

Nieprzerwane przepływy danych pomiędzy Zjednoczonym Królestwem

**i Polską: Dlaczego jest to problemem,
z jakiego powodu jest on ważny i jak
można go rozwiązać?**

Na czym polega problem?

W związku z wyjściem z Unii Europejskiej, Zjednoczone Królestwo opuści także europejskie ramy ochrony danych. Przepisy dotyczące ochrony danych obowiązujące w UE określają sposoby postępowania z danymi osobowymi, a także okoliczności, w jakich dane osobowe mogą być przesyłane między państwami. Z racji tego, że wszystkie państwa członkowskie UE oraz EOG podlegają tym samym ramom ochrony danych, możliwy jest swobodny przepływ danych pomiędzy wszystkimi państwami wchodzącymi w skład Europejskiego Obszaru Gospodarczego. Będąc jednym z państw członkowskich Unii Europejskiej, Zjednoczone Królestwo korzystało dotychczas z przepisów umożliwiających przepływ danych ze Zjednoczonego Królestwa do Unii Europejskiej bez żadnych dodatkowych ograniczeń.

W wyniku odejścia Zjednoczonego Królestwa z Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego, państwo utraci korzyści płynące z automatycznego swobodnego przepływu danych pomiędzy Zjednoczonym Królestwem oraz EOG. Zamiast tego Zjednoczone Królestwo będzie traktowane jako „państwo trzecie”, które będzie zmuszone do przestrzegania przepisów prawa UE w zakresie ochrony danych dotyczących przekazywania danych osobowych poza EOG.

Duża liczba przedsiębiorstw ze Zjednoczonego Królestwa, pozostałych 27 państw członkowskich Unii Europejskiej oraz państw trzecich niebędących członkami Unii Europejskiej polegało na możliwości swobodnego przekazywania danych pomiędzy Zjednoczonym Królestwem a resztą UE. Wiele spośród nich od dawna stosuje praktyki biznesowe oparte na takim przekazywaniu danych. Zmiana stosunku prawnego Zjednoczonego Królestwa do zasad ochrony danych obowiązujących w EOG może wywołać znaczną niepewność i spowodować powstanie dodatkowych kosztów dla wszystkich przedsiębiorstw, które przechowują dane osobowe.

Dlaczego jest to ważne?

Szacuje się, że do 2020 roku ogólna wartość europejskiej gospodarki opartej na danych wyniesie 739 miliardów euro, co będzie stanowiło 4 procent całkowitego PKB Unii Europejskiej.¹ Przekazywanie danych osobowych jest częścią codziennej działalności przedsiębiorstw, niezależnie od ich wielkości i sektora, w którym prowadzą działalność. W nowoczesnej gospodarce cyfrowej dane i handel idą ze sobą w parze. Dzieje się tak dlatego, ponieważ przepływy danych są kluczowe nie tylko dla sektora technologicznego — niemal każdy sektor gospodarki polega bowiem na przepływach danych, wśród nich można wymienić między innymi sektory usług finansowych, handlu detalicznego, rolnictwa i wiele innych. Przepływy danych niosą ze sobą również korzyści wykraczające poza spektrum gospodarcze. Na transgranicznych przepływach danych polegają między innymi kluczowe badania medyczne, a także działania polecające na zwalczaniu przestępstw gospodarczych, istnieją również istotne korzyści wynikające ze swobodnego przepływu danych. Nieprzerwane przepływy danych między Zjednoczonym Królestwem a UE przyniosłyby korzyści każdemu spośród pozostałych 27 państw członkowskich UE z różnych powodów. Zjednoczone Królestwo jest dla Polski bardzo ważnym partnerem handlowym, a także drugim co do wielkości rynkiem eksportowym o wartości wynoszącej 10,5 miliarda euro rocznie. We współczesnym, coraz bardziej powiązanym i cyfrowym świecie, handel i dane idą ze sobą w parze.

Z tego powodu także stosunki handlowe Zjednoczonego Królestwa i Polski są w dużej mierze oparte na swobodnym przepływie danych. Wśród inicjatyw, które pojawiły się w ostatnich latach jest między innymi chęć cyfryzacji polskiego przemysłu motoryzacyjnego, który zatrudnia około 180000 pracowników. Co więcej, niemal 40 procent polskiego handlu ze Zjednoczonym Królestwem jest związana z przemysłem środków transportu. Ważnym elementem dwustronnych stosunków między Polską i Zjednoczonym Królestwem jest również turystyka — każdego roku Polskę odwiedza ponad dwa miliony mieszkańców Wysp Brytyjskich. Tego rodzaju transakcje i wymiana handlowa opierają się na bezproblemowym przekazywaniu danych, bez którego nastąpiłoby ich zakłócenie.

¹ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

Przepływy danych są ważne dla całej gospodarki światowej. Szacuje się, że w ciągu ostatniej dekady globalne przepływy danych spowodowały wzrost światowego PKB o ponad 10 procent.² W tym kontekście jednak relacje związane z przepływem danych pomiędzy Unią Europejską i Zjednoczonym Królestwem są szczególnie ważne. Zjednoczone Królestwo stanowi źródło około 3 procent globalnego PKB, jednocześnie odpowiadając za 11,5 procenta globalnych przepływów danych.³ Najbardziej istotny w tym kontekście jest fakt, że 75 procent tych przepływów danych odbywa się wewnątrz Unii Europejskiej, co jasno pokazuje, dlaczego tak ważne staje się zapewnienie nieprzerwanego swobodnego przepływu danych pomiędzy Zjednoczonym Królestwem i Unią Europejską. Rozwiązanie tej kwestii będzie miało znaczący wpływ na wszystkie brytyjskie i unijne przedsiębiorstwa, które zamierzają prowadzić handel po opuszczeniu Unii Europejskiej przez Zjednoczone Królestwo.

Jakie istnieją możliwości zapewnienia nieprzerwanego swobodnego przepływu danych?

RODO określa szereg mechanizmów przekazywania danych poza państwa Unii Europejskiej do państw trzecich, niebędących członkami UE. Mechanizmy te obejmują: decyzje stwierdzające odpowiedni stopień ochrony; wiążące reguły korporacyjne; standardowe klauzule umowne; kodeksy postępowania i zgoda. Organizacja techUK dokonała dogłębnej oceny i w jej wyniku odrzuciła wszystkie powyższe mechanizmy przekazywania danych w swoim sprawozdaniu opracowanym we współpracy z organizacją UK Finance zatytułowanym 'No Interruptions: options for the future UK EU data sharing relationship'⁴.

Powszechnie przyjmuje się, że najbardziej odpowiednim i stabilnym mechanizmem zapewnienia ciągłości przepływów danych pomiędzy Zjednoczonym Królestwem i Unią Europejską są wzajemne uzgodnienia dotyczące odpowiedniego stopnia ochrony.

Czym są decyzje stwierdzające odpowiedni stopień ochrony?

Decyzje stwierdzające odpowiedni stopień ochrony są wydawane przez Komisję Europejską po dokonaniu przeglądu ram ochrony danych państwa niebędącego członkiem Unii Europejskiej w celu zweryfikowania, czy dane państwo trzecie charakteryzuje się poziomem ochrony danych zasadniczo równoważnym z poziomem Unii Europejskiej. Takie działanie ma zagwarantować, że w przypadku przetwarzania lub przechowywania danych europejskich na terytorium państwa niebędącego członkiem Unii Europejskiej będzie istniała pewność tego, że dane będą chronione w wystarczającym stopniu, zgodnie z podejściem UE do ochrony danych.

Po wydaniu, decyzja stwierdzająca odpowiedni stopień ochrony pozwala na swobodny przepływ danych z UE do państwa trzeciego bez konieczności wdrażania przez przedsiębiorstwa dodatkowych zabezpieczeń. To właśnie postawienie wymogów związanych ze zgodnością na poziomie krajowym, zamiast na poziomie poszczególnych przedsiębiorstw stanowi jedną z największych korzyści wpływających z zastosowania właśnie tego mechanizmu. Co więcej, jest to jednocześnie najbardziej stabilny i najtańszy sposób przekazywania danych przez przedsiębiorstwa.

Dlaczego Zjednoczone Królestwo i Unia Europejska powinny zawrzeć porozumienie dotyczące odpowiedniego stopnia ochrony?

Nie ma żadnych wątpliwości, że najlepszym sposobem zapewnienia ciągłości przepływu danych pomiędzy Zjednoczonym Królestwem i Unią Europejską są decyzje stwierdzające odpowiedni stopień ochrony. Uważamy, że istnieją wyraźne argumenty przemawiające za przyznaniem decyzji stwierdzającej odpowiedni stopień ochrony Zjednoczonemu Królestwu przez Unię Europejską. Wśród nich można wymienić między innymi następujące:

² <https://www.mckinsey.com/-/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20Globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx>

³ <https://www.techuk.org/insights/news/item/10086-the-uk-digital-sectors-after-brexit>

⁴ <https://www.techuk.org/insights/news/item/11824-rapid-action-needed-to-safeguard-uk-eu-businesses-consumers-following-brexit>

- Od wielu lat Zjednoczone Królestwo i Unia Europejska współpracowały ściśle na polu ochrony danych i mają wspólne podejście do tej kwestii.
- Zjednoczone Królestwo w pełni wdrożyło ogólne rozporządzenie o ochronie danych UE, a nowa brytyjska ustawa o ochronie danych z 2018 roku stanowi obecnie część porządku prawnego. Rząd Zjednoczonego Królestwa wyraźnie zobowiązał się do utrzymania przepisów RODO nawet po opuszczeniu Unii Europejskiej.
- W Zjednoczonym Królestwie działa jeden z czołowych organów regulacyjnych zajmujących się kwestią ochrony danych na świecie — Information Commissioner's Office (ICO, Urząd ds. Danych), cieszący się międzynarodowym uznaniem i renomą w związku ze swoim podejściem do przepisów w zakresie ochrony danych oraz ich egzekwowaniem.
- Pomimo tego, że istnieją pewne obawy związane z uprawnieniami Zjednoczonego Królestwa w zakresie bezpieczeństwa narodowego określonymi w brytyjskiej ustawie regulującej uprawnienia śledcze (Investigatory Powers Act), z zadowoleniem przyjmujemy przejrzystość tych środków i uważamy, że nie powinny one uniemożliwiać zawarcia porozumienia dotyczącego odpowiedniego stopnia ochrony danych.

Rozmowy pomiędzy Zjednoczonym Królestwem i UE na temat odpowiedniego stopnia ochrony danych będą różniły się od poprzednich negocjacji dotyczących tej kwestii. Żadne państwo w historii nie wdrożyło identycznych ram ochrony danych jak Unia Europejska. W Zjednoczonym Królestwie obecnie obowiązuje to samo rozporządzenie o ochronie danych, co oznacza, że po opuszczeniu Unii Europejskiej państwo będzie zobowiązane do przeprowadzenia własnych ocen odpowiedniego stopnia ochrony danych w państwach trzecich, w tym również w Unii Europejskiej. Z tego powodu zarówno Zjednoczone Królestwo, jak i Unia Europejska powinny zatem dążyć do porozumienia w sprawie wzajemnych decyzji stwierdzających odpowiedni stopień ochrony tak szybko, jak to możliwe.

Jakie uzgodnienia zostały dokonane w wyniku negocjacji pomiędzy Zjednoczonym Królestwem i UE?

Po trwających niemal dwa lata negocjacjach, rząd Zjednoczonego Królestwa i Komisja Europejska uzgodniły dwa kluczowe dokumenty: umowę o wystąpieniu oraz deklarację polityczną ustalającą ramy przyszłych stosunków pomiędzy Zjednoczonym Królestwem i UE.

Umowa o wystąpieniu stanowi dokument prawny określający warunki opuszczenia Unii Europejskiej przez Zjednoczone Królestwo. Jednym z kluczowych postanowień zawartych w tym dokumencie jest okres przejściowy, trwający nawet do grudnia 2020 roku. W tym czasie przepisy i prawa Unii Europejskiej będą w dalszym ciągu obowiązywały w Zjednoczonym Królestwie, co w praktyce oznacza, że status quo zostanie w dużej mierze utrzymany pomimo tego, że Zjednoczone Królestwo przestanie być oficjalnie jednym z państw członkowskich Unii Europejskiej. W okresie przejściowym dane osobowe nadal będą mogły swobodnie przepływać pomiędzy Zjednoczonym Królestwem i Unią Europejską bez żadnych dodatkowych ograniczeń.

Deklaracja polityczna ustalająca ramy przyszłych stosunków zawiera bardzo ważne zobowiązanie do uzgodnienia porozumień w sprawie odpowiedniego stopnia ochrony danych pomiędzy Zjednoczonym Królestwem i Unią Europejską przed zakończeniem okresu przejściowego oraz do poszukiwania możliwości współpracy regulacyjnej pomiędzy brytyjskim komisarzem ds. informacji i Europejską Radą Ochrony Danych.

Organizacje takie jak techUK oraz ZISPEE dostrzegają korzyści płynące z utrzymywania bliskich stosunków między Zjednoczonym Królestwem a UE w zakresie ochrony danych i z zadowoleniem przyjmują zobowiązania zawarte zarówno w umowie o wystąpieniu, jak i w deklaracji politycznej. Utrzymanie nieprzerwanego i stabilnego przepływu danych leży we wspólnym interesie Zjednoczonego Królestwa oraz Unii Europejskiej, a także wszystkich sektorów gospodarki, których codzienna działalność opiera się na przepływie danych. Bliska współpraca zapewniłaby również konsumentom z całej Unii Europejskiej pewność, że ich dane osobowe będą w dalszym ciągu podlegać ścisłym zasadom ochrony danych, a także możliwość dochodzenia roszczeń, jeśli zaistnieje taka konieczność.

Zachęcamy rząd brytyjski i Komisję Europejską do dalszego zajęcia się tą niezwykle ważną kwestią, jaką jest nieprzerwany i niezakłócony przepływ danych między Wielką Brytanią a UE oraz do jak najszybszego podjęcia negocjacji w sprawie porozumień dotyczących odpowiedniego stopnia ochrony danych.

Co się stanie w sytuacji, gdy porozumienie między Zjednoczonym Królestwem i Unią Europejską nie dojdzie do skutku?

Pomimo tego, że zarówno Zjednoczone Królestwo, jak i Unia Europejska pragną dojść do porozumienia przed dniem 29 marca 2019 roku, nikt nie jest w stanie zagwarantować, że właśnie taki będzie ostateczny rezultat negocjacji. Sytuacją domyślną w przypadku braku porozumienia pomiędzy Zjednoczonym Królestwem i Unią Europejską jest opuszczenie wspólnoty bez porozumienia. W praktyce oznacza to, że zarówno rządy, jak i przedsiębiorstwa czy organy regulacyjne muszą być przygotowane na taką możliwość.

Brytyjski Urząd ds. Danych (Information Commissioner's Office) opublikował niedawno szczegółowe informacje dotyczące konsekwencji opuszczenia wspólnoty przez Zjednoczone Królestwo bez uzgodnienia porozumienia dotyczących przekazywania danych oraz działań, które będą musiały podjąć w związku z tym przedsiębiorstwa, w tym dotyczące sytuacji, w których będzie wymagane zastosowanie standardowych klauzul umownych. Co więcej, rząd brytyjski oświadczył, że w przypadku braku porozumienia nie nastąpi wprowadzenie żadnych ograniczeń dotyczących przekazywania danych ze Zjednoczonego Królestwa do państw członkowskich Unii Europejskiej, oświadczając tym samym jednostronnie uznanie odpowiedniego stopnia ochrony danych w całej Unii Europejskiej. Jednocześnie Komisja Europejska oświadczyła, że w sytuacji opuszczenia wspólnoty europejskiej bez porozumienia, Zjednoczone Królestwo będzie traktowane jako państwo trzecie ze wszystkimi konsekwencjami tego faktu, a w przypadku braku decyzji Komisji w sprawie odpowiedniego stopnia ochrony danych będzie konieczne zastosowanie innych gwarancji prawnych, zgodnie z przepisami ujętymi w RODO.

- Biorąc pod uwagę ogromne znaczenie tej kwestii, skalę przepływów danych pomiędzy Zjednoczonym Królestwem i Unią Europejską, a także sytuację, jakiej być może będą musiały stawić czoła przedsiębiorstwa z dniem 29 marca 2019 roku, organizacje techUK oraz ZIPSEE zachęcają organy ochrony danych pozostałych państw członkowskich UE oraz Europejską Radę Ochrony Danych do rozważenia możliwych działań, których podjęcie pozwoliłoby na zapewnienie pewności dotyczącej stanu prawnego europejskim przedsiębiorstwom zastanawiającym się nad skutkami wyjścia Zjednoczonego Królestwa z Unii Europejskiej bez porozumienia. Możliwe działania mogą obejmować:
- Zagwarantowanie, że przepływy danych z Unii Europejskiej do Zjednoczonego Królestwa na podstawie standardowych klauzul umownych nie będą kwestionowane oraz że poszczególne organy ochrony danych aktywnie zaangażują się w promowanie tego przekazu. Istnieje już precedens dla takiego kierunku działań, kiedy działająca wówczas grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych ujęła podobne stwierdzenie w swoim oświadczeniu z 16 października 2015 roku wydanym po wyroku TSUE nr C-362/14 w sprawie Maximillian Schrems przeciwko Data Protection Commissioner. Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych stwierdziła wówczas również, że jej członkowie „rozpoczną odpowiednią kampanię informacyjną na poziomie krajowym” w celu upewnienia się, że wszystkie zainteresowane podmioty będą wystarczająco poinformowane. Oba te działania dałyby pewność przedsiębiorstwom wykorzystującym w swojej działalności standardowe klauzule umowne oraz rozważającym korzystanie z tego mechanizmu.
- Stwierdzenie, że przepływy danych z Unii Europejskiej do Zjednoczonego Królestwa nie będą kwestionowane przez żadnego z jej członków przed przeprowadzeniem pełnej oceny tego, czy stopień ochrony danych w Zjednoczonym Królestwie powinien zostać uznany za odpowiedni. Takie działanie jest również zgodne z oświadczeniem prasowym grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych z dnia 16 października 2015 roku. Tego rodzaju deklaracja mogłaby być uzależniona od pewnych kryteriów, takich jak dalsze przestrzeganie i wdrażanie RODO przez Zjednoczone Królestwo, do czego rząd Zjednoczonego Królestwa już się zobowiązał. Dodatkowo deklaracja może być również wydana na określony czas z możliwością jego przedłużenia w przypadku nieukończenia pełnej oceny stopnia ochrony danych.
- Oba te działania byłyby proporcjonalne, oparte na istniejącym precedensie i zapewniłyby europejskim przedsiębiorstwom wyjaśnienie dotyczące ram prawnych dotyczących przekazywanych przez nie danych.



techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. Over 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

techUK.org | [@techUK](https://twitter.com/techUK) | [#techUK](https://hashtechUK)



**CYFROWA
POLSKA**

The Association of Importers and Producers of Electrical and Electronic Equipment – ZIPSEE “Digital Poland” is an industry employers’ organisation, non-profit organisation bringing together the largest companies from the consumer electronics and IT sectors operating in Poland, including both manufacturers and importers and distributors of electrical and electronic equipment.

zipsee.pl/en/ | [@ ZIPSEE_Cyfrowa](https://twitter.com/ZIPSEE_Cyfrowa)