Ministerstwo Administracji i Cyfryzacji

Departament Społeczeństwa Informacyjnego

ANALIZA PROGRAMU „BEZPIECZNA PRZYSTAŃ”
(„Safe Harbour”)

w zakresie przekazywania danych osobowych z terytorium Polski do odbiorców w Stanach Zjednoczonych Ameryki

Departament Społeczeństwa Informacyjnego
Ministerstwo Administracji i Cyfryzacji

stan prawny na dzień 10 kwietnia 2014 r.

I. Wstęp

Wymiana informacji, w tym danych osobowych, pomiędzy Polską a Stanami Zjednoczonymi Ameryki (dalej: **USA**) jest istotnym elementem wzajemnych relacji, w szczególności stosunków gospodarczych[1]. W obecnych realiach gospodarczych – opierających się w coraz większym stopniu na szybkim przepływie informacji, łączności za pośrednictwem Internetu oraz coraz bliższej współpracy biznesowej pomiędzy podmiotami z całego świata, realiach, w których coraz powszechniejszy staje się outsourcing poszczególnych zadań i stale rośnie wartość usług cyfrowych, przepływ danych odgrywa kluczową rolę. Dlatego też istnieje potrzeba funkcjonowania efektywnych instrumentów, które taką wymianę umożliwiają, jednocześnie gwarantując przestrzeganie odpowiednich standardów bezpieczeństwa oraz należytą ochronę przekazywanych danych osobowych. Potrzeba ta jest tym pilniejsza, że poziom ochrony danych osobowych w poszczególnych państwach świata jest bardzo zróżnicowany, a tylko kilkanaście z nich wprowadziło standardy porównywalne z – uważanym za jeden z najwyższych na świecie – unijnym poziomem ochrony danych osobowych. **Właśnie z uwagi na brak odpowiednich rozwiązań gwarantujących adekwatny**

[1] Stany Zjednoczone Ameryki są jednym z głównych partnerów handlowych Polski, zwłaszcza w dziedzinie importu. W roku 2011 import z USA do Polski stanowił 2,3% całości importu, podczas gdy w 2012 r. było to już 2,6% - dane za Głównym Urzędem Statystycznym, *Obroty handlu zagranicznego ogółem i według krajów w 2012 r. (wyniki ostateczne)* http://www.stat.gov.pl/gus/5840_6704_PLK_HTML.htm, 12.02.2014 r. Z kolei Komisja Europejska wycenia wartość wymiany towarów i usług pomiędzy Unią Europejską a Stanami Zjednoczonymi Ameryki na 2 miliardy euro dziennie. Wartość danych osobowych obywateli UE, według raportu Boston Consulting Group *The value of our digital identity*, w 2011 r. wyniosła 315 miliardów dolarów, a do 2020 r. może się potroić.

do europejskiego poziom ochrony danych osobowych, obowiązuje zakaz przekazywania danych osobowych z terytorium Unii Europejskiej do USA na zasadach ogólnych. Taki transfer jest możliwy jedynie z wykorzystaniem przepisów szczególnych, w tym specjalnie opracowanych na ich podstawie instrumentów. Jednym z nich jest transfer w ramach „bezpiecznej przystani".

Chcąc wyjść naprzeciw oczekiwaniom rynku, w szczególności unijnych i amerykańskich przedsiębiorców, Komisja Europejska wydała **decyzję uznającą adekwatność zasad programu amerykańskiej „bezpiecznej przystani"** (decyzja Komisji Europejskiej 2000/520/WE[2], dalej: **Decyzja**). Jej podstawą jest art. 25 ust. 6 Dyrektywy Parlamentu Europejskiego i Rady nr 95/46/WE z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[3] (dalej: **Dyrektywa 95/46**) a sama decyzja została wydana zgodnie z procedurą wymienioną w art. 31 ust. 2 ww. Dyrektywy.

Od czasu wydania Decyzji minęło już kilkanaście lat, podczas których miał miejsce ciągły rozwój społeczeństwa informacyjnego. Komisja Europejska w lipcu 2013 r. zapowiedziała kolejną, trzecią już, ewaluację programu „bezpieczna przystań", której celem miało być ustalenie czy w obecnych warunkach i przy aktualnie istniejących sposobach przetwarzania danych, w szczególności danych osobowych użytkowników Internetu, nie tworzy on wyłomu w unijnych zasadach ochrony danych osobowych[4]. Odpowiedni komunikat Komisji Europejskiej został opublikowany w listopadzie 2013 r.[5] Jest on przedmiotem osobnego dokumentu przygotowanego przez Ministerstwo Administracji i Cyfryzacji, który prezentuje pełne stanowisko Rządu RP w zakresie wspomnianego dokumentu.

Niniejsza analiza nie zmierza do dokonania definitywnej oceny decyzji Komisji Europejskiej o uznaniu adekwatności ochrony przewidzianej przez zasady „bezpiecznej przystani" a ma jedynie stanowić materiał do dyskusji dotyczącej tej kwestii. **Jej celem jest wskazanie możliwych zmian w programie „bezpieczna przystań", które zwiększyłyby ochronę danych**

[2] Decyzja Komisji Europejskiej 2000/520/WE z dnia 26 lipca 2000 r. (O.J. L 215, 25.08.2000 s. 0007 – 0047).
[3] Dz. Urz. UE L 95.281.31 z dnia 23 listopada 1995 r.
[4] Oficjalna informacja w tej sprawie została opublikowana przez Komisję Europejską dnia 19 lipca 2013 r.: http://europa.eu/rapid/press-release_MEMO-13-710_en.htm, 12.02.2014 r.
[5] *Communication from the Commission to the European Parlament and the Council on the Functioning of the Safe Harbour from the Pespective of EU Citizens and Companies Established in the EU*, COM(2013) 847.

osobowych polskich obywateli przekazywanych do USA w ramach tego programu oraz dostosowałyby jego wymogi do obecnych realiów cyfrowego świata.

II. „Bezpieczna przystań" – kontekst

Do stworzenia zasad „bezpiecznej przystani" doprowadził brak adekwatnych, federalnych regulacji prawnych w zakresie ochrony danych osobowych, który uniemożliwia zakwalifikowanie USA do grona państw gwarantujących odpowiedni poziom ochrony danych osobowych w rozumieniu przepisów Dyrektywy 95/46, a przez to także przepisów ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych[6] (dalej: **Ustawa**). Mając na względzie komplikacje, jakie potencjalnie mogą wyniknąć z braku adekwatności ochrony danych, tak Unia Europejska, jak i USA uznały, że powinien istnieć instrument, który pozwoli na przekazywanie danych osobowych z terytorium UE do USA. Decyzja Komisji Europejskiej w sprawie uznania adekwatności „bezpiecznej przystani" ma nie tylko kontekst prawny, ale także swój aspekt ekonomiczny – brak rozwiązań umożliwiających efektywne przekazywanie danych osobowych z terytorium Unii Europejskiej do USA mógłby mieć negatywny wpływ na pozycję europejskich, w tym polskich, przedsiębiorstw na globalnym rynku. Mógłby on też mieć niekorzystny wpływ na rozwój usług społeczeństwa informacyjnego – Internet nie zna granic a duża część największych, najbardziej innowacyjnych firm działających *online*, z usług których na co dzień korzystają m.in. Polacy oraz polskie przedsiębiorstwa ma swoje siedziby w USA[7]. Prócz kwestii prawnych i ekonomicznych ważny jest także aspekt polityczny – zarówno strona europejska jak i amerykańska podczas prac nad zasadami „bezpiecznej przystani" mogła pójść na pewne ustępstwa, istniała bowiem silna polityczna wola wypracowania kompromisu, nawet kosztem pewnych ustępstw.

Przeprowadzona kilkanaście lat temu przez Komisję Europejską pozytywna ocena adekwatności zasad „bezpiecznej przystani", umożliwiła dalszy rozwój i zacieśnianie współpracy gospodarczej pomiędzy Unią Europejską a USA. Państwa członkowskie zostały zobowiązane do podjęcia wszelkich środków niezbędnych do wdrożenia Decyzji w swoich

[6] Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.).
[7] Choć sam program nie jest umową międzynarodową i dotyczy jedynie podmiotów, które dobrowolnie do niego przystąpią (wciąż stanowią one jedynie niewielki odsetek wszystkich przedsiębiorstw w USA), to przystąpiło do niego wiele firm o zasięgu globalnym, na przykład Facebook Inc., Google Inc. czy Microsoft Corporation.

porządkach prawnych. W związku z tym w praktyce, od dnia 1 maja 2004 r., to jest od dnia przystąpienia Polski do Unii Europejskiej, polski organ nadzorczy, Generalny Inspektor Ochrony Danych Osobowych (dalej: **GIODO**), co do zasady nie może odmówić uznania odpowiedniego poziomu ochrony danych osobowych w przypadku transferów danych do odbiorców, którzy certyfikowali się w ramach „bezpiecznej przystani", jak również nie może wymagać w tym zakresie dodatkowych autoryzacji.

Od czasu wydania Decyzji miał miejsce intensywny postęp technologiczny. Dziś nawet podczas najbardziej błahych spraw codziennych załatwianych poprzez urządzenia elektroniczne pozostawiamy po sobie informacje – cyfrowe ślady, które mogą stanowić nasze dane osobowe. Technologia pozwala obecnie gromadzić i analizować informacje na nieosiągalną jeszcze kilka lat temu skalę a jednym z efektów postępu technicznego jest rozwój coraz bardziej efektywnych sposobów przetwarzania danych osobowych. Pojawiły się nowe, nieznane wcześniej metody ich przetwarzania na przykład poprzez analizę tzw. Big Data (dużych zbiorów z pozoru nieistotnych informacji, których analiza pozwala uzyskać dane osobowe) czy też przetwarzanie w chmurze obliczeniowej. Zjawisk takich jak na przykład rozwój serwisów społecznościowych nie można było całkowicie przewidzieć kilkanaście lat temu, podczas prac poprzedzających wydanie Decyzji. Nieustannie rośnie liczba firm, dla których przetwarzanie danych osobowych jest głównym modelem prowadzenia biznesu. Jednocześnie, operacje na danych stają się coraz łatwiejsze do przeprowadzania. Coraz większą rolę odgrywa, nieznający granic państw, Internet.

Przekazywanie danych z terytorium Polski do państw trzecich, które nie zapewniają odpowiedniego poziomu ochrony danych osobowych, w tym do USA, jest obecnie dopuszczalne przede wszystkim w oparciu o zasady wskazane w art. 47 ust. 3 Ustawy, który stanowi iż administrator danych może przekazać dane osobowe do państwa trzeciego, jeżeli:
(i) osoba, której dane dotyczą, udzieliła na to zgody na piśmie;

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

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

(iv) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych;

(v) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;

(vi) dane są ogólnie dostępne. Jest ono możliwe także gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych.

Ponadto, w ostatnich latach można zaobserwować rozwój alternatywnych do „bezpiecznej przystani" instrumentów, umożliwiających odbiorcy uzyskanie odpowiedniego poziomu ochrony danych osobowych poprzez samoregulację, jak choćby wiążących reguł korporacyjnych (ang. *binding corporate rules*)[8] czy kontraktów modelowych opartych na standardowych klauzulach umownych (ang. *standard contractual clauses*)[9]. Są one coraz częściej wykorzystywane przez amerykańskie korporacje. W Polsce istnieje także możliwość uzyskania uprzedniej zgody GIODO na transfer danych osobowych do państwa trzeciego – zgodnie ze sprawozdaniem GIODO za rok 2012, w tymże roku wyrażono 55 takich zgód, na przestrzeni ostatnich lat było ich około 200. **W związku z tym należy pamiętać, że ewentualne uchylenie Decyzji, gdyby okazało się, że zasady „bezpiecznej przystani" nie chronią w sposób dostateczny danych osobowych obywateli UE, nie uniemożliwi przekazywania danych osobowych z terytorium Polski do USA**. Istnieją bowiem inne rozwiązania umożliwiające transfer danych, które budzą mniej kontrowersji niż „bezpieczna przystań', niemniej co najmniej część z nich może być droższa w implementacji dla administratorów danych.

III. Przekazywanie danych osobowych z Polski do Stanów Zjednoczonych Ameryki

[8] Na mocy dokumentu roboczego Grupy Roboczej Artykułu 29 *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"* przyjętego dnia 14 kwietnia 2005 r. 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.

[9] Komisja Europejska na mocy art. 26 ust. 4 dyrektywy została uprawniona do uznania w drodze decyzji, że tzw. standardowe klauzule umowne, wzorcowe postanowienia, które mogą być stosowane w umowach regulujących przekazywanie danych osobowych, zapewniają odpowiednią ochronę danych osobowych oraz praw i wolności jednostek.

Program „bezpieczna przystań" jest administrowany przez Departament Handlu USA, a egzekwowaniem przestrzegania jego wymogów zajmuje się Federalna Komisja Handlu, która wykorzystuje w tym celu swoje uprawnienia w zakresie ochrony konsumentów. W ostatnich latach jesteśmy świadkami szybkiego wzrostu liczby podmiotów certyfikowanych w ramach „bezpiecznej przystani" – jeszcze w 2004 roku należało do niego około 400 podmiotów, we wrześniu 2013 certyfikowanych było już ponad 3200 podmiotów gospodarczych zlokalizowanych w USA[10]. Jest to niewielki promil całkowitej liczby amerykańskich przedsiębiorstw, niemniej do programu należą największe podmioty z branży internetowej i nowych technologii. Te 3200 podmiotów przetwarza setki milionów rekordów danych osobowych obywateli państw członkowskich UE.

Stany Zjednoczone Ameryki, w świetle przepisów Ustawy, są uznawane za „państwo trzecie". Zgodnie z artykułem 47 ustęp 1 Ustawy, transfer danych osobowych z Polski może nastąpić, co do zasady, jedynie do państwa trzeciego dającego gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej. Pojęcie „państwo trzecie" pojawia się zarówno w Ustawie, jak i w samej dyrektywie 95/46. Artykuł 7 punkt 7 Ustawy definiuje „państwo trzecie" jako państwo nienależące do Europejskiego Obszaru Gospodarczego (dalej: „EOG")[11]. Przekazywanie danych osobowych w ramach EOG należy traktować jako „przetwarzanie danych na terytorium RP"[12]. Dyrektywa oraz Ustawa zakazują, co do zasady, przekazywania danych osobowych do państw trzecich niezapewniających odpowiedniego poziomu ochrony danych.

IV. „Bezpieczna przystań" – zasady

Podporządkowanie zasadom „bezpiecznej przystani" odbywa się na podstawie dobrowolnej certyfikacji (podmiot chcący się certyfikować sam ocenia czy spełnia zasady programu, po czym notyfikuje tą okoliczność Departamentowi Handlu). Program „bezpieczna przystań" wprowadza następujące zasady:

[10] Dane uzyskane z Komisji Europejskiej – DG Justice. Należy przy tym zaznaczyć, iż ponad 50% certyfikowanych podmiotów (1671 z 3246), to przedsiębiorstwa zajmujące się przetwarzaniem danych osobowych europejskich pracowników – dane za komunikatem Komisji Europejskiej COM (2013) 847.
[11] Prócz krajów Unii Europejskiej do EOG należą także Norwegia, Islandia oraz Lichtenstein.
[12] J. Barta, P. Fajgielski, R. Markiewicz**,** *Ochrona danych osobowych. Komentarz*, wyd. 3, Kraków 2004, s. 720.

notice (informacja) – spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą, podobnego do analogicznego wymogu wprowadzonego przez przepisy Dyrektywy i Ustawy;

choice (wybór) – „bezpieczna przystań" wprowadza model *opt-out*, zgodnie z którym można sprzeciwić się przekazaniu swoich danych do podmiotu trzeciego oraz przetwarzaniu danych w celu niezgodnym w stosunku do tego, w jakim zostały pierwotnie zebrane; w odniesieniu do udostępniania osobom trzecim danych wrażliwych[13] stosowany jest model *opt-in*, w którym wymagana jest wyraźna zgoda podmiotu danych na ujawnienie danych podmiotowi trzeciemu, czy też użycie ich w celu innym, niż ten dla którego zostały pierwotnie zebrane;

onward transfer (dalsze przekazanie) – dalsze przekazanie danych może nastąpić jedynie do podmiotu trzeciego zgodnie z zasadami informacji i wyboru. W przypadku transferu do takiego podmiotu, można go przeprowadzić pod warunkiem uprzedniego upewnienia się, iż strona trzecia przystąpiła do zasad „bezpiecznej przystani" albo podlega Dyrektywie bądź adekwatnym zasadom ochrony. Alternatywnie, odbiorca może zawrzeć z taką stroną trzecią pisemną umowę wymagającą, aby strona trzecia zapewniła, co najmniej taki sam poziom ochrony prywatności, jaki jest wymagany przez zasady „bezpiecznej przystani".

Co ważne, jeżeli podmiot przetwarzający dane będzie przestrzegać odpowiednich wymagań, to nie będzie on ponosić odpowiedzialności (o ile nie postanowi inaczej) za to, że strona trzecia, do której przekazuje informacje, przetwarza je w sposób niezgodny z wymogami albo oświadczeniami, chyba że wiedział on albo powinien był wiedzieć, że strona trzecia może przetwarzać dane w taki nieodpowiedni sposób i nie podjął kroków, żeby zapobiec takiemu przetwarzaniu danych lub je powstrzymać;

access (dostęp) – prawo dostępu do własnych danych wraz z możliwością ich poprawiania, zmieniania lub usuwania, gdy są one nieprawidłowe, z wyjątkiem przypadków, gdy obciążenie kosztami udzielenia informacji byłoby nieproporcjonalne w stosunku do zagrożenia dla ochrony prywatności danej osoby lub w przypadku gdy w wyniku dostępu zostałyby naruszone prawa osób innych niż dana osoba;

[13] Zgodnie z art. 27 ust. 1 polskiej Ustawy, danymi wrażliwymi są dane ujawniające 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.

security (bezpieczeństwo) – stosowanie rozsądnych środków ostrożności w celu ochrony danych przed utratą, niewłaściwym wykorzystaniem oraz nieuprawnionym dostępem, ujawnieniem, zmianą i zniszczeniem;

data integrity (integralność danych) – wykorzystywanie danych osobowych tylko do celów, dla których zostały zebrane lub na które podmiot danych udzielił następnie zezwolenia oraz obowiązek podjęcia kroków w celu zapewnienia dokładności, kompletności i aktualności danych;

enforcement (zapewnienie prawu skuteczności) – przyjęcie mechanizmów pozwalających na egzekwowanie zasad programu „bezpiecznej przystani", w szczególności odpowiednich procedur postępowania, zagwarantowanie prawa do odwoływania się dla osób, których dane dotyczą, w tym które poniosły szkodę wskutek nieprzestrzegania zasad, oraz rozwiązania przewidującego konsekwencje dla amerykańskich odbiorców danych z powodu nieprzestrzegania zasad.

V. Program „bezpiecznej przystani" a sprawa PRISM

Program „bezpiecznej przystani" przez wiele osób jest łączony z amerykańskim programem inwigilacji PRISM. Dzieje się tak między innymi dlatego, że praktycznie wszystkie amerykańskie koncerny, które były wymieniane w doniesieniach Edwarda Snowdena są certyfikowane w ramach „bezpiecznej przystani". Komisja Europejska sama przyznaje, iż w momencie negocjacji zasad „bezpiecznej przystani" nie była w stanie przewidzieć skali, jaką może osiągnąć inwigilacja przez agencje wywiadowcze danych przekazywanych w Internecie w związku z działalnością gospodarczą (takie dane są przekazywane w ramach „bezpiecznej przystani"). Dostrzega ona także zagrożenie w postaci dostępu do danych przez organy amerykańskie poza niezbędnym i proporcjonalnym, ze względu na bezpieczeństwo narodowe, porządek publiczny oraz egzekwowanie prawa, zakresem[14]. Te trzy przesłanki interpretowane są przez stronę amerykańską szeroko. Przekazywanie danych amerykańskim służbom przez podmioty certyfikowane odbywa się bez żadnej kontroli ze strony europejskiej. Reakcje europejskich organów nadzorczych na informację o bliskiej współpracy

[14] Informacje za Komunikatem Komisji Europejskiej COM(2013) 847, s. 17.

części certyfikowanych podmiotów z amerykańską National Security Agency w ramach PRISM były różnorakie. Z jednej strony, w dniu 24 lipca 2013 r., niemieccy rzecznicy ochrony danych osobowych wskazali, na duże prawdopodobieństwo, iż zasady „bezpiecznej przystani" są naruszane w związku z funkcjonowaniem programu PRISM[15]. Takie publiczne oświadczenie jednoznacznie świadczy o ich poważnych wątpliwościach w tym zakresie. Z drugiej strony, irlandzki[16] i luksemburski[17] organ ochrony danych nie uznały ryzyka inwigilacji w ramach PRISM za okoliczność stanowiącą przeszkodę w transferze danych osobowych obywateli UE do odbiorców podejrzewanych o udostępnianie ich amerykańskim służbom wywiadowczym, uznały bowiem iż takie działanie nie narusza zasad programu[18]. Mając na uwadze rozbieżności w ocenie programu „bezpieczna przystań" pozytywnie należy ocenić zaangażowanie Komisji Europejskiej w tej sprawie.

Ujawnione w 2013 r. informacje dotyczące programu PRISM spowodowały konieczność ponownego przyjrzenia się programowi „bezpieczna przystań" w celu ustalenia czy nie stanowi on wyłomu w unijnej ochronie danych osobowych. **Istnieje ryzyko, iż program „bezpiecznej przystani" nie przyznaje rzecznikom ochrony danych z państw członkowskich Unii Europejskiej skutecznych uprawnień kontrolnych. W szczególności treść decyzji nie umożliwia rzecznikom przeciwdziałania czynnościom podejmowanym przez amerykańskie służby wywiadowcze, w przypadku gdy czynności te są nie do pogodzenia z unijnymi standardami ochrony danych osobowych lecz zgodne z amerykańskim prawem**. W zakresie kontroli certyfikowanych odbiorców danych w USA, właściwe są bowiem wyłącznie organy amerykańskie. W obecnym stanie prawnym możliwość wstrzymania przekazywania danych osobowych do uczestnika programu „bezpiecznej przystani" wiąże się co do zasady z jego własnymi działaniami, a nie działaniami osób trzecich. Bez uzasadnionego podejrzenia naruszenia zasad programu, *de facto* nie ma możliwości podjęcia przez organ nadzorczy z UE odpowiednich działań. Jednocześnie, udokumentowanie takiego naruszenia nastręcza wiele problemów, gdyż europejskie organy nadzorcze nie mogą żądać od odbiorców danych udowodnienia, że faktycznie spełniają oni zasady programu. Odpowiednią kontrolę może przeprowadzić Federalna Komisja Handlu.

[15] Informacja za: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870, 12.02.2014 r.
[16] Treść odpowiedniego pisma dostępna na: http://www.europe-v-facebook.org/Response_23_7_2013.pdf, 12.02.2014.
[17] Informacja o decyzji: http://www.cnpd.public.lu/de/actualites/national/2013/11/skype-microsoft/index.html?highlight=microsoft%22nsa, 12.02.2014 r.
[18] Artykuł z dziennika *The Guardian*: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, 12.02.2014 r.

Warto zaznaczyć, że Decyzja dopuszcza wyjątek od zasad „bezpiecznej przystani", jak wskazuje jej oficjalne tłumaczenie:

(i) w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo egzekwowania prawa;

(ii) ustawą, rozporządzeniem rządu albo prawem precedensowym, ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia odbiorca danych potrafi wykazać, że nieprzestrzeganie przez niego zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie; lub

(iii) jeżeli efektem dyrektywy 95/46 w prawie państwa członkowskiego jest dopuszczenie wyjątków lub odstępstw, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych kontekstach[19].

Kontrowersje budzi m.in. interpretacja takich pojęć jak „niezbędny zakres" czy „bezpieczeństwo narodowe" – wydaje się, że odnośnie nich amerykańska i europejska wykładnia mogą się w wielu konkretnych sytuacjach różnić a rozumienie amerykańskie jest znacznie szersze.

VI. Funkcjonowanie „bezpiecznej przystani" – przestrzeganie zasad

Departament Handlu USA coraz aktywniej podejmuje działania mające na celu zwiększenie efektywności funkcjonowania „bezpiecznej przystani", w tym zmożoną aktywność w zakresie kontroli certyfikowanych podmiotów a także kroki prawne przeciwko podmiotom, które nie odnowiły certyfikatu a nadal powołują się na przynależność do zasad programu. Na przestrzeni kilku ostatnich lat widać wzrost wagi, jaką strona amerykańska przywiązuje do funkcjonowania programu. Wciąż jednak w zakresie jego wdrażania są obszary wymagające pracy. Z perspektywy MAiC największe zastrzeżenie budzi realizacja zasady wyboru (*choice*) oraz praktyka w zakresie realizacji zasady zapewniania prawu skuteczności (*enforcement*). Odnośnie zasady wyboru, rozwiązanie amerykańskie jest odmienne od stosowanych powszechnie w Unii rozwiązań opartych na *opt-in* – wymagających uprzedniej zgody

[19] Załącznik i zasady ochrony prywatności w ramach „bezpiecznej przystani", wydane przez Departament Handlu USA dnia 21 lipca 2000 r.

podmiotu danych na przetwarzanie jego danych. **Podejście amerykańskie dopuszcza w szeregu sytuacji możliwość wyrażenia sprzeciwu** (*opt-out*), a udzielenie zgody jest domniemane. W kwestii zasady zapewniania prawu skuteczności, w ocenie MAiC rolę podmiotu rozstrzygającego ewentualne spory w zakresie „bezpiecznej przystani" powinna wziąć na siebie Federalna Komisja Handlu bądź specjalnie powołane do tego ciało (godnym uwagi przykładem jest tu ustanowienie *Data Protection Panel*[20], który jednak obecnie jest właściwy jedynie do rozstrzygania spraw dotyczących przetwarzania danych osobowych w związku z zarządzaniem zasobami ludzkimi bądź w przypadkach, gdy administrator danych sam wyznaczył go do rozstrzygania sporów wynikłych w związku z „bezpieczną przystanią"). Mechanizmy rozstrzygania sporów dotyczących „bezpiecznej przystani" powinny być dla podmiotów danych bezpłatne.

Należy zaznaczyć, iż niejasności powstają na tle wykonywania przez amerykańskich odbiorców danych obowiązku informacyjnego, na co uwagę zwraca Komisja Europejska we wspominanym już dokumencie COM (2013) 847. Komisja Europejska podkreśliła w nim, iż pomimo upływu kilkunastu lat od wydania decyzji o adekwatności „bezpiecznej przystani" certyfikowane podmioty w wielu przypadkach nie udostępniają publicznie swoich polityk prywatności, często już dostępne polityki są napisane niezrozumiałym językiem; 30% polityk nie wskazuje instytucji właściwej do rozpatrywania sporów, niektóre podają nieprawdziwe informacje w tym zakresie. Wiele polityk nieprawidłowo implementuje zasady „bezpiecznej przystani" – ewaluacja polityk prywatności certyfikowanych przedsiębiorców przez Departament Handlu ma miejsce dopiero od dnia 1 stycznia 2009 r. a Departament Handlu wciąż nie weryfikuje jak ich postanowienia są realizowane w praktyce. Dodatkowo problemem są nieprawdziwe oświadczenia – około 10% przedsiębiorców deklarujących publicznie przestrzeganie zasad „bezpiecznej przystani" nie znajduje się na liście prowadzonej przez Departament Handlu USA. Pomimo powyższych zastrzeżeń, do dnia dzisiejszego żaden przedsiębiorca nie został usunięty z listy certyfikowanych podmiotów za brak przestrzegania zasad programu. Z listy przede wszystkim usuwa się podmioty, które rezygnują dobrowolnie z uczestnictwa w programie. Jednocześnie informacja na stronie Departamentu Handlu o usunięciu danego odbiorcy z listy certyfikowanych podmiotów nie

[20] Aktualnie w skład panelu wchodzą przedstawiciele organów nadzorczych z Danii, Niemiec, Finlandii, Wielkiej Brytanii, Francji, Irlandii i Holandii, informacja za: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/files/ussh/dp_panel_authorities_faq5_en.pdf, 12.02.2014 r.

jest dostatecznie czytelna i może wprowadzać obywateli UE w błąd. Co więcej, Komisja Europejska wskazuje, że Departament Handlu USA jest świadomy wyżej wymienionych zaniedbań. Podejmowane przez niego działania należy ocenić jako niedostatecznie stanowcze. Kolejne zastrzeżenie MAiC jest związane z wysokością opłat za rozstrzyganie sporów. Podmioty certyfikowane dla rozstrzygania sporów dotyczących programu muszą wskazać jedną z organizacji arbitrażowych, m.in. BBB, TRUSTe, AICPA czy WebTrust. Wciąż niektóre z tych podmiotów pobierają opłaty za rozpatrzenie skargi osoby, której dane są przetwarzane w ramach „bezpiecznej przystani", często dużej wysokości. Między innymi ponad 460 certyfikowanych podmiotów jako instytucję właściwą do rozwiązywania sporów wskazuje American Arbitration Association, która za samo złożenie skargi przez obywatela Unii Europejskiej (bez kosztów postępowania) pobiera opłatę w wysokości 200 USD[21]. Ochrona prawa jakim jest prawo do ochrony danych osobowych, w ocenie MAiC powinna przysługiwać podmiotom danych z terytorium UE bezpłatnie.

VII. Funkcjonowanie „bezpiecznej przystani" – egzekwowanie przestrzegania zasad programu

Egzekwowanie zasad programu „bezpiecznej przystani" obecnie leży poza kompetencją europejskich rzeczników ochrony danych osobowych i należy do zadań Federalnej Komisji Handlu. Wielu obserwatorów zarzuca Federalnej Komisji Handlu, iż przez wiele lat niedostatecznie kontrolowała certyfikujące się podmioty[22]. Między innymi z tego względu w grudniu 2010 r. niemieckie organy ochrony danych osobowych z krajów związkowych (tzw. *Düsseldorfer Kreis*) zalecały podmiotom przekazującym dane do odbiorców znajdujących się w USA i deklarujących przynależność do programu „bezpiecznej przystani", weryfikację na własną rękę czy aby na pewno odbiorcy ci spełniają zasady programu[23]. Taki krok jasno wskazywał na wątpliwości ww. organów w tym zakresie. Mogły one jednak żądać wyjaśnień

[21] Informacje dotyczące pobieranych opłat dostępne są na: http://images.go.adr.org/Web/AmericanArbitrationAssociation/%7B8ab12e8b-f636-4258-9dff-412dc96a4de9%7D_SafeHarbor_Fees.pdf, dostęp: 12.02.2014 r.

[22] Bardzo kompleksowo tę kwestię omawia raport *The US Safe Harbor – Fact or Fiction?* Przygotowany w 2008 r. przez Chrisa Connolly z Galexia.

[23] *Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen*, dokument dostępny na: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html?nn=409242, 12.02.2014 r.

jedynie od niemieckich eksporterów danych, ich amerykańscy odbiorcy pozostawali bowiem poza niemiecką jurysdykcją.

Skuteczność programu w jego obecnym kształcie w dużej mierze zależy od inicjatywy i działań podejmowanych przez Departament Handlu USA i Federalną Komisję Handlu, a wpływ instytucji europejskich na praktyczną stronę funkcjonowania programu jest niewielki. Poważniejsze kontrole podmiotów certyfikowanych w ramach „bezpiecznej przystani" Federalna Komisja Handlu rozpoczęła dopiero w 2009 r.[24] Pierwszą, szeroko komentowaną, sprawą dotyczącą programu „bezpieczna przystań" była sprawa Google Buzz z 2011 r.

MAiC dostrzega i docenia działania Federalnej Komisji Handlu po 2009 r., w tym postępowania dotyczące wielu podmiotów, z których usług często korzystają mieszkańcy Polski, takich jak Google Inc.[25], Facebook Inc.[26] czy MySpace LLC[27]. **Z perspektywy Polski kluczowym elementem dla prawidłowego funkcjonowania programu „bezpieczna przystań" jest należyte egzekwowanie przestrzegania jego postanowień**. Na tym tle pozostaje jednak sporo wątpliwości. Jak już wspomniano, przez cały okres funkcjonowania „bezpiecznej przystani" nie miało miejsca usunięcie z listy certyfikowanego podmiotu w związku z niezgodnością jego działania z zasadami programu. Usunięcie z programu następowało najczęściej na żądanie samego certyfikowanego podmiotu[28].

Federalna Komisja Handlu prowadzi wyrywkową weryfikację przestrzegania zasad programu „bezpieczna przystań" przez certyfikowane podmioty. Do stycznia 2014 r. lista podmiotów, wobec których podjęto kroki związane z egzekwowaniem programu „bezpieczna przystań" wyglądała następująco[29]:

Myspace LLC, *FTC File No. 102 3058*, 2012,
http://www.ftc.gov/os/caselist/1023058/index.shtm
Facebook, Inc., *FTC File No. 092 3184*, 2011,
http://www.ftc.gov/os/caselist/0923184/index.shtm

[24] Dane za: http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_052211.pdf, 12.02.2014 r.
[25] FTC File No. 102 3136.
[26] FTC File No. 092 3184.
[27] FTC File No. 102 3058.
[28] COM(2013) 847, s. 8.
[29] Informacja za http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_052211.pdf, 12.02.2014 r.

Google Inc., *FTC File No. 102 3136*, 2011,

http://www.ftc.gov/os/caselist/1023136/index.shtm

Collectify LLC, *FTC File No. 092 3142,* 2009,

http://www.ftc.gov/os/caselist/0923142/index.shtm

Progressive Gaitways LLC, *FTC File No. 092 3141,* 2009,
http://www.ftc.gov/os/caselist/0923141/index.shtm

Directors Desk LLC, *FTC File No. 092 3140,* 2009,
http://www.ftc.gov/os/caselist/0923140/index.shtm

Onyx Graphics, Inc., *FTC File No. 092 3139,* 2009,
http://www.ftc.gov/os/caselist/0923139/index.shtm

ExpatEdge Partners, LLC, *FTC File No. 092 3138,* 2009,
http://www.ftc.gov/os/caselist/0923138/index.shtm

In the Matter of World Innovators, Inc., *FTC File No. 092 3137,* 2009,
http://www.ftc.gov/os/caselist/0923137/index.shtm

FTC v. Javian Karnani and Balls of Kryptonite, LLC, *Civil Action No. 09-CV- 5276 FTC File No. 092 3081,* 2009,

http://www.ftc.gov/os/caselist/0923081/index.shtm

W styczniu 2014 r., to jest dwa miesiące po opublikowaniu komunikatu Komisji Europejskiej COM(2013) 847, Federalna Komisja Handlu ogłosiła zawarcie ugód w 12 kolejnych postępowaniach, dotyczących wprowadzania konsumentów w błąd informacją o przynależności do programu „bezpiecznej przystani”[30]. Sprawy dotyczyły podmiotów, które pomimo nie odnowienia certyfikatu nie usunęły informacji o przynależności do „bezpiecznej przystani” ze stron internetowych czy też polityk prywatności. Postępowania Federalnej Komisji Handlu dotyczyły następujących podmiotów: **Apperian, Inc.**; **Atlanta Falcons Football Club, LLC**; **Baker Tilly Virchow Krause, LLP**; **BitTorrent, Inc.**; **Charles River Laboratories International, Inc.**; **DataMotion, Inc.**; **DDC Laboratories, Inc.**; **Level 3 Communications, LLC**; **PDB Sports, Ltd.; d/b/a Denver Broncos Football Club**; **Reynolds Consumer Products Inc.**; **Receivable Management Services Corporation**; **Tennessee Football, Inc**.

[30] Informacja za stroną Federalnej Komisji Handlu: http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply, dostęp 12.02.2014 r.

VIII. Zasady bezpiecznej przystani a przepisy prawa polskiego – kwestia adekwatności

Zgodnie z polskimi przepisami, jeżeli dane państwo nie zapewnia odpowiedniego poziomu ochrony, odbiorca danych musi spełnić dodatkowe przesłanki, określone w art. 47 ust. 2 lub 3 Ustawy. Jeżeli przesłanki te nie zostaną spełnione, to przekazanie danych osobowych wymaga uzyskania uprzedniej zgody GIODO (art. 48 Ustawy). GIODO, badając czy dla danego transferu został zapewniony odpowiedni poziom ochrony danych osobowych, bierze pod uwagę wszystkie okoliczności dotyczące operacji przekazania danych, a w szczególności charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia danych, przepisy prawa obowiązujące w danym państwie trzecim oraz stosowane w tym państwie środki bezpieczeństwa i zasady zawodowe (por. art. 47 ust. 1a Ustawy). Przekazanie danych osobowych z terytorium Polski do odbiorcy, który przystąpił do zasad „bezpiecznej przystani" należy jednak traktować jako transfer do państwa bezpiecznego w trybie art. 47 ust. 1 ustawy. W tym świetle, nie wymaga ono wyrażenia przez GIODO uprzedniej zgody w trybie art. 48 Ustawy.

Z uzyskanych przez MAiC informacji wynika jednocześnie, że mogą wystąpić okoliczności, w których polski rzecznik ochrony danych wymaga uzyskania zgody na przekazywanie danych do odbiorcy w USA, pomimo przystąpienia przez niego do „bezpiecznej przystani". Taki wymóg może wystąpić, jeżeli kategorie przekazywanych danych oraz cele ich przetwarzania wykraczałyby poza zakres określony w certyfikacie programu. Zgodnie z informacjami otrzymanymi od GIODO, w praktyce zdarzają się takie przypadki – niekiedy amerykańscy przedsiębiorcy nie zgłaszają wybranych kategorii przetwarzanych przez siebie danych do „bezpiecznej przystani".

Należy zwrócić uwagę, iż w związku z wysokimi wymogami przewidzianymi w Ustawie, zwłaszcza w zakresie technicznych i organizacyjnych środków bezpieczeństwa , dochodzi do sytuacji, w których **odbiorcę danych należącego do programu „bezpieczna przystań" obowiązują w praktyce *de facto* niższe wymogi w porównaniu do tych, które musi spełnić odbiorca amerykański, do którego podmiot polski chce przekazać dane w oparciu o inną podstawę prawną** (to jest odbiorca nie należący do „bezpiecznej przystani"). Dzieje się tak w szczególności przy transferach w oparciu o uprzednią zgodę GIODO na przekazanie danych do państwa trzeciego, wydaną zgodnie z art. 48 Ustawy. Uzyskanie takiej zgody wymaga

spełnienia wysokich, nawet na tle innych państw członkowskich UE, wymogów, znacząco przewyższających swoją restrykcyjnością zasady „bezpiecznej przystani".

Zgodnie z danymi przekazanymi MAiC przez GIODO, w odniesieniu do zbiorów danych osobowych, zgłoszonych do rejestracji od dnia 1 maja 2004 r., to jest od dnia przystąpienia Polski do Unii Europejskiej, odnotowano stosunkowo niewielką liczbę zgłoszeń wskazujących na możliwość przekazywania danych do USA. Obecnie ta liczba wynosi około 500 zbiorów. Otwarte pozostaje pytanie ile podmiotów przekazuje dane osobowe z Polski do USA bez ujawniania tego w zgłoszeniach rejestracji zbiorów.

Przekazywanie danych osobowych w ramach „bezpiecznej przystani" nie wymaga uzyskania zgody GIODO, nie ma więc statystyk w zakresie ilości transferów danych z terytorium Polski do certyfikowanych amerykańskich podmiotów. Jednocześnie GIODO jest związany treścią Decyzji, która określa warunki uzasadniające wstrzymanie transferu danych. Zgodnie ze stanowiskiem GIODO wyrażonym w piśmie do MAiC z dnia 11 października 2013 r., GIODO w praktyce nie może nawet żądać od administratorów danych przedstawienia dowodów potwierdzających, iż rzeczywiście amerykańscy odbiorcy danych w ramach „bezpiecznej przystani" przestrzegają zasad programu[31]. W tym zakresie GIODO musi polegać na ocenie Federalnej Komisji Handlu. Ewentualne działania władcze GIODO w zakresie przekazywania danych w ramach programu „bezpieczna przystań", mogą mieć jedynie charakter wyjątkowy. Jedynie w sytuacji, gdy polski organ nadzorczy miałby uzasadnione podstawy wskazujące, że w konkretnych okolicznościach zasady „bezpiecznej przystani" są łamane, mógłby zbadać okoliczności sprawy. GIODO jak dotąd nie nakazał żadnemu podmiotowi podlegającemu pod przepisy Ustawy wstrzymania przekazywania danych osobowych do odbiorcy należącego do programu „bezpieczna przystań". Podejście GIODO można ocenić jako formalistyczne, nie uwzględniające wykładni celowościowej art. 3 Decyzji, który przecież ma służyć ochronie danych osobowych przekazywanych do USA. Zgodnie z art. 3 Decyzji, GIODO, tak jak każdy unijny rzecznik ochrony danych osobowych, ma prawo do zawieszenia przekazywania danych osobowych do podmiotu należącego do programu „bezpieczna przystań" jeżeli:

[31] Pismo GIODO do MAiC z dnia 11 października 2013 r.

(i) odpowiedni organ amerykański (Federalna Komisja Handlu) bądź mechanizm niezależnej ochrony prawnej stwierdził, iż dany podmiot naruszył zasady „bezpiecznej przystani"; bądź jeżeli

(ii) istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że mechanizm realizacji prawa o którym mowa w Decyzji 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 GIODO dołożył należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi.

Słuszność działania GIODO w każdym przypadku będzie podlegać ocenie przez niezawisły sąd. **MAiC stoi na stanowisku, że GIODO na mocy Decyzji jest uprawnione do zawieszenia transferu danych w ramach „bezpiecznej przystani", gdy ma podstawy, aby podejrzewać, że dochodzi do naruszenia ochrony danych osobowych, nawet pomimo istnienia formalnej adekwatności ochrony odbiorcy danych**. Należy jednak zaznaczyć, że na tak daleko idące posuniecie – zawieszenia przekazywana danych, nie zdecydowały się dotąd, nawet publicznie krytykujące „bezpieczną przystań" organy niemieckie. Stąd ostateczna interpretacja art. 3 Decyzji wciąż jest otwartą kwestią.

IX. Zasady bezpiecznej przystani a przepisy prawa polskiego – kwestia dalszego powierzenia przetwarzania

Jednym z zagadnień, które wywołują kontrowersje wokół „bezpiecznej przystani" jest powierzenie przetwarzania danych osobowych przez podmiot certyfikowany podmiotowi znajdującemu się poza programem. W przypadku dalszego powierzenia przetwarzania danych osobowych, to podmiot, któremu powierzono przetwarzanie danych przekazuje je dalej, do kolejnego podmiotu np. podwykonawcy, który może być zlokalizowany w innym państwie trzecim. Już w przypadku „zwykłego" powierzenia przetwarzania podmiotowi certyfikowanemu zasady „bezpiecznej przystani" mają charakter na tyle ogólny, że faktyczny poziom ochrony danych osobowych jest w praktyce uzależniony od treści umowy zawartej przez administratora danych z Unii Europejskiej z odbiorcą w USA. Efektywność „bezpiecznej przystani" w tym zakresie kwestionuje m.in. Grupa Robocza Art. 29. Uznała ona, że spółki

eksportujące dane nie powinny opierać się jedynie na oświadczeniu odbiorcy danych, który twierdzi że uzyskał certyfikację w ramach programu „bezpieczna przystań". Wręcz przeciwnie, w ocenie ww. Grupy Roboczej, spółka eksportująca dane sama powinna uzyskać dowody, że certyfikacja w ramach programu „bezpieczna przystań" istnieje i domagać się wykazania, że przestrzegane są jej zasady[32]. Obecnie, zgodnie ze stanowiskiem GIODO, jeżeli dalsze powierzenie przetwarzania danych przez podmiot uczestniczący w programie „bezpiecznej przystani" odbywa się zgodnie z zasadami ochrony prywatności w ramach „bezpiecznej przystani", a w szczególności jeśli dochodzi do niego na podstawie pisemnej umowy, to powierzenie to jest zgodne z art. 47 ust. 1 Ustawy. Tym samym, takie transfery nie wymagają np. wyrażenia przez GIODO zgody na podstawie art. 48 ustawy. Takie rozwiązanie, dopuszczające dalsze powierzenie nie tylko na podstawie umowy, wydaje się nie chronić w dostateczny sposób podmiotów danych, stwarza bowiem warunki do utraty przez administratora danych z UE kontroli nad danymi, które przekazane są do dalszego przetwarzania. Słusznym wydaje się więc postulat, zgodnie z którym dalsze powierzenie powinno mieć miejsce na podstawie umowy, a **w przypadku zawarcia umowy dotyczącej dalszego powierzenia przetwarzania danych osobowych przez podmiot certyfikowany, powinien on o tym fakcie powiadomić Departament Handlu, tak aby ten znał skalę dalszych transferów i mógł je, chociaż wyrywkowo, kontrolować.**

X. Zasady bezpiecznej przystani a projektowane przepisy prawa unijnego

Aktualnie na forum Unii Europejskiej toczą się prace nad reformą przepisów w zakresie ochrony danych osobowych. W dniu 25 stycznia 2012 r. Komisja Europejska przedstawiła pakiet zmian prawa UE w zakresie ochrony danych, w tym wniosek dotyczący ogólnego rozporządzenia o ochronie danych[33]. Nowa regulacja ma zastąpić Dyrektywę. Celem reformy jest przede wszystkim wzmocnienie ochrony danych osobowych obywateli, w tym zapewnienie im jak najpełniejszej kontroli nad ich danymi, w szczególności w Internecie. Projektowane rozporządzenie, w przeciwieństwie do obecnie obowiązujących przepisów, ma m.in. nakładać obowiązki także na podmioty, które nie mają siedziby na terytorium Unii

[32] Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej, s. 20.
[33] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM(2012)11 final 2012/0011 (COD).

Europejskiej, a oferują swoje towary lub usługi na terytorium UE, bądź monitorują zachowanie osób na tym terytorium. Obejmie więc swoim zakresem wiele podmiotów amerykańskich. Także kwestia transferów danych osobowych stanowi ważny element projektowanych ram prawnych. Wśród proponowanych rozwiązań jest m.in. usankcjonowanie w przepisach ogólnego rozporządzenia narzędzi samoregulacji administratorów danych w zakresie transferów danych (tj. BCR i standardowych klauzul umownych), które stanowią alternatywę dla zasad „bezpiecznej przystani". Ponadto, rozporządzenie ma zawierać przepis wprowadzający dodatkowe obostrzenia w zakresie dostępu do danych osobowych, w szczególności przez służby z państw trzecich. Zgodnie z nim, wszelkie orzeczenia sądu bądź trybunału bądź jakakolwiek decyzja organu administracyjnego państwa trzeciego wymagająca od administratora bądź podmiotu, któremu powierzono przetwarzanie danych, przekazywania danych osobowych, powinny być uznawane bądź wykonywane jedynie na podstawie i zgodnie z umową o wzajemnej pomocy prawnej bądź umową międzynarodową zawartą pomiędzy żądającym państwem trzecim a Unią bądź państwem członkowskim bądź też na podstawie prawa UE lub państwa członkowskiego. W innym przypadku na przekazanie danych osobowych potrzebna ma być zgoda właściwego organu nadzoru. Dodatkowo, projektowany przepis przewiduje obowiązek informowania podmiotów danych o tym, że ich dane mają być w powyżej opisanym trybie udostępnione podmiotom z państw trzecich.

Ministerstwo Administracji i Cyfryzacji traktuje unijną reformę ochrony danych jako jeden ze swoich priorytetów, dostrzegając, że obecnie obowiązujące rozwiązania w zakresie ochrony danych, w tym w zakresie transferów danych, nie do końca są dostosowane do dynamicznie zmieniającej się rzeczywistości społeczeństwa informacyjnego. Nasze, wspierające reformę, stanowisko jest prezentowane tak na forum unijnym, jak i krajowym.

XI. Podsumowanie i rekomendacje

Ministerstwo Administracji i Cyfryzacji dostrzega korzyści płynące z funkcjonowania programu „bezpieczna przystań" dla wymiany gospodarczej pomiędzy Polską a USA. Docenia także starania podejmowane przez Federalną Komisję Handlu, zwłaszcza w ostatnich latach, w zakresie egzekwowania przestrzegania postanowień programu. Niemniej „bezpieczna

przystań" w swoim obecnym kształcie posiada szereg wad i luk, mogących stwarzać zagrożenia dla ochrony danych osobowych. W związku z tym MAiC stoi na stanowisku, iż **strona amerykańska w porozumieniu z Komisją Europejską powinna podjąć działania mające na celu zmodernizowanie programu**, a przez to zwiększenie poziomu ochrony danych osobowych obywateli UE, w tym Polski, przekazywanych do USA. W tym celu Ministerstwo Administracji i Cyfryzacji proponuje następujące zmiany:

- konieczna jest **proaktywna działalność Federalnej Komisji Handlu**. Bierna postawa jaką prezentowała ona przez pierwsze dziesięć lat funkcjonowania programu „bezpiecznej przystani", pomimo zastrzeżeń ze strony Komisji Europejskiej czy podmiotów niezależnych, takich jak Galexia[34], wydaje się niewłaściwa. Federalna Komisja Handlu w zakresie „bezpiecznej przystani" nie może podejmować działań tylko w wyniku otrzymania skargi – powinna ona podejmować działania zmierzające do kontroli przetwarzania danych osobowych w programie z urzędu a także kontrolować jak w praktyce są realizowane zasady programu;
- działania podejmowane przez Federalną Komisję Handlu powinny być **efektywne**. Jest szereg problemów, z których Federalna Komisja Handlu zdaje sobie sprawę (np. braki w politykach prywatności certyfikowanych podmiotów, fałszywe oświadczenia w zakresie spełnienia zasad czy wyznaczenia organizacji arbitrażowej), a które pozostają nierozwiązane. Brak efektywności działań Federalnej Komisji Handlu oznacza w praktyce brak efektywności zasad programu „bezpieczna przystań";
- Federalna Komisja Handlu powinna dokonywać co najmniej **wstępnej oceny każdego z podmiotów chcących przystąpić do programu** (np. poprzez analizę polityki prywatności i strony internetowej) pod kątem spełniania przez nie zasad „bezpiecznej przystani", tak aby eliminować przynajmniej te z nich, które już po najbardziej podstawowej, ogólnej ocenie nie spełniają stawianych przez zasady programu wymogów. W ocenie MAiC, w celu lepszej ochrony danych osobowych obywateli UE, w tym Polski, należałoby zdecydowanie rozszerzyć i wzmocnić **mechanizmy kontroli certyfikujących się podmiotów**;

[34] Zob. przypis 22.

- w kontroli certyfikowanych podmiotów powinny móc uczestniczyć także europejskie krajowe organy ochrony danych osobowych, w tym GIODO (np. poprzez wspólne powoływanie audytorów czy poprzez rozszerzenie uprawnień i składu *Data Protection Panel*). W związku z powyższym w ocenie MAiC należy stworzyć **silne ramy umożliwiające zacieśnianie współpracy organów ochrony danych osobowych państw członkowskich UE z Federalną Komisją Handlu USA**;
- należy ustanowić **jedną, wyspecjalizowaną instytucję**, jurysdykcji której poddawałyby się wszystkie podmioty przystępujące do programu i do której trafiałyby wszystkie skargi związane z funkcjonowaniem „bezpiecznej przystani". Zdaniem MAiC, powinno się rozważyć prawne możliwości dopuszczenia składania **skarg na funkcjonowanie programu bezpośrednio do Federalnej Komisji Handlu bądź co najmniej dopuścić, aby obywatele państw członkowskich UE mieli możliwość złożenia skargi za pośrednictwem swojego krajowego organu nadzorczego**;
- należy zwiększyć transparentność samego programu „bezpiecznej przystani", tak aby osoby, których dane są przetwarzane w jego ramach miały **pełną wiedzę o przysługujących im prawach i mogły z nich korzystać bez ponoszenia dodatkowych kosztów**. Brak transparentności ma wpływ na efektywne korzystanie przez podmioty danych z uprawnień, jakie przyznają im zasady programu, w szczególności zasada informacji i wyboru. Odnośnie opłat, zasady „bezpiecznej przystani" stanowią jedynie, iż mechanizm ochronny przysługujący osobom fizycznym musi być dla nich łatwo dostępny i finansowo przystępny. Z punktu widzenia obywateli UE, w tym Polski, ważne jest, aby mechanizm ochrony przysługujących im praw był **bezpłatny**;
- należy rozszerzyć kontrolę nad podmiotami, które przetwarzają dane na zlecenie podmiotów certyfikowanych (**dalsze powierzenie przetwarzania danych** przez podmiot certyfikowany podmiotowi spoza „bezpiecznej przystani") poprzez **wprowadzenie obowiązku regulowania tej kwestii umownie oraz zgłaszania przypadków dalszego powierzenia przetwarzania do Federalnej Komisji Handlu**;
- podmioty certyfikowane, powinny jasno informować w polityce prywatności **w jakim zakresie do przetwarzanych przez nie w ramach „bezpiecznej przystani" danych mogą mieć dostęp amerykańskie służby**;

- europejskie organy nadzorcze powinny mieć możliwość podejmowania działań mających na celu ochronę danych osobowych obywateli Unii Europejskiej, w szczególności **zawieszenia przekazywania danych, jeżeli dostęp do danych mają amerykańskie służby** na przykład w ramach PRISM. Taka możliwość powinna być zagwarantowana w szczególności, gdy działania służb są nie do pogodzenia z unijnymi standardami ochrony danych osobowych. Powinny także mieć, choćby pośrednio, na przykład za pośrednictwem Federalnej Komisji Handlu, możliwość żądania wyjaśnień od amerykańskich odbiorców danych. Należy przy tym pamiętać, że reakcja na PRISM powinna przebiegać co najmniej dwutorowo – sprawa przetwarzania danych obywateli państw członkowskich UE w ramach „bezpiecznej przystani" to tylko jej jeden aspekt, inną kwestią jest zapewnienie obywatelom UE możliwości odwołania się do sądu w przypadku inwigilacji przez służby amerykańskie, tematyka ta nie wchodzi jednak w zakres „bezpiecznej przystani";
- w przypadku braku zmian w samym programie „bezpieczna przystań" oraz wyraźnej poprawy egzekwowania jego zasad przez stronę amerykańską, **w dłużej perspektywie czasu rozsądnym krokiem będzie rozważenie uchylenia Decyzji przez Komisję** i zastąpienie programu nowym narzędziem; instrument jakim jest „bezpieczna przystań" w chwili obecnej nie spełnia bowiem jednej ze swoich podstawowych ról – zapewnienia odpowiedniej ochrony danych osobowych obywateli UE przekazywanych do USA.