



STANOWISKO RZĄDU

I. METRYKA DOKUMENTU

Tytuł	
KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY Transatlantyczne przepływy danych: odbudowa zaufania dzięki ustanowieniu silniejszych gwarancji	
Data skierowania wniosku przez Parlament RP	Data przyjęcia stanowiska przez Komitet do Spraw Europejskich
18 marca 2016 r.	19 maja 2016 r.
Sygnatura Komisji Europejskiej	COM(2016)117
Instytucja wiodąca	
Ministerstwo Cyfryzacji	
Instytucje współpracujące	
Ministerstwo Spraw Wewnętrznych i Administracji Ministerstwo Rozwoju Ministerstwo Sprawiedliwości Generalny Inspektor Ochrony Danych Osobowych	

II. CEL DOKUMENTU

Komunikat Komisji Europejskiej COM(2016) 117 (dalej: Komunikat) służy przedstawieniu podjętych w ostatnim czasie inicjatyw mających na celu odbudowanie zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi Ameryki oraz tym samym realizacji zapowiedzi przedstawionych w Komunikacie z 2013 r.: *Komunikat Komisji do Parlamentu Europejskiego i Rady - Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi, COM(2013) 846 final z 27 listopada 2013 r.* Komunikat z 2013 r. był bezpośrednią reakcją na doniesienia w zakresie masowej inwigilacji użytkowników Internetu przez amerykańskie służby i identyfikował działania niezbędne do przywrócenia zaufania obywateli UE do transferów danych, takie jak m.in.: (i) przyjęcie unijnej reformy ochrony danych osobowych; (ii) zwiększenie

bezpieczeństwa przetwarzania danych w ramach programu „bezpieczna przystań”; oraz (iii) wzmocnienie gwarancji ochrony danych w ramach współpracy w obszarze egzekwowania prawa. W komunikacie Komisja podkreśla rolę wymiany danych we wzajemnych relacjach Unia Europejska - USA, tak przekazywanych w celach komercyjnych, jak i w celu egzekwowania przepisów prawa. Podkreśla także konieczność zapewnienia odpowiedniego, w rozumieniu przepisów unijnych, poziomu ochrony przekazywanych w ten sposób danych.

Kluczowym osiągnięciem w budowaniu wzajemnych relacji w obszarze przekazywania danych między UE a USA jest zakończenie negocjacji nad projektem mechanizmu tzw. „tarczy prywatności” (ang. *EU-U.S. Privacy Shield*), który ma służyć przekazywaniu danych osobowych z terytorium Unii Europejskiej do USA w celach komercyjnych. Z punktu widzenia przepisów prawa Unii Europejskiej oraz implementujących je przepisów prawa polskiego, Stany Zjednoczone Ameryki nie zapewniają bowiem odpowiedniego do unijnego poziomu ochrony danych osobowych, w związku z czym obowiązuje zakaz przekazywania danych osobowych z terytorium Unii Europejskiej do USA na zasadach ogólnych. Taki transfer jest możliwy jedynie na podstawie przepisów szczególnych oraz rozwiązań, których adekwatność potwierdziła Komisja Europejska. Jednym z nich, funkcjonującym w latach 2000-2015, był transfer danych osobowych w ramach tzw. „bezpiecznej przystani” (ang. *Safe Harbour*). W 2000 r. Komisja Europejska swoją decyzją¹ potwierdziła adekwatność zasad ochrony prywatności w ramach programu „bezpiecznej przystani”, w następstwie czego dane osobowe mogły być swobodnie przekazywane z terytorium Unii do przedsiębiorstw amerykańskich, które zobowiązały się do ich przestrzegania. Decyzja Komisji Europejskiej uznająca adekwatność „bezpiecznej przystani” została jednak uchylona przez Trybunał Sprawiedliwości UE w wyroku z dnia 6 października 2015 r. w sprawie C-362/14 Schrems².

W dniu 2 lutego 2016 r., Komisja Europejska i Departament Handlu USA osiągnęły porozumienie polityczne odnośnie do Tarczy Prywatności. Efektem tego porozumienia jest wydanie komunikatu COM(2016)117, który opisuje najważniejsze elementy osiągniętego kompromisu i którego dotyczy niniejsze stanowisko.

Zgodnie z treścią Komunikatu, w ocenie Komisji Europejskiej, „tarcza prywatności” realizuje wytyczne Trybunału Sprawiedliwości ze sprawy C-362/14 Schrems oraz zapewnia odpowiedni do unijnego poziom ochrony danych osobowych. Niemniej, zgodnie z informacjami uzyskanymi przez przedstawiciela Polski na posiedzeniu tzw. Komitetu Artykułu 31 w dniu 29 kwietnia br., mając na względzie uwagi zgłoszone przez Grupę Roboczą Artykułu 29³, Komisja Europejska zmierza do rewizji tekstu „tarczy prywatności”, tak aby rozwiązać jak najwięcej podniesionych przez ww. ciało doradcze wątpliwości.

Sama „tarcza prywatności” ma formę listów poszczególnych organów administracji amerykańskiej, które zawierają zobowiązania konkretnych instytucji amerykańskiego rządu do określonego działania. Listy te są skierowane do Departamentu Handlu USA, który odpowiadał za negocjacje nowego porozumienia z Komisją Europejską. Zobowiązania strony amerykańskiej, zgodnie z przedstawioną dokumentacją, zostaną opublikowane w publicznym rejestrze federalnym (U.S. Federal Register). W skład listów tworzących Tarczę Prywatności wchodzi:

- listy Penny Pritzker, Sekretarza Handlu USA, oraz Stefana M. Seliga, Podsekretarza Handlu Międzynarodowego w Departamencie Handlu USA do Very Jourovej, Komisarza ds. sprawiedliwości, spraw konsumenckich i równości płci (aneks I);
- opracowane przez Departament Handlu USA szczegóły mechanizmu „tarczy prywatności” (aneks II);

¹ Decyzja Komisji 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, Dziennik Urzędowy L 215 , 25/08/2000 P. 0007 – 0047.

² Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner.

³ Grupa Robocza Artykułu 29 to niezależny organ doradczy, w którym zasiadają przedstawiciele wszystkich organów ochrony danych z państw członkowskich, jak również Europejski Inspektor Ochrony Danych.

- list Johna F. Kerry, z Departamentu Stanu USA, wraz z memorandum dotyczące nowo powołanej instytucji Ombudsperson (aneks III);
- list Edith Ramirez z Federalnej Komisji Handlu opisujący egzekwowalność „tarczy prywatności” (aneks IV);
- list Anthony’ego R. Foxxa z Departamentu Transportu USA opisujący egzekwowalność Tarczy Prywatności (aneks V);
- list Roberta S. Litta, Dyrektora Wywiadu Narodowego (ODNI) dotyczący zabezpieczeń i ograniczeń znajdujących zastosowanie do amerykańskich służb (aneks VI);
- list Bruce’a C. Swartza z Departamentu Sprawiedliwości USA dotyczący zabezpieczeń i ograniczeń w zakresie dostępu Rządu USA do danych osobowych na potrzeby egzekwowania przepisów prawa i interesu publicznego (aneks VII).

Komunikat Komisji Europejskiej analizuje również zmiany w ochronie danych osobowych wprowadzone wskutek przyjęcia unijnego ogólnego rozporządzenia o ochronie danych⁴.

Komunikat podejmuje także zagadnienie projektu porozumienia międzynarodowego między Unią Europejską a Stanami Zjednoczonymi Ameryki w sprawie ochrony danych osobowych przekazywanych i przetwarzanych do celów działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych, w tym terroryzmu, w ramach współpracy policyjnej i sądowej w sprawach karnych - tzw. umowy parasolowej (ang. *Umbrella agreement*).

III. DOKUMENTY POWIĄZANE

- Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/14 Schrems;
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2015 r., poz. 2135 z późn. zm., dalej: Ustawa);
- Dyrektywa Parlamentu Europejskiego i Rady nr 95/46/WE z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej: Dyrektywa);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylenia decyzji ramową Rady 2008/977/WSiSW;
- Decyzja Komisji 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;

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG).

- Komunikat Komisji do Parlamentu Europejskiego i Rady - Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi, COM(2013) 846 final z 27 listopada 2013 r. wraz z przyjętym do niego stanowiskiem Rządu RP;
- 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, COM(2013) 847 final z 27 listopada 2013 r. wraz z przyjętym do niego stanowiskiem Rządu RP;
- Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie przekazywania danych osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (Schrems), COM(2015) 566, wraz z przyjętym do niego stanowiskiem Rządu RP;
- Decyzja Rady 2009/820/WPZiB z dnia 23 października 2009 r. w sprawie zawarcia w imieniu Unii Europejskiej Umowy o ekstradycji między Unią Europejską a Stanami Zjednoczonymi Ameryki oraz Umowy o wzajemnej pomocy prawnej między Unią Europejską a Stanami Zjednoczonymi Ameryki;
- Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.

IV. STANOWISKO RZĄDU

Tarcza Prywatności

Rząd RP jest w pełni świadomy roli wymiany informacji, w tym danych osobowych, we wzajemnych stosunkach handlowych pomiędzy Polską a Stanami Zjednoczonymi Ameryki. Stąd, Rząd RP z zadowoleniem przyjmuje wydanie Komunikatu (2016)117 doceniając znaczące wzmocnienie praw obywateli UE, których dane osobowe są przekazywane do USA, jakie przewiduje „tarcza prywatności”.

„Tarcza prywatności” będzie jednostronnym zobowiązaniem Rządu USA, którego adekwatność poziomu ochrony danych osobowych do obowiązującego na terytorium UE ma potwierdzić w swojej decyzji Komisja Europejska. Funkcjonowanie „tarczy prywatności” ma się opierać na dobrowolności i samocertyfikacji przystępujących do programu podmiotów. Podmioty przystępujące do programu będą zobowiązywać się do przestrzegania szeregu przewidzianych w nim zasad, weryfikowanych przez Departament Handlu USA. Za egzekwowanie zasad programu odpowiedzialne będą Departament Handlu, Federalna Komisja Handlu USA oraz powołana w Departamencie Stanu USA Ombudsperson.

„Tarcza prywatności” jest przez Rząd RP oceniana jako instrument, który umożliwi łatwe i szybkie przekazywanie danych osobowych z terytorium Unii Europejskiej, w tym Polski, do USA, przy zapewnieniu większej pewności prawnej, a jednocześnie w sposób zapewniający większe poszanowanie praw osób, których dane są przekazywane, niż to miało miejsce w przypadku „bezpiecznej przystani”.

Jednocześnie Rząd RP jest świadomy zastrzeżeń zgłaszanych wobec „tarczy prywatności”, m.in. przez Grupę Roboczą Artykułu 29 oraz przez Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO). Szczególnie niepokojące są zarzuty dotyczące braku odniesienia w „tarczy prywatności” do podstawowych zasad ochrony danych jak np. zasady ograniczonego celu przetwarzania czy niepodejmowania decyzji w oparciu o profilowanie, a także wątpliwości odnośnie do niezależności i odpowiednich uprawnień do efektywnego wykonywania zadań w ramach skutecznego mechanizmu odwoławczego w zakresie dostępu służb do danych przez stanowisko Ombudsperson. Rząd RP w swojej ocenie bierze jednak pod uwagę, że „tarcza prywatności” przewiduje mechanizm corocznego

przeglądu jej funkcjonowania, w który będą zaangażowane organy nadzorcze z poszczególnych państw członkowskich. To pozwala sądzić, że wszelkie potencjalne problemy, także związane z przeglądem „tarczy prywatności” w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych, uda się rozwiązać w tym trybie. Jak wskazuje Komisja Europejska, do prawidłowego funkcjonowania „tarczy prywatności” potrzebna jest współpraca amerykańskich odbiorców danych, amerykańskich organów administracji publicznej, europejskich organów ochrony danych osobowych oraz samej Komisji Europejskiej. Rząd RP liczy, że taka współpraca będzie miała miejsce, a „tarcza prywatności” stanie się mechanizmem umożliwiającym bezpieczne przekazywanie danych osobowych do USA.

Umowa Parasolowa

Rząd RP uznaje, że skuteczne reagowanie na wspólne zagrożenia dla bezpieczeństwa i wyzwania w sposób skoordynowany i oparty na współpracy wymaga odpowiednich możliwości w zakresie wymiany danych osobowych w ramach współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. W tym kontekście, co do zasady, pozytywnie należy ocenić wzmożone działania na poziomie UE na rzecz uregulowania relacji w tym zakresie ze Stanami Zjednoczonymi.

W ocenie Rządu RP odpowiednio zharmonizowany i kompleksowy zestaw gwarancji ochrony danych pozwoli na bardziej efektywną współpracę organów ścigania i większą pewność prawa przy przekazywaniu danych.

Reforma unijnych przepisów o ochronie danych osobowych

W kwietniu 2016 r., po czterech latach negocjacji, przyjęto ogólne rozporządzenie o ochronie danych, jak również dyrektywę w sprawie ochrony danych osobowych w sektorze bezpieczeństwa, w które Rząd RP był aktywnie zaangażowany od początku prac. Oba akty prawne zostały opublikowane w Dzienniku Urzędowym UE w dniu 4 maja br.

Rozporządzenie wprowadza szereg zmian mających na celu zmodernizowanie i lepsze dostosowanie przepisów o ochronie danych do warunków cyfrowego świata. Przewiduje również rozwiązania wzmacniające ochronę danych przekazywanych poza Unię Europejską i przetwarzanych przez podmioty z państw trzecich, a także rozszerza zakres terytorialny stosowania nowych reguł, obejmując nim podmioty z państw trzecich w przypadku, gdy oferują one produkty lub usługi osobom fizycznym w UE lub monitorują zachowanie takich osób. Wzmacnia również uprawnienia organów nadzorczych, m.in. wprowadzając możliwość nakładania dotkliwych sankcji. Rozporządzenie wprowadza także istotną zmianę w zakresie decyzji Komisji Europejskiej o adekwatności poziomu ochrony w państwie trzecim – nakładając na Komisję obowiązek ich przeglądu w okresie co cztery lata. Powyższe rozwiązania były popierane przez Rząd RP w trakcie prac nad tym aktem prawnym.

Celem dyrektywy w sprawie ochrony danych osobowych w sektorze bezpieczeństwa jest ułatwienie swobodnego przepływu danych osobowych między właściwymi organami do celów zapobiegania i zwalczania przestępczości, zapewniając przy tym wysoki oraz równorzędny we wszystkich państwach członkowskich stopień ochrony danych osobowych. Przedmiotowa dyrektywa obejmuje swoim zakresem zarówno krajowe, jak i transgraniczne przetwarzanie danych osobowych w tym obszarze. Ustanawia ona również stosowne gwarancje w zakresie przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych.

V. UZASADNIENIE STANOWISKA RZĄDU

Obecne stanowisko Rządu RP jest kontynuacją stanowiska do *Komunikatu Komisji do Parlamentu Europejskiego i Rady na temat odbudowy zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi* [COM (2013) 846], stanowiska do *Komunikatu 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* [COM (2013) 847] oraz stanowiska do *Komunikatu Komisji do Parlamentu Europejskiego i Rady w sprawie przekazywania danych*

osobowych z UE do Stanów Zjednoczonych na mocy dyrektywy 95/46/WE w następstwie wyroku Trybunału Sprawiedliwości w sprawie C-362/14 (*Schrems*) [COM(2015) 566], w których Rząd RP opowiadał się za modernizacją programu „bezpiecznej przystani” w celu zapewnienia wyższego poziomu ochrony danych osobowych w przypadku ich przekazywania z terytorium Unii Europejskiej do Stanów Zjednoczonych Ameryki⁵. Jednocześnie, w 2014 r. Ministerstwo Administracji i Cyfryzacji opublikowało własną analizę w zakresie programu „bezpiecznej przystani”, zawierającą szereg wątpliwości odnośnie do zasad jego funkcjonowania i postulatów, z których wiele zostało skonsumowanych w toku prac nad „tarczą prywatności”⁶.

Kontekst „tarczy prywatności” - wyrok w sprawie C-362/14 Schrems

Spór w sprawie *Schrems* powstał na gruncie toczącego się przed irlandzkim sądem postępowania, którego istota sprowadzała się do problematyki przekazywania do Stanów Zjednoczonych danych osobowych obywateli UE, przetwarzanych w ramach serwisu społecznościowego Facebook. Dane osobowe europejskich użytkowników tego serwisu są przekazywane do serwerów znajdujących się na terytorium Stanów Zjednoczonych i tam przetwarzane. Facebook Inc. (spółka prawa kalifornijskiego) i Facebook Ireland (spółka irlandzka), deklarowały przestrzeganie zasad poprzedniczki „tarczy prywatności” - „bezpiecznej przystani”. W postępowaniu sądowym skarżący, Maximilian Schrems, podniósł jednak, że z informacji ujawnionych przez Edwarda Snowdena w 2013 r., dotyczących działalności amerykańskiej Agencji Bezpieczeństwa Narodowego w ramach programu PRISM wynika, iż nie istnieje żadna rzeczywista ochrona danych osobowych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych w ramach programu „bezpieczna przystań”.

W wyroku wydanym w październiku 2015 r. Trybunał Sprawiedliwości UE stwierdził, że decyzja Komisji Europejskiej ws. adekwatności ochrony danych osobowych „bezpiecznej przystani” jest nieważna. Trybunał uznał, że amerykańskie wymogi dotyczące bezpieczeństwa narodowego, interesu publicznego i przestrzegania prawa USA nie mogą przeważać nad unijnym prawem podstawowym do poszanowania życia prywatnego. Natomiast w przypadku „bezpiecznej przystani” relacja była odwrotna, tj. przedsiębiorstwa amerykańskie należące do programu były zobowiązane do stosowania unijnych standardów ochrony danych osobowych pod warunkiem, że nie stało to w sprzeczności z amerykańskimi wymogami dotyczącymi bezpieczeństwa narodowego. Jednocześnie obywatele UE nie dysponowali odpowiednimi środkami ochrony sądowej, które umożliwiłyby im dochodzenie swoich praw.

Towarzyszący komunikatowi Komisji projekt decyzji ws. „tarczy prywatności” realizuje wytyczne wyroku Trybunału w sprawie *Schrems*. Komisja Europejska w omawianym komunikacie wskazuje, iż „tarcza prywatności” opiera się na:

- rygorystycznych obowiązkach nałożonych na amerykańskie przedsiębiorstwa przetwarzające dane osobowe Europejczyków i konsekwentnym egzekwowaniu przepisów: firmy pragnące pobierać dane osobowe z Europy będą musiały przestrzegać rygorystycznych zobowiązań dotyczących sposobu przetwarzania danych i poszanowania praw jednostek;
- wyraźnych zabezpieczeniach i wymogach przejrzystości regulujących dostęp administracji rządowej USA do danych osobowych: USA przedstawiły Unii po raz pierwszy wiążące zapewnienie, że dostęp organów publicznych do danych – związany z egzekwowaniem prawa i kwestiami bezpieczeństwa narodowego – będzie ograniczony oraz że będzie podlegać zabezpieczeniom i mechanizmom nadzoru, w szczególności przez specjalnie powołaną w tym celu instytucję Omudsperson;

⁵ Stanowisko Rządu RP w odniesieniu do oceny i propozycji ulepszenia programu „bezpieczna przystań”, przedstawionych przez KE w Komunikacie (2013) 847, zostało przyjęte przez Komitet do Spraw Europejskich w dniu 31 stycznia 2014 r. Stanowisko Rządu RP w odniesieniu do Komunikatu (2013) 846 zostało przyjęte przez Komitet do Spraw Europejskich w dniu 3 września 2014 r. Stanowisko Rządu RP w odniesieniu do Komunikatu (2015) 566 zostało przyjęte przez Komitet do Spraw Europejskich w dniu 21 grudnia 2015 r.

⁶ Por. dokument „Analiza programu 'bezpieczna przystań' (ang. Safe Harbour) w zakresie przekazywania danych osobowych z terytorium Polski do odbiorców w Stanach Zjednoczonych Ameryki”, stan prawny na dzień 10 kwietnia 2014 r., dostępna na https://mac.gov.pl/files/raport_ewaluacyjny_stosowania_programu_safe_harbour_-_dsi_mac.pdf

- efektywnej ochronie praw osób fizycznych z terytorium Unii Europejskiej, poprzez wprowadzenie alternatywnych możliwości dochodzenia ochrony swoich praw. Wprowadzono także szczegółowe regulacje dla przedsiębiorstw przetwarzających dane pracownicze, które obowiązkowo muszą poddać się nadzorowi europejskich organów nadzorczych. Dla pozostałych podmiotów amerykańskich, takie poddanie się nadzorowi jest dobrowolne. Jednocześnie wzmocniona zostanie współpraca europejskich organów ochrony danych z amerykańskim Departamentem Handlu oraz Federalną Komisją Handlu.

- aby regularnie monitorować funkcjonowanie porozumienia, co roku przeprowadzany będzie jego wspólny przegląd, który obejmie również kwestię dostępu do danych dla celów bezpieczeństwa narodowego. Przeglądu dokonywać będą Komisja Europejska i Departament Handlu USA, przy współpracy specjalistów z krajowych służb wywiadu w USA i europejskich organów ochrony danych. W przypadku, gdy podmioty amerykańskie, tak prywatne, jak i publiczne, nie będą stosować się do postanowień „tarczy prywatności”, Komisja Europejska może rozpocząć procedurę zawieszenia decyzji o adekwatności.

Komisja Europejska podkreśla jednocześnie, iż funkcjonowanie „tarczy prywatności” będzie wymagać zaangażowania wielu różnych grup interesów. Prócz uczestniczących w nowym programie podmiotów amerykańskich oraz poszczególnych organów amerykańskich, które będą odpowiadać za nadzór i egzekwowanie nowego mechanizmu, konieczne jest także zaangażowanie europejskich organów ochrony danych osobowych (w Polsce takim organem jest Generalny Inspektor Ochrony Danych Osobowych) oraz samej Komisji Europejskiej.

Opinia Grupy Roboczej Art. 29

W dniu 13 kwietnia 2016 r. swoją opinię odnośnie do Tarczy Prywatności wydała Grupa Robocza Artykułu 29, wskazując na zastrzeżenia m.in. w zakresie retencji danych osobowych, przestrzegania zasad niezbędności oraz proporcjonalności przetwarzania danych osobowych, zwłaszcza w kontekście zbierania danych osobowych dla celów bezpieczeństwa narodowego Stanów Zjednoczonych, niezależności powołanej Ombudsperson oraz tzw. dalszych transferów danych osobowych do państw trzecich.

Przekazywanie danych osobowych a prawo polskie

Przekazywanie danych z terytorium Polski do państw trzecich, które nie zapewniają odpowiedniego poziomu ochrony danych osobowych, w tym do USA, jest obecnie dopuszczalne przede wszystkim w oparciu o zasady wskazane w art. 47 ust. 3 Ustawy, który stanowi iż administrator danych może przekazać dane osobowe do państwa trzeciego, jeżeli: (i) osoba, której dane dotyczą, udzieliła na to zgody na piśmie; (ii) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie; (iii) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem; (iv) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych; (v) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą; (vi) dane są ogólnie dostępne. Jest ono możliwe także gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej, gwarantującymi odpowiedni poziom ochrony tych danych. W Polsce istnieje także możliwość uzyskania uprzedniej zgody GODO na transfer danych osobowych do państwa trzeciego. Jednocześnie, zgodnie z art. 48 ust. 2 ustawy, zgoda Generalnego Inspektora nie jest wymagana, jeżeli administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez: (i) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 Dyrektywy; lub (ii) prawnie wiążące reguły lub polityki ochrony danych osobowych, które zostały zatwierdzone przez Generalnego Inspektora.

Jednocześnie, zgodnie z art. 47 ust. 1 Ustawy, przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe zapewnia na swoim terytorium odpowiedni poziom ochrony danych osobowych. Wydanie przez Komisję Europejską decyzji o adekwatności, sprawia że dane

terytorium jest w polskim porządku prawnym uznawane za zapewniające odpowiedni poziom ochrony danych osobowych. Dotyczy to także decyzji o adekwatności w zakresie „tarczy prywatności”.

Samo wydanie decyzji o adekwatności poziomu ochrony danych osobowych, zgodnie z art. 25 ust. 6 Dyrektywy jest wyłączną kompetencją Komisji Europejskiej, dokonywaną w tzw. procedurze komitologii, po zasięgnięciu opinii przedstawicieli państw członkowskich.

Przekazywanie danych osobowych a negocjacje TTIP

Rząd RP zwraca także uwagę na prowadzone ze Stanami Zjednoczonymi Ameryki negocjacje umowy Transatlantyckiego Partnerstwa Handlowo-Inwestycyjnego (TTIP) oraz Porozumienia w sprawie handlu usługami (TiSA). Umowy te mają zawierać rozdział poświęcony handlowi elektronicznemu, w tym kwestiom przepływu danych. Podczas negocjacji ww. umów Polska konsekwentnie podkreśla niezmiernie istotną kwestię, jaką jest konieczność zachowania wysokich europejskich standardów ochrony danych osobowych, stąd też Rząd RP opowiada się za wykluczeniem kwestii ochrony danych osobowych z zakresu negocjacji.

Umowa Parasolowa

W dniu 26 maja 2010 r. Komisja Europejska przedłożyła projekt upoważnienia do prowadzenia negocjacji dotyczących umowy parasolowej. W dniu 3 grudnia 2010 r. Rada przyjęła decyzję upoważniającą Komisję do podjęcia negocjacji. W dniu 28 marca 2011 r. Komisja rozpoczęła negocjacje ze stroną amerykańską. Ostatecznie, KE oraz USA parafowały umowę w dniu 8 września 2015 r. W zależności od dalszego przebiegu realizowanych obecnie procedur zawarcia umowy międzynarodowej pomiędzy UE a Stanami Zjednoczonymi, umowa parasolowa mogłaby zostać podpisana podczas spotkania ministerialnego UE-USA, które odbędzie się w dniach 1-2 czerwca 2016 r. w Amsterdamie.

Celem projektu umowy jest zapewnienie wysokiego poziomu ochrony danych obywateli, których dane są przedmiotem wymiany w kontekście współpracy w obszarze bezpieczeństwa, a tym samym dalsze zacieśnianie współpracy między Unią Europejską i Stanami Zjednoczonymi w zwalczaniu przestępczości i terroryzmu na podstawie wspólnych wartości i zatwierdzonych gwarancji. Umowa parasolowa uzupełniać będzie dotychczasowe umowy zawarte pomiędzy UE-USA oraz pomiędzy państwami członkowskimi oraz Stanami Zjednoczonymi Ameryki w obszarze współpracy organów ścigania, jak również wyznaczać będzie wysokie standardy w kontekście ewentualnych przyszłych umów. W ocenie Komisji Europejskiej, wiążąca umowa międzynarodowa podniesie obecne standardy ochrony danych osobowych.

Konsekwencje Komunikatu COM (2016)117

- gospodarcze

Komunikat, opisując nowy instrument dla transferów danych osobowych do USA nie wywołuje konsekwencji gospodarczych. Natomiast wydanie przez Komisję Europejską decyzji o adekwatności „tarczy prywatności”, z przyczyn opisanych powyżej, pozytywnie wpłynie na polską gospodarkę, ułatwiając przepływ informacji i wymianę danych pomiędzy Polską a Stanami Zjednoczonymi Ameryki, co jest warunkiem niezbędnym dla wzajemnej wymiany handlowej.

- budżetowe

Komunikat nie niesie ze sobą konsekwencji budżetowych.

- legislacyjne

Komunikat nie niesie za sobą konieczności zmiany obowiązujących w Polsce przepisów prawa. Jednocześnie należy podkreślić, że w polskim porządku prawnym to GIODO, w ramach wykonywania swoich zadań ustawowych, dokonuje ostatecznej oceny przestrzegania wymogów w zakresie transferów danych osobowych do państw trzecich, a jego decyzje podlegają weryfikacji przez niezależne sądy. Generalny Inspektor Ochrony Danych Osobowych, po powzięciu uzasadnionych

podejrzeń o naruszenie standardów ochrony danych, może również zawiesić transfer danych do państwa trzeciego, pomimo istnienia formalnej decyzji Komisji Europejskiej o adekwatności.

VI. STANOWISKO PARTNERÓW SPOŁECZNYCH

Dokument został poddany konsultacjom publicznym. W ich toku swoje stanowiska przedstawili:

Fundacja Panoptykon, która wskazała na to, iż zasady „tarczy prywatności” oraz „umowy parasolowej” nie zmieniają faktu, że Stany Zjednoczone Ameryki nie posiadają uniwersalnego i mocnego systemu ochrony danych osobowych. Jako zły oceniła system oparty na samo-regulacji i samo-certyfikacji przy braku, zdaniem fundacji, efektywnych mechanizmów kontroli oraz środków ochrony i szerokich wyjątkach w zakresie bezpieczeństwa narodowego. Fundacja Panoptykon zwraca także uwagę na niedostosowanie zasad tarczy prywatności do standardów ogólnego rozporządzenia o ochronie danych. Fundacja Panoptykon podkreśla także szeroki dostęp amerykańskich służb do serwerów usługodawców oraz masowe gromadzenie i wykorzystywanie danych użytkowników Internetu. Zaznacza jednocześnie brak w „tarczy prywatności” indywidualnych środków ochrony sądowej, które zastąpiono powołaniem instytucji Ombudsperson, nie będącej, zdaniem fundacji, niezależnym organem. Zdaniem Fundacji Panoptykon przewidziane środki ochrony są skomplikowane i nieprzejrzyste. Fundacja podkreśla, że z opisanych w zasadach „tarczy prywatności” środków ochrony i egzekucji praw jedynie Federalna Komisja Handlu posiada kompetencje i możliwości prowadzenia dochodzeń oraz rozpatrywania spraw. Fundacja wskazuje także m.in. na brak jasności co do możliwości zawieszenia transferu danych przez europejskie organy ochrony danych w sytuacji ustalenia naruszenia lub wysokiego prawdopodobieństwa naruszenia zasad „tarczy prywatności”.

Polska Izba Informatyki i Telekomunikacji, która stoi na stanowisku, że ocena tego czy „tarcza prywatności” zapewnia rzeczywistą ochronę danych przekazywanych do USA będzie możliwe dopiero po pewnym okresie czasu. Niemniej, na chwilę obecną PIIT uznaje, że jest to krok w dobrym kierunku. PIIT wskazuje na instrumenty w „tarczy prywatności”, które umożliwiają egzekwowanie przez obywateli Unii Europejskiej swoich praw w amerykańskim systemie prawnym, a także transparentność nowego rozwiązania. PIIT wskazuje też na podejmowane w ostatnich latach starania rządu USA zmierzające do zwiększenia ochrony wszystkich osób fizycznych. Podkreśla także wyraźne ograniczenia dostępu organów państwowych USA do danych osobowych, które wprowadza „tarcza prywatności”. PIIT dokonał także analizy „tarczy prywatności” pod kątem spełniania przesłanek z wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/14 Schrems i uznał, że przesłanki te są w tym przypadku spełnione.

Amerykańska Izba Handlowa w Polsce (American Chamber of Commerce in Poland - AmCham), która wskazała na negatywne konsekwencje biznesowe unieważnienia adekwatności programu „bezpieczna przystań” przez Trybunał Sprawiedliwości Unii Europejskiej w wyroku w sprawie C-362/14 Schrems. Firmy amerykańskie działające w Polsce nie miały żadnego okresu przejściowego pozwalającego na przygotowanie innych podstaw prawnych do kontynuowania transatlantyckiego przekazywania danych. Podobnie jak PIIT, AmCham zajmuje stanowisko, iż ocena tego czy „tarcza prywatności” zapewnia rzeczywistą ochronę danych przekazywanych do USA będzie możliwe dopiero po pewnym okresie czasu. Jednak, po dokonaniu analizy przedstawionych dokumentów, uznaje, że ramy prawne „tarczy prywatności” zapewniają zasadniczo ekwiwalentny poziom ochrony danych osobowych przesyłanych z Unii Europejskiej do USA. Wskazane w „tarczy prywatności” instrumenty prawne służące zapewnieniu egzekwowania zasad przekazywania danych osobowych stanowią w ocenie AmCham kluczowe elementy tego rozwiązania przez pryzmat których należy odczytywać i analizować jej zasady. AmCham dokonał także analizy „tarczy prywatności” pod kątem spełniania przesłanek z wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-362/14 Schrems i uznał, że przesłanki te są w tym przypadku spełnione.

Związek Pracodawców Branży Internetowej Interactive Advertising Bureau Polska (IAB Polska), który dokonał obszernej analizy wytycznych z wyroku Trybunału Sprawiedliwości Unii

Europejskiej

w sprawie C-362/14 Schrems i zajął stanowisko, zgodnie z którym w przypadku niektórych kryteriów nie ma żadnych wątpliwości, że ramy prawne „tarczy prywatności” spełniają postulaty Trybunału Sprawiedliwości. IAB Polska podkreśla, że potencjalne słabe strony nie mają wpływu na ogólną skuteczność ram „tarczy prywatności” oraz zapewniany przez nią poziom prywatności i ochrony danych. Tak jak PIIT i AmCham, IAB Polska zaznaczyło, że ocena skuteczności nowych ram prawnych dla transatlantyckiego transferu danych możliwa będzie dopiero po wejściu w życie „tarczy prywatności”, gdyż tylko wtedy możliwa będzie weryfikacja, czy organizacje do niej przystępujące zapewniają wymagany poziom bezpieczeństwa.

Olesiński i Wspólnicy, kancelaria adwokacka, która zaznaczyła, że „tarcza prywatności” z uwagi w szczególności na wprowadzenie szeregu mechanizmów kontroli, ma teoretycznie szansę zapewnić skuteczniejszy nadzór nad amerykańskimi przedsiębiorstwami pozyskującymi dane osobowe z UE oraz wzmocnić prawa obywateli z UE w przypadku nieuprawnionego wykorzystania ich danych. Jednak brak skonkretyzowanych odpowiednich obowiązków i uprawnień amerykańskich przedsiębiorców, czy organów kontroli i obywateli z UE w amerykańskim porządku prawnym (a oparcie się w głównej mierze na określonych zobowiązaniach amerykańskich urzędników) oraz nieuwzględnianie nadchodzącej reformy systemu ochrony danych osobowych w UE, zdaniem kancelarii, może wskazywać na jej iluzoryczny charakter. Kancelaria zaznaczyła, że w przypadku przyjęcia „tarczy prywatności” w obecnym kształcie, amerykańscy przedsiębiorcy świadczący usługi związane z transmisją danych osobowych w relacji UE-USA, z uwagi na obowiązujące ich bardziej liberalne regulacje prawne, mogą być bardziej konkurencyjni na rynku unijnym niż przedsiębiorcy europejscy. Kancelaria zwróciła uwagę m.in. na to, iż aby zapewnić bezstronność tzw. Ombudsperson należałoby ją powoływać z grona osób z zasady bezstronnych, np. sędziów.

VII. WNIOSKI

Rząd RP z zadowoleniem przyjmuje wydanie przez Komisję Europejską komunikatu dotyczącego „tarczy prywatności”, dostrzegając znaczący postęp w zakresie standardów ochrony danych osobowych przekazywanych do USA w stosunku do jej poprzedniczki – programu „bezpieczna przystań”. Jednocześnie, Rząd RP zdaje sobie sprawę z pewnych braków proponowanego rozwiązania, które szczegółowo w swojej opinii omówiła Grupa Robocza Artykułu 29. Zdaniem Rządu RP zalety, w szczególności zwiększenie pewności prawnej w zakresie przekazywania danych osobowych do USA przy zachowaniu wysokiego poziomu ochrony danych, przeważają nad możliwymi słabościami proponowanego rozwiązania. Rząd RP ma nadzieję, że wszelkie potencjalne problemy w zakresie „tarczy prywatności” uda się rozwiązać w ramach corocznego przeglądu tego instrumentu i liczy w tym zakresie na aktywną postawę unijnych organów ochrony danych. Jednocześnie nie można wykluczyć, że „tarcza prywatności” będzie przedmiotem analizy Trybunału Sprawiedliwości Unii Europejskiej i dopiero jego wyrok może ostatecznie potwierdzić słuszność decyzji Komisji Europejskiej, w szczególności w kontekście wytycznych ze sprawy C-362/14 Schrems.

PRZEDSTAWICIEL KIEROWNICTWA RESORTU WIODĄCEGO UPOWAŻNIONY DO PREZENTOWANIA STANOWISKA

Pani Anna Streżyńska, Minister Cyfryzacji.