Urząd Ochrony Danych Osobowych

Wpisz frazę której szukasz

Infolinia Urzędu 606-950-000

ENG

Poradniki i wskazówki

Filmy

» Poradniki » Poradniki i wskazówki

Prezes UODO wyjaśnia, jak przekazywać dane osobowe z Polski do Wielkiej Brytanii na wypadek brexitu

Wobec dużego prawdopodobieństwa wystąpienia Wielkiej Brytanii z Unii Europejskiej bez zawarcia regulującej to umowy międzynarodowej, Prezes UODO wyjaśniła 17 stycznia br. podczas briefingu prasowego, jakie będą tego konsekwencje dla polskich administratorów danych i podmiotów je przetwarzających oraz radzi, jak się do tego właściwie przygotować.

Obecne zasady przekazywania danych będą obowiązywały tylko do 29 marca 2019 r.

Do 29 marca 2019 r. – czyli tak długo, jak Wielka Brytania będzie członkiem Unii Europejskiej – przekazywanie danych do podmiotów działających na terytorium tego państwa będzie mogło się odbywać swobodnie bez żadnych dodatkowych ograniczeń tak, jak to miało miejsce dotychczas. Transfery danych w obrębie UE korzystają z zasady swobodnego przepływu danych. Zgodnie z nią przekazywanie danych z Polski do innych państw Europejskiego Obszaru Gospodarczego (UE oraz Islandia, Liechtenstein i Norwegia) jest traktowane tak samo, jakby miało miejsce na terenie Polski. Wymagane jest przestrzegania podstawowych zasad przetwarzania danych i wynikających z nich obowiązków.

Od 30 marca 2019 r. Wielka Brytania będzie traktowana jako państwo trzecie

Od 30 marca Wielka Brytania w świetle ogólnego rozporządzenia o ochronie danych (2016/679; dalej: RODO) będzie traktowana jako państwo trzecie. Oznacza to, że wszystkie transfery danych do tego państwa muszą spełniać dodatkowe wymogi dotyczące przekazywania danych do państw trzecich lub organizacji międzynarodowych, które zostały określone w rozdziale V RODO.

Jak zapewnić legalność transferów danych po 29 marca 2019 r.?

Zarówno polscy przedsiębiorcy, jak i podmioty publiczne muszą się do tego wcześniej przygotować tak, aby zapewnić legalność transferów danych do Wielkiej Brytanii w nowym stanie prawnym, który będzie obowiązywał od 30 marca 2019 r.

Jakie kroki należy podjąć przed 30 marca 2019 r.?

Każdy administrator danych lub podmiot przetwarzający, którzy obecnie przekazują dane do Wielkiej Brytanii, powinien:

- Zidentyfikować, jakie dane, w jakich celach i na jakiej podstawie prawnej są obecnie przekazywane do Wielkiej Brytanii;
- Zdecydować, czy te transfery będą kontynuowane po 29 marca 2019 r.;
- Wybrać i wdrożyć odpowiedni mechanizm, bądź podstawę prawną umożliwiającą przekazywanie danych;
- W razie potrzeby zmodyfikować:
  - wewnętrzną dokumentację przetwarzania danych, w tym rejestr czynności przetwarzania,
  - klauzule informacyjne,
  - istniejące wiążące reguły korporacyjne;
- Śledzić informacje dotyczące przebiegu procesu wyjścia Wielkiej Brytanii z UE, gdyż nie jest jeszcze pewne na jakich zasadach to nastąpi, co może mieć wpływ na obowiązki związane z transferem danych.

W zależności od przebiegu wydarzeń w najbliższych tygodniach Prezes UODO będzie przekazywał aktualne informacje i wskazówki.

Przekazywanie danych do państwa trzeciego

Co do zasady przekazywanie danych do państwa trzeciego może mieć miejsce, **gdy Komisja Europejska stwierdzi, że to państwo zapewnia odpowiedni poziom ochrony danych osobowych**. W ramach objętych taką decyzją przekazanie danych jest dopuszczalne bez konieczności podejmowania dodatkowych działań. KE wydała takie decyzje np. wobec Kanady, Nowej Zelandii, czy Izraela.

Niestety nie jest możliwe, by KE wydała w sprawie Wielkiej Brytanii taką decyzję pod koniec marca 2019 roku. Dlatego **do czasu wydania przez KE stosownej decyzji należy sprawdzić alternatywne rozwiązania**, które umożliwią przekazywanie danych.

Standardowe klauzule umowne

Przedsiębiorcy w pierwszej kolejności powinni pomyśleć o zastosowaniu standardowych klauzul umownych ochrony danych, które zostały zatwierdzone przez KE.

Obecnie obowiązują trzy decyzje Komisji Europejskiej:

1) **decyzja 2001/497/WE** w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE. Tekst dostępny jest na stronie internetowej:

http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32001D0497&from=en

2) **decyzja 2004/915/WE** zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich. Decyzja jest dostępna na stronie internetowej:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:PL:PDF

3) **decyzja 2010/87/UE** w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, która umożliwia przekazywanie danych w ramach ich powierzenia. Tekst decyzji jest dostępny na stronie internetowej:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:PL:PDF

Wiążące reguły korporacyjne

Międzynarodowe grupy kapitałowe mogą także skorzystać z wiążących reguł korporacyjnych, które zostały wcześniej zatwierdzone przez GIODO, bądź jeden z organów ochrony danych osobowych z państw członkowskich UE w ramach przewidzianej przez RODO procedury spójności. Należy pamiętać, że dotychczasowe wiążące reguły korporacyjne muszą zostać zmodyfikowane poprzez umieszczenie importerów danych z Wielkiej Brytanii w grupie państw trzecich.

Zabezpieczenia w sektorze publicznym

Przekazywanie danych przez organy i podmioty publiczne może się odbywać bez konieczności uzyskania zgody Prezesa UODO na podstawie prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi. Transfer danych jest także możliwy za zgodą Prezesa UODO na podstawie uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

Wyjątki w szczególnych sytuacjach

RODO dopuszcza przekazywanie danych do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony lub gdy nie zapewniono odpowiednich zabezpieczeń jak standardowe klauzule umowne, czy wiążące reguły korporacyjne. Jest to możliwe w szczególnych sytuacjach. Mowa o nich w art. 49 RODO. Są to następujące szczególne sytuacje:

1) Osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę. Należy podkreślić, że zgoda musi:

1. być wyraźna,
2. dotyczyć konkretnie danego jednorazowego/wielokrotnego przekazania danych,
3. być świadoma, w szczególności osoba udzielająca zgody musi być zdawać sobie sprawę z ewentualnego ryzyka, z którym może się wiązać przekazanie.

2) Przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą.

3) Przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną.

4) Przekazanie jest niezbędne ze względu na ważne względy interesu publicznego.

5) Przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń.

6) Przekazanie niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

7) Przekazanie danych następuje z publicznego rejestru.

8) Przekazanie jest niezbędne ze względu na ważne prawnie uzasadnione interesy administratora i zostały spełnione dodatkowe wymogi.

Europejska Rada Ochrony Danych szczegółowo omówiła ww. podstawy przekazania danych
w wytycznych, które są dostępne na stronie internetowej:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_pl

Sytuacja przedsiębiorców, którzy przetwarzają dane polskich obywateli świadcząc im swoje usługi z Wielkiej Brytanii

Do takich przedsiębiorców nadal będzie się bezpośrednio stosować RODO. RODO ma bowiem zastosowanie także do przetwarzania danych dotyczących osób przebywających w UE przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności te wiążą się z:

- oferowaniem towarów lub usług takim osobom znajdującym się w UE – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
- monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

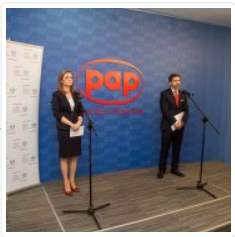
Tacy przedsiębiorcy muszą wyznaczyć na piśmie swojego przedstawiciela w UE w tym państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane.

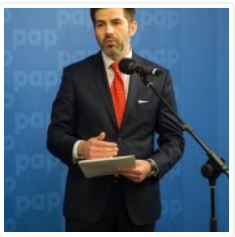
Przedsiębiorcy nie muszą wyznaczać swojego przedstawiciela jeżeli prowadzone przez nich operacje przetwarzania, mają charakter sporadyczny, nie obejmują – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych.

Europejska Rada Ochrony Danych przyjęła pierwszą wersję wytycznych 3/2018 w sprawie zakresu terytorialnego zastosowania RODO, których tekst w języku angielskim jest dostępny na stronie internetowej:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_pl

2019-01-17


Inne aktualności

- Nie podejmując współpracy z organem nadzorczym, administrator naraża się na karę finansową
- Życzenia Świąteczne
- WSA podzielił argumenty UODO. Rejestracja dźwięku tylko na podstawie prawa
- Skarga WhatsApp na decyzję EROD uznana przez TSUE za niedopuszczalną
- Pierwszy w Polsce kodeks postępowania zgodnego z RODO zatwierdzony
- Zaproszenie na spotkanie poświęcone kodeksom postępowania
- UODO po raz kolejny zbadał naruszenie ochrony danych osobowych przez Virgin Mobile

- EROD przyjęła wiążące decyzje w odniesieniu do Facebooka, Instagrama i WhatsApp
- Prace EROD nad zaleceniami dotyczącymi wiążących reguł korporacyjnych
- Kolejna kara dla operatora telekomunikacyjnego za brak zgłoszenia naruszenia
- #ODOlekcje: porozmawiajmy o prywatności
- „Projektowanie systemów SI zgodnych z RODO" tematem kolejnego webinarium UODO
- Analiza ryzyka i działanie zgodnie z przyjętymi procedurami przeciwdziałają utracie danych
- #ODOlekcje – nowa inicjatywa w programie „Twoje dane – Twoja sprawa"
- WSA: podmiot danych należy poinformować o naruszeniu bez zbędnej zwłoki

Infolinia UODO
606-950-000
czynna w dni robocze od: 10:00-14:00

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
kancelaria@uodo.gov.pl
Godziny pracy: 8.00-16.00