GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH
dr Wojciech R. Wiewiórowski

MAC
BAA 0101143

DESIWM-072-37/13/67119

Warszawa, dnia 11 października 2013 r.

MINISTERSTWO ADMINISTRACJI I CYFRYZACJI
KANCELARIA GŁÓWNA
Wpłynęło dn. 16.10.2013
Nr 49336 zał./kart. ...../.....
DSI

Pan
Michał Boni
Minister Administracji
i Cyfryzacji

Szanowny Panie Ministrze

odpowiadając na pismo z dnia 2 sierpnia 2013 r., znak: DSI-WSE-0748-2/2013, w sprawie oceny wdrożenia decyzji Komisji Europejskiej nr 2000/520/WE z dnia 26 lipca 2000 r. (Decyzja 2000/520/WE) przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady 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 (Dz. Urz. WE L 215/7 z 25.8.2000 r.), uprzejmie przedstawiam stanowisko Generalnego Inspektora Ochrony Danych Osobowych oparte na dogmatycznych rozważaniach co do charakteru Decyzji 2000/520/WE, zasad jej stosowania w polskim porządku prawnym oraz praktyki działań Generalnego Inspektora w zakresie decyzji o wyrażenie zgody na transfer danych osobowych do państw trzecich. Jednocześnie w ostatniej części niniejszego

ul. Stawki 2
00-193 Warszawa

MINISTERSTWO ADMINISTRACJI I CYFRYZACJI
DEPARTAMENT SPOŁECZEŃSTWA INFORMACYJNEGO
KANCELARIA
Idz. ..... przyjął 2013 10. 16
DSI-S-415-2013r.

tel. 860-73-12
fax 860-73-13
www.giodo.gov.pl

stanowiska przedstawiono wątpliwości dotyczące praktyki stosowania Decyzji 2000/520/WE, które pojawiły się w 2013 r. po ujawnieniu sposobu funkcjonowania systemu PRISM w Stanach Zjednoczonych.

1. Pierwszym tematem, który wymaga rozważenia jest charakter prawny Decyzji 2000/520/WE i jej konsekwencje dla oceny operacji przekazania danych do odbiorców objętych jej zakresem w świetle polskich przepisów o ochronie danych osobowych. Zgodnie z art. 47 ust. 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, 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).

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 stanie faktycznym 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).

Mając na względzie to, że Komisja Europejska wydała Decyzję 2000/520/WE na podstawie 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 95/46/WE, zgodnie z którym jest ona 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, podkreślenia wymaga, iż na jej mocy ewentualne przekazanie danych do odbiorcy z siedzibą w Stanach Zjednoczonych, który

przystąpił do programu „bezpiecznej przystani" należy oceniać jako transfer do państwa bezpiecznego w trybie art. 47 ust. 1 ustawy.

Decyzja 2000/520/WE w swym art. 1 wyraźnie wskazuje, że dla celów art. 25 ust. 2 dyrektywy 95/46/WE, 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 państwa członkowskie zostały zobowiązane do podjęcia wszelkich środków niezbędnych do jej wdrożenia w swoich porządkach prawnych (art. 5). Tym samym od dnia 1 maja 2004 r. polski organ ochrony danych osobowych co do zasady nie może odmówić uznania odpowiedniego poziomu ochrony danych osobowych w odniesieniu do transferów danych objętych zakresem decyzji Komisji Europejskiej nr 2000/520/WE, jak również nie może wymagać dodatkowych autoryzacji (w trybie określonym w art. 48 ustawy).

W tym kontekście należy dodać, że zgodnie z art. 3 decyzji Komisji Europejskiej nr 2000/520/WE wstrzymanie przekazywania danych do odbiorcy należącego do programu „bezpiecznej przystani" jest dopuszczalne jedynie następujących sytuacjach, tj. gdy:

a) organ rządowy w Stanach Zjednoczonych, określony w załączniku VII do decyzji nr 2000/520/WE lub mechanizm niezależnej ochrony prawnej w rozumieniu lit. a) Zasady Realizacji Prawa określonej w załączniku I do tej decyzji ustali, że organizacja narusza zasady wdrożone zgodnie z Najczęściej Zadawanymi Pytaniami; lub

b) istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że mechanizm realizacji prawa, o którym mowa nie podejmuje lub nie podejmie właściwych kroków w odpowiednim czasie w celu załatwienia spornej sprawy; dalszy przekaz tworzyłby bezpośrednie ryzyko wystąpienia poważnej szkody dla osób, których dane dotyczą; a właściwe władze Państwa Członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi.

W konsekwencji wydaje się, że ewentualne działania władcze organów ochrony danych osobowych z państw członkowskich UE w wyżej wymienionych sytuacjach mogą mieć jedynie charakter wyjątkowy i dotyczyć jednostkowych spraw. Krajowe organy ochrony danych osobowych nie mogą również żądać od administratorów danych przedstawienia dowodów na rzeczywistą realizację przez odbiorców należących do programu „bezpiecznej przystani" wprowadzonych przez ten program zasad ochrony prywatności, chyba że w konkretnych okolicznościach sprawy zostałyby spełnione ww. przesłanki.

W związku z powyższym chciałbym potwierdzić, że w stanie prawnym obowiązującym od dnia 1 maja 2004 r. transfery danych objęte zakresem decyzji Komisji Europejskiej nr 2000/520/WE odbywają się na podstawie art. 47 ust. 1 ustawy, a co za tym idzie nie wymagają uprzedniego wyrażenia zgody przez polski organ ochrony danych w trybie art. 48 ustawy. Niemniej należy odnotować sytuacje, w których pomimo przystąpienia odbiorcy danych do programu „bezpiecznej przystani" może być w szczególności wymagane uzyskanie zgody Generalnego Inspektora jeżeli kategorie przekazywanych danych oraz cele ich przetwarzania wykraczałby poza zakres określony certyfikatem przystąpienia do programu.

Należy też zwrócić uwagę, że w ostatnich miesiącach rzecznicy ochrony danych osobowych w Europie ponownie zaczęli rozważać, czy zasady wynikające z Decyzji 2000/520/WE są wciąż aktualne dla procesów przekazywania danych do podmiotów podlegających prawodawstwu Stanów Zjednoczonych.

2. Należy zwrócić uwagę na ewolucję w podejściu Generalnego Inspektora do kwestii dalszych transferów odbywających się w ramach powierzenia danych do podmiotu uczestniczącego w programie „bezpiecznej przystani" i dalszego ich podpowierzenia przez ten podmiot podmiotowi poza programem. Pierwotnie w takich okolicznościach GIODO wymagał zawarcia odpowiednich klauzul lub objęcia transferu wiążącymi regułami korporacyjnymi, a w konsekwencji uzyskania jego zgody na przekazanie danych. Jednak po analizie Zasad ochrony prywatności GIODO odstąpił od tej praktyki. W konsekwencji, obecnie jeżeli dalsze powierzenie danych przez podmiot uczestniczący w programie „bezpiecznej przystani" odbywa się zgodnie z Zasadami ochrony prywatności w ramach „bezpiecznej przystani", a w szczególności poprzez zawarcie pisemnej umowy, to odbywa się ono na podstawie przepisów art. 47 ust. 1 ustawy. Tym samym, takie transfery nie wymagają wyrażenia przez Generalnego Inspektora zgody na podstawie art. 48 ustawy.

3. Odnosząc się do prośby o przekazanie dostępnych informacji statystycznych chciałbym wyjaśnić, że przepisy ustawy nie wymagają zgłaszania Generalnemu Inspektorowi informacji o planowanych transferach do importerów należących do programu „bezpiecznej przystani". Należy bowiem pamiętać, że art. 40 ustawy nakłada na administratorów danych obowiązek zgłoszenia do rejestracji Generalnemu Inspektorowi prowadzonych przez siebie zbiorów danych, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. Zgodnie zaś z art. 41 ust. 1 pkt 7 ustawy, w zgłoszeniu do rejestracji należy również przekazać informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego, a w pkt 14 formularza zgłoszenia zbioru danych,

którego wzór stanowi załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536), jeżeli planowane jest przekazanie danych osobowych do państwa trzeciego, to należy jedynie podać nazwę tego państwa. Nie jest natomiast wymagane wskazanie jednej z przesłanek określonych w art. 47 lub 48 ustawy, uprawniających do takich operacji. Tym samym nie jest możliwe uzyskanie wiarygodnych informacji o liczbie transferów do odbiorców w programie „bezpiecznej przystani". Pamiętając o powyższych zastrzeżeniach podkreślenia wymaga, że nawet w odniesieniu do zbiorów, które zostały zgłoszone do rejestracji od dnia 1 maja 2004 r. odnotowano stosunkowo niewielką liczbę zgłoszeń, w których wskazano na możliwość przekazania danych osobowych do Stanów Zjednoczonych Ameryki. Analiza rejestru zbiorów danych osobowych pokazuje, że liczba takich zgłoszeń wynosi około 500. Przy czym obecnie rocznie jest zgłaszanych do rejestracji od kilkunastu do ponad dwudziestu tysięcy zbiorów.

4. Przechodząc do analizy programu „bezpiecznej przystani" wyraźnie należy zaznaczyć, że nie wszystkie zastrzeżenia i wątpliwości, które Grupa Art. 29 ds. ochrony danych osobowych zgłaszała Komisji Europejskiej zostały przez nią uwzględnione w Decyzji 2000/520/WE. Tym niemniej przyjmując do wiadomości fakt, że sam program „bezpiecznej przystani", jak i decyzja Komisji Europejskiej były wynikiem możliwego do osiągnięcia kompromisu, późniejsze podejście organów ochrony danych osobowych koncentrowało się na kwestiach związanych z wdrożeniem Zasad ochrony prywatności i zapewnieniem efektywnego funkcjonowania samego programu. Należy przypomnieć, że działanie programu „bezpiecznej przystani" wzbudzało liczne zastrzeżenia już od samego początku jego funkcjonowania. Wiele wątpliwości odnotowywano również w trakcie wcześniej przeprowadzanych przez Komisję ocen wdrożenia decyzji nr 2000/520/WE, a w szczególności w analizach przygotowanych na zalecenie Komisji przez ekspertów zewnętrznych. Dla porządku odnotować można m.in. problemy związane z procesem certyfikacji, zakresem zastosowania programu, nieaktualnością listy podmiotów należących do programu, brakiem umieszczenia na stronach internetowych uczestników programu polityk prywatności. Zastrzeżenia wzbudzało także funkcjonowanie mechanizmów rozpatrywania skarg, czy niewielkie zainteresowaniem kwestią wdrażania programu „bezpiecznej przystani" wśród władz amerykańskich. Przez długi okres było również niewielkie zainteresowanie programem ze strony przedsiębiorców amerykańskich. Z perspektywy czasu można jednak odnotować zwiększenie się liczby uczestników programu, jak również zwiększenie się aktywności organów amerykańskich w związku z wdrażaniem programu. W szczególności należy odnotować pewną intensyfikację działań

przez Federalną Komisję Handlu i Departament Handlu. Niewątpliwie jest to wynikiem prowadzonego już od jakiegoś czasu dialogu UE z USA. Na marginesie należy dodać, że Federalna Komisja Handlu coraz aktywniej uczestniczy w różnych formach współpracy pomiędzy organami ochrony danych osobowych i prywatności. Jakkolwiek liczba spraw, które były przez nią rozpatrywane była niewielka, co jest m.in. związane z przyjętymi przez nią priorytetami w zakresie działań władczych.

5. Generalny Inspektor był informowany przez władze amerykańskie o wprowadzanych usprawnieniach w realizacji programu dotyczących m.in. wymogów dotyczących odpowiedniej treści polityk prywatności w sposób zapewniający ich przejrzystość, czy zapewnienia łatwo dostępnych, dla osób, których dane dotyczą, mechanizmów dochodzenia roszczeń i rozpatrywania skarg. Należy zauważyć, że w odniesieniu do istotnego zakresu przekazywanych do uczestników programu danych (przede wszystkim dotyczy to danych związanych z zatrudnieniem), mechanizm wdrażania prawa opiera się na współpracy z organami ochrony danych z UE i wiąże się z koniecznością zobowiązania się przez uczestników programu do takiej współpracy. Jednakże w świetle posiadanych przez Generalnego Inspektora informacji wydaje się, że ten mechanizm, a w szczególności tzw. panel organów ochrony danych osobowych w praktyce nie działa. W tym zakresie należałoby zatem zwiększyć świadomość wśród uczestników programu, jak i osób, których dane dotyczą, ale także usprawnić i ułatwić do niego dostęp wszystkim zainteresowanym.

6. Kolejna kwestia wiąże się ze zmianami technologicznymi oraz nowymi modelami świadczenia usług, co również przekłada się na potencjalne problemy ze stosowaniem programu „bezpiecznej przystani". Takie wątpliwości w szczególności rodzą się w odniesieniu do obowiązków i zakresu odpowiedzialności w ramach programu „bezpiecznej przystani" podmiotów, które przetwarzają dane w ramach powierzenia. Otóż 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 przetwarzania (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. Jednocześnie organizacja amerykańska uczestnicząca w programie „bezpiecznej przystani", która

otrzymuje dane osobowe z UE jedynie w celu przetwarzania nie musi stosować zasad do tych informacji, ponieważ administrator danych z UE jest za nie bezpośrednio odpowiedzialny wobec zainteresowanej osoby. Tym samym w istocie zapewnienie odpowiednich gwarancji jest uzależnione od treści odpowiedniej umowy zawartej przez administratora danych z UE. Problem ten nabiera szczególnego znaczenia w kontekście przekazania danych w związku ze świadczeniem usług w chmurze również. W związku z tym warto zwrócić uwagę na stanowisko wyrażone przez Grupę roboczą art. 29 ds. ochrony danych osobowych w opinii 05/2012 na temat przetwarzania danych w chmurze obliczeniowej przyjętej 1.7.2012 (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 USA zastosował właściwe środki bezpieczeństwa, co może być wymagane przez ustawodawstwa krajowe oparte na dyrektywie 95/46".

7. Obecnie należałoby również przeanalizować wpływ ustawodawstwa, które w amerykańskim porządku prawnym pojawiło się po wydaniu przez Komisję decyzji nr 2000/520/WE, na kształtowanie się obowiązków uczestników programu „bezpiecznej przystani". Zgodnie z Zasadami ich przyjęcie może być ograniczone: a) w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa; b) ustawą, rozporządzeniem rządu albo prawem precedensowym, ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie; lub c) jeżeli efektem dyrektywy w prawie Państwa Członkowskiego jest dopuszczenie wyjątków lub odstępstw, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych kontekstach. Zgodnie z celem zwiększenia ochrony prywatności, organizacje powinny dążyć do pełnego wdrożenia niniejszych zasad w sposób całkowity i przejrzysty, wskazując ponadto w swoich politykach ochrony prywatności przypadki, w których wyjątki od zasad dozwolone lit. b) powyżej będą stosowane na bieżąco. Z tego samego powodu w przypadku gdy zasady i/lub prawo amerykańskie dopuszcza taką możliwość, oczekuje się, że w miarę możliwości organizacje będą decydować się na wyższy poziom ochrony. Odniesienie do odrębnego ustawodawstwa szczególnie nabrało znaczenia w świetle wydarzeń ostatnich miesięcy dotyczących działań organów bezpieczeństwa wewnętrznego USA. Pamiętając, że kwestia ta, będąc kluczową w relacjach z USA, jest analizowana odrębnie, jednak często jest ona łączona z działaniem programu „bezpiecznej przystani". Podkreślenia jednak wyraźnie wymaga, że program „bezpiecznej

przystani" zarówno w zakresie podmiotowym, jak i przedmiotowym obejmuje swym zakresem podmioty prowadzące działalność gospodarczą w związku z przetwarzaniem przez nie danych osobowych w celach związanych z tą działalnością. Wskazuje również na to konstrukcja programu „bezpiecznej przystani" oraz Decyzji 2000/520/WE. Jak wskazano powyżej jakakolwiek możliwość wstrzymania przekazywania danych osobowych do uczestnika programu „bezpiecznej przystani" wiąże się z jego działaniami. Natomiast de facto nie wprowadzono mechanizmów, które umożliwiałyby reakcję organów z państw członkowskich UE w związku z działaniami władz amerykańskich, które nie byłyby do pogodzenia ze standardami ochrony danych osobowych w UE.

8. Tym niemniej, jak wspomniano powyżej, w ostatnich miesiącach rzecznicy ochrony danych osobowych w Europie ponownie zaczęli rozważać, czy zasady wynikające z Decyzji 2000/520/WE są wciąż aktualne dla procesów przekazywania danych do podmiotów podlegających prawodawstwu Stanów Zjednoczonych. Najdalej posunęli się tu rzecznicy - federalny i landowi - z Republiki Federalnej Niemiec, którzy 24 lipca 2013 r. podczas krajowej konferencji uznali, że działania wywiadowcze zagranicznych agencji publicznych niosą istotne zagrożenie dla wyniany danych pomiędzy Europejskim Obszarem Gospodarczym a państwami trzecimi. Poinformowali, że, biorąc pod uwagę swe uprawnienia i obowiązki wynikające z prawa nimieckiego i europejskiego, zadecydowali

a) zaprzestać wydawania zgód na międzynarodowy transfer danych dopóki niemecki rząd nie udowodni, że nielimitowany dostęp zagranicznych służb wywiadowczych do danych obywateli niemieckich spełnia wymagania wynikające z podstawowych zasad prawa ochrony danych osobowych (np. w zakresie niezbędności, propocjonalności i celowości),

b) rozważyć, czy nie powstrzymać transferu danych na podstawie porozumienia o „bezpiecznej przystani" oraz standardowych klauzul umownych.

9. Mając to na względzie wydaje się, że jakiekolwiek działania władz amerykańskich dotyczące danych pochodzących z terytorium UE, w szczególności prowadzone na masową skalę, powinny zostać rozwiązane odrębnie. Chciałbym zauważyć, że taka sytuacja już miała miejsce w odniesieniu do przekazywania danych przez stowarzyszenie SWIFT, kiedy kwestia przekazywania danych władzom amerykańskim przez stowarzyszenie SWIFT na potrzeby zwalczania terroryzmu została uregulowana odrębnie, choć po ujawnieniu działań władz amerykańskich w późniejszym czasie stowarzyszenie SWIFT przystąpiło do programu „bezpiecznej przystani". Na marginesie warto zaznaczyć, że kwestia wprowadzenia odpowiednich gwarancji w związku z przekazywaniem

danych w celach zwalczania terroryzmu i poważnej przestępczości jest także przedmiotem toczących od kilku lat negocjacji w sprawie mającej to uregulować tzw. umowy parasolowej.

10. Generalny Inspektor Ochrony Danych Osobowych podziela wątpliwości wyrażone w ostatnich tygodniach przez rzeczników ochrony danych osobowych reprezentowanych w pracach Parlamentu Europejskiego przez przewodniczącego Grupy Roboczej Art. 29 Jacoba Kohnstamma oraz przez Europejskiego Inspektora Ochrony Danych Petera Hustinxa w zakresie praktyki stosowania programu „bezpiecznej przystani".

Warto wzorem Petera Hustinxa przeprowadzać trójstopniową analizę uprawnień i obowiązków wynikających z programu „bezpiecznej przystani" dla wszystkich podmiotów, do których program ten się odnosi, rozważając najpierw adekwatność jako podstawę dla Decyzji 2000/520/WE, a następnie samą treść Decyzji i wynikające z niej wyjątki dla potrzeb bezpieczeństwa narodowego.

Nawet uwzględniając fakt, że porozumienie będące podstawą dla stworzenia programu „bezpiecznej przystani" było kompromisem pomiędzy stronami, Komisja Europejska uznaje je za wykonanie przepisów dotyczących adekwatności ochrony. Oznacza to, że wszelkie rozważania należy prowadząc jednoczesną ocenę, czy praktyka stosowania porozumienia odpowiada wymaganiom stawianym podmiotom przewidującym adekwatną ochronę, co słusznie charakteryzował Peter Hustinx w wystąpieniu przed Komisją LIBE Parlamentu Europejskiego w dniu 7 października 2013 r. Uwzględniając wątpliwości jaki rodzą się co do "niezbędnego zakresu" danych przekazywanych władzom publicznym, bez pełnej oceny, na ile w praktycznym działaniu zapis ten był i jest przekraczany przez amerykańskich partnerów, nie ma możliwości pełnej odpowiedzi na pytanie jak powinna wyglądać przyszłość Decyzji 2000/520/WE w świetle dziś obowiązujących przepisów prawa europejskiego i w świetle przygotowywanego ogólnego rozporządzenia w sprawie bezpieczeństwie danych.

W tym samym kontekście należy również zwrócić uwagę na wątpliwości przedstawione w dokumencie *"The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights"* przygotowanym we wrześniu 2013 r. przez Caspara Bowdena dla Komisji JURI i LIBE Parlamentu Europejskiego, dotyczące nie tylko samego programu „bezpiecznej przystani" ale i sposobu jego ewaluacji przez instytucje unijne w 2004 r.

Podsumowując niniejsze rozważania należy przypomnieć, że od początku funkcjonowania programu „bezpiecznej przystani" było oczywistym, że nie rozwiązuje on wszystkich problemów

związanych z przekazywaniem danych UE do USA i jako efekt osiągniętego kompromisu nie w pełni zadowala. Jednakże na przestrzeni ostatnich lat nastąpił zauważalny postęp w zakresie wdrożenia jego zasad, będący w dużym stopniu wynikiem prowadzonego dialogu z władzami amerykańskimi. Jednocześnie wydarzenia ostatnich miesięcy znacząco naruszyły pozytywne zdanie o działaniach podejmowanych w ostatnich latach przez Federalną Komisję Handlu. Niewątpliwym jest również, że wymagane są dalsze działania mające na celu lepsze funkcjonowanie programu oraz umożliwiające rozwiązanie problemów, których nie przewidziano w czasie tworzenia programu (np. w odniesieniu do usług chmurowych).

Z poważaniem