

## BREXIT A RODO

Proces opuszczania Unii Europejskiej przez Wielką Brytanię zwany potocznie brexitem stał się nie tylko doniosłym wydarzeniem polityczno-gospodarczym, ale także zapisał się w świadomości europejskiej opinii publicznej jako zjawisko popkultury (niejeden mem i żart oparty o brexitowe widowisko oblekł się w platynę). Nadszedł jednak rok 2020 i swoją dynamiką przyćmił nieco brytyjską telenowelę, także w dziedzinie ochrony danych osobowych. Na pierwszy plan wysunęła się przyspieszona cyfryzacja wszystkiego, spowodowana przez antycovidowe lockdowny i wyrok TSUE w sprawie Facebooka tzw. Schrems II, który zmiotł z planszy Privacy Shield, stanowiącą podstawę transferu danych do USA. Wyspiarze nie powiedzieli jednak ostatniego słowa i brexitowe igrzyska mogą znów wrócić w wielkim stylu do naszych codziennych prasówek za sprawą konsekwencji, jakie dla transferu danych osobowych spowoduje wygaśnięcie z końcem roku 2020 okresu przejściowego, w którym RODO na Wyspach jeszcze obowiązuje.

### Coś się kończy, coś się zaczyna

Wyjście Wielkiej Brytanii z Unii Europejskiej rodzi pytania o dalsze losy transferu danych osobowych. Przez jakiś czas temat pozostawał na uboczu, lecz wraz z upływem okresu przejściowego należy ponownie zadać sobie pytanie co będzie czekać nas po brexicie. Zasadniczo istnieją trzy scenariusze. Pierwszy zakłada, że Wielka Brytania po opuszczeniu Unii Europejskiej bardzo szybko, jeśli nie od razu, uzyska decyzję Komisji Europejskiej o adekwatności poziomu ochrony danych, co sprawi, że problem praktycznie przestanie istnieć. Transfer będzie bowiem możliwy bez żadnych dodatkowych zabezpieczeń, tj. innych niż w przypadku przesyłania danych pomiędzy krajami Unii. Drugi scenariusz przewiduje, że relacje pomiędzy Wielką Brytanią a Unią zostaną uregulowane przez szereg szczegółowych umów w poszczególnych aspektach społeczno-gospodarczych, w tym ochrony danych osobowych i ich transferu. W takim wypadku transfer mógłby się oprzeć o jakiś instrument prawny podobny do uchylonej przez TSUE EU-US Privacy Shield. Trzeci scenariusz zakłada, że nie powstanie żadna specyficzna podstawa prawna do przetwarzania danych osobowych i z chwilą upływu okresu przejściowego z końcem 2020 roku Wielka Brytania stanie się krajem trzecim w rozumieniu RODO. W takim wypadku transfer danych będzie należało oprzeć o instrument z ogólnego arsenału przewidzianego przez RODO, czyli standardowe klauzule umowne, wiążące reguły korporacyjne, zatwierdzony kodeks postępowania, mechanizm certyfikacji lub któryś z wyjątków określonych w art. 49.

### Na rozstaju dróg

Na pierwszy rzut oka najbardziej prawdopodobny byłby pierwszy scenariusz, w którym wraz z wyjściem Wielkiej Brytanii z Unii lub zaraz po tym zostanie wydana decyzja o adekwatności poziomu ochrony danych osobowych. To rozwiązanie byłoby najbardziej naturalne w przypadku kraju, który był częścią europejskiego rynku wspólnotowego, na terenie którego bezpośrednio obowiązywało RODO. Co więcej brytyjski organ nadzorczy działający w ramach RODO cieszył się dużą estymą w całej Europie i dostarczał merytorycznego wkładu w funkcjonowanie całego europejskiego systemu ochrony prywatności. Takie nadzieje można było żywić bez obaw do 6 października 2020 r. kiedy to TSUE w połączonych sprawach C-623/17, C-511/18 oraz C-520/18 dotyczących Wielkiej Brytanii, Francji i Belgii orzekł, że uprawnienia do masowego gromadzenia danych osób, które zostały

przyznane służbom specjalnym w tych krajach, stoją w sprzeczności z unijnym prawem, w szczególności naruszając prawo do prywatności i powinny podlegać daleko idącym ograniczeniom i ścisłej kontroli. W tej sytuacji może okazać się, że decyzja o adekwatności nie zostanie wydana tak szybko, jak mogłoby się wydawać, a nawet może nie być wydana w ogóle, jeśli nie zostanie zmienione w tym zakresie brytyjskie prawo. Biorąc pod uwagę motywacje stojące za brexitem trudno spodziewać się, żeby Wielka Brytania zrezygnowała z uprawnień służb w zakresie bezpieczeństwa narodowego w celu dostosowania się do unijnego prawa.

Wedle drugiego możliwego scenariusza, nawet jeśli nie zostanie wydana decyzja o adekwatności, to Wielka Brytania i Unia Europejska mogą jeszcze zawrzeć szczegółową umowę określającą zasady transferu danych osobowych, która dawałaby podstawę prawną do takich procesów. Rzecz w tym, że doniesienia medialne wskazują na daleko idące problemy w negocjowaniu porozumień pomiędzy stronami, premier Wielkiej Brytanii regularnie oskarża unijnych partnerów o brak chęci do porozumienia i zbyt nieustępliwe stanowisko wobec brytyjskich propozycji. Obawy te potęguje fakt, że do zakończenia okresu przejściowego pozostały zaledwie dwa miesiące, a nie wiemy nawet, czy rozmowy nad takim dokumentem regulującym transfer danych trwają i jaki jest ich proponowany kształt. Wśród komentatorów pojawia się coraz częściej opinia, że Wielka Brytania może opuścić Unię bez żadnego porozumienia, a to oznacza, że z dnia na dzień stanie się ona krajem trzecim w rozumieniu RODO.

Wiele wskazuje na to, że coraz bardziej prawdopodobny staje się trzeci scenariusz, czyli nadanie Wielkiej Brytanii statusu kraju trzeciego w rozumieniu RODO. Dodatkowym utrudnieniem tej sytuacji będzie ciągle aktualny wyrok TSUE z 6 października 2020 r., który wprost wskazuje na regulacje brytyjskie naruszające unijne prawo, co może utrudnić korzystanie ze standardowych klauzul umownych (z czym mamy do czynienia także na gruncie transferu danych do USA), a także innych środków opierających się na zatwierdzeniu przez organ nadzorczy zasad takiego transferu. Zupełnie niewykluczone jest, że z upływem roku 2020 będziemy musieli dopisać Wielką Brytanię obok USA do listy państw trzecich, wobec których stwierdzono wyrokiem brak adekwatności poziomu ochrony danych.

### **Brace yourselves, brexit is coming**

Uzyskanie przez Wielką Brytanię statusu kraju trzeciego może spowodować problemy z transferem danych do tego kraju, podobne do sytuacji z transferem do USA, którego po trzęsieniu ziemi wywołanego przez wyrok Schrems II jeszcze nie uporządkowano. Dodatkową obawę powodują sygnały pochodzące z brytyjskiego rządu, który najwyraźniej wcale nie zamierza dorównywać do europejskich standardów ochrony prywatności, a raczej skorzysta z okazji pojawiającej się po wyjściu z Unii i bardziej zwiększyć potencjał wykorzystywania przetwarzania danych do celów biznesowych i politycznych, nawet kosztem praw osób, których te dane dotyczą. Jeśli Wielka Brytania wybierze tę drogę rozwoju, a Unia Europejska pozostanie na ścieżce dalszych regulacji wzmacniających ochronę prywatności osób poprzez ochronę ich danych osobowych, to wraz z upływem czasu standardy ochrony danych mogą rozjechać się na tyle, że dopuszczalność transferu danych stanie pod znakiem zapytania.

Pozostawiając na boku dywagacje na temat możliwego scenariusza dalszych wypadków, należy już dziś pomyśleć o przygotowaniu organizacji na zbliżający się brexit. Warto w tym miejscu powtórzyć ścieżkę działania wskazywaną przez organy nadzorcze w przypadku reakcji na wyrok Schrems II - dokonać przeglądu swoich procesów przetwarzania, zidentyfikować procesy i dostawców, u których

występuje transfer danych do Wielkiej Brytanii, zweryfikować jakie dane i w jakim celu są przekazywane. Zdaje się, że to ostatni moment, żeby rozpocząć przygotowanie sobie planu awaryjnego na wypadek, gdyby z dnia na dzień ustała podstawa do transferu danych na Wyspy.

W największym uproszczeniu, do wszystkich czynności podjętych w ramach reagowania na skutki Schrems II można sobie roboczo dopisać "UK też".

**Bartosz Migas, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.**