FUNDACJA PANOPTYKON

Safe Harbour – czyli jak (nie)bezpieczne są dane Europejczyków w Stanach Zjednoczonych

WSTĘP

Dla wielkich międzynarodowych podmiotów gospodarczych transgraniczny przepływ danych osobowych ma niezwykle istotne znaczenie. Dyrektywa Unii Europejskiej 95/46/WE[1] pozwala na transfer danych osobowych do krajów spoza Europejskiego Obszaru Gospodarczego, jeżeli państwo docelowe stwarza odpowiednie gwarancje ochrony danych osobowych na swoim terytorium. Decyzję stwierdzającą odpowiedni stopień ochrony danych osobowych przez państwo trzecie wydaje Komisja Europejska[2]. Adresatem takiej decyzji w wąskim zakresie są również podmioty amerykańskie, biorące udział w programie Safe Harbour.

W powszechnej opinii Stany Zjednoczone nie są krajem bezpiecznym, jeżeli chodzi o przetwarzanie danych osobowych. Amerykańskie prawo nie gwarantuje w tym zakresie standardów analogicznych do obowiązujących w Unii Europejskiej. Kompromis w postaci programu Safe Harbour – który miał z jednej strony zapewnić swobodę prowadzenia działalności gospodarczej, a z drugiej zagwarantować Europejczykom ochronę ich prawa do prywatności – zawiódł. Wskazują na to oficjalne ewaluacje dokonane przez Komisję Europejską oraz niezależne badania. Problem dostrzegła również wiceprzewodnicząca Komisji Europejskiej Viviane Reding, która zleciła ponowną analizę obowiązywania programu.

W poniższym opracowaniu przedstawiamy podstawowe założenia programu Safe Harbour oraz najważniejsze problemy związane z jego funkcjonowaniem, m.in.: wadliwe mechanizmy egzekwowania prawa, błędy w inkorporowaniu zasad programu Safe Harbour do konkretnych polityk prywatności czy naruszenia obowiązku informowania podmiotu danych o przysługujących mu prawach. W ostatniej części przedstawiamy rekomendacje Fundacji Panoptykon skierowane do Komisji Europejskiej i polskiego rządu.

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie

[2] Krajami wobec, których Komisja Europejska podjęła decyzję o adekwatności są: Argentyna, Australia, Guernsey, Izrael, Jersey, Kanada, Nowej Zelandia, Szwajcaria, Urugwaj, Wyspa Man, Wyspy Owczye.

1) Podstawowe informacje

Program **Safe Harbour (SH)** funkcjonuje na mocy decyzji Komisji Europejskiej z dnia 26 czerwca 2000 roku[3]. Komisja uznała, że poziom ochrony danych gwarantowany przez podmioty biorące udział w programie SH jest „odpowiedni" w myśl art. 25 i 26 Dyrektywy 95/46. Decyzja Komisji Europejskiej została poprzedzona negocjacjami na linii Unia Europejska – Stany Zjednoczone. Na jej podstawie podmioty, które przystąpią do programu SH, mogą korzystać z przywilejów wynikających z uznania odpowiedniości stopnia ochrony danych osobowych, czyli zniesienia barier w zakresie transferu danych osobowych ze wszystkich krajów członkowskich Unii Europejskiej[4].

By przystąpić do programu Safe Harbour administratorzy danych muszą zadeklarować przestrzeganie siedmiu następujących zasad: *Ogłoszenia*, *Wyboru, Dalszego Przekazywania Danych, Bezpieczeństwa, Integralności Danych, Dostępu oraz Zapewnienia Prawu Skuteczności*. Po dokonaniu swoistej samo-certyfikacji, przedsiębiorstwo zgłasza się do **Departamentu Handlu USA (Department of Commerce, DH),** który umieszcza je na liście podmiotów będących członkami programu. Ta lista jest dostępna na stronie DH[5]. Reguły programu Safe Harbour mają zastosowanie tylko do określonych sektorów i podmiotów przetwarzających dane. Program jest zarezerwowany dla organizacji podlegających jurysdykcji **Federalnej Komisji Handlu (Federal Trade Commission, FKH)** lub **Departamentu Transportu (Department of Transportation, DoT)**. W związku z tym poza reżimem Safe Harbour znajdują się m.in: instytucje finansowe i przedsiębiorstwa telekomunikacyjne. W 2011 roku w programie SH uczestniczyło około 2 500 podmiotów[6].

System ochrony danych osobowych w USA zdecydowanie odbiega od standardów prawnych obowiązujących w Europie. Jest on rozporoszony i ma ograniczony charakter – przede wszystkim dotyczy ochrony przed naruszeniem prywatności ze strony podmiotów publicznych. Na amerykański reżim prawny dotyczący ochrony prywatności składa się duża liczba aktów prawnych o charakterze federalnym i stanowym oraz spora liczba programów o charakterze samo-regulacji[7]. Regulacje amerykańskie nie mają kompleksowego charakteru i nie zapewniają tak wszechstronnych gwarancji ochrony prywatności jak Dyrektywa 95/46. Dlatego **prawo Stanów Zjednoczonych nie może zostać uznane za zapewniające „odpowiedni"** poziom ochrony danych Europejczyków[8].

---

[3] Decyzja Komisji z dnia 26 lipca 2000 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwaności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441), (Dz. Urz. WE L. 215 z 25.08.2000, s.7-47).

[4] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie,* Wolters Kluwer, 2010, s.194.

[5] Lista podmiotów uczestniczących w programie Safe Harbour udostępniania przez Departament Handlu USA: https://safeharbor.export.gov/list.aspx .

[6] D. Greer, *Safe Harbour – a framework that works,* International Data Privacy Law, vol 1, nr 3, 2011, s. 147.

[7] Są to min. ustawy : The Cable Communication Policy Act z 1984, The Video Privacy Protection Act, The Federal Privacy Act; The Fair Credit Reporting Act; The Telecommunications Act of 1996, The Children On-Line Privacy Protection Act czy The Health Insurance Portability and Accountability Act of 1996.

[8] H. Farrell, *Constructing the International Foundations of E- Commerce: The EU-US Safe Harbor Arrangement*, International Organization, 57, 2003, s. 285.

2) Krytyka programu Safe Harbour

Decyzja Komisji Europejskiej z 2000 roku była postrzegana jako kompromis między dwoma, bardzo różnymi reżimami prawnymi dotyczącymi ochrony danych. Niestety, **powszechna krytyka programu Safe Harbour dowodzi, że nawet na poziomie podstawowym jego zasady nie są w pełni przestrzegane**. Wskazują na to dotychczasowe ewaluacje przeprowadzone przez Komisję Europejską (w 2002 oraz 2004 roku[9]) oraz australijskie badania z 2008 roku[10]. Na problemy dotyczące zasad Safe Harbour zwracała uwagę również Grupa Robocza Art. 29 (GR29)[11]. W opinii Grupy szczególne zagrożenia wiążą się **z egzekwowaniem i zakresem obowiązywania zasad SH** w Stanach Zjednoczonych. GR29 odnosiła również do wyjątków od stosowania zasad SH oraz kwestii wyrażenia sprzeciwu wobec dalszego przekazywania danych przez członków programu Safe Harbour.

Z kolei w 2010 roku tzw. Düsseldorf Group, czyli ciało zrzeszające rzeczników ochrony danych wszystkich niemieckich landów, uznała, że transfery danych przeprowadzane w ramach programu Safe Harbour powinny opierać się o ostrzejsze kryteria[12]. W 2013 roku wiceprzewodnicząca Komisji Europejskiej Viviane Reding stwierdziła, że program Safe Harbour może nie stwarzać **wystarczających gwarancji ochrony danych osobowych**. Tym samym zapowiedziała ponowną ewaluację programu, która ma zakończyć się w 2013 roku[13].

Poniżej szczegółowo prezentujemy dwie grupy problemów związanych z przestrzeganiem programu Safe Harbour, na które wskazują zarówno dokumenty Komisji Europejskiej, jak i niezależne badania:

(i) Mechanizmy egzekwowania zasad programu Safe Harbour

Zgodnie z raportem Komisji Europejskiej z 2004 roku, jednym z najpoważniejszych problemów dotyczących SH jest **brak skutecznych mechanizmów egzekwowania zasad programu**. Niewątpliwe przyczyną tego stanu rzeczy są popularne w USA rozwiązania samoregulacyjne, które **nie opierają się na powszechnej ingerencji organów publicznych**. Podmiotem odpowiedzialnym za egzekwowanie zasad Safe Harbour jest Federalna Komisja Handlu. Jej kompetencja odnosi się do zbadania, czy zostały naruszone przepisy sekcji 5 Ustawy o FKH, zakazujące nieuczciwych bądź wprowadzających w błąd czynów lub praktyk handlowych. Jeżeli FKH uzna, że przepisy te zostały naruszone, może wydać nakaz zaprzestania stosowania określonych praktyk lub skierować sprawę

---

[9] Komisja Europejska, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce,* 2002; oraz Komisja Europejska, *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, 2004.

[10] C. Connolly, *The US Safe Harbor – Fact or Fiction?,* Galexia, 2008.

[11] Article 29 Data Prtotection Working Party, *Opinion 4/200 on the level of protection provided by the „Safe Harbour Principles*", 2000.

[12] Düsseldorfer Kreises, Beschluss der obersten Aufsichtsbehör den für den Datenschutz im nichtöffentlichen Bereich am 28/29, April 2010,(http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile).

[13] European Commission, MEMO: Informal Justice Council in Vilnius, Brussels, 19 July 2013, (http://europa.eu/rapid/press-release_MEMO-13-710_en.htm).

do sądu. Jednak zdaniem Komisji Europejskiej, **FKH nie działa wystraczająco proaktywnie i nie wykorzystuje w pełni swoich kompetencji** w odniesieniu do uczestników programu Safe Harbour.

Kolejnym istotnym problemem dotyczącym SH jest **ograniczona możliwość składania skarg przez osoby fizyczne na działalność członków programu Safe Harbour**. Amerykańskie przedsiębiorstwa mogą wybrać jeden z dwóch sposobów badania i rozpatrywania indywidualnych skarg. Jedną z dostępnych możliwości są organy **alternatywnego rozpatrywania sporów**, czyli prywatne organizacje arbitrażowe np. BBB OnLine, TRUSTe, AICPA WebTrust. Zgodnie z zasadami programem Safe Harbour, procedury alternatywnego rozstrzygania sporów powinny: (i) zapewnić łatwo dostępny i przystępny finansowo mechanizm niezależnej ochrony prawnej; (ii) obejmować kontrole mające na celu sprawdzenie, że poświadczenia i zapewnienia firm w odniesieniu do praktyk ochrony prywatności są prawdziwe i wdrożone zgodnie z deklaracjami; (iii) zawierać obowiązki dotyczące zaradzenia problemom wynikającymi z nieprzestrzegania zasad przez organizacje deklarujące ich przestrzeganie; (iv) gwarantować, że sankcje wynikające z nieprzestrzegania zasad będą dostatecznie surowe.

Niestety, z raportu Komisji przygotowanego w 2004 r. wynika, że niektóre z mechanizmów alternatywnego rozstrzygania sporów są **nietransparentne** i **niezrozumiałe** dla indywidualnych użytkowników. Często skarżący nie są informowani o tym, jak dokładnie przebiega procedura alternatywnego rozpatrywania sporu. W niektórych przypadkach mechanizmy rozstrzygania sporów w ogóle nie zmierzały do zaradzenia problemom wynikającym z nieprzestrzegania zasad Safe Harbour. Inne procedury zaś w ogóle **nie przewidują wymierzenia sankcji** za naruszenie zasad SH. Podobne wnioski wynikają również z raportu przedstawionego przez australijską firmę consultingową Galexia. Dodatkowo ta publikacja wskazuje m.in. na to, że mechanizmy alternatywnego rozstrzygania sporów są **programami odpłatnymi**. Ze względu na wysokie koszty postępowania te mechanizmy nie zawsze spełniają wymóg finansowej przystępności.

Podmioty uczestniczące w programie Safe Harbour mogą również wskazać, że organem odpowiedzialnym za rozpatrywanie skarg od osób fizycznych będzie specjalnie do tego powołany **panel** składający się z przedstawicieli różnych organów ochrony danych osobowych działających w Unii Europejskiej[14]. Zgodnie z informacjami podanymi przez Komisję w 2004 roku, 73% podmiotów uczestniczących w programie wybrało taką opcję. Dodatkowo, takiemu panelowi z urzędu podlegają sprawy dotyczące przetwarzania informacji związanych z zarządzaniem zasobami ludzkimi. Jak wynika z opublikowanych raportów, **jak dotąd panel złożony z przedstawicieli europejskich organów ochrony danych osobowych nie zbadał ani jednej skargi**. Komisja Europejska w 2004 roku sygnalizowała, że bardzo niewiele wiadomo na temat funkcjonowania tego panelu. Często podmioty amerykańskie na swoich stronach w ogóle nie wskazywały, że ten organ jest odpowiedzialny za rozpatrywanie skarg indywidualnych. Z kolei Galexia podała, że tylko cztery podmioty na swoich stronach internetowych podawały dane kontaktowe panelu.

(ii) Poziom implementacji zasad programu Safe Harbour

Zasady programu Safe Harbour wymagają, by podmioty w nim uczestniczące udostępniały wszystkim zainteresowanym swoje polityki prywatności. Zarówno ewaluacja Komisji Europejskiej, jak i badania Galexii wykazały, że **bardzo duża liczba podmiotów w ogóle nie upublicznia na**

[14] Komisja Europejska, *DATA PROTECTION PANEL (related to FAQs 5 and 9 issued by the US Department of Commerce, and annexed to Commission Decision 2000/520/EC on the adequacy of the 'safe harbor' privacy principles)* (http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_en.pdf).

swoich stronach internetowych zasad ochrony prywatności. Kolejnym problemem okazała się implementacja zasad SH na poziomie konkretnych polityk prywatności. W raporcie z 2004 roku Komisja zauważyła, że szczególne trudności implementacyjne wiązały się z obowiązkiem poinformowania podmiotu danych m.in. o tym, jakie dokładnie dane oraz dla jakich celów są przetwarzane. Polityki prywatności często posługiwały się też terminologią odmienną od stosowanej w zasadach programu Safe Harbour.

Polityki prywatności poszczególnych podmiotów często nie dawały też możliwości wyrażenia sprzeciwu wobec udostępniania danych podmiotom trzecim oraz nie informowały o sposobach złożenia skargi. Jak zauważyła Komisja, tylko niewielka liczba organizacji opublikowała polityki prywatności, które były w całości zgodnie z zasadami programu Safe Harbour. Ten zarzut potwierdza również badanie Galexii. Wynika z niego, że firmy bardzo często publikują niezwykle lakoniczne polityki prywatności. Czasami zdarza się, że publikowane jest tylko oświadczenie o przestrzeganiu zasad Safe Harbour i odnośnik do strony Departamentu Handlu USA.

Krytyka programu Safe Harbour spotyka się jednak również z kontrargumentami[15]. Zgodnie z informacjami dostarczonymi przez firmę rozstrzygającą spory TRUSTe, do 2009 roku rozstrzygnęła ona z sukcesem ok. 4 tys. indywidualnych skarg między obywatelami Unii Europejskiej a podmiotami należącymi do programu Safe Harbour. Z kolei Federalna Komisja Handlu w październiku 2009 roku zawarła ugodę z sześcioma przedsiębiorstwami, które fałszywie twierdziły, że są członkami programu. W marcu 2011 roku FKH zawarła ugodę z Google dotyczącą łamania zasad SH w odniesieniu do usługi Google Buzz.

3) Wnioski końcowe i rekomendacje

Dotychczas przeprowadzone ewaluacje oraz badania dotyczące programu Safe Harbour wskazują, że praktyka przestrzegania zasad tego programu jest daleka od ideału. **Brak jasnych i precyzyjnych reguł egzekwowania prawa, słaby mechanizm ochrony praw osób indywidualnych i wreszcie ogólnie niski poziom standardów ochrony danych osobowych w USA sprawiają, że Komisja Europejska oraz poszczególne państwa członkowskie powinny poddać rewizji decyzję Komisji z 2000 roku**. Przytaczane dowody przestrzegania zasad SH mają szczątkowy charakter, a tym samym trudno uznać je za wystarczające.

W tym kontekście niezbędna wydaje się kolejna ewaluacja tego programu, już zapowiedziana przez komisarz Viviane Reding. Wyniki tej ewaluacji powinny stanowić jedną z podstaw podjęcia decyzji o przyszłych zasadach przekazywania danych osobowych do Stanów Zjednoczonych. Kolejnym argumentem za rewizją programu Safe Harbour jest spodziewane przyjęcie nowego europejskiego rozporządzenia o ochronie danych osobowych. **Nie można dopuścić do tego, by zasady programu Safe Harbour były niekompatybilne z nowymi europejskimi standardami**.

Biorąc pod uwagę powyższe, **rekomendujemy**:

- Szczegółowe przeanalizowanie wniosków z ewaluacji funkcjonowania programu Safe Harbour dokonanego przez Komisję Europejską.

[15] D.Greer, *Safe Harbour – a framework that works,* International Data Privacy Law, vol 1, nr 3, 2011,

- Stworzenie listy rozbieżności między zasadami programu Safe Harbour a projektem rozporządzenia o ochronie danych osobowych.
- **Wypracowanie nowego modelu współpracy ze stroną amerykańską w zakresie przekazywania danych do podmiotów prywatnych, zgodnego z europejskimi standardami ochrony danych osobowych i opartego o wiążące dla strony amerykańskiej instrumenty prawne, a nie program działający na zasadzie samo-regulacji.**
- Jeżeli wypracowanie porozumienia w tym zakresie okaże się niemożliwe, transfery danych do Stanów Zjednoczonych powinny odbywać się na zasadach ogólnych, zawartych w Dyrektywie 95/46/.
- **W toku wypracowywania nowych zasad przekazywania danych osobowych do USA należy położyć szczególny nacisk na:** (i) egzekwowalność standardów ochrony danych osobowych i rolę amerykańskich podmiotów administracji publicznej: FHK, DH i DT powinny brać aktywny udział w egzekwowaniu zobowiązań wynikających z nowego porozumienia; (ii) odstąpienie od samo-certyfikacji: podstawowe obowiązki firm uprawnionych do przetwarzania danych obywateli UE powinny wynikać z prawnie wiążących instrumentów; (iii) skuteczne i dostępne procedury składania skarg indywidualnych: przewidziane w nowym porozumieniu mechanizmy rozpatrywania sporów powinny być zgodne z zasadami uczciwego procesu i gwarantować powszechne prawo do sądu.
- Jeżeli rewizja programu Safe Harbour okaże się niemożliwa, polskie organy administracji rządowej oraz Generalny Inspektor Ochrony Danych Osobowych powinny rozważyć zaostrzenie wymogów przekazywania danych osobowych do Stanów Zjednoczonych w ramach tego programu, na wzór przyjętych przez Düsseldorf Group.

Opracowanie: Jędrzej Niklas, Katarzyna Szymielewicz

O nas

Fundacja Panoptykon powstała w kwietniu 2009 r. Jej celem jest działanie na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego" – współczesnych form kontroli i nadzoru nad społeczeństwem. W obszarze zainteresowania Fundacji znajdują się takie zagadnienia jak: powstawanie i rozbudowa baz danych, rozwój monitoringu wizyjnego, retencja danych telekomunikacyjnych, wykorzystywanie technologii biometrycznych, uprawnienia służb specjalnych, techniki nadzoru nad pracownikami, praktyki kontroli przepływu informacji w Internecie.