Warszawa, dn. 16.12.2020 r.

Blanka Wawrzyniak, Damian Iwanowski
Fundacja Instrat, Polska Karta Suwerenności Cyfrowej
blanka.wawrzyniak@instrat.pl , damian.iwanowski@instrat.pl

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Wniosek ws. respektowania wyroku Schrems II przez krajowe instytucje publiczne

16 lipca 2020 r. zapadł długo wyczekiwany wyrok Schrems II (C-311/18) będący kontynuacją toczącego się od 2013 r. sporu pomiędzy Maximilianem Schremsem a firmą Facebook Ireland Ltd. oraz irlandzkim organem ds. ochrony danych osobowych. Orzeczenie to zostało wydane na skutek pytania prejudycjalnego wystosowanego przez irlandzki sąd, przed którym to Schrems podtrzymał swoje uprzednie żądanie zakazania transferu danych do Stanów Zjednoczonych. Głównym zastrzeżeniem skarżącego odnoszącym się do bezpieczeństwa danych osobowych eksportowanych do Stanów Zjednoczonych był fakt, że prawo wewnętrzne USA przewiduje możliwość nakazania firmom takim jak Facebook, aby te udostępniały dane obywateli innych państw do amerykańskich wewnętrznych agencji wywiadowczych, takich jak National Security Agency (NSA).

W wydanym 16 lipca 2020 r. orzeczeniu Trybunał Sprawiedliwości przychylił się do żądania Schremsa, podważając skuteczność Tarczy Prywatności (zastępującej Bezpieczną Przystań). Jak wskazał TSUE, mechanizm Tarczy nie zapewniał bowiem odpowiednich, przewidzianych prawem unijnym standardów bezpieczeństwa w zakresie przekazywania danych do państw trzecich (art. 45 ust. 2 RODO). Co więcej, choć TSUE uznał ważność decyzji KE nr 2010/87 zatwierdzającej standardowe klauzule umowne (SCC) jako instrument transferu danych osobowych w rozumieniu art. 46 RODO, to wyraźnie zaznaczył, że SCC nie mogą być stosowane bezkrytycznie, a ich wykorzystywanie wymaga przeprowadzenia testu adekwatności oraz stwierdzenia, czy nie jest koniecznym zastosowanie dodatkowych zabezpieczeń ponad te, które są przewidziane w klauzulach. Co więcej, istotnym jest także fakt, że w przypadku negatywnego wyniku badania ochrony danych w państwie trzecim, konieczne jest wdrożenie dodatkowych środków mających na celu zapewnienie przestrzegania odpowiedniego stopnia ochrony danych w państwie trzecim, a jeżeli jest to niemożliwe - niezwłoczne zaprzestanie transferu. O ile więc dotychczas możliwym było przekazywanie danych osobowych do państw trzecich na podstawie dobrowolnej certyfikacji (Tarczy Prywatności) bądź na gruncie modelowych i powtarzalnych SCC, o tyle od chwili uprawomocnienia się wyroku automatyczne domniemanie odpowiedniej ochrony danych osobowych na podstawie powyższych mechanizmów stało się niedopuszczalne.

Dla firm stosujących rozwiązania oparte na amerykańskich chmurach oznacza to więc powrót do relacji, jaka występuje pomiędzy UE a przedsiębiorstwami z Chin czy Rosji, które w ocenie europejskich organów nie zasługują na miano bezpiecznych administratorów. Wyrok Schrems II niewątpliwie zaburzył *status quo* dotyczący przekazywania danych osobowych do państw trzecich, a w szczególności wymusił istotne zmiany w zakresie ich transferu z firm zlokalizowanych w UE do tych położonych na terenie USA. Omawiane orzeczenie ma niebagatelne znaczenie nie tylko dla prywatnych przedsiębiorstw, lecz odnosi się do wszelkich transferów danych, w tym tych dokonywanych przez podmioty państwowe i instytucje publiczne.

Już od dłuższego czasu szkoły, szpitale i organy administracji publicznej wykorzystują oprogramowania, aplikacje i usługi chmurowe dostarczane przez największych przedsiębiorców cyfrowych. Rozpowszechnienie wykorzystywania programów pochodzących (najczęściej) z USA dodatkowo przyspieszył wybuch COVID-19 oraz konieczność natychmiastowego przeniesienia części sfery publicznej do przestrzeni cyfrowej. Obecnie mamy do czynienia z coraz szerszym zastosowaniem aplikacji wykorzystywanych do zdalnego nauczania, organizowania konferencji online, czy przeprowadzania e-wizyt. Choć okazały się one dużym ułatwieniem w okresie pandemii, otworzyły także nowe kanały przepływu ogromnych ilości danych do podmiotów zlokalizowanych w USA. Opieranie ochrony zdrowia, oświaty, czy usług administracji publicznej na rozwiązaniach zagranicznych z państw trzecich, które nie są bezpiecznymi administratorami, budzi słuszne obawy o ochronę danych osobowych zarówno z perspektywy cyberbezpieczeństwa (ochrony państwa), jak i samych standardów przechowywania i przetwarzania tych danych (ochrony obywateli).

Co więcej, nie sposób pominąć jest kwestię zależności podmiotów państwowych od tzw. cyfrowych gigantów. Jak ustaliły już wielokrotnie organy ochrony konkurencji i organy ochrony danych osobowych krajów UE, jak również sama Komisja Europejska, globalne platformy często wykorzystują swoją dominującą pozycję oraz naginają prawo i zasady etyczne, aby czerpać maksymalne zyski z przetwarzania danych. Uzależniając więc usługi publiczne od globalnych operatorów cyfrowych, państwo skazuje niejako swoich obywateli na konieczność podporządkowania się platformom oraz dostarczania im szeregu nowych danych (w tym również tych wrażliwych), co w dalszej kolejności potęguje wzrost obrotów cyfrowych gigantów. Większe przychody podmiotów zagranicznych nie przekładają się jednak na wpływy do Skarbu Państwa, gdyż najwięksi gracze na rynkach cyfrowych w dalszym ciągu unikają sprawiedliwego opodatkowania w Polsce.

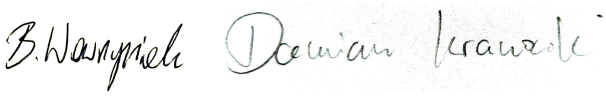
Przekazywanie przez instytucje publiczne danych osobowych do USA jest więc ryzykowne z perspektywy ochrony tych danych, a ponadto stanowi działanie szkodliwe dla budżetu Polski i pogłębiające wyzysk pracy informacyjnej obywateli na globalnych platformach cyfrowych. Biorąc pod uwagę wyrok Trybunału Sprawiedliwości Unii Europejskiej oraz konieczność wzmacniania autonomii

podmiotów publicznych i suwerenności cyfrowej kraju, wzywamy Urząd Ochrony Danych Osobowych do:

- respektowania wyroku Schrems II i podjęcia działań na rzecz ograniczenia transferowania danych do krajów spoza Europejskiego Obszaru Gospodarczego;
- nakazywania zaprzestania przekazywania danych do państw trzecich w sytuacji, gdy wiązałoby się ono z naruszeniem zasad wynikających z wyroku Schrems II;
- wyrażenia całkowitego poparcia dla odejścia od kupowania i wykorzystywania jakichkolwiek rozwiązań opartych na chmurze pochodzących z państw nienależących do EOG;
- egzekwowania od eksporterów danych raportowania do UODO analiz standardowych klauzul umownych (zawierających badanie ustawodawstwa wewnętrznego importera danych pod kątem zasad dostępu do przekazywanych danych podmiotów publicznych w tym państwie trzecim);
- bieżącego raportowania podejmowanych i planowanych przez UODO działań wskazujących na realizację postanowień wynikających z wyroku Schrems II;
- aktywnego udziału w procesie rozbudowywania państwowej infrastruktury cyfrowej, która pozwoli na efektywne realizowanie zadań użyteczności publicznej, niezależnie od wpływów zagranicznych.

Jak orzekł TSUE w wyżej omawianym wyroku, "*właściwe organy nadzorcze są zobowiązane do zawieszenia lub zakazania przekazania danych osobowych do państwa trzeciego, jeżeli w świetle wszystkich okoliczności wynika, że standardowe klauzule ochrony danych nie są lub nie mogą być przestrzegane w tym kraju oraz że ochrona przekazywanych danych, która jest wymagana przez prawo Unii, nie może być zapewniona innymi środkami*". Inne państwa, jak chociażby Francja już teraz wybierają, by nie korzystać z usług dostawców chmurowych z USA (lub innych dostawców „*podlegających jurysdykcji Stanów Zjednoczonych*") do przetrzymywania danych zdrowotnych (decyzja 444937 CNIL). Jednak polski Urząd Ochrony Danych Osobowych, dla dobra obywateli RP, może i powinien iść o krok dalej - skłaniając do odejścia od korzystania z chmur spoza EOG nie tylko w zakresie przetrzymywania danych zdrowotnych, lecz także jakichkolwiek danych pochodzących od instytucji publicznych.

Blanka Wawrzyniak
Damian Iwanowski



Do wiadomości:

1. Pan Mateusz Morawiecki, Prezes Rady Ministrów, Minister Cyfryzacji
2. Pan Jarosław Gowin, Wiceprezes Rady Ministrów, Minister Rozwoju, Pracy i Technologii
3. Pan Marek Zagórski, Sekretarz Stanu w KMRP, Pełnomocnik Rządu ds. Cyberbezpieczeństwa
4. Pan Jan Nowak, Prezes Urzędu Ochrony Danych Osobowych
5. Pan Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych Osobowych
6. Pani Weronika Frydryszek, Kierownik Wydziału Polityki Zagranicznej i Relacji Zewnętrznych w Stałym Przedstawicielstwie RP przy UE
7. Pan Michał Tudorowski, Kierownik Wydziału Sprawiedliwości i Spraw Wewnętrznych w Stałym Przedstawicielstwie RP przy UE
8. Pani Justyna Romanowska, Kierownik Referatu Cyfryzacji w Stałym Przedstawicielstwie RP przy UE