RADA UNII EUROPEJSKIEJ

Bruksela, 29 listopada 2013 r.
(OR. en)

17069/13

DATAPROTECT 191
USA 65
JAI 1097

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	28 listopada 2013 r.
Do:	Uwe CORSEPIUS, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2013) 847 final
Dotyczy:	Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE

Delegacje otrzymują w załączeniu dokument COM(2013) 847 final.

Zał.: COM(2013) 847 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 27.11.2013
COM(2013) 847 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE

1. Wprowadzenie

W dyrektywie 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (zwanej dalej „dyrektywą o ochronie danych") określone zostały zasady przekazywania danych osobowych z państw członkowskich UE do innych państw spoza UE[1] w zakresie, w jakim takie przekazywanie danych osobowych objęte jest zakresem stosowania przedmiotowego instrumentu[2].

Na mocy dyrektywy Komisja może stwierdzić, czy państwo trzecie zapewnia prawidłowy stopień ochrony, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło w celu ochrony praw osób fizycznych. W takim przypadku do danego państwa nie miałyby zastosowania szczególne ograniczenia dotyczące przekazywania danych. Takie decyzje powszechnie nazywa się „**decyzjami w sprawie odpowiedniej ochrony danych osobowych**".

W dniu 26 lipca 2000 r. Komisja przyjęła decyzję 2000/520/WE[3] (zwaną dalej „**decyzją w sprawie zasad bezpiecznego transferu danych osobowych"**), w której uznano, że zasady bezpiecznego transferu danych osobowych i najczęściej zadawane pytania (odpowiednio „zasady" i „Najczęściej zadawane pytania") wydane przez Departament Handlu Stanów Zjednoczonych stanowią właściwą ochronę do celów przekazywania danych osobowych z UE. Decyzję w sprawie zasad bezpiecznego transferu danych osobowych przyjęto w związku z opinią Grupy Roboczej Art. 29 i opinią Komitetu Art. 31 wydaną przez większość kwalifikowaną państw członkowskich. Zgodnie z decyzją Rady 1999/468 decyzja w sprawie zasad bezpiecznego transferu danych osobowych podlegała uprzedniej kontroli Parlamentu Europejskiego.

W rezultacie w obecnej decyzji w sprawie zasad bezpiecznego transferu danych osobowych dopuszcza się swobodne przekazywanie[4] danych osobowych z państw członkowskich UE[5] przedsiębiorstwom w Stanach Zjednoczonych, które zobowiązały się do przestrzegania zasad w okolicznościach, w których w przeciwnym wypadku takie przekazywanie danych nie spełniałoby norm UE w zakresie prawidłowego poziomu ochrony danych ze względu na znaczne różnice systemów ochrony prywatności po jednej i drugiej stronie Atlantyku.

---

1 W art. 25 i 26 dyrektywy o ochronie danych określa się ramy prawne dotyczące przekazywania danych osobowych z UE do państw trzecich spoza EOG.

2 Dodatkowe zasady określono w art. 13 decyzji ramowej 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, w zakresie, w jakim takie przekazywanie dotyczy danych osobowych przekazywanych lub udostępnianych przez jedno państwo członkowskie innemu państwu członkowskiemu, które następnie zamierza przekazać takie dane państwu trzeciemu lub instytucji międzynarodowej w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania lub do wykonywania sankcji karnych.

3 Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjęta 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.U. 215 z 28.8.2000, s. 7.

4 Powyższe stwierdzenie nie wyklucza stosowania wobec przetwarzania danych innych wymogów, które mogą obowiązywać na mocy przepisów krajowych wykonujących dyrektywę UE o ochronie danych.

5 Wpływ na przekazywanie danych przez państwa-strony Porozumienia EOG jest podobny, w następstwie rozszerzenia zakresu stosowania dyrektywy 95/46/WE o Porozumienie EOG, decyzja nr 83/1999 z dnia 25 czerwca 1999 r., Dz.U. L 296/41 z 23.11.2000.

Funkcjonowanie obecnych ustaleń w zakresie bezpiecznego transferu danych opiera się na zobowiązaniach i poświadczeniu zgodności uczestniczących przedsiębiorstw. Zobowiązanie się do przestrzegania przedmiotowych ustaleń jest dobrowolne, jednak zasady są wiążące dla tych, którzy takie zobowiązanie podejmują. Do podstawowych zasad przewidzianych w takich ustaleniach należą:

a) przejrzystość polityki ochrony prywatności przedsiębiorstw przestrzegających zasad,

b) włączenie zasad bezpiecznego transferu danych osobowych do polityki ochrony prywatności przedsiębiorstw, oraz

c) egzekwowanie, w tym przez organy publiczne.

Należy dokonać przeglądu zasadniczej podstawy bezpiecznego transferu danych w **nowym kontekście,** jakim są:

a) gwałtowny wzrost przepływów danych, które niegdyś miały charakter dodatkowy, jednak obecnie stanowią podstawowy element szybkiego wzrostu gospodarki cyfrowej oraz bardzo znacznych zmian w gromadzeniu, przetwarzaniu i wykorzystaniu danych,

b) kluczowe znaczenie przepływów danych w szczególności dla gospodarki transatlantyckiej[6],

c) szybko rosnąca liczba przedsiębiorstw w Stanach Zjednoczonych przestrzegających programu bezpiecznego transferu danych, która wzrosła ośmiokrotnie od roku 2004 (z 400 w 2004 r. do 3 246 w 2013 r.),

d) niedawno ujawnione informacje dotyczące amerykańskich programów nadzoru, które wzbudziły nowe wątpliwości dotyczące poziomu ochrony, który uznaje się za gwarantowany w ramach bezpiecznego transferu danych osobowych.

W tym kontekście w niniejszym komunikacie dokonuje się podsumowania funkcjonowania programu bezpiecznego transferu danych. Komunikat **opiera się na dowodach** zgromadzonych przez Komisję, pracach grupy kontaktowej UE-USA ds. ochrony prywatności prowadzonych w 2009 r., badaniu przeprowadzonym przez niezależnego wykonawcę w 2008 r.[7] oraz informacjach uzyskanych w ramach grupy roboczej UE-USA *ad hoc* („grupa robocza") ustanowionej w następstwie ujawnionych informacji na temat amerykańskich programów nadzoru (zob. *równoległy dokument*). Komunikat poprzedziły dwa **sprawozdania z oceny Komisji** dokonanej w początkowym okresie ustaleń w zakresie bezpiecznego transferu danych, odpowiednio w 2002 r.[8] i 2004 r.[9].

---

[6] Z niektórych badań wynika, że gdyby zaprzestano usług i transgranicznych przepływów danych wskutek braku ciągłości wiążących reguł korporacyjnych, wzorcowych klauzul umownych i bezpiecznego transferu danych, negatywny wpływ na PKB UE mógłby osiągnąć poziom od -0,8 % do -1,3 %, a eksport usług UE do Stanów Zjednoczonych zmalałby o -6,7 % wskutek utraty konkurencyjności. Zob. „The Economic Importance of Getting Data Protection Right", badanie z marca 2013 r. przeprowadzone dla Izby Handlowej Stanów Zjednoczonych przez Europejskie Centrum Międzynarodowej Ekonomii Politycznej (ECIPE – European Centre for International Political Economy).

[7] Analiza oceny skutków przeprowadzona w 2008 r. dla Komisji Europejskiej przez *Centre de Recherche Informatique et Droit* („CRID") Uniwersytetu w Namur.

[8] Dokument Służb Komisji „Stosowanie decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r. 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", SEC (2002) 196 z 13.12.2002.

[9] Dokument Służb Komisji „Wdrożenie decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r. 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", SEC (2004) 1323 z 20.10.2004.

2. STRUKTURA I FUNKCJONOWANIE BEZPIECZNEGO TRANSFERU DANYCH

2.1. Struktura bezpiecznego transferu danych

Przedsiębiorstwo w Stanach Zjednoczonych, które pragnie przestrzegać zasad bezpiecznego transferu danych osobowych musi: a) określić w swojej publicznie dostępnej polityce ochrony prywatności, że przestrzega zasad bezpiecznego transferu danych osobowych i faktycznie stosuje się do tych zasad, a także b) poświadczyć zgodność, tj. musi przedstawić Departamentowi Handlu Stanów Zjednoczonych deklarację zgodności z zasadami bezpiecznego transferu danych osobowych. Poświadczenie zgodności należy składać co rok. Zasady bezpiecznego transferu danych osobowych przedstawione w załączniku I do decyzji w sprawie zasad bezpiecznego transferu danych osobowych obejmują wymagania dotyczące zarówno ochrony danych osobowych (zasady integralności, bezpieczeństwa, wyboru i dalszego przekazywania danych), jak i praw procesowych osób, których dane dotyczą (zasady dotyczące ogłoszenia, dostępu i egzekwowania).

Jeżeli chodzi o egzekwowanie programu bezpiecznego transferu danych w Stanach Zjednoczonych, główną rolę odgrywają dwie instytucje Stanów Zjednoczonych: Departament Handlu Stanów Zjednoczonych i Federalna Komisja Handlu Stanów Zjednoczonych.

Departament Handlu dokonuje przeglądu wszystkich poświadczeń zgodności z zasadami bezpiecznego transferu danych oraz wszystkich odnawianych poświadczeń zgodności składanych co roku przez przedsiębiorstwa, aby upewnić się, czy zawierają one wszystkie elementy, jakich wymaga uczestnictwo w programie[10]. Departament Handlu aktualizuje wykaz przedsiębiorstw, które złożyły pisma w sprawie poświadczenia zgodności i publikuje przedmiotowy wykaz oraz pisma na swoich stronach internetowych. Ponadto Departament Handlu monitoruje funkcjonowanie programu bezpiecznego transferu danych i usuwa z wykazu przedsiębiorstwa, które nie stosują się do zasad.

W ramach swoich uprawnień w dziedzinie ochrony konsumentów zgodnie z sekcją 5 ustawy o Federalnej Komisji Handlu **Federalna Komisja Handlu** prowadzi interwencje w zakresie zwalczania nieuczciwych i wprowadzających w błąd praktyk. Działania Federalnej Komisji Handlu w zakresie egzekwowania obejmują dochodzenia dotyczące fałszywych oświadczeń zgodności z zasadami ochrony prywatności w ramach bezpiecznego transferu danych oraz dotyczące nieprzestrzegania przedmiotowych zasad przez przedsiębiorstwa uczestniczące w programie. W szczególnych przypadkach egzekwowania zgodności z zasadami bezpiecznego transferu danych od przewoźników lotniczych właściwym organem jest Departament Transportu Stanów Zjednoczonych[11].

Obecna decyzja w sprawie zasad bezpiecznego transferu danych osobowych stanowi element prawa UE, które muszą stosować organy państw członkowskich. Na mocy decyzji krajowe **organy ochrony danych** (OOD) UE w szczególnych przypadkach mają prawo do zawieszenia przekazywania danych przedsiębiorstwom, które poświadczyły zgodność z zasadami bezpiecznego transferu danych osobowych[12]. Komisja nie została powiadomiona o

---

[10] Jeżeli poświadczenie zgodności lub odnawiane poświadczenie przedsiębiorstwa nie spełnia wymogów bezpiecznego transferu danych, Departament Handlu powiadamia o tym dane przedsiębiorstwo, określając działania (np. przedstawienie wyjaśnień, wprowadzenie zmian w opisie polityki), jakie przedsiębiorstwo musi podąć, aby jego poświadczenie można było zatwierdzić.

[11] Na mocy tytułu 49 sekcji 41712 Kodeksu Stanów Zjednoczonych.

[12] A konkretnie, zawieszenia przekazywania danych można wymagać w dwóch sytuacjach, w których:
a) organ rządowy w Stanach Zjednoczonych ustalił, że przedsiębiorstwo narusza zasady bezpiecznego transferu danych osobowych lub
b) istnieje duże prawdopodobieństwo, że zasady bezpiecznego transferu danych osobowych są łamane; istnieje uzasadnione domniemanie, że mechanizm egzekwowania 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

żadnych przypadkach takiego zawieszenia przekazywania danych dokonanego przez krajowe organy ochrony danych od momentu ustanowienia zasad bezpiecznego transferu danych w 2000 r. Niezależnie od uprawnień przysługujących krajowym organom ochrony danych UE na mocy decyzji w sprawie zasad bezpiecznego transferu danych osobowych organy te posiadają kompetencje uprawniające do interwencji, w tym w przypadku międzynarodowego przekazywania danych, w celu zapewnienia zgodności z ogólnymi zasadami ochrony danych określonymi w dyrektywie o ochronie danych z 1995 r.

Jak przypomina się w obecnej decyzji w sprawie zasad bezpiecznego transferu danych osobowych, do **kompetencji Komisji** – działającej zgodnie z procedurą sprawdzającą ustanowioną w rozporządzeniu nr 182/2011 – należy dostosowanie decyzji, jej zawieszenie lub ograniczenie zakresu jej stosowania w dowolnym czasie, w świetle doświadczeń wynikających z jej wdrażania. Możliwość tę przewidziano w szczególności na wypadek wystąpienia błędu systemowego po stronie Stanów Zjednoczonych, jeżeli na przykład organ odpowiedzialny za zapewnienie zgodności z zasadami bezpiecznego transferu danych osobowych w Stanach Zjednoczonych nie spełnia swojej roli skutecznie, lub jeżeli wymogi prawa Stanów Zjednoczonych przewyższają poziom ochrony zapewniony w ramach zasad bezpiecznego transferu danych osobowych. Podobnie jak w przypadku innych decyzji Komisji decyzję można zmienić z innych powodów, a nawet uchylić.

2.2. Funkcjonowanie bezpiecznego transferu danych

Wśród 3246[13] **przedsiębiorstw, które poświadczyły zgodność,** znajdują się zarówno małe, jak i duże przedsiębiorstwa[14]. O ile zakres uprawnień Federalnej Komisji Handlu w zakresie przestrzegania prawa nie obejmuje usług finansowych ani branży telekomunikacyjnych, przez co są one wyłączone z zasad bezpiecznego transferu danych, to jednak wśród przedsiębiorstw, które poświadczyły zgodność, znajdują się przedstawiciele wielu sektorów przemysłu i usług, w tym szeroko rozpoznawalne przedsiębiorstwa internetowe i branże obejmujące usługi informatyczne i komputerowe aż po usługi w zakresie farmaceutyki, podróży i turystyki, opieki zdrowotnej lub kart kredytowych[15]. Należą do nich głównie przedsiębiorstwa amerykańskie świadczące usługi na rynku wewnętrznym UE. Ponadto takie przedsiębiorstwa obejmują jednostki zależne niektórych przedsiębiorstw UE, takich jak Nokia lub Bayer. 51 % przedsiębiorstw przetwarza dane pracowników z Europy przeniesionych do Stanów Zjednoczonych ze względów kadrowych[16].

Przekazywanie danych w ramach obecnego programu bezpiecznego transferu danych osobowych budzi **coraz większe obawy** wśród niektórych organów ochrony danych w UE. Niektóre organy ochrony danych państw członkowskich krytykują bardzo ogólny sposób sformułowania zasad oraz poleganie w znacznym stopniu na poświadczeniu zgodności i

---

szkody dla osób, których dane dotyczą; a właściwe władze państwa członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danego przedsiębiorstwa i umożliwienia mu udzielenia odpowiedzi.

13 W dniu 26 września 2013 r. liczba organizacji objętych programem bezpiecznego transferu danych wymienionych w wykazie uczestników bezpiecznego transferu danych ze statusem „**aktualny**" wyniosła **3246**, natomiast liczba organizacji o statusie „**nieaktualny**" – **935.**

14 Organizacje objęte programem bezpiecznego transferu danych, zatrudniające nie więcej niż 250 pracowników: 60 **%** (1925 z 3246). Organizacje objęte programem bezpiecznego transferu danych zatrudniające co najmniej 251 pracowników: **40 % (1295 z 3246).**

15 Przykładowo organizacja MasterCard zrzeszająca tysiące banków jest wyraźnym przykładem sytuacji, w której programu bezpiecznego transferu danych nie można zastąpić innymi instrumentami prawnymi w zakresie przekazywania danych osobowych, takimi jak wiążące reguły korporacyjne czy ustalenia umowne.

16 Organizacje uczestniczące w programie bezpiecznego transferu danych, których certyfikat zgodności z bezpiecznym transferem danych obejmuje dane o zasobach ludzkich organizacji (i które tym samym zgadzają się na współpracę z organami ochrony danych UE i na stosowanie się do ich warunków): **51 %** (1671 z 3246).

samoregulacji. Podobne obawy zgłosił przemysł, który odniósł się do przypadków zakłócenia konkurencji wynikającego z braku egzekwowania zasad.

Obecne ustalenia w zakresie bezpiecznego transferu danych osobowych opierają się na dobrowolnym przestrzeganiu zasad przez przedsiębiorstwa, poświadczeniu zgodności przez te przedsiębiorstwa i egzekwowaniu przez organy publiczne zobowiązań wynikających z poświadczenia zgodności. W tym kontekście brak przejrzystości i wszelkie niedociągnięcia w zakresie egzekwowania podważają podstawy, na których opiera się program bezpiecznego transferu danych.

Każda luka w przejrzystości lub egzekwowaniu po stronie Stanów Zjednoczonych powoduje przeniesienie odpowiedzialności na europejskie organy ochrony danych i przedsiębiorstwa korzystające z programu. W dniu 29 kwietnia 2010 r. niemieckie organy ochrony danych wydały decyzję, w której wezwały przedsiębiorstwa przekazujące dane z Europy do Stanów Zjednoczonych o aktywne kontrolowanie, czy przedsiębiorstwa importujące dane w Stanach Zjednoczonych faktycznie przestrzegają zasad bezpiecznego transferu danych osobowych i zaleciły, aby „przynajmniej przedsiębiorstwa eksportujące musiały ustalać, czy poświadczenie zgodności z zasadami bezpiecznego transferu danych osobowych wystawione przez importera jest nadal ważne”[17].

W dniu 24 lipca 2013 r. po ujawnieniu informacji na temat amerykańskich programów nadzoru, niemieckie organy ochrony danych wyraziły jeszcze poważniejsze obawy, stwierdzając, że „istnieje duże prawdopodobieństwo naruszania zasad określonych w decyzji Komisji”[18]. Istnieją przypadki, w których określony organ ochrony danych (np. OOD w Bremie) zwrócił się do przedsiębiorstwa przekazującego dane osobowe dostawcom ze Stanów Zjednoczonych o przekazanie informacji OOD w kwestii, czy dany dostawca zapobiega uzyskaniu dostępu do takich informacji przez Agencję Bezpieczeństwa Krajowego oraz informacji na temat sposobu zapobiegania takiemu dostępowi. Irlandzki organ ochrony danych zgłosił, że ostatnio wpłynęły do niego dwie skargi dotyczące programu bezpiecznego transferu danych w następstwie relacji mediów na temat programów agencji wywiadowczych Stanów Zjednoczonych, jednak odmówił on zbadania tych skarg, ponieważ przedmiotowe przekazanie danych osobowych państwu trzeciemu było zgodne z wymogami irlandzkich przepisów o ochronie danych. Po otrzymaniu podobnej skargi organ ochrony danych w Luksemburgu ustalił, że Microsoft i Skype przestrzegają luksemburskiej ustawy o ochronie danych, przekazując dane do Stanów Zjednoczonych[19]. Irlandzki Sąd Najwyższy po tych wydarzeniach uznał jednak wniosek o kontrolę sądową, w ramach którego zbada kwestię braku działania ze strony irlandzkiego Komisarza ds. Ochrony Danych w związku z amerykańskimi programami nadzoru. Jedną z dwóch skarg złożyła grupa studencka Europe v Facebook (EvF), która złożyła również podobną skargę przeciwko Yahoo w Niemczech, którą obecnie rozpatrują odpowiednie organy ochrony danych.

---

17 Zob. decyzja Düsseldorfer Kreis z 28/29 kwietnia 2010 r. Zob. Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich z 28/29 kwietnia 2010 r., w Hanowerze: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile. Na posiedzeniu w ramach dochodzenia Komisji Parlamentu Europejskiego – Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) – w dniu 7 października 2013 r. Europejski Inspektor Ochrony Danych (EIOD) Peter Hustinx wyraził jednak opinię, że, jeżeli chodzi o program bezpiecznego transferu danych, „dokonano znacznych usprawnień, a większość kwestii została już rozwiązana”. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf.

18 Zob. rezolucja niemieckiej konferencji komisarzy ochrony danych, w której podkreśla się, że usługi wywiadowcze stanowią poważne zagrożenie dla przesyłu danych między Niemcami a państwami spoza Europy: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870.

19 Zob. komunikat prasowy OOD z Luksemburga z dnia 18 listopada 2013 r.

Takie zróżnicowane reakcje organów zajmujących się ochroną danych na ujawnienie informacji dotyczących nadzoru świadczą o istnieniu faktycznego ryzyka fragmentacji programu bezpiecznego transferu danych osobowych i budzą wątpliwości co do zakresu egzekwowania programu.

3. PRZEJRZYSTOŚĆ POLITYKI OCHRONY PRYWATNOŚCI PRZEDSIĘBIORSTW PRZESTRZEGAJĄCYCH ZASAD

W oparciu o najczęściej zadawane pytanie 6 załączone do decyzji w sprawie zasad bezpiecznego transferu danych osobowych (załącznik II) przedsiębiorstwa zainteresowane poświadczeniem zgodności z zasadami bezpiecznego transferu danych muszą przedstawić swoją politykę ochrony prywatności Departamentowi Handlu i opublikować ją. Polityka prywatności musi zawierać zobowiązanie do przestrzegania zasad ochrony prywatności. Wymóg **upublicznienia polityki ochrony prywatności** przedsiębiorstw, które poświadczyły zgodność, oraz ich oświadczenia o przestrzeganiu zasad ochrony prywatności mają kluczowe znaczenie dla funkcjonowania programu.

Niewystarczający dostęp do polityki ochrony prywatności takich przedsiębiorstw działa na szkodę osób fizycznych, których dane osobowe są gromadzone i przetwarzane, oraz może stanowić **naruszenie zasady ogłoszenia**. W takich przypadkach osoby fizyczne, których dane są przekazywane z UE, mogą nie znać swoich praw ani obowiązków, których przedsiębiorstwo, które poświadczyło zgodność, musi przestrzegać.

Ponadto **Federalna Komisja Handlu jest uprawniona do egzekwowania przestrzegania zasad** ochrony prywatności od przedsiębiorstw, które zobowiązały się do przestrzegania tych zasad, w sytuacjach, w których przedsiębiorstwa te nie przestrzegają zasad, stosując nieuczciwe lub wprowadzające w błąd praktyki. Brak przejrzystości ze strony przedsiębiorstw w Stanach Zjednoczonych utrudnia Federalnej Komisji Handlu prowadzenie nadzoru oraz obniża skuteczność egzekwowania przestrzegania zasad.

Przez lata wiele przedsiębiorstw, które poświadczyły zgodność, nie upubliczniło swojej polityki ochrony prywatności lub nie przedstawiło publicznego oświadczenia o przestrzeganiu zasad ochrony prywatności. W sprawozdaniu dotyczącym bezpiecznego transferu danych z 2004 r. wskazano na konieczność przyjęcia przez Departament Handlu **bardziej aktywnej postawy w zakresie sprawdzania zgodności** z przedmiotowym wymogiem.

Od 2004 r. Departament Handlu opracował **nowe narzędzia informacyjne** służące udzielaniu pomocy przedsiębiorstwom w przestrzeganiu ich obowiązków w zakresie przejrzystości. Odpowiednie informacje na temat programu są dostępne na stronach internetowych Departamentu Handlu poświęconych bezpiecznemu transferowi danych[20], na których przedsiębiorstwa mogą również zamieszczać informacje o swojej polityce ochrony prywatności. Departament Handlu zgłosił, że przedsiębiorstwa korzystają z przedmiotowej funkcji i publikują informacje o swojej polityce ochrony prywatności na stronach internetowych Departamentu Handlu, ubiegając się o przystąpienie do programu bezpiecznego transferu danych[21]. Ponadto w latach 2009–2013 Departament Handlu opublikował szereg wytycznych dla przedsiębiorstw pragnących przystąpić do programu bezpiecznego transferu danych, takich jak „Przewodnik dotyczący poświadczenia zgodności”

[20] http://www.export.gov/SafeHarbour/
[21] https://SafeHarbour.export.gov/list.aspx

(ang. „Guide to Self-Certification") i „Przydatne wskazówki dotyczące zgodności z zasadami poświadczenia zgodności" (ang. „Helpful Hints on Self-Certifying Compliance")[22].

Poszczególne przedsiębiorstwa w różnym stopniu przestrzegają obowiązków w zakresie przejrzystości. Chociaż niektóre przedsiębiorstwa ograniczają się do zgłoszenia Departamentowi Handlu ich polityki ochrony prywatności w ramach procesu poświadczania zgodności, to jednak większość, oprócz opublikowania swojej polityki prywatności na stronach internetowych Departamentu Handlu, udostępnia ją na swoich stronach internetowych. Taka **polityka nie zawsze** jednak **zostaje przedstawiona w przyjaznej konsumentom i czytelnej formie**. Łącza do polityki ochrony prywatności nie zawsze działają prawidłowo oraz nie zawsze kierują do właściwych stron internetowych.

Z decyzji i jej załączników wynika, że wymóg, zgodnie z którym przedsiębiorstwa powinny publicznie ujawniać swoją politykę ochrony prywatności, wykracza **poza zwykłe powiadomienie** Departamentu Handlu o poświadczeniu zgodności. Wymogi dotyczące poświadczenia zgodności określone w „Najczęściej zadawanych pytaniach" obejmują opis polityki ochrony prywatności i przejrzyste informacje dotyczące miejsca, w którym została ona udostępniona do wglądu dla ogółu społeczeństwa[23]. Oświadczenia o polityce ochrony prywatności muszą być przejrzyste i łatwo dostępne dla ogółu społeczeństwa. Muszą one zawierać łącze do strony internetowej Departamentu Handlu poświęconej bezpiecznemu transferowi danych, zawierającej wykaz wszystkich „aktualnych" uczestników programu oraz łącze do informacji o podmiocie świadczącym usługi w zakresie pozasądowego rozstrzygania sporów. W latach 2000–2013 wiele przedsiębiorstw uczestniczących w programie nie spełniło przedmiotowych wymogów. W trakcie kontaktów roboczych z Komisją w lutym 2013 r. Departament Handlu przyznał, że nawet 10 % przedsiębiorstw, które poświadczyły zgodność, mogło w praktyce nie zamieścić na swoich publicznych stronach internetowych informacji dotyczących polityki prywatności zawierających oświadczenie potwierdzające przestrzeganie zasad bezpiecznego transferu danych osobowych.

Z ostatnich danych statystycznych wynika również, że ciągle utrzymuje się problem składania **fałszywych oświadczeń o uczestnictwie w programie bezpiecznego transferu danych**. Około 10 % przedsiębiorstw, które twierdzą, że są uczestnikami programu bezpiecznego transferu danych, nie zostało wymienionych w wykazie prowadzonym przez Departament Handlu jako aktualni uczestnicy programu[24]. Takie fałszywe oświadczenia składają zarówno przedsiębiorstwa, które nigdy nie były uczestnikami programu bezpiecznego transferu danych, jak i przedsiębiorstwa, które w przeszłości przystąpiły do programu, jednak nie składały corocznie poświadczeń zgodności w Departamencie Handlu. W takim przypadku przedsiębiorstwa nadal widnieją w wykazie opublikowanym na stronie internetowej poświęconej programowi bezpiecznego transferu danych, jednak ich poświadczenie zgodności posiada status „nieaktualne", co oznacza, że przedsiębiorstwo było uczestnikiem programu, a zatem ma obowiązek nadal zapewniać ochronę danych już przetworzonych. Federalna Komisja Handlu jest organem właściwym do interweniowania w przypadkach stosowania praktyk wprowadzających w błąd oraz braku zgodności z zasadami bezpiecznego

[22] Przewodnik jest dostępny na stronie internetowej programu pod adresem: http://export.gov/SafeHarbour/Przydatne wskazówki: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

[23] W dniu 12 listopada 2013 r. Departament Handlu potwierdził, że „Obecnie przedsiębiorstwa, które posiadają publiczne strony internetowe i zabezpieczają dane dotyczące konsumentów/klientów/odwiedzających", muszą na swoich stronach internetowych opublikować politykę ochrony prywatności zgodną z zasadami bezpiecznego transferu danych osobowych" (dokument „U.S.-EU Cooperation to Implement the Safe Harbor Framework" z dnia 12 listopada 2013 r.).

[24] We wrześniu 2013 r. australijska firma konsultingowa Galexia porównała liczbę „fałszywych oświadczeń" o uczestnictwie w programie bezpiecznego transferu danych w 2008 r. i w 2013 r. W drodze powyższego porównania ustalono w szczególności, że wzrostowi liczby uczestników programu, jaki dokonał się w latach 2008–2013 (z 1 109 do 3 246) towarzyszył wzrost liczby fałszywych oświadczeń z 206 do 427. http://www.galexia.com/public/about/news/about_news-id225.html.

transferu danych osobowych (zob. sekcja 5.1). Brak przejrzystości w kwestii „fałszywych oświadczeń" wpływa na wiarygodność programu.

Komisja Europejska ostrzegała Departament Handlu w ramach regularnych kontaktów w latach 2012 i 2013, że przedstawienie przez przedsiębiorstwa opisu ich polityki ochrony prywatności jedynie Departamentowi Handlu nie jest wystarczające do dopełnienia przez nie obowiązków w zakresie przejrzystości. Oświadczenia o polityce ochrony prywatności należy podać do publicznej wiadomości. Departament Handlu wezwano również do **intensyfikacji prowadzonych przezeń okresowych kontroli stron internetowych przedsiębiorstw**, które następują po procedurze weryfikacji przeprowadzanej w kontekście procesu pierwszego poświadczenia zgodności lub jego corocznego odnawiania, oraz do podjęcia działań wobec przedsiębiorstw, które nie przestrzegają wymogów w zakresie przejrzystości.

Pierwszą reakcją na obawy UE było **wprowadzenie od marca 2013 r. przez Departament Handlu** wobec przedsiębiorstwa uczestniczącego w programie bezpiecznego transferu danych i posiadającego publiczną stronę internetową **obowiązku** zapewnienia na swojej publicznej stronie internetowej łatwego dostępu do informacji na temat jego polityki ochrony prywatności w zakresie danych dotyczących konsumentów/użytkowników. Jednocześnie Departament Handlu zaczął zawiadamiać wszystkie przedsiębiorstwa, których informacje dotyczące polityki ochrony prywatności nie zawierały jeszcze łącza do strony internetowej Departamentu Handlu poświęconej programowi bezpiecznego transferu danych, o konieczności dodania takiego łącza, dzięki któremu konsumenci odwiedzający stronę internetową przedsiębiorstwa mogą uzyskać bezpośredni dostęp do oficjalnego wykazu przedsiębiorstw przestrzegających zasad bezpiecznego transferu danych osobowych oraz do strony internetowej poświęconej programowi. Dzięki temu osoby w Europie, których dane dotyczą, będą mogły bezpośrednio, bez dodatkowego wyszukiwania w internecie, zweryfikować zobowiązania przedsiębiorstwa przedłożone Departamentowi Handlu. Ponadto Departament Handlu zaczął zawiadamiać przedsiębiorstwa, że opublikowane przez nie informacje dotyczące polityki ochrony prywatności powinny obejmować dane kontaktowe ich niezależnego podmiotu świadczącego usługi w zakresie rozstrzygania sporów[25].

Proces ten **należy przyspieszyć**, aby wszystkie przedsiębiorstwa, które poświadczyły zgodność, w pełnym zakresie spełniły wymogi dotyczące bezpiecznego transferu danych najpóźniej do marca 2014 r. (tj. przed upływem terminu, w którym przedsiębiorstwa muszą dokonać corocznego ponownego poświadczenia zgodności, licząc od wprowadzenia nowych wymogów w marcu 2013 r.).

Pozostają jednak wątpliwości, czy wszystkie przedsiębiorstwa, które poświadczyły zgodność, w pełni przestrzegają wymogów w zakresie przejrzystości. Departament Handlu powinien bardziej skrupulatnie monitorować i badać zgodność z przedmiotowymi obowiązkami zapewnianą na etapie wstępnego poświadczenia zgodności lub jego corocznego odnawiania.

[25] W okresie między marcem a wrześniem 2013 r. Departament Handlu:
• powiadomił 101 przedsiębiorstw, *które opublikowały już informacje o swojej polityce ochrony prywatności zgodną z zasadami bezpiecznego transferu danych osobowych na stronie internetowej dotyczącej programu bezpiecznego transferu danych*, że muszą one opublikować takie informacje o swojej politykę ochrony prywatności również na swoich stronach internetowych;
• powiadomił 154 przedsiębiorstwa, które jeszcze tego nie dokonały, że w informacjach o swojej polityce ochrony prywatności muszą zawrzeć łącze do strony internetowej dotyczącej programu bezpiecznego transferu danych;
• powiadomił ponad 600 przedsiębiorstw, że w informacjach o swojej polityce ochrony prywatności powinny zawrzeć dane kontaktowe ich niezależnego podmiotu świadczącego usługi w zakresie rozstrzygania sporów.

4. WŁĄCZENIE ZASAD BEZPIECZNEGO TRANSFERU DANYCH OSOBOWYCH DO POLITYKI OCHRONY PRYWATNOŚCI PRZEDSIĘBIORSTW

Aby uzyskać i utrzymać korzyści płynące z uczestnictwa w programie bezpiecznego transferu danych, przedsiębiorstwa, które poświadczyły zgodność, muszą przestrzegać zasad bezpiecznego transferu danych osobowych, określonych w załączniku I do decyzji.

W sprawozdaniu z 2004 r. Komisja ustaliła, że znaczna liczba **przedsiębiorstw nie włączyła w prawidłowy sposób zasad bezpiecznego transferu danych osobowych** do ich polityki przetwarzania danych. Przykładowo osobom fizycznym nie zawsze udzielano wyraźnych i przejrzystych informacji dotyczących celów przetwarzania ich danych lub nie dawano im możliwości rezygnacji w przypadku gdy ich dane miały być ujawnione stronie trzeciej lub wykorzystane do celu niezgodnego z celami, do których zostały pierwotnie uzyskane. W sprawozdaniu Komisji z 2004 r. uznano, że Departament Handlu „powinien przyjąć bardziej aktywną postawę w kwestii dostępu do bezpiecznego transferu danych osobowych i wiedzy na temat zasad”[26].

Poczyniono ograniczony postęp w tym zakresie. Od dnia 1 stycznia 2009 r. polityka ochrony prywatności każdego przedsiębiorstwa dążącego do odnowienia statusu swojego poświadczenia zgodności z zasadami bezpiecznego transferu danych osobowych, które musi zostać odnowione co roku, jest oceniana przez Departament Handlu przed takim odnowieniem. Zakres przedmiotowej oceny jest jednak ograniczony. Nie dokonuje się **pełnej oceny faktycznej praktyki** stosowanej przez przedsiębiorstwa, które poświadczyły zgodność, co w znacznym stopniu zwiększyłoby wiarygodność procesu poświadczenia zgodności.

Ponadto w odpowiedzi na wezwanie Komisji, aby Departament Handlu bardziej rygorystycznie i systematycznie nadzorował przedsiębiorstwa, które poświadczyły zgodność, **obecnie uważniej przetwarza się nowe wnioski**. W latach 2010–2013 znacznie wzrosła liczba nowych wniosków, których nie zaakceptowano, lecz odesłano przedsiębiorstwom, aby te wprowadziły poprawki do polityki ochrony prywatności: w przypadku przedsiębiorstw odnawiających poświadczenie zgodności liczba ta uległa podwojeniu, a w przypadku przedsiębiorstwo ubiegających się o przystąpienie do programu bezpiecznego transferu danych, potrojeniu[27]. Departament Handlu zapewnił Komisję, że proces poświadczania zgodności lub ponownego poświadczania zgodności można uznać za zakończony wyłącznie, jeżeli polityka ochrony prywatności danego przedsiębiorstwa spełnia wszystkie wymogi, w szczególności jeżeli obejmuje zobowiązanie do przestrzegania odpowiedniego zbioru zasad bezpiecznego transferu danych osobowych i jeżeli została podana do publicznej wiadomości. Przedsiębiorstwo ma obowiązek wskazać w swojej ewidencji wykazów bezpiecznego transferu danych, gdzie została przedstawiona odpowiednia polityka. Przedsiębiorstwo musi również wyraźnie wskazać na swoich stronach internetowych podmiot świadczący usługi w zakresie pozasądowego rozstrzygania sporów oraz umieścić łącze do poświadczenia zgodności z zasadami bezpiecznego transferu danych osobowych, znajdującego się na stronach internetowych Departamentu Handlu. Szacuje się jednak, że ponad 30 %

[26] Zob. s. 8 sprawozdania z 2004 r. SEC (2004) 1323.

[27] Z danych statystycznych przedstawionych przez Departament Handlu we wrześniu 2013 r. wynika, że w 2010 r. Departament Handlu powiadomił 18 % (93) z 512 przedsiębiorstw, które po raz pierwszy potwierdziły zgodność z zasadami, i 16 % (231) z 1 417 przedsiębiorstw, które po raz kolejny potwierdziły zgodność z zasadami, o konieczności wprowadzenia przez nie poprawek w ich polityce ochrony prywatności lub we wnioskach o uczestnictwo w programie bezpiecznego transferu danych W ramach działań następczych, w związku z wnioskami Komisji o prowadzenie ścisłego, należytego i systematycznego nadzoru w zakresie wszystkich przedkładanych wniosków, w połowie września 2013 r. Departament Handlu wysłał jednak powiadomienie do 56 % (340) z 602 przedsiębiorstw, które po raz pierwszy potwierdziły zgodność z zasadami, i 27 % (493) z 1 809 przedsiębiorstw, które po raz kolejny potwierdziły zgodność z zasadami, wzywając je do wprowadzenia poprawek w ich polityce ochrony prywatności.

uczestników programu bezpiecznego transferu danych nie podaje informacji dotyczących rozstrzygania sporów w polityce ochrony prywatności na swoich stronach internetowych[28].

Większość przedsiębiorstw usuniętych przez Departament Handlu z wykazu bezpiecznego transferu danych została usunięta na swoje wyraźne żądanie (np. przedsiębiorstw, które dokonały fuzji lub zostały przejęte, zmieniły branżę lub zaprzestały działalności). Mniejszą liczbę rejestrów dotyczących przedsiębiorstw, które nie są już uczestnikami, usunięto, kiedy okazało się, że strony internetowe podane w rejestrach nie działały, a poświadczenia zgodności przedsiębiorstw od lat miały status „nieaktualne"[29]. Co ważne, wydaje się, że żadnego takiego usunięcia nie dokonano wskutek wykrycia problemów w zakresie zgodności w ramach weryfikacji przeprowadzonej przez Departament Handlu.

Wykaz bezpiecznego transferu danych pełni rolę ogłoszenia publicznego oraz rejestru zobowiązań danego przedsiębiorstwa w zakresie zasad bezpiecznego transferu danych osobowych. **Zobowiązanie do przestrzegania zasad bezpiecznego transferu danych osobowych nie jest ograniczone w czasie** w odniesieniu do danych uzyskanych w okresie, w którym dane przedsiębiorstwo czerpało korzyści z bezpiecznego transferu danych, w związku z czym dane przedsiębiorstwo musi nadal stosować zasady wobec takich danych przez cały okres ich przechowywania, wykorzystywania lub ujawniania, nawet jeżeli z jakiejkolwiek przyczyny nie uczestniczy już w programie bezpiecznego transferu danych.

Liczba **wnioskodawców** występujących o uczestnictwo w programie bezpiecznego transferu danych, **którzy zostali odrzuceni w wyniku kontroli administracyjnej** Departamentu Handlu, a zatem których nigdy nie dodano do wykazu bezpiecznego transferu danych, jest następująca: **w 2010 r.** jedynie **6 %** (33) z 513 przedsiębiorstw, które złożyły swoje pierwsze poświadczenie, nigdy nie włączono do wykazu, ponieważ nie spełniały norm Departamentu Handlu w odniesieniu do poświadczenia zgodności. W **2013 r. 12 %** (75) z 605 przedsiębiorstw, które złożyły swoje pierwsze poświadczenie, nigdy nie włączono do wykazu, ponieważ nie spełniały norm Departamentu Handlu w odniesieniu do poświadczenia zgodności.

Aby zwiększyć przejrzystość nadzoru, Departament Handlu powinien co najmniej zamieścić na swoich stronach internetowych wykaz wszystkich przedsiębiorstw, które usunięto z programu bezpiecznego transferu danych, i podać przyczyny, dla których nie odnowiono poświadczenia zgodności. Oznaczenie „nieaktualny" w prowadzonym przez Departament Handlu wykazie przedsiębiorstw będących uczestnikami programu bezpiecznego transferu danych nie należy traktować jedynie jako informacji, lecz należy umieścić przy nim **wyraźne ostrzeżenie** – zarówno werbalne, jak i graficzne – że dane przedsiębiorstwo obecnie nie spełnia wymogów bezpiecznego transferu danych.

Ponadto niektórym przedsiębiorstwom nadal nie udaje się w pełni wprowadzić wszystkich zasad bezpiecznego transferu danych osobowych. Polityka ochrony prywatności przedsiębiorstw, które poświadczyły zgodność, poza brakiem przejrzystości, o którym mowa w sekcji 3 powyżej, nie jest też często przejrzysta w odniesieniu do celów gromadzenia danych oraz prawa wyboru, czy dane mogą zostać ujawnione osobom trzecim, co budzi wątpliwości pod względem zgodności z zasadami „ogłoszenia" i „wyboru" w zakresie

[28] Wystąpienie Chrisa Connolly'ego (Galexia) na posiedzeniu w ramach dochodzenia prowadzonego przez Komisję LIBE Parlamentu Europejskiego w dniu 7 października 2013 r.

[29] Od grudnia 2011 r. Departament Handlu Stanów Zjednoczonych usunął z wykazu bezpiecznego transferu danych 323 przedsiębiorstwa: 94 przedsiębiorstwa zostały usunięte, ponieważ zakończyły swoją działalność; 88 przedsiębiorstw – ze względu na przejęcie lub fuzję, 95 – na wniosek spółki dominującej; 41 przedsiębiorstw – ze względu na kolejne niezłożenie wniosku o ponowną certyfikację oraz 5 przedsiębiorstw – z różnych przyczyn.

ochrony prywatności. Ogłoszenie i wybór są niezbędnymi atrybutami, umożliwiającymi osobom, których dane dotyczą, kontrolę nad tym, co dzieje się z ich danymi osobowymi.

Podstawowy pierwszy etap procesu potwierdzania zgodności, tj. włączenie zasad bezpiecznego transferu danych osobowych do polityki ochrony prywatności przedsiębiorstw, nie jest zapewniony w wystarczającym stopniu. Departament Handlu powinien potraktować tę kwestię priorytetowo, opracowując metodykę wprowadzania zgodności w ramach praktyki operacyjnej przedsiębiorstw i ich kontaktów z klientami. **Departament Handlu musi aktywnie monitorować skuteczne włączanie zasad bezpiecznego transferu danych osobowych do polityki ochrony prywatności przedsiębiorstw**, a nie podejmować działania w zakresie egzekwowania zasad dopiero w momencie wpłynięcia skarg od osób fizycznych.

5. EGZEKWOWANIE PRZEZ ORGANY PUBLICZNE

Dostępnych jest szereg mechanizmów służących zapewnieniu skutecznego wykonania programu bezpiecznego transferu danych oraz prawa odwołania się osób fizycznych w przypadkach, w których brak zgodności z zasadami ochrony prywatności wpływa na ochronę ich danych osobowych.

Zgodnie z zasadą „egzekwowania" polityka ochrony prywatności organizacji, które poświadczyły zgodność, musi obejmować skuteczny mechanizm zgodności. Zgodnie z zasadą „egzekwowania" ochrony prywatności, bardziej szczegółowo wyjaśnioną w Najczęściej zadawanych pytaniach 11, 5 i 6, wymóg ten można spełnić, stosując niezależne **mechanizmy odwoławcze**, których kompetencje do rozpatrywania indywidualnych skarg dotyczących nieprzestrzegania zasad zostały podane do wiadomości publicznej. Można to osiągnąć również w ramach zobowiązania się organizacji do współpracy z **grupą UE ds. ochrony danych**[30]. Ponadto przedsiębiorstwa, które poświadczyły zgodność, podlegają jurysdykcji Federalnej Komisji Handlu na mocy sekcji 5 ustawy o Federalnej Komisji Handlu, w której zabrania się nieuczciwych lub wprowadzających w błąd działań lub praktyk w handlu lub wpływających na handel[31].

W sprawozdaniu z 2004 r. wyrażono obawy dotyczące egzekwowania zasad programu bezpiecznego transferu danych, a konkretnie stwierdzono, że Federalna Komisja Handlu powinna aktywniej wszczynać dochodzenia i informować osoby fizyczne o ich prawach. Obawy wzbudził również brak przejrzystości w kwestii kompetencji Federalnej Komisji Handlu w zakresie egzekwowania zasad dotyczących danych o zasobach ludzkich.

Do organu odwoławczego odpowiedzialnego za dane o zasobach ludzkich – grupa UE ds. ochrony danych – wpłynęła jedna skarga dotycząca danych o zasobach ludzkich[32]. Brak skarg

---

[30] Grupa UE ds. ochrony danych jest organem właściwym do badania i rozstrzygania skarg wnoszonych przez osoby fizyczne, dotyczących domniemanego naruszenia zasad bezpiecznego transferu danych osobowych przez przedsiębiorstwo ze Stanów Zjednoczonych będące uczestnikiem programu bezpiecznego transferu danych osobowych. Przedsiębiorstwa, które poświadczają, że przestrzegają zasad bezpiecznego transferu danych osobowych, muszą dokonać wyboru między przestrzeganiem zasad niezależnego mechanizmu ochrony prawnej a współpracą z grupą UE ds. ochrony danych w celu rozwiązywania problemów powstających wskutek nieprzestrzegania zasad bezpiecznego transferu danych osobowych. Współpraca z grupą UE ds. ochrony danych jest jednak obowiązkowa w sytuacji, w której przedsiębiorstwo ze Stanów Zjednoczonych przetwarza dane osobowe o zasobach ludzkich przekazywane z UE w kontekście stosunku pracy. Jeżeli przedsiębiorstwo zobowiązuje się do współpracy z grupą UE, musi ono również zobowiązać się do stosowania się do porad udzielanych przez grupę UE, jeżeli grupa uzna, że przedsiębiorstwo musi podjąć szczególne działania w celu przestrzegania zasad bezpiecznego transferu danych osobowych, włącznie ze stosowaniem środków zaradczych albo odszkodowawczych.

[31] Departament Transportu posiada podobne uprawnienia wobec przewoźników lotniczych na mocy tytułu 49 Kodeksu Stanów Zjednoczonych, sekcja 41712.

[32] Ponieważ skargę wniósł obywatel Szwajcarii, grupa UE ds. ochrony danych przekazała skargę szwajcarskiemu organowi ochrony danych (Stany Zjednoczone posiadają oddzielny program bezpiecznego transferu danych dla Szwajcarii).

nie pozwala jednak wyciągnąć wniosku, czy program funkcjonuje w pełnym zakresie. Należy wprowadzić urzędowe kontrole przestrzegania zasad przez przedsiębiorstwa w celu weryfikacji faktycznego wykonania zobowiązań w zakresie ochrony danych. Organy ochrony danych UE powinny również prowadzić działania służące informowaniu o istnieniu grupy.

Wskazywano na problemy dotyczące sposobu funkcjonowania alternatywnych mechanizmów ochrony prawnej jako organów egzekwowania prawa. Szereg takich organów nie dysponuje odpowiednimi środkami służącymi rozwiązywaniu spraw dotyczących nieprzestrzegania zasad. Należy wyeliminować przedmiotowe niedociągnięcie.

5.1. Federalna Komisja Handlu

Federalna Komisja Handlu może podejmować środki egzekucyjne w przypadku naruszenia zobowiązań podjętych przez przedsiębiorstwa w zakresie zasad bezpiecznego transferu danych osobowych. W momencie ustanowienia programu bezpiecznego transferu danych Federalna Komisja Handlu podjęła się rozpatrywania na zasadzie pierwszeństwa wniosków wpływających od organów państw członkowskich UE[33]. Ponieważ przez pierwsze dziesięć lat obowiązywania umowy nie wpłynęły żadne skargi, Federalna Komisja Handlu postanowiła podjąć starania w kierunku określenia wszystkich naruszeń zasad bezpiecznego transferu danych osobowych w każdym prowadzonym przez siebie dochodzeniu dotyczącym ochrony prywatności i bezpieczeństwa danych. Od 2009 r. Federalna Komisja Handlu podjęła działania egzekwujące przepisy w 10 sprawach przeciwko przedsiębiorstwom na podstawie naruszenia zasad bezpiecznego transferu danych osobowych. Sprawy te przeważnie kończyły się poleceniami zawarcia ugody – obejmującymi znaczne kary – w których zabrania się świadomego wprowadzania w błąd w odniesieniu do ochrony prywatności, w tym co do zgodności z zasadami bezpiecznego transferu danych osobowych, oraz obejmuje się przedsiębiorstwa kompleksowymi programami ochrony prywatności i audytami na 20 lat. Na żądanie Federalnej Komisji Handlu przedsiębiorstwa muszą zgodzić się na niezależną ocenę ich programów ochrony prywatności. Sprawozdania z takich ocen są regularnie przedstawiane Federalnej Komisji Handlu. W nakazach Federalnej Komisji Handlu zabrania się również takim przedsiębiorstwom świadomego wypaczania ich praktyk w zakresie ochrony prywatności i ich uczestnictwa w programie bezpiecznego transferu danych lub podobnych programach ochrony prywatności. Miało to miejsce przykładowo w przypadku dochodzeń Federalnej Komisji Handlu przeciwko Google, Facebook i Myspace[34]. W 2012 przedsiębiorstwo Google zgodziło się uiścić karę w wysokości 22,5 mln USD w ramach rozstrzygnięcia sprawy dotyczącej zarzutów naruszenia wymogu udzielenia zgody. We wszystkich dochodzeniach dotyczących ochrony prywatności Federalna Komisja Handlu z urzędu bada kwestię, czy doszło do naruszenia zasad bezpiecznego transferu danych osobowych.

Federalna Komisja Handlu powtórzyła ostatnio swoje deklaracje i zobowiązanie do rozpatrywania na zasadzie pierwszeństwa wszystkich wniosków wpływających od instytucji

---

33 Zob. załącznik V do decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r.

34 W latach 2009–2012 Federalna Komisja Handlu przeprowadziła dziesięć spraw związanych z egzekwowaniem zobowiązań w zakresie zasad bezpiecznego transferu danych osobowych: Federalna Komisja Handlu przeciwko Javianowi Karnaniemu, i Balls of Kryptonite, LLC (2009 r.), World Innovators, Inc. (2009 r.), Expat Edge Partners, LLC (2009 r.), Onyx Graphics, Inc. (2009 r.), Directors Desk LLC (2009 r.), Progressive Gaitways LLC (2009 r.), Collectify LLC (2009 r.), Google Inc. (2011 r.), Facebook, Inc. (2011 r.), Myspace LLC (2012 r.). Zob. „Federal Trade Commission of Safe Harbour Commitments": http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Zob. również: „Case Highlights": http://business.ftc.gov/us-eu-Safe-Harbour-framework. Większość przedmiotowych spraw dotyczyła problemów związanych z przedsiębiorstwami, które przystąpiły do programu bezpiecznego transferu danych osobowych i nadal podawały się za uczestników programów, mimo że nie dokonały corocznego odnowienia poświadczenia zgodności.

samoregulujących ochronę prywatności oraz państw członkowskich UE podnoszących zarzuty nieprzestrzegania zasad bezpiecznego transferu danych osobowych przez dane przedsiębiorstwo[35]. W ciągu ostatnich trzech lat do Federalnej Komisji Handlu wpłynęło jedynie kilka wniosków ze strony europejskich organów ochrony danych.

W ostatnich miesiącach zaczęto rozwijać współpracę transatlantycką między organami ochrony danych. Przykładowo w dniu 26 czerwca 2013 r. Federalna Komisja Handlu zawarła z Biurem Komisarza ds. Ochrony Danych Irlandii protokół ustaleń dotyczących wzajemnej pomocy w egzekwowaniu praw zapewniających ochronę danych osobowych w sektorze prywatnym. Protokół ustaleń stanowi ramy na rzecz większej, usprawnionej i skuteczniejszej współpracy w zakresie egzekwowania przepisów dotyczących ochrony prywatności[36].

W sierpniu 2013 r. Federalna Komisja Handlu zapowiedziała dalsze wzmocnienie kontroli przedsiębiorstw kontrolujących duże bazy danych osobowych. Federalna Komisja Handlu utworzyła również portal, za pośrednictwem którego konsumenci mogą złożyć skargę dotyczącą ochrony prywatności na przedsiębiorstwo działające w Stanach Zjednoczonych[37].

Federalna Komisja Handlu powinna również zwiększyć starania na rzecz badania fałszywych oświadczeń o przestrzeganiu zasad bezpiecznego transferu danych osobowych. Przedsiębiorstwo, które na swoich stronach internetowych zamieszcza oświadczenie, że przestrzega wymogów zasad bezpiecznego transferu danych osobowych, ale które nie widnieje w wykazie prowadzonym przez Departament Handlu jako „aktualny" uczestnik programu, wprowadza konsumentów w błąd i nadużywa ich zaufania. Fałszywe oświadczenia zmniejszają wiarygodność systemu jako całości, a zatem należy je niezwłocznie usunąć ze stron internetowych przedsiębiorstw. Przedsiębiorstwa powinny być związane możliwym do wyegzekwowania zakazem wprowadzania konsumentów w błąd. Federalna Komisja Handlu powinna nadal prowadzić starania na rzecz identyfikacji fałszywych oświadczeń, takich jak oświadczenie w sprawie *Karnaniego*, w której Federalna Komisja Handlu zlikwidowała stronę internetową w Kalifornii w odpowiedzi na zamieszczone na niej fałszywe oświadczenie o rejestracji w programie bezpiecznego transferu danych oraz prowadzone za jej pośrednictwem oszukańcze praktyki w zakresie handlu elektronicznego ukierunkowane na europejskich konsumentów[38].

W dniu 29 października 2013 r. Federalna Komisja Handlu ogłosiła, że wszczęła „szereg dochodzeń dotyczących przestrzegania zasad bezpiecznego transferu danych osobowych w ostatnich miesiącach" oraz że „w nadchodzących miesiącach" można oczekiwać większej liczby działań w zakresie egzekwowania zasad. Federalna Komisja Handlu potwierdziła również, że „zobowiązuje się do szukania sposobów na poprawę skuteczności swoich działań" oraz że będzie nadal z zadowoleniem przyjmować wszystkie istotne wskazówki, takie jak skarga, którą w ostatnim miesiącu złożył rzecznik praw konsumenta z siedzibą w Europie, zarzucając szereg naruszeń związanych z zasadami bezpiecznego transferu danych osobowych"[39]. Agencja zobowiązała się również do „systematycznego monitorowania

---

35 Przedmiotowe zobowiązanie ponowiła komisarz Julie Brill z Federalnej Komisji Handlu na spotkaniu z organami ochrony danych UE (Grupą Roboczą Art. 29) w Brukseli w dniu 17 kwietnia 2013 r.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n.

37 Konsumenci mogą składać swoje skargi za pośrednictwem Trade Commission Complaint Assistant (https://www.ftccomplaintassistant.gov/), natomiast konsumenci międzynarodowi mogą składać skargi za pośrednictwem econsumer.gov (http://www.econsumer.gov).

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf.

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf oraz http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf.

przestrzegania nakazów w zakresie bezpiecznego transferu danych, co czynimy w przypadku wszystkich nakazów, które wydajemy”[40].

W dniu 12 listopada 2013 r. Federalna Komisja Handlu poinformowała Komisję Europejską, że „**jeżeli w polityce ochrony prywatności prowadzonej przez dane przedsiębiorstwo składa obietnicę ochrony w ramach bezpiecznego transferu danych, to w takiej sytuacji sam brak rejestracji lub jej utrzymania ze strony danego przedsiębiorstwa nie może zwolnić takiego przedsiębiorstwa z egzekwowania przez Federalną Komisję Handlu przedmiotowych zobowiązań w zakresie zasad bezpiecznego transferu danych osobowych**”[41].

W listopadzie 2013 r. Departament Handlu poinformował Komisję Europejską, że „w ramach działania mającego na celu dopilnowanie, aby przedsiębiorstwa nie przedstawiały »fałszywych oświadczeń« o uczestnictwie w programie bezpiecznego transferu danych, Departament Handlu będzie kontaktować się z uczestnikami programu bezpiecznego transferu danych na miesiąc przed datą ponownego poświadczenia zgodności, aby zapoznać ich z działaniami, jakie muszą podjąć, gdyby zdecydowali się nie odnawiać poświadczenia zgodności”. **Departament Handlu „uprzedzi przedsiębiorstwa** należące do tej kategorii, że muszą one usunąć wszystkie odniesienia do uczestnictwa w programie bezpiecznego transferu danych, co dotyczy również stosowania znaku poświadczenia zgodności bezpiecznego transferu danych osobowych Departamentu Handlu, z polityki ochrony prywatności i stron internetowych przedsiębiorstwa, **oraz wyraźnie da im do zrozumienia, że w stosunku do przedsiębiorstw, które tego nie uczynią, Federalna Komisja Handlu może podjąć kroki prawne”[42].**

Do celów zwalczania fałszywych oświadczeń o uczestnictwie w programie bezpiecznego transferu danych informacja o polityce ochrony prywatności umieszczana na stronach internetowych przedsiębiorstw, które dokonały poświadczenia zgodności, powinna zawsze zawierać łącze do strony internetowej Departamentu Handlu dotyczącej programu bezpiecznego transferu danych, zawierającej wykaz wszystkich „aktualnych” uczestników programu. Dzięki temu osoby w Europie, których dane dotyczą, będą mogły od razu sprawdzić, bez dodatkowego wyszukiwania w internecie, czy dane przedsiębiorstwo jest aktualnie uczestnikiem tego programu. Od marca 2013 r. Departament Handlu wymaga od przedsiębiorstw umieszczania takiego łącza, jednak proces ten należy zintensyfikować.

Kluczowym priorytetem do celów zapewnienia prawidłowego i skutecznego funkcjonowania programu jest w dalszym ciągu prowadzenie przez Federalną Komisję Handlu stałego monitorowania i późniejszego egzekwowania faktycznego przestrzegania zasad bezpiecznego transferu danych osobowych jako uzupełnienie wyżej przedstawionych środków podejmowanych przez Departament Handlu. W szczególności konieczne jest nasilenie **kontroli i dochodzeń z urzędu dotyczących przestrzegania przez przedsiębiorstwa** zasad bezpiecznego transferu danych osobowych. Należy również w większym stopniu uprościć przekazywanie skarg w sprawie naruszeń do Federalnej Komisji Handlu.

[40] Pismo przewodniczącej Federalnej Komisji Handlu Edith Ramirez do wiceprzewodniczącej Viviane Reding.
[41] Pismo przewodniczącej Federalnej Komisji Handlu Edith Ramirez do wiceprzewodniczącej Viviane Reding.
[42] „U.S.-EU Cooperation to Implement the Safe Harbor Framework”, 12 listopada 2013 r.

5.2. Grupa UE ds. ochrony danych

Grupa UE ds. ochrony danych jest organem ustanowionym na mocy decyzji w sprawie zasad bezpiecznego transferu danych osobowych. Grupa posiada kompetencje do badania skarg wniesionych przez osoby fizyczne dotyczących danych osobowych zgromadzonych w kontekście stosunku pracy oraz spraw dotyczących przedsiębiorstw, które dokonały poświadczenia zgodności i które wybrały taki sposób rozstrzygania sporów w ramach programu bezpiecznego transferu danych (53 % wszystkich przedsiębiorstw). Grupa składa się z przedstawicieli różnych organów ochrony danych UE.

Do tej pory do grupy wpłynęły cztery skargi (dwie w 2010 r. i dwie w 2013 r.). Grupa przekazała dwie skargi w 2010 r. krajowym organom ochrony danych (Zjednoczone Królestwo i Szwajcaria). Trzecia i czwarta skarga są obecnie badane. Niewielką liczbę skarg można tłumaczyć ograniczeniem uprawnień grupy głównie do określonego rodzaju danych, o czym mowa powyżej.

Ograniczoną liczbę spraw napływających do grupy można również częściowo tłumaczyć brakiem wiedzy o istnieniu grupy. Od 2004 r. Komisja w większym stopniu wyeksponowała informacje o grupie na swoich stronach internetowych[43].

W celu lepszego wykorzystania grupy, przedsiębiorstwa ze Stanów Zjednoczonych, które zdecydowały się na współpracę z grupą i przestrzeganie jej decyzji w zakresie określonych lub wszystkich kategorii danych osobowych, które są objęte ich poświadczeniem zgodności, powinny wyraźnie i w widocznym miejscu zaznaczyć ten fakt w zobowiązaniach zawartych w ich polityce ochrony prywatności, aby umożliwić Departamentowi Handlu zbadanie tej kwestii. Witryna internetowa każdego organu ochrony danych UE powinna zawierać stronę dotyczącą bezpiecznego transferu danych, aby informować europejskie przedsiębiorstwa i osoby, których dane dotyczą, o programie bezpiecznego transferu danych.

5.3. Poprawa egzekwowania prawa

Określone powyżej słabe punkty w zakresie przejrzystości i egzekwowania wzbudzają wśród europejskich przedsiębiorstw obawy dotyczące negatywnych skutków programu bezpiecznego transferu danych dla konkurencyjności europejskich przedsiębiorstw. Jeżeli europejskie przedsiębiorstwo konkuruje z przedsiębiorstwem ze Stanów Zjednoczonych prowadzącym działalność w ramach programu bezpiecznego transferu danych, które jednak w praktyce nie stosuje zasad programu, takie europejskie przedsiębiorstwo znajduje się w niekorzystnej sytuacji konkurencyjnej względem danego przedsiębiorstwa ze Stanów Zjednoczonych.

Ponadto w zakres jurysdykcji Federalnej Komisji Handlu wchodzą nieuczciwe lub wprowadzające w błąd czyny lub praktyki „w handlu lub wpływające na handel”. W sekcji 5 ustawy o Federalnej Komisji Handlu ustanowiono wyjątki od uprawnień Federalnej

[43] Zgodnie ze sprawozdaniem z 2004 r. na stronach internetowych Komisji (DG ds. Sprawiedliwości) opublikowano ogłoszenie informacyjne w formie pytań i odpowiedzi grupy UE ds. ochrony danych w celu informowania osób fizycznych i udzielenia im pomocy w złożeniu skargi w sytuacji, w której uznają, że ich dane osobowe zostały przetworzone w sposób naruszający zasady bezpiecznego transferu danych osobowych. http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_pl.pdf.
Standardowy formularz skargi jest dostępny pod adresem http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf.

Komisji Handlu w zakresie nieuczciwych lub wprowadzających w błąd czynów lub praktyk w odniesieniu między innymi do **telekomunikacji**. Ponieważ Federalna Komisja Handlu nie może egzekwować prawa w stosunku do przedsiębiorstw telekomunikacyjnych, takie przedsiębiorstwa nie mogą uczestniczyć w programie bezpiecznego transferu danych. Wraz z rosnącą konwergencją technologii i usług wielu bezpośrednich konkurentów takich przedsiębiorstw w sektorze ICT w Stanach Zjednoczonych jest jednak uczestnikami programu bezpiecznego transferu danych. Wyłączenie przedsiębiorstw telekomunikacyjnych z wymiany danych w ramach programu bezpiecznego transferu danych stanowi problem dla niektórych europejskich operatorów sieci telekomunikacyjnych. Według Stowarzyszenia Europejskich Operatorów Sieci Telekomunikacyjnych „jest to wyraźnie sprzeczne z najważniejszym apelem operatorów sieci telekomunikacyjnych dotyczącym konieczności zapewnienia równych szans”[44].

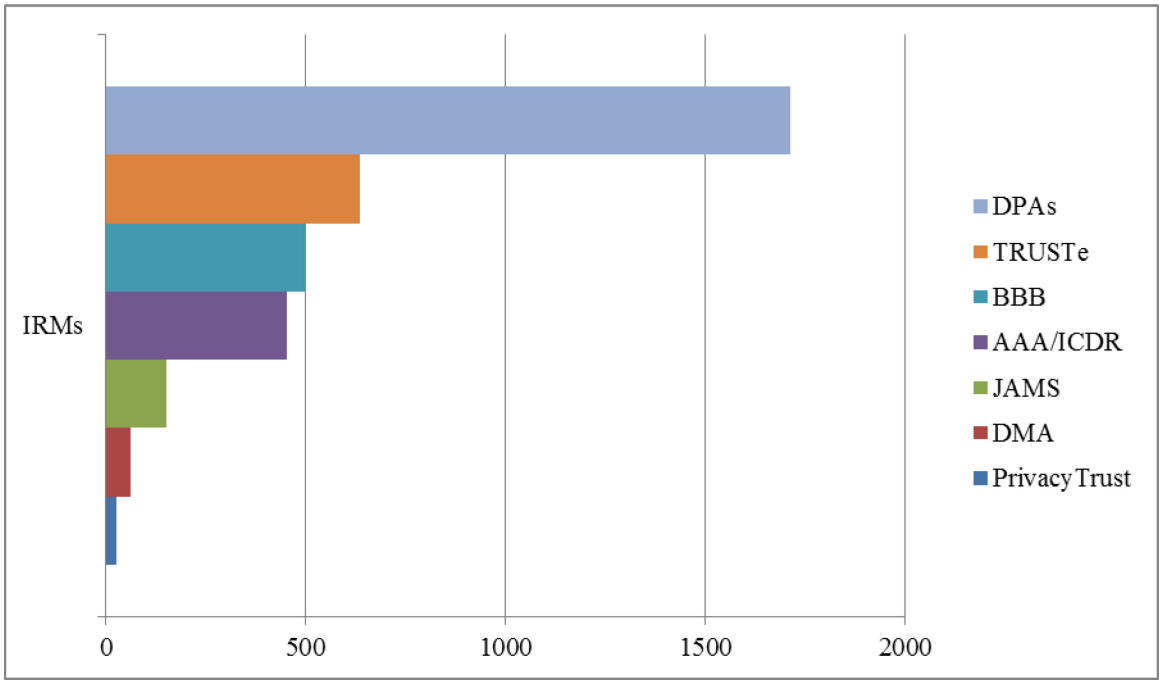
6. WZMOCNIENIE ZASAD BEZPIECZNEGO TRANSFERU DANYCH OSOBOWYCH

6.1. Pozasądowe rozstrzyganie sporów

Zgodnie z zasadą zapewnienia prawu skuteczności musi istnieć „**łatwo dostępny i finansowo przystępny mechanizm** (…) **ochrony prawnej**, dzięki któremu bada się (…) skargi oraz spory poszczególnych osób”. W tym celu w ramach programu bezpiecznego transferu danych ustanawia się system pozasądowego rozstrzygania sporów (ADR) przez niezależną stronę trzecią[45] w celu zapewnienia osobom fizycznym szybkich rozwiązań. Trzy główne organy zapewniające mechanizmy ochrony prawnej to grupa UE ds. ochrony danych, BBB (Better Business Bureaus) i TRUSTe.

[44] W „uwagach Stowarzyszenia Europejskich Operatorów Sieci Telekomunikacyjnych”, które wpłynęły do służb Komisji w dniu 4 października 2013 r., omawia się również 1) definicję danych osobowych w programie bezpiecznego transferu danych, 2) brak monitorowania programu bezpiecznego transferu danych, 3) oraz „ istnienie znacznie mniejszych ograniczeń w przekazywaniu danych przez przedsiębiorstwa ze Stanów Zjednoczonych, niż to ma miejsce w przypadku przedsiębiorstw europejskich”, co „stanowi wyraźną dyskryminację europejskich przedsiębiorstw i ma wpływ na konkurencyjność europejskich przedsiębiorstw”. Zgodnie z zasadami bezpiecznego transferu danych osobowych w celu ujawnienia informacji stronie trzeciej, organizacje muszą stosować zasady ogłoszenia i wyboru. W przypadku gdy organizacja chce przesłać informację stronie trzeciej, będącej przedstawicielem, może to zrobić pod warunkiem uprzedniego upewnienia się, iż strona trzecia przystąpiła do zasad albo podlega dyrektywie 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 w odnośnych zasadach.

[45] W dyrektywie Parlamentu Europejskiego i Rady 2013/11/UE w sprawie ADR w sporach konsumenckich podkreśla się znaczenie niezależnych, bezstronnych, przejrzystych, skutecznych, szybkich i uczciwych alternatywnych metod rozstrzygania sporów.



Od 2004 r. wykorzystanie ADR wzrosło, a Departament Handlu wzmocnił monitorowanie amerykańskich podmiotów świadczących usługi w zakresie ADR, aby zapewniane przez nich informacje dotyczące procedury składania skarg były przejrzyste, dostępne i zrozumiałe. Skuteczność przedmiotowego systemu nie została jeszcze jednak potwierdzona ze względu na ograniczoną liczbę rozpatrzonych do tej pory spraw[46].

Chociaż Departament Handlu z powodzeniem doprowadził do ograniczenia opłat pobieranych przez ADR, dwa z siedmiu głównych podmiotów świadczących usługi w zakresie ADR nadal pobierają opłaty od osób fizycznych, które składają skargę[47]. Dotyczy to podmiotów świadczących usługi w zakresie ADR, z których usług korzysta około 20 % przedsiębiorstw będących uczestnikami programu bezpiecznego transferu danych. Przedsiębiorstwa te wybrały podmiot świadczący usługi w zakresie ADR pobierający opłatę od konsumentów za złożenie skargi. Takie praktyki są niezgodne z zasadą „zapewniania prawu skuteczności" w ramach bezpiecznego transferu danych osobowych, w której osobom fizycznym przyznaje się prawo do „łatwo dostępnego i finansowo przystępnego mechanizmu niezależnej ochrony prawnej". W Unii Europejskiej dostęp do usługi niezależnego rozstrzygania sporów

[46] Przykładowo jeden z głównych usługodawców („TRUSTe") zgłosił, że w 2010 r. otrzymał 881 wniosków, z których jednak jedynie trzy uznano za dopuszczalne i uzasadnione. W następstwie przedmiotowych trzech wniosków od danego przedsiębiorstwa zażądano zmiany polityki ochrony prywatności i stron internetowych. W 2011 r. liczba skarg wyniosła 879, a zmiany polityki ochrony prywatności zażądano od przedsiębiorstwa w jednym przypadku. Zdaniem Departamentu Handlu znaczną większość skarg składanych do podmiotów świadczących usługi w zakresie ADR stanowią wnioski od konsumentów, na przykład od użytkowników, którzy zapomnieli swojego hasła i nie są w stanie go uzyskać w ramach danej usługi internetowej. W następstwie wniosków Komisji Departament Handlu opracował nowe kryteria w zakresie zgłaszania danych statystycznych, z których mają korzystać wszystkie podmioty świadczące usługi w zakresie ADR. W kryteriach odróżnia się zwykłe wnioski od skarg, oraz zawierają one dalsze wyjaśnienie rodzajów otrzymanych skarg. Przedmiotowe nowe kryteria wymagają jednak dalszego omówienia w celu dopilnowania, aby nowe dane statystyczne w 2014 r. dotyczyły wszystkich dostawców ADR, były porównywalne i zawierały informacje kluczowe do oceny skuteczności mechanizmu ochrony prawnej.

[47] Międzynarodowe Centrum Rozstrzygania Sporów / Amerykańskie Stowarzyszenie Arbitrażowe (ang. ICDR/AAA – International Centre for Dispute Resolution/American Arbitration Association) pobiera „opłatę za złożenie skargi" w wysokości 200 USD, a JAMS – 250 USD. Departament Handlu poinformował Komisję, że podjął współpracę z AAA, czyli najdroższym podmiotem świadczącym usługi w zakresie rozstrzygania sporów dla osób fizycznych, w celu opracowania programu bezpiecznego transferu danych, w którym ogranicza się koszt ponoszony przez konsumentów z kilku tysięcy USD do zryczałtowanej stawki wynoszącej 200 USD.

świadczonej przez grupę UE ds. ochrony danych jest nieodpłatny dla wszystkich osób, których dane dotyczą.

W dniu 12 listopada 2013 r. Departament Handlu potwierdził, że „będzie nadal opowiadać się za prywatnością obywateli UE i współpracować z podmiotami świadczącymi usługi w zakresie ADR, aby ustalić, czy jest możliwe dalsze obniżenie pobieranych przez nich opłat".

Jeżeli chodzi o sankcje, nie wszystkie podmioty świadczące usługi w zakresie ADR dysponują niezbędnymi narzędziami do naprawy sytuacji, w których zasady ochrony prywatności nie są przestrzegane. Ponadto wydaje się, że sankcje i środki, którymi dysponują wszystkie podmioty świadczące usługi w zakresie ADR, nie przewidują publikacji ustalonych przypadków nieprzestrzegania zasad.

Od podmiotów świadczących usługi w zakresie ADR wymaga się również, aby przekazywali sprawy Federalnej Komisji Handlu, jeżeli po zastosowania procesu ADR dane przedsiębiorstwo nie przestrzega zasad lub odrzuca decyzję podmiotu świadczącego usługi w zakresie ADR, aby Federalna Komisja Handlu mogła skontrolować i zbadać sprawę oraz w razie potrzeby podjąć środki egzekucyjne. Do tej pory nie odnotowano przypadków przekazania przez podmioty świadczące usługi w zakresie ADR Federalnej Komisji Handlu spraw dotyczących nieprzestrzegania zasad[48].

Podmioty świadczące usługi w zakresie pozasądowego rozstrzygania sporów prowadzą na swoich stronach internetowych wykaz przedsiębiorstw (uczestników systemu rozstrzygania sporów) korzystających z ich usług. Dzięki takiemu rozwiązaniu konsumenci mogą z łatwością sprawdzić, czy w przypadku sporu z danym przedsiębiorstwem osoba fizyczna może złożyć skargę u określonego podmiotu świadczącego usługi w zakresie rozstrzygania sporów. Przykładowo zatem podmiot świadczący usługi w zakresie rozstrzygania sporów, BBB, prowadzi wykaz wszystkich przedsiębiorstw należących do systemu rozstrzygania sporów BBB. Istnieje jednak wiele przedsiębiorstw, które twierdzą, że należą do konkretnego systemu rozstrzygania sporów, a jednak nie są wymienione przez podmioty świadczące usługi w zakresie ADR jako uczestnicy ich systemu rozstrzygania sporów[49].

Mechanizmy ADR powinny być łatwo dostępne, niezależne i finansowo przystępne dla osób fizycznych. Osoba, której dane dotyczą, powinna być w stanie bez większych trudności złożyć skargę. Wszystkie organy ADR powinny publikować na swoich stronach internetowych dane statystyczne dotyczące rozpatrywanych skarg oraz szczegółowe informacje dotyczące wyniku takich spraw. Ponadto należy w większym stopniu monitorować organy ADR w celu dopilnowania, aby informacje, jakie takie organy przedstawiają na temat procedury i sposobu składania skargi, były przejrzyste i zrozumiałe, tak aby rozstrzyganie sporów stało się skutecznym, wiarygodnym i przynoszącym wyniki mechanizmem. Należy ponadto jeszcze raz stwierdzić, że zakres obowiązkowych sankcji w ramach ADR powinien obejmować publikację ustalonych przypadków nieprzestrzegania zasad.

---

[48] Zob. NZP nr 11.

[49] Przykłady: Przedsiębiorstwo Amazon poinformowało Departament Handlu, że korzysta z usług BBB jako podmiotu rozstrzygającego spory. BBB nie wymienia jednak przedsiębiorstwa Amazon wśród uczestników swojego programu rozstrzygania sporów. Z kolei przedsiębiorstwo Arsalon Technologies (www.arsalon.net), dostawca usług hostingu w chmurze, widnieje w wykazie członków programu rozstrzygania sporów BBB, mimo że nie jest aktualnym uczestnikiem programu bezpiecznego transferu danych (sytuacja od dnia 1 października 2013 r.). BBB, TRUSTe i inne podmioty świadczące usługi ADR powinny usunąć lub poprawić zapewnienia dotyczące poświadczania zgodności. Podmioty świadczące usługi ADR powinny być związane wykonalnym wymogiem poświadczania zgodności wyłącznie tych przedsiębiorstw, które są uczestnikami programu bezpiecznego transferu danych.

6.2. Dalsze przekazywanie danych

Wraz z gwałtownym wzrostem przepływów danych zachodzi potrzeba zapewnienia stałej ochrony danych osobowych na wszystkich etapach przetwarzania danych, w szczególności jeżeli przedsiębiorstwo uczestniczące w programie bezpiecznego transferu danych przekazuje dane **podmiotowi przetwarzającemu będącemu stroną trzecią**. Dlatego też konieczność lepszego egzekwowania zasad bezpiecznego transferu danych osobowych dotyczy nie tylko uczestników programu bezpiecznego transferu danych, lecz także podwykonawców.

W programie bezpiecznego transferu danych dopuszcza się dalsze przekazywanie danych stronom trzecim będącym „przedstawicielami", jeżeli dane przedsiębiorstwo – uczestnik programu bezpiecznego transferu danych – „upewni się, iż strona trzecia przystąpiła do zasad albo podlega dyrektywie 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"[50]. Przykładowo Departament Handlu wymaga od dostawcy usług przetwarzania w chmurze zawarcia umowy, nawet jeżeli taki dostawca „przestrzega zasad bezpiecznego transferu danych osobowych i otrzymuje dane osobowe do przetworzenia[51]. Przepis ten nie jest jednak jasno sformułowany w załączniku II do decyzji w sprawie zasad bezpiecznego transferu danych osobowych.

Ponieważ w ostatnich latach znacznie częściej korzysta się z usług podwykonawców, szczególnie w kontekście przetwarzania w chmurze, przedsiębiorstwo będące uczestnikiem programu bezpiecznego transferu danych powinno poinformować Departament Handlu o zawarciu takiej umowy oraz powinno być zobowiązane do upublicznienia udzielonych gwarancji w zakresie ochrony prywatności[52].

Należy doprecyzować trzy wyżej przedstawione kwestie: mechanizm pozasądowego rozwiązywania sporów, ściślejszy nadzór i dalsze przekazywanie danych.

7. DOSTĘP DO DANYCH PRZEKAZANYCH W RAMACH PROGRAMU BEZPIECZNEGO TRANSFERU DANYCH

W 2013 r. informacje dotyczące skali i zakresu amerykańskich programów nadzoru wzbudziły obawy dotyczące ciągłości ochrony danych osobowych przekazanych zgodnie z prawem Stanom Zjednoczonym w ramach programu bezpiecznego transferu danych. Wydaje się na przykład, że wszystkie przedsiębiorstwa, które biorą udział w programie PRISM i udzielają dostępu organom Stanów Zjednoczonych do danych przechowywanych i przetwarzanych w Stanach Zjednoczonych, dokonały poświadczenia zgodności z programem bezpiecznego transferu danych. W ten sposób program bezpiecznego transferu danych stał się

---

50 Zob. decyzja Komisji 2000/520/WE, s. 7 (dalsze przekazywanie danych).

51 Zob. „Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing": http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf.

52 Uwagi te dotyczą dostawców usług przetwarzania w chmurze, którzy nie uczestniczą w programie bezpiecznego transferu danych. Według firmy konsultingowej Galeria „poziom uczestnictwa w programie bezpiecznego transferu danych (i przestrzegania tego programu) wśród dostawców usług przetwarzania w chmurze jest całkiem wysoki. Dostawcy usług przetwarzania w chmurze posiadają zwykle wiele poziomów ochrony prywatności, często obejmujące bezpośrednie kontakty z klientami i nadrzędną politykę ochrony danych. Z jednym lub dwoma istotnymi wyjątkami, dostawcy usług przetwarzania w chmurze uczestniczący w programie bezpiecznego transferu danych przestrzegają kluczowych przepisów dotyczących rozstrzygania sporów i egzekwowania prawa. Aktualnie w wykazie podmiotów, które przedstawiły fałszywe oświadczenia o uczestnictwie, nie widnieją żadni główni dostawcy usług przetwarzania w chmurze.". (Wystąpienie Chrisa Connolly'ego z Galexia przed Komisją LIBE prowadzącą dochodzenie w sprawie „masowej inwigilacji elektronicznej obywateli UE").

jednym z kanałów dostępu organów wywiadowczych Stanów Zjednoczonych do danych osobowych wstępnie przetworzonych w UE.

W załączniku I do decyzji w sprawie **zasad bezpiecznego transferu danych osobowych** przewidziano, że przyjęcie zasad ochrony prywatności może być ograniczone, jeżeli jest to uzasadnione wymaganiami bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa, lub ustawą, rozporządzeniem rządu albo prawem procesowym. Aby ograniczenia i restrykcje dotyczące korzystania z praw podstawowych były ważne, muszą mieć wąską wykładnię, muszą zostać określone w publicznie dostępnych przepisach oraz muszą być konieczne i proporcjonalne w demokratycznym społeczeństwie. W szczególności decyzja w sprawie zasad bezpiecznego transferu danych osobowych stanowi, że tego rodzaju ograniczenia dopuszcza się wyłącznie „**w zakresie niezbędnym"** do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa[53]. Chociaż w ramach programu bezpiecznego transferu danych zapewnia się wyjątkowe przetwarzanie danych do celów bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa, w czasie przyjęcia programu bezpiecznego transferu danych nie można było przewidzieć, że agencje wywiadowcze uzyskają szeroki dostęp do danych przekazywanych Stanom Zjednoczonym w kontekście transakcji handlowych.

Ponadto ze względu na przejrzystość i pewność prawa Departament Handlu powinien informować Komisję Europejską o każdej ustawie lub rozporządzeniu rządu wpływających na przestrzeganie zasad bezpiecznego transferu danych osobowych[54]. Należy ściśle monitorować stosowanie wyjątków, których nie można stosować w sposób osłabiający ochronę zapewnianą w ramach **zasad**[55]. W szczególności szeroki dostęp organów Stanów Zjednoczonych do danych przetwarzanych przez przedsiębiorstwa, które dokonały poświadczenia zgodności z zasadami bezpiecznego transferu danych osobowych, stwarza ryzyko obniżenia poziomu poufności łączności elektronicznej.

7.1. Proporcjonalność i konieczność

Jak wynika z ustaleń grupy roboczej ad hoc UE-USA ds. ochrony danych, w szeregu podstaw prawnych w prawie Stanów Zjednoczonych dopuszcza się gromadzenie i przetwarzanie na szeroką skalę danych osobowych przechowywanych lub w inny sposób przetwarzanych przez przedsiębiorstwa z siedzibą w Stanach Zjednoczonych. Może dotyczyć to danych wcześniej przekazanych z UE do Stanów Zjednoczonych w ramach programu bezpiecznego transferu danych, co wzbudza wątpliwości co do ciągłości przestrzegania zasad bezpiecznego transferu danych osobowych. Szeroko zakrojony charakter takich programów może prowadzić do uzyskiwania dostępu i dalszego przetwarzania przez organy Stanów Zjednoczonych danych przekazywanych w ramach programu bezpiecznego transferu danych w stopniu

---

[53] Zob. załącznik I do decyzji w sprawie zasad bezpiecznego transferu danych osobowych: „Przyjęcie zasad 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".

[54] Dokument Opinion 4/2000 on the level of protection provided by the "Safe Harbour Principles", przyjęty przez Grupę Roboczą Art. 29 w dniu 16 maja 2000 r.

[55] Dokument Opinion 4/2000 on the level of protection provided by the "Safe Harbour Principles", przyjęty przez Grupę Roboczą Art. 29 w dniu 16 maja 2000 r.

wykraczającym poza zakres ściśle niezbędny i proporcjonalny do ochrony bezpieczeństwa narodowego, przewidziany w wyjątku określonym w decyzji w sprawie bezpiecznego transferu danych osobowych.

7.2. Ograniczenia i możliwości dochodzenia roszczeń

Jak wynika z ustaleń grupy roboczej ad hoc UE-USA ds. ochrony danych, gwarancje przewidziane w prawie Stanów Zjednoczonych są głównie dostępne dla obywateli lub legalnych rezydentów Stanów Zjednoczonych. Ponadto ani w UE ani w Stanach Zjednoczonych osoby, których dane dotyczą, nie mają możliwości uzyskania dostępu do danych, ich zmiany ani usunięcia. Nie istnieją również środki odwoławcze na drodze sądowej lub administracyjnej w związku z gromadzeniem i dalszym przetwarzaniem danych osobowych takich osób w ramach amerykańskich programów nadzoru.

7.3. Przejrzystość

W informacjach dotyczących swojej polityki ochrony prywatności |przedsiębiorstwa nie informują systematycznie o tym, kiedy stosują wyjątki od zasad bezpiecznego transferu danych osobowych. Osoby fizyczne i przedsiębiorstwa nie wiedzą zatem, co dzieje się z ich danymi. Ma to szczególne znacznie w kontekście funkcjonowania przedmiotowych amerykańskich programów nadzoru. W rezultacie Europejczycy, których dane są przekazywane przedsiębiorstwu ze Stanów Zjednoczonych w ramach programu bezpiecznego transferu danych, mogą nie być informowani przez takie przedsiębiorstwa o ewentualnym udostępnianiu ich danych[56]. Taka sytuacja budzi wątpliwości co do przestrzegania zasad bezpiecznego transferu danych osobowych w odniesieniu do przejrzystości. Należy zapewnić jak największy poziom przejrzystości bez narażania bezpieczeństwa narodowego. Przedsiębiorstwa należy zachęcać, aby w informacjach dotyczących ich polityki ochrony prywatności wskazywały, oprócz przypadków, w których zasady mogą być ograniczone ustawą, rozporządzeniem rządu albo prawem procesowym, czego już wymaga się od przedsiębiorstw, również przypadki, w których stosują wyjątki od przedmiotowych zasad w celu spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa.

8. WNIOSKI I ZALECENIA

Od chwili jej przyjęcia w 2000 r., decyzja w sprawie zasad bezpiecznego transferu danych osobowych stała się instrumentem regulującym przepływ danych osobowych między UE a Stanami Zjednoczonymi. Znaczenie skutecznej ochrony w przypadku przekazywania danych osobowych wzrosło wskutek gwałtownego wzrostu przepływów danych, mających podstawowe znaczenie dla gospodarki cyfrowej, oraz bardzo istotnych zmian w gromadzeniu, przetwarzaniu i wykorzystywaniu danych. Przedsiębiorstwa internetowe, takie jak Google, Facebook, Microsoft, Apple, Yahoo, posiadają setki milionów klientów w Europie i

[56] Niektóre europejskie przedsiębiorstwa uczestniczące w programie bezpiecznego transferu danych udzielają stosunkowo przejrzystych informacji w tym względzie. Przykładowo przedsiębiorstwo Nokia, prowadzące działalność w Stanach Zjednoczonych i będące uczestnikiem programu, włączyło do informacji o swojej polityce ochrony prywatności następujące oświadczenie: *Bezwzględnie obowiązujące przepisy prawa mogą nakładać na nas obowiązek udostępniania danych osobowych użytkownika określonym władzom państwowym lub osobom trzecim, na przykład organom ścigania w państwie, gdzie działamy bądź gdzie w naszym imieniu działają osoby trzecie.*

przekazują dane osobowe w celu ich przetwarzania do Stanów Zjednoczonych na skalę niewyobrażalną w roku 2000, w którym ustanowiono zasady bezpiecznego transferu danych osobowych.

Ze względu na niedostateczną przejrzystość i niedostateczne egzekwowanie umowy, nadal utrzymują się określone problemy, które należy rozwiązać:

a) przejrzystość polityki ochrony prywatności uczestników programu bezpiecznego transferu danych,

b) skuteczne stosowanie zasad ochrony prywatności przez przedsiębiorstwa w Stanach Zjednoczonych; oraz

c) skuteczność egzekwowania prawa.

Ponadto **szeroki dostęp agencji wywiadowczych do danych przekazywanych Stanom Zjednoczonym przez przedsiębiorstwa, które dokonały poświadczenia zgodności z zasadami bezpiecznego transferu danych osobowych**, budzi dodatkowe poważne wątpliwości co do ciągłości przestrzegania praw Europejczyków do ochrony danych w przypadku przekazywania ich danych Stanom Zjednoczonym.

Na podstawie powyższego Komisja określiła następujące **zalecenia**:

Przejrzystość

1. *Przedsiębiorstwa, które dokonały poświadczenia zgodności, powinny publicznie ujawniać swoją politykę ochrony prywatności.* Nie wystarczy przekazywanie przez przedsiębiorstwa opisu ich polityki ochrony prywatności Departamentowi Handlu. Informacje dotyczące polityki ochrony prywatności należy udostępnić publicznie na stronach internetowych przedsiębiorstw i sformułować w przejrzysty i jednoznaczny sposób.

2. *Do informacji dotyczących polityki ochrony prywatności zamieszczanych na stronach internetowych przedsiębiorstw, które dokonały poświadczenia zgodności, należy zawsze dołączać łącze do strony internetowej Departamentu Handlu dotyczącej bezpiecznego transferu danych osobowych, zawierającej wykaz wszystkich „aktualnych" uczestników programu.* Dzięki temu osoby w Europie, których dane dotyczą, będą mogły od razu sprawdzić, bez dodatkowego wyszukiwania w internecie, czy dane przedsiębiorstwo jest aktualnie uczestnikiem programu bezpiecznego transferu danych. Ograniczenie możliwości składania fałszywych oświadczeń o uczestnictwie w programie doprowadzi do zwiększenia jego wiarygodności. Od marca 2013 r. Departament Handlu wymaga od przedsiębiorstw umieszczania takiego łącza, jednak proces ten należy zintensyfikować.

3. *Przedsiębiorstwa, które dokonały poświadczenia zgodności, powinny publikować warunki dotyczące ochrony prywatności określone we wszystkich umowach, które zawierają z podwykonawcami, na przykład w zakresie usług przetwarzania w chmurze.* W programie bezpiecznego transferu danych dopuszcza się dalsze przekazywanie danych stronom trzecim będącym „przedstawicielami", na przykład dostawcom usług przetwarzania w chmurze, przez przedsiębiorstwa, które dokonały

poświadczenia zgodności z zasadami bezpiecznego transferu danych. W naszym rozumieniu, w takich przypadkach Departament Handlu wymaga zawarcia umowy od przedsiębiorstw, które dokonały poświadczenia zgodności. Zawierając taką umowę, przedsiębiorstwo będące uczestnikiem programu bezpiecznego transferu danych powinno również jednak poinformować Departament Handlu o zawarciu takiej umowy oraz powinno być zobowiązane do upublicznienia udzielonych gwarancji w zakresie ochrony prywatności.

4. *Wszystkie przedsiębiorstwa, które aktualnie nie uczestniczą w programie, powinny być wyraźnie oznakowane na stronach internetowych Departamentu Handlu.* Przy oznaczeniu „nieaktualny" w prowadzonym przez Departament Handlu wykazie uczestników programu bezpiecznego transferu danych należy umieścić wyraźne ostrzeżenie, że dane przedsiębiorstwo obecnie nie spełnia wymogów bezpiecznego transferu danych. Przedsiębiorstwo posiadające status „nieaktualny" musi jednak nadal stosować wymogi bezpiecznego transferu danych wobec danych uzyskanych w ramach programu bezpiecznego transferu danych.

Dochodzenie roszczeń

5. *Do informacji dotyczących polityki ochrony prywatności dostępnych na stronach internetowych przedsiębiorstw należy dołączać łącze do podmiotu świadczącego usługi w zakresie pozasądowego rozstrzygania sporów (ADR) lub grupy UE.* Dzięki temu Europejczycy, których dane dotyczą, mogą bezpośrednio skontaktować się z podmiotem świadczącym usługi w zakresie ADR lub grupą UE w przypadku wystąpienia problemów. Od marca 2013 r. Departament Handlu wymaga od przedsiębiorstw podawania takiego łącza, jednak proces ten należy zintensyfikować.

6. *Pozasądowe rozstrzyganie sporów powinno być łatwo dostępne i finansowo przystępne.* Niektóre organy ADR w programie bezpiecznego transferu danych nadal pobierają od osób fizycznych opłaty za rozpatrzenie skargi, które bywają dość wysokie jak na indywidualnego użytkownika (200 USD – 250 USD). Natomiast w Europie dostęp do grupy ds. ochrony danych przewidzianej do celów rozpatrywania skarg w ramach programu bezpiecznego transferu danych jest nieodpłatny.

7. *Departament Handlu powinien bardziej systematycznie monitorować organy ADR pod względem przejrzystości i dostępności przedstawianych przez nie informacji dotyczących stosowanej przez nie procedury i podejmowanych przez nie działań następczych w związku ze skargami.* Dzięki temu rozstrzyganie sporów stanowi skuteczny, wiarygodny i przynoszący wyniki mechanizm. Należy ponadto jeszcze raz stwierdzić, że zakres obowiązkowych sankcji w ramach ADR powinien obejmować publikację ustalonych przypadków nieprzestrzegania zasad.

Egzekwowanie prawa

8. *Po poświadczeniu zgodności lub ponownym poświadczeniu zgodności przedsiębiorstw w ramach programu bezpiecznego transferu danych określony odsetek takich przedsiębiorstw należy objąć urzędowymi dochodzeniami dotyczącymi faktycznego*

przestrzegania przez nie polityki ochrony prywatności (wykraczającymi poza kontrolę zgodności z formalnymi wymogami).

9. *Zawsze w przypadku wykrycia niezgodności, w następstwie skargi lub dochodzenia, po upływie 1 roku w stosunku do danego przedsiębiorstwa należy przeprowadzić uzupełniające szczegółowe dochodzenie.*

10. *Departament Handlu powinien informować właściwy organ ochrony danych o wątpliwościach co do przestrzegania zasad przez dane przedsiębiorstwo lub o rozpatrywanych skargach.*

11. *Należy nadal prowadzić dochodzenia w sprawie fałszywych oświadczeń o uczestnictwie w programie bezpiecznego transferu danych.* Przedsiębiorstwo, które na swoich stronach internetowych zamieszcza oświadczenie, że przestrzega wymogów zasad bezpiecznego transferu danych, ale które nie widnieje w wykazie prowadzonym przez Departament Handlu jako „aktualny" uczestnik programu, wprowadza konsumentów w błąd i nadużywa ich zaufania. Fałszywe oświadczenia zmniejszają wiarygodność systemu jako całości, a zatem tego rodzaju oświadczenia należy niezwłocznie usunąć ze stron internetowych przedsiębiorstw.

Dostęp organów Stanów Zjednoczonych

12. *Polityka ochrony prywatności przedsiębiorstw, które dokonały poświadczenia zgodności, powinna obejmować informacje dotyczące zakresu, w jakim prawo Stanów Zjednoczonych zezwala organom publicznym na gromadzenie i przetwarzanie danych przekazywanych w ramach programu bezpiecznego transferu danych. W szczególności należy zachęcać przedsiębiorstwa do wskazywania w ich polityce ochrony prywatności przypadki, w których stosują wyjątki od zasad w celu spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa.*

13. *Istotne jest, aby wyjątek dotyczący bezpieczeństwa narodowego przewidziany w decyzji w sprawie zasad bezpiecznego transferu danych osobowych stosowano w ściśle niezbędnym lub proporcjonalnym zakresie.*