Komisja Europejska – Arkusz informacyjny

Pytania i odpowiedzi: Wytyczne dotyczące transatlantyckiego przekazywania danych po wydaniu wyroku w sprawie Schrems

Bruksela, 6 listopada 2015 r.

Czym było porozumienie w sprawie programu bezpiecznej przystani (Safe Harbour)?

Dyrektywa UE o ochronie danych z 1995 r. określa zasady przekazywania danych osobowych z UE do krajów spoza UE. Na mocy tych przepisów Komisja może wydać decyzję stwierdzającą, że kraj spoza UE zapewnia „odpowiedni poziom ochrony danych". Decyzje takie powszechnie określa się mianem "decyzji stwierdzających odpowiedni poziom ochrony".

Na podstawie dyrektywy o ochronie danych z 1995 r. w dniu 26 lipca 2000 r. Komisja Europejska przyjęła decyzję ("decyzję w sprawie programu bezpiecznej przystani (Safe Harbour)") uznającą "Zasady ochrony prywatności Safe Harbour" wydane przez Departament Handlu Stanów Zjednoczonych, jako zapewniające odpowiednią ochronę na potrzeby przekazywania danych osobowych z UE.

W rezultacie decyzja w sprawie programu bezpiecznej przystani pozwalała na przekazywanie danych osobowych w celach komercyjnych z przedsiębiorstw w UE do przedsiębiorstw w USA, które zobowiązały się do przestrzegania Zasad.

Funkcjonowanie porozumienia w sprawie bezpiecznej przystani oparte było na zobowiązaniach i samo-certyfikacji przedsiębiorstw, które przystąpiły do porozumienia. Przedsiębiorstwa musiały przystąpić do porozumienia poprzez zawiadomienie Departamentu Handlu USA, podczas gdy Federalna Komisji Handlu USA była odpowiedzialna za egzekwowanie Safe Harbour. Przystąpienie jest dobrowolne, ale zasady były wiążące dla tych, którzy do nich przystąpili.

2013: Doniesienia o działaniach Agencji Bezpieczeństwa Narodowego (NSA) oraz 13 Zaleceń

Doniesienia dotyczące NSA w 2013 r. wywołały szereg ważnych pytań dotyczących nadzoru i ochrony danych osobowych. Program bezpiecznej przystani pozwalał na ograniczenia zasad ochrony danych, gdy to konieczne ze względu na bezpieczeństwo narodowe. W związku z tym powstało pytanie, czy gromadzenie i przetwarzanie danych osobowych na dużą skalę na mocy amerykańskich programów nadzoru było konieczne i proporcjonalne w celu zaspokojenia interesów bezpieczeństwa narodowego.

Po doniesieniach Snowdena Komisja postanowiła dokonać przeglądu programu bezpiecznej przystani i wydała 13 zaleceń mających na celu jego ulepszenie w listopadzie 2013 r.:

Przejrzystość

1. Przedsiębiorstwa, które dokonały samo-certyfikacji, powinny udostępnić do wiadomości publicznej swoje polityki prywatności.

2. Polityki prywatności stron internetowych przedsiębiorstw, które dokonały samo-certyfikacji, zawsze powinny zawierać link do strony internetowej Departamentu Handlu poświęconej programowi Safe Harbour, na której wymienieni są wszyscy 'obecni' członkowie programu.
3. Przedsiębiorstwa, które dokonały samo-certyfikacji, powinny publikować warunki ochrony prywatności dotyczące wszelkich umów zawieranych przez nie z podwykonawcami, np. dotyczących usług przetwarzania w chmurze.
4. Wyraźne oznaczenie na stronie internetowej Departamentu Handlu wszystkich przedsiębiorstw, które nie są obecnie członkami programu.

Odszkodowania

1. Polityki prywatności na stronach internetowych przedsiębiorstw powinny zawierać link odnoszący do podmiotu zapewniającego alternatywne metody rozwiązywania sporów (ADR).
2. ADR powinny być łatwo dostępne i przystępne pod względem kosztów.
3. Departament Handlu powinien systematyczniej nadzorować dostawców ADR pod względem przejrzystości i dostępności informacji przez nie zapewnianych dotyczących procedury, którą wykorzystują, i dalszych działań, które podejmują w związku ze skargami.

Egzekwowanie prawa

1. Po dokonaniu certyfikacji lub ponownej certyfikacji przedsiębiorstw w ramach programu bezpiecznej przystani, określony procent tych przedsiębiorstw powinien podlegać kontroli z urzędu w zakresie skutecznej zgodności ich polityk prywatności z zasadami ochrony danych (wykraczającej poza kontrolę zgodności z wymogami formalnymi).
2. Zawsze gdy stwierdza się niezgodność, w wyniku skargi lub postępowania/kontroli, przedsiębiorstwo powinno podlegać następczej konkretnej kontroli po upływie 1 roku.
3. W przypadku wątpliwości co do zapewnienia zgodności przez przedsiębiorstwo lub skarg w toku, Departament Handlu powinien poinformować właściwy organ ochrony danych UE.
4. Bezpodstawne roszczenia dotyczące przestrzegania programu nadal powinny być przedmiotem postępowań/kontroli.

Dostęp władz USA

1. Polityki prywatności przedsiębiorstw, które dokonały samo-certyfikacji, powinny obejmować informacje dotyczące stopnia, do jakiego prawo USA pozwala władzom publicznym na gromadzenie i przetwarzanie danych przekazywanych na mocy programu bezpiecznej przystani. W szczególności przedsiębiorstwa należy zachęcać do wskazania w ich politykach prywatności, gdy stosują wyłączenia od Zasad w celu zapewnienia bezpieczeństwa narodowego, zaspokojenia interesu publicznego czy też przestrzegania wymogów w zakresie egzekwowania prawa.
2. Ważne jest, aby wyłączenie ze względu na bezpieczeństwo narodowe przewidziane przez decyzję w sprawie programu bezpiecznej przystani wykorzystywać tylko w stopniu, w jakim jest to absolutnie konieczne lub proporcjonalne.

Co oznaczała niedawna sprawa *Schrems* dla programu bezpiecznej przystani?

6 października Trybunał Sprawiedliwości oświadczył w sprawie *Schrems*, że decyzja Komisji w sprawie programu bezpiecznej przystani jest nieważna. W orzeczeniu podkreślił znaczenie podstawowego prawa do ochrony danych, w tym przypadku, gdy dane osobowe są przekazywane do krajów trzecich. W wyroku potwierdzono podejście stosowane przez Komisję od listopada 2013 r. Porozumienie w sprawie bezpiecznej przystani nie zapewniało wystarczającego poziomu ochrony danych wymaganego przez prawo UE.

W świetle wyroku do najważniejszych priorytetów Komisji należą:

- **Zapewnienie wysokiego poziomu ochrony danych osobowych,** gdy przekazywane są one przez Atlantyk;
- **Dalsze prowadzenie transatlantyckiego przekazywania danych** przy odpowiednich zabezpieczeniach.
- **Skoordynowana odpowiedź z krajowymi organami ochrony danych** w celu zapewnienia jednolitego stosowania prawa UE na rynku wewnętrznym oraz jasnych wytycznych dla europejskich przedsiębiorstw.

Jakie mechanizmy mogą wykorzystywać przedsiębiorstwa zamiast programu bezpiecznej przystani?

W międzyczasie, przed uzgodnieniem poddanych przeglądowi zasad Safe Harbour, transatlantyckie przepływy danych między przedsiębiorstwami mogą nadal mieć miejsce przy użyciu innych mechanizmów służących do międzynarodowego przekazywania danych osobowych dostępnych na mocy prawa ochrony danych UE.

Do tych innych mechanizmów należą:

- **Standardowe klauzule umowne** dla przedsiębiorstw po obu stronach Atlantyku, które określają obowiązki w zakresie ochrony danych oraz są zatwierdzone przez Komisję
- **Wiążące Reguły Korporacyjne** dla przekazywania w ramach międzynarodowej grupy przedsiębiorstw, które są zatwierdzane przez krajowe organy ochrony danych.

Zasady ochrony danych obejmują również **odstępstwa,** na mocy których dane mogą być przekazywane na podstawie:

- Zawarcia lub realizacji umowy [w tym sytuacje przed zawarciem umowy, np. dane mogą być przekazywane w celu rezerwacji lotu lub pokoju hotelowego w USA];
- Ustanowienie, realizacja lub ochrona roszczeń prawnych;
- Jeżeli brak jest innych podstaw, dobrowolna i świadoma zgoda osoby.

Co postanowiły organy ochrony danych po wydaniu wyroku?

Grupa Robocza Artykułu 29 – niezależny organ doradczy, który zrzesza przedstawicieli wszystkich organów ochrony danych – 16 października wydała oświadczenie dotyczące pierwszych wniosków, jakie należy wyciągnąć z wyroku.

Oświadczenie to zawiera m.in. następujące wytyczne dotyczące przekazywania danych:

- Przekazywanie danych nie może być już oparte na decyzji Komisji w sprawie programu bezpiecznej przystani;

- Standardowe klauzule umowne ("SCCs") oraz Wiążące Reguły Korporacyjne ("BCR") mogą być w międzyczasie wykorzystywane jako podstawa operacji przekazywania danych, choć Grupa Robocza Artykułu 29 stwierdziła również, że nadal będzie analizowała wyrok pod względem tych alternatywnych narzędzi;

- W dalszej części oświadczenia wezwano państwa członkowskie i instytucje unijne do rozpoczęcia dyskusji z władzami Stanów Zjednoczonych celem znalezienia prawnych i technicznych rozwiązań umożliwiających przekazywanie danych; obecne negocjacje dotyczące Safe Harbour mogą, zdaniem Grupy Roboczej Artykułu 29, być częścią tego rozwiązania.

Grupa Robocza Artykułu 29 ogłosiła, że, jeżeli do końca stycznia 2016 r., we współpracy z władzami Stanów Zjednoczonych oraz w zależności od oceny narzędzi wykorzystywanych przy przekazywaniu danych, nie znajdzie odpowiedniego rozwiązania, organy ochrony danych UE będą zobowiązane do podjęcia wszelkich koniecznych i właściwych działań, które mogą obejmować skoordynowane działania w zakresie egzekwowania prawa.

I wreszcie, Grupa Robocza Artykułu 29 podkreśla podział odpowiedzialności pomiędzy organy danych osobowych, instytucje Unii Europejskiej, państwa członkowskie i przedstawicieli biznesu, tak aby znaleźć zrównoważone rozwiązania dla wdrożenia wyroku Trybunału. W szczególności Grupa Robocza wezwała przedstawicieli biznesu do rozważenia wprowadzenia prawnych i technicznych rozwiązań, aby zmniejszyć wszelkie możliwe zagrożenia, z jakimi mają do czynienia przy przekazywaniu danych.

Dlaczego Komisja wydaje Komunikat?

Dopóki negocjacje nie zostaną zakończone, przedsiębiorstwa muszą przestrzegać postanowień wyroku i polegać na alternatywnych narzędziach służących do przekazywania danych, gdy są dostępne. Komunikat wyjaśniający Komisji zawiera analizę konsekwencji wyroku i określa alternatywne mechanizmy służące do przekazywania danych osobowych do USA. Komisja będzie także nadal ściśle współpracować z niezależnymi organami ochrony danych w celu zapewnienia jednolitego stosowania wyroku.

Co się stało po wydaniu wyroku Trybunału Sprawiedliwości?

Nowe porozumienie ogólne to najlepszy sposób ochrony obywateli UE w erze coraz większej liczby operacji przekazywania danych handlowych przez Atlantyk. Jest to ważne nie tylko dla transatlantyckich kontaktów handlowych, ale przede wszystkim dla obywateli UE i ich praw do ochrony danych. Tylko szczegółowe ramy prawne, przewidujące zobowiązania i egzekwowanie przez władze USA, mogą zapewnić w praktyce poziom ochrony danych, na jaki Europejczycy zasługują i do jakiego są uprawnieni na mocy prawa ochrony danych UE.

Alternatywne operacje przekazywania stanowią rozwiązanie krótkoterminowe; jednak zważywszy na ilość operacji przekazywania kluczowe jest, aby istniały proste i skuteczne ramy prawne.

Tuż po wydaniu wyroku Komisarz **Jourová** była w kontakcie z Sekretarzem ds. Handlu **Pritzker** w sprawie dalszych kroków, a negocjacje na poziomie technicznym są kontynuowane w szybkim tempie.

Komisarz **Jourová** uda się do Waszyngtonu 13 listopada celem kontynuacji negocjacji dotyczących odnowionych i bezpiecznych ram odnoszących się do przekazywania danych osobowych. Nowe porozumienie w sprawie programu bezpiecznej przystani zapewni dalsze transatlantyckie przepływy danych, które pozwolą na solidne zabezpieczenia i pewność prawną tak samo dla przedsiębiorstw, jak i obywateli.

Na jakim etapie znajdują się negocjacje na rzecz *bezpieczniejszej* przystani?

Co do Zaleceń dotyczących przejrzystości, egzekwowania i odszkodowań (1 - 11) co do zasady istnieje porozumienie, ale Komisja nadal prowadzi dyskusje nad tym, jak zapewnić, aby te zobowiązania były wystarczająco wiążące, aby w pełni spełnić wymogi Trybunału.

USA faktycznie zareagowały na te punkty, zobowiązując się do silniejszego nadzoru przez Departament Handlu, silniejszej współpracy z europejskimi organami ochrony danych oraz priorytetowego traktowania skarg przez Federalną Komisję Handlu. Doprowadzi to do przekształcenia systemu z czysto samoregulujacego się w system nadzoru szybciej reagujący, proaktywny i zapewniający wsparcie przez istotne egzekwowanie prawa, w tym sankcje.

Europejskie krajowe organy ochrony danych będą miały bardziej aktywną i widoczną rolę w systemie niż wcześniej. Na przykład usprawniono interfejs i kanały komunikacji między organami ochrony danych i Departamentem Handlu.

Trybunał potwierdził, że decyzja w sprawie odpowiedniego poziomu ochrony to "żywy" dokument; musi być poddawana okresowym przeglądom w świetle zmian obcego systemu. Komisja pracuje nad tym aspektem z USA, aby wprowadzić mechanizm corocznego wspólnego przeglądu, który obejmie wszystkie aspekty funkcjonowania nowych ram, w tym wykorzystywania wyłączeń do celów egzekwania prawa oraz ze względów bezpieczeństwa narodowego, oraz który obejmie wszystkie istotne organy z obu stron.

Jeżeli chodzi o interwencje organów publicznych, w szczególności ze względów egzekwowania prawa i bezpieczeństwa narodowego, Trybunał podkreśla, że taki dostęp musi podlegać jasnym warunkom i ograniczeniom. Wyraźnie odzwierciedla do zalecenie wydane przez Komisję dwa lata temu, aby " wyłączenie z uwagi na bezpieczeństwo narodowe przewidziane przez decyzję w sprawie programu bezpiecznej przystani było wykorzystywane tylko w takim zakresie, jaki jest absolutnie konieczny i proporcjonalny". Komisja współpracuje z USA na rzecz zapewnienia, aby istniały wystarczające ograniczenia i zabezpieczenia w celu zapobieżenia dostępowi lub wykorzystywaniu danych na "uogólnionej podstawie" oraz zapewnienia, aby istniała wystarczająca kontrola sądowa nad takimi działaniami.

Więcej informacji:

IP/15/6015

Komunikat