PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 101 (2722), 27 LIPCA 2023 © PISM

BIULETYN

Do trzech razy sztuka: nowe zasady przepływu danych między UE i USA

Stefania Kolarz

Decyzją z 10 lipca br. Komisja Europejska (KE) potwierdziła, że uważa nowo uzgodniony poziom ochrony danych osobowych w USA za odpowiadający unijnym standardom. Choć ułatwi to współdziałanie europejskich i amerykańskich firm, może okazać się rozwiązaniem krótkotrwałym. Na niedoskonałości w zakresie amerykańskiej ochrony danych wskazali już m.in. Europejska Rada Ochrony Danych iaktywiści. Potencjalne skargi sądowe oparte na ich argumentach mogą doprowadzić do unieważnienia przez Trybunał Sprawiedliwości UE (TSUE) kolejnej – po tzw. Safe Harbor i Privacy Shield – decyzji KE upraszczającej przekazywanie danych osobowych do USA.

Przekazywanie danych do państw trzecich. Obowiązujące w UE oraz w Norwegii, Liechtensteinie i Islandii unijne rozporządzenie o ochronie danych osobowych (RODO) przewiduje rygorystyczne warunki legalności przekazywania danych do państw trzecich. Konieczne jest ustalenie, że państwo, do którego one trafią, zapewnia prawa i środki odwoławcze porównywalne z RODO. Najpewniejszym potwierdzeniem takiego statusu jest decyzja Komisji Europejskiej (KE) stwierdzająca istnienie odpowiedniego poziomu ochrony, zrównująca zasady przekazywania danych do państwa trzeciego ze stosowanymi w UE. Takie decyzje są jednak nieliczne – dotychczas objęły m.in. Izrael, Japonię, Wielką Brytanię. W pozostałych przypadkach przekazywanie danych jest możliwe, ale obarczone dodatkowymi obowiązkami i większym ryzykiem naruszenia RODO. Jego podstawą mogą być m.in. standardowe klauzule umowne (SCC) lub – dla przedsiębiorstw działających w kilku państwach – wiążące reguły korporacyjne (BCR), a także przeprowadzenie oceny skutków przekazania danych do państwa trzeciego (TIA). Ponieważ SCC są wdrażane indywidualnie przez poszczególne firmy, często różnią się od modelu proponowanego przez KE, a ich weryfikacja i przeprowadzenie TIA są czasochłonne. Wadą tego rozwiązania jest też możliwa rozbieżność oceny jakości ochrony przez firmę przekazującą dane i przez organ kontroli, do którego mogą zgłaszać skargi osoby, których dane są przetwarzane. Natomiast BCR muszą zostać uprzednio zatwierdzone na poziomie krajowym, a następnie przez Europejską Radę Ochrony Danych (EROD), co także jest uciążliwe dla firm.

Problem zgodności z prawem pojawia się też przy przekazywaniu danych do USA. W 2000 r. USA uzyskały decyzję KE (tzw. Safe Harbor), ale ujawnienie przez Edwarda Snowdena szerokiego dostępu amerykańskich służb do danych Europejczyków wywołało obawy o skutki transferów. Zostały one wykorzystane w sprawach wytaczanych Facebookowi przez aktywistę Maxa Schremsa. W ich wyniku w 2015 r. TSUE unieważnił decyzję Safe Harbor, a w 2020 r. podważył kolejne ramy współpracy – wprowadzoną w 2016 r. Privacy Shield. W drugiej sprawie Schrems wykazał m.in., że USA nie przewidują dla Europejczyków możliwości zaskarżenia sposobu przetwarzania ich danych, zaś TSUE uznał, że amerykańskie prawo daje władzom dostęp do danych nieproporcjonalny do celu zapewnienia bezpieczeństwa narodowego. Zmusiło to amerykańskie firmy do stosowania innych rozwiązań, np. SCC, BCR, przenoszenia się do UE lub otwierania w niej filii (by ograniczyć przekazywanie danych do USA), a w niektórych przypadkach do rezygnacji ze współpracy firm z Europy i USA. Przykładowo firma Meta nie planuje wprowadzenia Threads (przygotowywanego przez nią odpowiednika Twittera) na europejski rynek, a gdy w maju br.

irlandzki urząd unieważnił stosowane przez nią SCC, zasugerowała, że może wycofać z Europy portale społecznościowe Facebook i Instagram.

Nowe zasady. Po drugim orzeczeniu w sprawie Schrems KE i Departament Handlu USA podjęły negocjacje w kwestiach podniesionych przez TSUE, które w marcu ub.r. zakończyły się wstępnym porozumieniem dotyczącym nowych ram współpracy UE i USA w zakresie przekazywania danych, tzw. Data Privacy Framework (DPF). W jego wyniku jesienią prezydent Joe Biden podpisał dekret, który ograniczył przetwarzanie danych osobowych na potrzeby wywiadowcze. Obecnie jest ono dopuszczalne jedynie we wcześniej określonym celu związanym z bezpieczeństwem narodowym, w sposób proporcjonalny i z poszanowaniem życia prywatnego osoby, której dane dotyczą. Urząd Dyrektora Wywiadu Narodowego USA (ODNI) potwierdził zaś, że wspólnota wywiadowcza zrzeszająca 18 agencji wywiadu USA przyjęła nowe procedury w celu wykonania prezydenckiego dekretu, m.in. wzmocniła kontrolę nad dostępem do danych. Utworzono też drogi odwoławcze – stanowisko Civil Liberties Protection Officer przy ODNI i Data Protection Review Court w ramach urzędu Prokuratora Generalnego.

Na podstawie DPF osoby, których dane są przekazywane do USA, uzyskały prawo dostępu do swoich danych, skorygowania ich i zażądania usunięcia informacji nieprawidłowych lub uzyskanych z naruszeniem prawa. Dla firm z USA uczestnictwo w DPF jest dobrowolne. Pod warunkiem zobowiązania się do przestrzegania zawartych w nich zasad (minimalizacji przetwarzania danych, wprowadzenia określonych środków bezpieczeństwa przy transferach do państw trzecich itp.) otrzymają specjalne certyfikaty. Z DPF najszybciej skorzystają firmy, które miały atesty wystawione na podstawie Privacy Shield (ok. 3 tys.), bo dostosowanie się do nowych warunków będzie dla nich prostsze niż wprowadzanie ram ochrony danych osobowych od początku. Wydawane przez Departament Handlu USA certyfikaty umożliwią przekazywanie danych z UE bez dodatkowych obostrzeń.

Wady rozwiązania. DPF są rozwiązaniem częściowym. Certyfikacja dotyczy tylko firm podlegających jurysdykcji Federalnej Komisji Handlu lub Departamentu Transportu, co wyłącza możliwość ich stosowania do organizacji non-profit, banków i innych instytucji finansowych. Podstawą przekazywania do nich danych z Europy pozostają więc m.in. SCC i BCR. Niemniej nowe ramy mają ułatwić im przeprowadzanie TIA, bo wprowadzone zmiany (m.in. ograniczenia dostępu agencji do danych i środki odwoławcze) będą miały zastosowanie do wszystkich danych bez względu na podstawę ich przetwarzania.

Choć większość państw członkowskich i KE zaaprobowały zmiany wprowadzone w USA, budzą one kontrowersje w Unii. EROD ocenia nowe ramy pozytywnie w porównaniu z poprzednimi rozwiązaniami, ale wskazuje na pozostające luki w ochronie, np. brak szczególnych zasad zautomatyzowanego przetwarzania danych i profilowania oraz podporządkowanie organów odwoławczych amerykańskiej egzekutywie. Wątpliwości budzą też kwestie praktyczne, m.in. to, czy organy USA nie będą interpretowały proporcjonalności i konieczności przetwarzania danych bardziej liberalnie niż UE. Parlament Europejski krytykuje zaś wyjątki w DFP umożliwiające masowe przetwarzanie danych Europejczyków, np. ze względu na zmiany klimatyczne i kryzysy zdrowotne. Choć te opinie, jako niewiążące, nie doprowadziły do zablokowania decyzji KE, Schrems już zapowiedział zaskarżenie nowych ram do końca sierpnia br. Popiera zarzuty podnoszone na forum UE, a dodatkowo uważa zmiany za niewystarczające, by można było rozwiązać problem stosowania sekcji 702 amerykańskiej Foreign Intelligence Surveillance Act. Umożliwia ona m.in. zbieranie i przekazywanie do państw trzecich informacji o cudzoziemcach znajdujących się poza terytorium USA i uważanych za zagrożenie dla bezpieczeństwa narodowego. Rodzi więc ryzyko przekazania przez USA danych osobowych Europejczyków do państw trzecich stosujących niższe standardy ochrony.

Wnioski i perspektywy. DPF stanowią próbę zbalansowania kilku wartości: poszanowania prawa Europejczyków do prywatności, bezpieczeństwa USA oraz interesów unijnych i amerykańskich przedsiębiorców. Decyzja KE jest korzystna dla przedstawicieli europejskiego biznesu – zwiększa pewność prawa i zmniejsza ryzyko potencjalnych zarzutów naruszenia RODO przy współpracy z partnerami z USA. Jej pozytywne skutki odczują zwłaszcza duże firmy technologiczne, szczególnie narażone na skargi osób, których dane przetwarzają. Decyzja stanowi też udogodnienie dla mniejszych firm, które nierzadko rezygnują ze współpracy z firmami z USA, ponieważ nie mają wystarczających zasobów do przeprowadzania TIA, a ryzyko uważają za niewspółmierne do spodziewanych zysków.

Zarzuty stawiane DPF w perspektywie kilkunastu miesięcy mogą doprowadzić do kolejnego unieważnienia przez TSUE przekazywania danych z UE do USA na uproszczonych zasadach. Mając na uwadze daleko idące ustępstwa poczynione przez USA (UE de facto doprowadziła do zmiany ich prawa, a ochrona będzie też stosowana do danych amerykańskich obywateli), można przypuszczać, że kolejne postulaty Unii nie spotkają się z przychylną reakcją Stanów Zjednoczonych. W związku z tym istnieje ryzyko, że jedynym rezultatem potencjalnego zaskarżenia nowych ram staną się – ponownie – utrudnienia dla przedsiębiorców, co będzie niekorzystne również dla polskich firm dążących do intensyfikacji współpracy z USA.