



Warszawa, 12 grudnia 2011 r.

**Szanowny Pan**

**Jacek Cichocki**

Minister Spraw Wewnętrznych

*Szanowny Panie Ministrze,*

23 listopada Komisja Europejska podpisała porozumienie w sprawie przechowywania i udostępniania danych pasażerów lotniczych (PNR) między państwami członkowskimi Unii Europejskiej a Stanami Zjednoczonymi. Podczas posiedzenia Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych JHA Unii Europejskiej, które odbędzie się 13 grudnia, będzie Pan współdecydował o dalszych losach tego porozumienia. Zwracamy się do Pana z apelem o jego odrzucenie, gdyż – w naszej ocenie – treść tego dokumentu stoi w sprzeczności z europejskim oraz polskim prawem w zakresie ochrony danych osobowych.

Jak z pewnością Panu wiadomo, porozumienie wzbudza poważne kontrowersje nie tylko w Polsce i Europie, ale także na całym świecie. Poważne zastrzeżenia zgłaszają środowiska obywatelskie, organizacje działające na rzecz praw człowieka, a także Europejski Inspektor Ochrony Danych. Jako organizacja, która aktywnie angażuje się w działania na rzecz ochrony praw człowieka w przestrzeni cyfrowej, pragniemy zwrócić Pańską uwagę na szereg problemów, jakie wynikają lub mogą wyniknąć z akceptacji wspomnianego porozumienia.

Dane PNR (*Passanger Name Records*) to dane o pasażerach, zbierane zwyczajowo przez linie lotnicze w celach komercyjnych. Do takich danych zalicza się: imię, nazwisko, adres e-mail, telefon, trasę podróży, formę płatności za bilet, numer karty kredytowej, informację o bagażu itp. Dane PNR mogą zawierać także bardzo wrażliwe informacje, takie jak preferencje dotyczące posiłku serwowanego na pokładzie samolotu czy rezerwacje hotelowe. Posługując się odpowiednim programem komputerowym, w kilka sekund można ustalić rutynę podróżowania poszczególnych osób, a nawet powiązania zachodzące pomiędzy poszczególnymi podróżnymi.

Porozumienie o przekazywaniu danych PNR jest wynikiem lobbingu ze strony amerykańskich władz oraz przedsiębiorstw zajmujących się tworzeniem chmur obliczeniowych (*cloud computing*). Już w 2004 roku Komisja Europejska podpisała pierwszy dokument obligujący europejskie linie lotnicze do przekazywania danych o pasażerach Departamentowi Spraw Wewnętrznych Stanów Zjednoczonych na 72 godziny przed odlotem. Porozumienie z 2004 roku zostało jednak uznane przez Parlament Europejski za niezgodne z europejskimi standardami ochrony danych osobowych, co zmusiło Komisję Europejską i rząd Stanów Zjednoczonych do ponownych negocjacji.

Od kilku lat dane PNR wykorzystywane są przez organy ścigania, głównie amerykańskie, w celu walki z terroryzmem i przestępczością, jednak jak do tej pory nie przedstawiono żadnych statystyk sugerujących, że istnieje bezpośrednia zależność między wykrywalnością przestępstw o charakterze terrorystycznym a korzystaniem przez służby z danych PNR.

W naszej ocenie proponowane w porozumieniu rozwiązania nie chronią obywateli przed atakami terrorystycznymi i zorganizowaną przestępczością, natomiast w istotnym stopniu ograniczają prywatność pasażerów. W opinii Europejskiego Inspektora Ochrony Danych istotą porozumienia jest automatyczne profilowanie każdego podróżującego pod kątem tego, czy może on stanowić zagrożenie terrorystyczne oraz tworzenie tzw. czarnych list. O wadliwości i wypaczeniach mechanizmów porozumienia przekonała się niedawno Wielka Brytania, w której na skutek analizy danych PNR na „czarnych listach” znaleźli się m.in. wegetarianie, osoby wykupujące rezerwacje *last minute* czy pasażerowie podróżujące „w jedną stronę”.

Porozumienie ma istotne wady prawne. Podstawowym problemem jest brak mechanizmów zapewniających efektywność i egzekwowalność praw, które mają być zagwarantowane obywatelom. Zgodnie z treścią porozumienia, obywatele UE mają prawo do informacji o zgromadzonych na ich temat danych. Jest to jednak uprawnienie czysto teoretyczne ponieważ porozumienie nie tworzy skorelowanego z nim obowiązku udzielenia informacji po stronie amerykańskich władz czy linii lotniczych. Na gruncie porozumienia obywatel ma również prawo żądać korekty zgromadzonych informacji, jednak ani organy, ani linie lotnicze, nie są zobowiązane uwzględnić jego prośby. Ponadto, nie istnieje w tym względzie żadna procedura odwoławcza, gdyż właściwe w takich przypadkach prawo amerykańskie (*American Privacy Act*) ma zastosowanie jedynie do obywateli amerykańskich, a nie do cudzoziemców. Zgodnie z treścią porozumienia, każdy obywatel, którego dane zostały w sposób bezprawny zgromadzone lub przetworzone, ma prawo wystąpić o odszkodowanie, jednak ani porozumienie, ani inne amerykańskie akty prawne nie przewidują jurysdykcji sądów amerykańskich w zakresie orzekania o naruszeniu porozumienia lub prawa cudzoziemców do ochrony danych osobowych.

Porozumienie ma także szereg wad technicznych. Po pierwsze, proponuje się w nim obowiązkową depersonalizację danych po okresie 6 miesięcy. Depersonalizacja ma mieć jednak charakter „nieostateczny” i dotyczyć jedynie kopii plików udostępnianych Departamentowi Spraw Wewnętrznych Stanów Zjednoczonych. Umieszczony w pliku lokalizator rejestru ma gwarantować możliwość ponownego zestawienia informacji, czyli dotarcie do pełnych danych przechowywanych w systemie. W związku z tym, że porozumienie nie przewiduje żadnych mechanizmów kontroli nad uzyskiwaniem dostępu do systemu, okres w którym amerykańskie służby będą w stanie uzyskać pełne dane PNR może być arbitralnie przedłużany. Jest to praktyka naruszająca europejskie standardy ochrony danych osobowych. Po drugie, porozumienie zakłada, że raz uzyskane dane mogą być przechowywane przez 10 lat, a w przypadku przestępstw terrorystycznych – nawet przez 15. Wydaje się, że przy tak skonstruowanym podziale nie można uniknąć przechowywania wszystkich danych „na wszelki wypadek” przez maksymalny dopuszczalny okres.

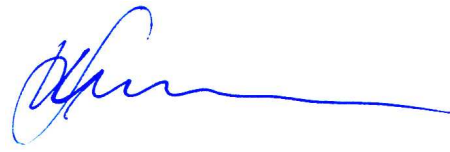
Wszystko to rodzi poważne wątpliwości, co do zgodności proponowanych rozwiązań z polskimi i europejskimi standardami prawnymi. Wątpliwości te nie zostały rozwiane w trakcie kilkuletnich prac nad porozumieniem. W naszej ocenie, przyjęcie proponowanych rozwiązań będzie skutkować naruszeniem prawa do prywatności oraz prawa do ochrony danych osobowych – ważnych w demokratycznym państwie prawnym. Dlatego apelujemy o rozważę i głosowanie za odrzuceniem porozumienia w całości.

Mamy nadzieję, że nasz apel spotka się z Pana pozytywnym przyjęciem,

w imieniu Fundacji PANOPTYKON



Katarzyna Szymielewicz  
Dyrektorka



Małgorzata Szumańska  
Członkini Zarządu