

Bruksela, 20 maja 2022 r.
(OR. fr)

9258/1/22
REV 1

DATAPROTECT 163
JAI 699
ENFOPOL 286
COPEN 203
RELEX 685
TITULAIRES 2
POLCOM 37

NOTA

Od:	Prezydencja
Do:	Delegacje
Dotyczy:	Przekazywanie danych osobowych – Dokument prezydencji

W związku z posiedzeniem Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych
9–10 czerwca 2022 r. delegacje otrzymują w załączeniu wyżej wymieniony dokument.

W ostatnich dziesięcioleciach przekazywanie danych osobowych stało się poważnym wyzwaniem gospodarczym, strategicznym i w zakresie bezpieczeństwa. Przyjmując w 2016 r. europejskie rozporządzenie o ochronie danych i dyrektywę o ochronie danych w sprawach karnych, Unia Europejska uzupełniła i wzmocniła i tak już nowoczesne europejskie ramy prawne dotyczące ochrony danych i podniosła je do rangi światowego standardu.

Europejski model przekazywania danych osobowych

W obszarze międzynarodowego przekazywania danych zestaw narzędzi ustanowionych europejskimi aktami zawiera instrument sztandarowy – decyzję stwierdzającą odpowiedni stopień ochrony. Jest to wyjątkowy i szczególny instrument prawny: stanowi owoc dwustronnych negocjacji, nie będąc umową międzynarodową, ale decyzją przyjmowaną przez Komisję Europejską po uzyskaniu opinii Europejskiej Rady Ochrony Danych i w wyniku procedury komitetowej przewidującej udział państw członkowskich. Także Parlament Europejski jest bardzo zainteresowany pracami w tym obszarze.

Najbardziej znanym przykładem decyzji stwierdzającej odpowiedni stopień ochrony jest Tarcza Prywatności (*Privacy Shield*). W istocie z Unii Europejskiej do Stanów Zjednoczonych przekazywana jest znaczna ilość danych, co stanowi po obu stronach Atlantyku duże wyzwanie gospodarcze i w zakresie bezpieczeństwa. Dlatego też, w kontekście handlowym, szerokim echem na obu kontynentach odbiło się unieważnienie przez Trybunał Sprawiedliwości Unii Europejskiej programu „Bezpieczna przystań” (*Safe Harbor*) w 2015 r.¹, a następnie, w lipcu 2020 r., Tarczy Prywatności².

¹ Wyrok w sprawie Schrems I C- 362/14 wydany przez TSUE 6 października 2015 r.

² Wyrok w sprawie Schrems II C- 311/18 wydany przez TSUE 16 lipca 2020 r.

25 marca 2022 r. przewodnicząca Komisji Europejskiej i prezydent Stanów Zjednoczonych ogłosili, że po blisko roku negocjacji osiągnięto porozumienie „co do zasady” w sprawie ogólnych założeń reform regulacyjnych, które Stany Zjednoczone potrzebują przeprowadzić, aby uzyskać niezbędny poziom zabezpieczeń umożliwiający przyjęcie nowej decyzji stwierdzającej odpowiedni stopień ochrony. Pozwoli to na przekazywanie danych osobowych certyfikowanym przedsiębiorstwom w Stanach Zjednoczonych. Komisja będzie mogła przyjąć decyzję stwierdzającą odpowiedni stopień ochrony, jeżeli – zgodnie z wymogami, o których przypominał TSUE – przewidziane zostaną wystarczające zabezpieczenia w odniesieniu do poszanowania zasad konieczności i proporcjonalności w kwestii dostępu organów publicznych do danych, a także jeżeli ustanowiony zostanie mechanizm odwoławczy do dyspozycji obywateli i mieszkańców Unii Europejskiej, spełniający kryteria ustalone w Karcie praw podstawowych. Chodzi więc zatem o zapewnienie pełnego poszanowania praw osób, których dane są przekazywane. Przyjęcie tej decyzji to duże wyzwanie dla Unii Europejskiej: problemem jest tutaj wypracowanie porozumienia, które umożliwiłoby podmiotom gospodarczym kontynuowanie działalności, przy pełnym poszanowaniu prawa Unii zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej.

Poza tym obecnie obowiązuje szereg innych decyzji stwierdzających odpowiedni stopień ochrony:

- jedenaście z nich Komisja przyjęła na podstawie prawa powstałego wcześniej niż RODO³;
- cztery z nich zostały przyjęte po wejściu w życie RODO: trzy wchodzą w zakres zastosowania RODO i odnoszą się do przekazywania danych do Japonii, Zjednoczonego Królestwa i Korei Południowej; jedna została przyjęta zgodnie z dyrektywą o ochronie danych w sprawach karnych i odnosi się do przekazywania danych do Zjednoczonego Królestwa.

³ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en/ - Andora, Argentyna, Guernsey, Izrael, Jersey, Kanada, Nowa Zelandia, Szwajcaria, Urugwaj, Wyspy Owcze, Wyspa Man.

Wymienione decyzje stwierdzające odpowiedni stopień ochrony są ważnym narzędziem upowszechniania europejskiego modelu. Należy przy tym zaznaczyć, że większość państw opracowała w swoim prawie krajowym podobne instrumenty przekazywania danych, a niektóre (w szczególności Zjednoczone Królestwo i Szwajcaria) automatycznie uznają przekazywanie danych do państw trzecich za odpowiednio chronione, jeżeli za takie uzna je Komisja. Co więcej, Japonia w odniesieniu do przekazywania danych do Unii Europejskiej przyjęła – równoległe do decyzji europejskiej – własną decyzję stwierdzającą odpowiedni stopień ochrony.

Aby decyzje stwierdzające odpowiedni stopień ochrony pozostały prawnie uzasadnione, należy je poddawać regularnej ocenie. Decyzje takie mogą mieć również charakter tymczasowy, jeżeli stwierdzone zostanie ryzyko wystąpienia konkretnych różnic ustawodawczych.

Ponadto RODO przewiduje inne narzędzia przekazywania danych, np. standardowe klauzule umowne będące najczęściej stosowanym narzędziem przekazywania danych, wiążące reguły korporacyjne oraz odpowiednie zabezpieczenia w innych prawnie wiążących instrumentach. Są one niezbędne z uwagi na to, że mechanizm stwierdzania odpowiedniego stopnia ochrony jest bardzo rygorystyczny, a co za tym idzie nie można go wprowadzić względem wszystkich państw trzecich, nawet gdy przekazywanie danych jest nieodzowne. Standardowe klauzule umowne są zresztą narzędziem przekazywania danych, które zyskuje na popularności w licznych państwach trzecich.

Sytuacja w zakresie przekazywania danych osobowych na międzynarodowych forach handlowych i politycznych

W ostatnich latach kwestia międzynarodowych przepływów danych osobowych nabrała wymiaru strategicznego w dwu- i wielostronnych negocjacjach handlowych oraz na forach wielostronnych takich jak G-7 i G-20. Łączy się ona często z zagadnieniem przekazywania danych nieosobowych, mającym również charakter strategiczny, ale wiążącym się z innymi wyzwaniami. Prezydencja francuska sporządziła mapę, by określić klauzule i oświadczenia dotyczące przekazywania danych osobowych w tych ramach. Mapa pozwala zidentyfikować główne trendy w tym obszarze, i pokazuje, jak ważna jest ścisła koordynacja na szczeblu krajowym i europejskim, aby zagwarantować spójność stanowisk na wszystkich forach. Prezydencja przygotowała sprawozdanie na ten temat.

Ponadto przy okazji forum ministerialnego z 22 lutego 2022 r. dotyczącego współpracy w regionie Indo-Pacyfiku Unia Europejska, Australia, Indie, Japonia, Komory, Korea Południowa, Mauritius, Nowa Zelandia, Singapur i Sri Lanka (państwa, których łączna liczba mieszkańców przekracza dwa miliardy) podpisały wspólne oświadczenie o życiu prywatnym i ochronie danych osobowych.

Co więcej, liczne inne organizacje międzynarodowe, takie jak Współpraca Gospodarcza Azji i Pacyfiku (APEC) czy Stowarzyszenie Narodów Azji Południowo-Wschodniej (ASEAN) zajęły się kwestią międzynarodowego przekazywania danych osobowych i na forach wielostronnych stopniowo pojawiają się równoległe modele.

Przekazywanie danych osobowych: priorytetowe wyzwanie dotyczące bezpieczeństwa i wymiaru sprawiedliwości

Coraz powszechniejsze wykorzystywanie narzędzi cyfrowych we wszystkich dziedzinach, a w szczególności do celów przestępczych, sprawia, że kwestia przekazywania danych staje się kluczowym wyzwaniem w zakresie bezpieczeństwa i zwalczania przestępczości. Możliwość udostępniania danych właściwym organom państw trzecich ma często zasadnicze znaczenie. Jednak przekazywanie danych jest dopuszczalne jedynie wówczas, gdy przestrzega się prawa europejskiego i uwzględnia podział kompetencji między Unią a państwami członkowskimi. Międzynarodowe negocjacje w tym zakresie mogą pomóc w upowszechnianiu europejskiego standardu oraz zwiększaniu konwergencji na szczeblu globalnym.

Przykładowo, przepisy dotyczące ochrony danych były ważnym elementem negocjacji w sprawie drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie. Stanowiska europejskie koordynowała Komisja Europejska. Prawdopodobnie tak samo będzie w przypadku rozpoczynających się negocjacji w sprawie projektu konwencji ONZ dotyczącej przeciwdziałania wykorzystywaniu technologii informacyjno-komunikacyjnych w celach przestępczych.

Ponadto w obszarze przekazywania danych PNR (*Passenger Name Record*) wynegocjowano i podpisano szereg umów, a negocjacje między Unią a kilkoma państwami trzecimi (Australią, Kanadą, Stanami Zjednoczonymi) w sprawie kolejnych umów są w toku. Dane PNR zbierane obowiązkowo przez przewoźników lotniczych zawierają takie informacje jak: imię i nazwisko pasażera, daty podróży, trasa, numer miejsca, dane dotyczące bagażu, dane kontaktowe pasażera i użyty środek płatniczy. W opinii wydanej 26 lipca 2017 r., o którą zwrócił się Parlament Europejski, TSUE doprecyzował wymogi w zakresie przekazywania danych PNR.

Kwestia przekazywania danych osobowych zajmuje również istotne miejsce w niektórych programach lub umowach międzynarodowych dotyczących wydawania wiz lub zwolnienia ze składania wniosku wizowego.

W kwestii Tarczy Prywatności prezydencja zwróci się do Komisji o przedstawienie stanu rozmów ze Stanami Zjednoczonymi, a ministrowie zostaną poproszeni o wypowiedź w szczególności na temat planowanej nowej decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do przekazywania danych do Stanów Zjednoczonych oraz na temat zabezpieczeń, które w tych ramach wydają się nieodzowne.

Ministrowie zostaną ponadto poproszeni o odpowiedź na następujące pytanie: czy – mając na uwadze, że międzynarodowe przekazywanie danych osobowych stało się dużym wyzwaniem strategicznym w licznych istotnych dziedzinach polityki publicznej – podzielają Państwo pogląd, że w związku z tym spójna i ambitna polityka europejska powinna być prowadzona w sposób jednolity przez różne podmioty instytucjonalne, w szczególności przez Komisję i przez Radę?