Warszawa, 5 listopada 2020 r.
KL/515/357/AM/2020

Pani
Justyna Romanowska
Kierownik Referatu Cyfryzacji
Stałe Przedstawicielstwo RP przy UE

Pani
Weronika Frydryszek
Kierownik Wydziału Polityka Zagraniczna i Relacje Zewnętrzne
Stałe Przedstawicielstwo RP przy UE

Szanowni Państwo,

Koalicja organizacji biznesowych pragnie wyrazić **głębokie zaniepokojenie** sprawą niedawnego zakwestionowania przekazywania danych osobowych poza terytorium Unii Europejskiej, wynikającego z niedawnego wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w tzw. sprawie *Schrems II*, a także wynikającym z decyzji TSUE przedłużającym się stanem niepewności co do jednoznacznych zasad pozwalających na transfer. Jednocześnie należy podkreślić, że międzynarodowe transfery danych osobowych są stosowane w ramach korzystania z najnowszych technologii informatycznych, takich jak chmury obliczeniowe, hostingi baz danych, narzędzia analityczne, statystyczne, rozwiązania służące zapewnieniu ochrony danych w strategicznych sektorach gospodarki, mechanizmy do uwierzytelniania a zatem weryfikacja chronionych dostępów do bezpiecznych narzędzi informatycznych. Możliwość korzystania z najbardziej rozwiniętych technologii ma kluczowe znaczenie dla wymiany gospodarczej, nie tylko dla wielkich firm międzynarodowych, ale również dla małych i średnich przedsiębiorstw, dla których często rozwiązania globalne, jako najbardziej ekonomiczne, stanowią o istnieniu ich działalności gospodarczej. Dostęp do międzynarodowych technologii, wykorzystujących operacyjnie transfer danych, jest także niezwykle istotny dla rozwoju współpracy społecznej i naukowej, nie tylko w dziedzinach techniki, inżynierii, chemii, fizyki, biotechnologii czy medycyny, ale w każdej działalności, w której konieczny jest codzienny dostęp do narzędzi informatycznych biurowych.

Warto zwrócić uwagę na najważniejsze aspekty wyroku z dnia 16 lipca 2020 roku, w którym Trybunał Sprawiedliwości Unii Europejskiej (TSUE):

- uznał za nieważny mechanizm autocertyfikacji „*Privacy Shield*", uznany wcześniej przez Komisję Europejską za spełniający poziom bezpieczeństwa właściwy dla danych osobowych przekazywanych przez podmiot europejski do przedsiębiorstw mających siedzibę w Stanach Zjednoczonych, oraz
- określił, że Standardowe Klauzule Umowne, zatwierdzone przez Komisję Europejską i wymienione w RODO, pozostają ważne jako mechanizm transferu danych poza terytorium UE, jednak niezbędnym może okazać się dodanie do nich gwarancji w celu zapewnienia poziomu bezpieczeństwa właściwego dla przekazywanych danych.

W związku z powyższym, można stwierdzić, że TSUE wymaga, aby przedsiębiorstwa eksportujące **same oceniły** czy poziom ochrony przez państwo trzecie jest odpowiedni, uwzględniając praktyki i prawa państwa, w którym znajduje się importer, a w szczególności praktyki umożliwiające dostęp do tych danych ze strony władz publicznych danego kraju. Przedsiębiorcy mają też zweryfikować zastosowane przez dostawców spoza EOG środki techniczne ochrony danych, co poza gwarancjami umownymi jest wysoce trudne bez eksperckiej wiedzy z zakresu bezpieczeństwa informatycznego i sieci, wobec braku instytucji certyfikującej na wzór dotychczasowej „Tarczy prywatności".

Takie zakwestionowanie istniejących mechanizmów ma bezpośredni wpływ na przedsiębiorstwa reprezentujące wszystkie sektory. Mechanizmy te umożliwiają dostęp do danych pochodzących z Europy poza granicami oraz gwarantują ich swobodny obrót w celu wspierania europejskiej gospodarki i innowacyjności. Warto także mieć na uwadze szybko rosnący eksport polskiego sektora IT, w szczególności bazującego na rozwiązaniach chmurowych. Rozproszone rynki, różne polityki w poszczególnych krajach, utrudniony transfer powodują, że firmy te mają mniejsze szanse w konfrontacji z firmami lokalnymi i firmami pochodzącymi z bogatych i najbardziej rozwiniętych krajów.

W celu zapewnienia ciągłości międzynarodowych transferów, niezbędnych dla ciągłości działalności gospodarczej, naukowej, społecznej, przy jednoczesnym poszanowaniu wartości i norm prawnych UE oraz uniknięcia gospodarczej, społecznej i naukowej izolacji Europy, będącej skutkiem takiego ograniczenia, koalicja organizacji biznesowych apeluje, aby:

- Europejskie i krajowe władze wdrożyły wszelkie możliwe środki w celu szybkiego wynegocjowania z władzami Stanów Zjednoczonych Ameryki Północnej następcy „*Privacy Shield*", uwzględniając aspekty gospodarcze oraz zasadnicze prawa i wolności, w tym swobodę działalności gospodarczej (art. 16 Karty Praw Podstawowych UE).
- Urzędy ds. ochrony danych osobowych współpracujące w ramach Europejskiej Rady Ochrony Danych (EROD) oraz Komisja Europejska jak najszybciej wypracowały wspólnie z przedsiębiorstwami i sektorem publicznym analizę oraz zalecenia w zakresie charakteru i wdrożenia dodatkowych gwarancji towarzyszących stosowaniu Standardowych Klauzul Umownych, a także w zakresie odstępstw od nich. Ważne jest, aby zalecenia urzędów ds. ochrony danych były precyzyjne, funkcjonalne oraz zgodne z międzynarodowymi traktatami handlowymi w celu umożliwienia skutecznego wdrożenia ich przez wszystkie zainteresowane podmioty. Jesteśmy zaniepokojeni potencjalnym negatywnym wpływem i obciążeniami biurokratycznymi dodatkowych środków (*supplementary measures*), jeżeli będą one obowiązywały wszystkie firmy w równym stopniu, nie biorąc pod uwagę jakie firmy te mają zasoby bądź też jakie kategorie danych transferują, co w efekcie spowoduje spowolnienie przepływu danych pod rygorem standardowych klauzul umownych. W rezultacie, może to zakłócić normalne funkcjonowanie firm.
- Komisja Europejska przystąpiła do aktualizacji Standardowych klauzul umownych, uwzględniając decyzję TSUE, w celu zagwarantowania stabilności prawnej mechanizmu transferu do państw trzecich.
- Komisja Europejska i urzędy ds. ochrony danych osobowych wypowiedziały się na temat ryzyka lub poziomu adekwatności ochrony państw trzecich w celu ułatwienia transferów oraz zagwarantowania zharmonizowanego i spójnego podejścia dla wszystkich europejskich organizacji.
- Oczekujemy, że europejscy regulatorzy przygotują jasne i praktyczne rekomendacje dla biznesu - oceny ryzyk czy dodatkowych środków, biorące pod uwagę rodzaj transferowanych danych oraz kategorii danych B2B vs B2C, cel danych, role przetwarzający vs kontroler oraz ilość żądań dostępu do danych

ze strony poszczególnych rządów. Mamy również nadzieję, że rekomendacje te będą spójne w całej Unii Europejskiej.

- Wskazujemy dodatkowo, że nowe rozwiązania oraz mechanizmy transferu danych poza EU/EEA powinny być wypracowane w ramach współpracy podmiotów biznesowych z organami ochrony danych.

Do wiadomości:

1. Pan Didier Reynders, Komisarz UE ds. Sprawiedliwości
2. Pan Mateusz Morawiecki, Prezes Rady Ministrów, Minister Cyfryzacji
3. Pan Jarosław Gowin, Wiceprezes Rady Ministrów, Minister Rozwoju, Pracy i Technologii
4. Pan Zbigniew Ziobro, Minister Sprawiedliwości
5. Pan Marek Zagórski, Sekretarz Stanu, w KMRP, Pełnomocnik Rządu ds. Cyberbezpieczeństwa
6. Pan Jan Nowak, Prezes Urzędu Ochrony Danych Osobowych
7. Pan Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych Osobowych
8. Pan Marek Prawda, Dyrektor Przedstawicielstwa Komisji Europejskiej w Polsce
9. Pan Michał Tudorowski, Stałe Przedstawicielstwo RP u UE, Kierownik Wydziału ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych