przystani”, z drugiej zaś musi mieć realną możliwość kontroli nad operacjami przetwarzania danych osobowych i wypełnienia ciążących na nim innych niż określone w rozdziale 7 przepisów ustawy. Dotyczy to w szczególności konieczności zawarcia umowy powierzenia, która w takich okolicznościach może przyjąć formę standardowych klauzul umownych, a nawet taka forma ze względów bezpieczeństwa i zakresu odpowiedzialności byłaby rekomendowana. Podobnie należałoby potraktować operacje podpowierzenia przetwarzania danych osobowych.

W tym kontekście należy zauważyć, że zgodnie z odpowiedzią na pytanie 10 Najczęściej Zadawanych Pytań, stanowiących Załącznik II do decyzji Komisji 2000/520/WE, od administratorów danych w Unii Europejskiej zawsze wymaga się zawarcia umowy, gdy dokonuje się przekazywania informacji jedynie w celu jej przetworzenia (powierzenia) niezależnie od tego, czy przetwarzanie odbywa się na terytorium UE czy poza nim. Celem umowy jest ochrona interesów administratora danych, tj. osoby albo organu, który decyduje o celach i sposobach przetwarzania oraz ponosi pełną odpowiedzialność za te dane wobec zainteresowanej osoby bądź osób fizycznych. Tak, więc umowa określa rodzaj przetwarzania, które ma być wykonane oraz wszelkie środki niezbędne do zapewnienia, że dane przechowywane są w bezpieczny sposób.

Na marginesie powyższych rozważań szczególnego podkreślenia wymaga konieczność zapewnienia dodatkowych gwarancji w odniesieniu do przekazania danych w związku ze świadczeniem usług w chmurze również wtedy, gdy dostawca tych usług jest uczestnikiem programu „bezpiecznej przystani”. W związku z tym Generalny Inspektor podziela stanowisko wyrażone przez Grupę roboczą ds. ochrony danych osobowych ustanowioną na mocy art. 29 dyrektywy 95/46/WE w opinii 05/2012 na temat przetwarzania danych w chmurze obliczeniowej przyjętej dnia 1 lipca 2012 (WP 196), zgodnie z którym ze względu na szczególne dla chmury obliczeniowej zagrożenia „zasady programu „bezpiecznej przystani” same w sobie również nie mogą zagwarantować eksporterowi danych niezbędnych środków, by zapewnić, że dostawca usług w chmurze w Stanach Zjednoczonych zastosował właściwe środki bezpieczeństwa, co może być wymagane przez ustawodawstwa krajowe oparte na dyrektywie 95/46/WE”.

Reasumując, pomimo braku w świetle okoliczności przedmiotowej sprawy konieczności uzyskania zgody Generalnego Inspektora, Wnioskodawca w dalszym ciągu jest obowiązany zapewnić zgodność zleczanych przez siebie operacji przetwarzania danych osobowych z przepisami ustawy.

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

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).