



Warszawa, 15 kwietnia 2016 r.

Uwagi dotyczące projektu komunikatu *Transatlantic Data Flows: Restoring Trust through Strong Safeguards*

Poniżej przedstawiamy uwagi Fundacji Panoptykon dotyczące projektu komunikatu Komisji Europejskiej *Transatlantic Data Flows: Restoring Trust through Strong Safeguards*. Nasze uwagi przedstawiamy jako komentarz do tez stawianych w projekcie komunikatu:

1. Privacy Shield stanowi zdecydowaną i skuteczną odpowiedź na krytykę Zasad Safe Harbour oraz orzeczenie TSUE w sprawie *Maximillian Schrems p. Data Protection Commissioner*

Punktem wyjścia dla oceny stopnia adekwatności ochrony danych osobowych przez amerykańskie firmy, jest fakt iż USA nie gwarantują uniwersalnego i mocnego systemu ochrony danych osobowych. Niestety ani Zasady Privacy Shield ani tzw. Umowa Parasolowa nie zmieniają tego stanu rzeczy. Zasady Privacy Shield opierają się na tych samych, złych założeniach, które były zawarte w Zasadach Safe Harbour: samo-regulacji, samo-certyfikacji, braku efektywnych mechanizmów kontroli oraz środków ochrony i szerokich wyjątkach w zakresie bezpieczeństwa narodowego. Co więcej decyzja w sprawie Privacy Shield będzie obowiązywać już po wprowadzeniu nowych, europejskich przepisów dotyczących ochrony danych osobowych. Pomimo, że tekst nowych przepisów znany jest od dawna to Zasady Privacy Shield tych standardów nie uwzględniają. Pogląd taki został zawarty m.in. w ostatniej opinii Grupy Roboczej Art. 29.

2. Privacy Shield zawiera jasne ograniczania i gwarancje ochrony w kontekście dostępu do danych przez amerykańskie instytucje rządowe

Zasady Privacy Shield podobnie jak Zasady Safe Harbour zawierają wyjątki dotyczące ochrony danych osobowych, podyktowane kwestiami bezpieczeństwa. Opisane szczegółowo w Zasadach Privacy Shield ustawodawstwo amerykańskie, dotyczące wykorzystywania danych osobowych do walki z terroryzmem i poważną przestępczością, wciąż nie spełnia wymogów niezbędności i proporcjonalności. Dotyczy to przede wszystkim szerokiego dostępu służb amerykańskich do serwerów usługodawców oraz masowego gromadzenia i wykorzystywania danych użytkowników (*bulk use i bulk collection*). Co więcej, amerykański porządek prawny nie będzie gwarantował podmiotom danych indywidualnych środków ochrony sądowej. W tym kontekście strona amerykańska proponuje by organem zajmującym się skargami został „Ombudsperson” – stanowisko, które funkcjonuje w ramach Departamentu Stanu USA. Stanowisku temu nie przypisano żadnych kompetencji do podejmowania wiążących rozstrzygnięć, a jedynie możliwość sygnalizowania odpowiednim instytucjom problemów wynikających z konkretnych spraw. Ombudsper-

son nie jest też niezależnym organem, ponieważ podlega bezpośrednio amerykańskiej administracji rządowej.

3. Privacy Shield ustanawia skuteczne środki ochrony dla obywateli Unii Europejskiej

Zasady Privacy Shield mówią o 6 mechanizmach ochrony i egzekwowania praw przez obywateli Unii Europejskiej. Trudno jednak uznać za w pełni skuteczne i odpowiadające na zarzuty podnoszone uprzednio przeciwko Zasadom Safe Harbour. Przede wszystkim przewidziane środki ochrony są skomplikowane i nieprzejrzyste. Organy, które mogą rozpatrywać skargi wnoszone przed podmiot danych nie zawsze są niezależne (np. organy alternatywnego rozpatrywania sporów) – co jest przecież wymogiem wynikającym z europejskich standardów prawnych. Z kolei rozpatrzenie sprawy przez firmę, wobec której skarga jest wnoszona, trudno w ogóle uznać za środek ochrony. Jest to raczej prawo do informacji i kontaktu z podmiotem naruszającym prawo. Podmiot danych zostaje więc skierowany na ścieżkę dochodzenia swoich praw, która *de facto* nie musi prowadzić do wiążących rozstrzygnięć. Z opisywanych w Zasadach Privacy Shield środków ochrony i egzekucji praw, jedynie Federalna Komisja Handlu posiada kompetencje i możliwości prowadzenia dochodzeń oraz rozpatrywania spraw, które mogą – do pewnego stopnia – spełniać wymogi wynikające z europejskiego prawa ochrony danych osobowych.

Oprócz powyższych kwestii z Zasadami Privacy Shield wiążą się dodatkowe problemy, w tym:

- ograniczenie zasady Wybór (*Choice*) tylko do sytuacji, kiedy dane mają zostać przekazane podmiotowi trzeciemu lub gdy następuje materialna zamiana podstaw przetwarzania;
- daleko idące wyjątki dotyczące możliwości przetwarzania danych wrażliwych;
- brak jasności co do możliwości zawieszenia transferu danych przez europejskie organy ochrony danych w sytuacji ustalenia naruszenia lub wysokiego prawdopodobieństwa naruszenia Zasad Privacy Shield;
- nieuwzględnienie zasady ograniczonego okresu przechowywania danych;
- brak gwarancji dotyczących profilowania oraz decyzji podejmowanych na podstawie automatycznego przetwarzania danych.