



Photo By Luke Stackpoole on Unsplash

RODO A BREXIT PORADNIK DLA PRZEDSIĘBIORCÓW

STYCZEŃ 2019





WIELKA BRYTANIA JAKO PAŃSTWO TRZECIE PO 29 MARCA 2019

Państwa trzecie to państwa nienależące do Europejskiego Obszaru Gospodarczego (EOG), który zrzesza kraje Unii Europejskiej oraz Islandię, Norwegię i Liechtenstein. W momencie bezumownego wyjścia UE Wielka Brytania opuści także Europejski Obszar Gospodarczy.

Co się zmieni?

30 marca 2019 roku Wielka Brytania, w przypadku z bezumownego wystąpienia z UE stanie się państwem trzecim w rozumieniu rozporządzenia 2016/679 z 27 kwietnia 2016 r. dalej „RODO”. Oznacza to, że po 29 marca RODO przestanie w Wielkiej Brytanii obowiązywać. Tym samym do transferu danych z państw członkowskich do Wielkiej Brytanii będą miały zastosowanie przepisy rozdziału V RODO: Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych.

Obecne zasady przekazywania danych będą obowiązywały tylko do 29 marca 2019 r. Po tym terminie Wielka Brytania stanie się „państwem trzecim” w rozumieniu RODO. W takim scenariuszu od 30 marca 2019 r. w Wielkiej Brytanii kwestie ochrony danych osobowych co do zasady nie będą już wprost regulowane przepisami RODO, lecz odpowiednich aktów prawa brytyjskiego.

ZGODNIE Z ROZDZIAŁEM V RODO,

dane do państwa trzeciego mogą być przekazywane, ale musi być spełniony jeden ze wskazanych warunków, bądź zastosowanie muszą mieć opisane wyjątki.

Dane mogą być przekazane:

1. Z zastosowaniem art. 45 – to jest na podstawie decyzji Komisji (takiej na dzień dzisiejszy brak).

Na dzień publikacji tego poradnika (28.01.2019) brak takiej decyzji. W związku z tym dane można przekazać z zapewnieniem odpowiednich zabezpieczeń, opisanych w art. 46 i 47 RODO (pkt. 2 i pkt. 3 poniżej). W momencie wydania i opublikowania przez Komisję takiej decyzji będzie ona stanowić

wystarczającą podstawę prawną dla polskich przedsiębiorców i organizacji do przekazania danych osobowych do Zjednoczonego Królestwa. Komisja Europejska wydała takie decyzje np. w stosunku Kanady, Nowej Zelandii, czy Izraela. Do momentu wydanie takiej decyzji należy skorzystać z pozostałych narzędzi pozwalających na transfer danych do państwa trzeciego, opisanych w rozdziale V RODO i w tym poradniku.





2. ZGODNIE Z WYTYCZNYMI ART. 46: PRZEKAZYWANIE Z ZASTRZEŻENIEM ODPOWIEDNIH ZABEZPIECZEŃ.

Przepis ten wskazuje, że administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią przynajmniej jedno z odpowiednich zabezpieczeń oraz pod warunkiem, że w państwie tym obowiązują egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

Egzekwowalne prawa osób, czyli między innymi takie jak prawo do bycia zapomnianym, prawo dostępu do danych, prawo do ich przeniesienia. Kraj, do którego danego są przekazywane musi posiadać mechanizmy do realizacji tych praw, jeśli pojawi się takie żądanie.

JAKIE TZW. ODPOWIEDNIE ZABEZPIECZENIE ZASTOSOWAĆ, ABY MÓC PRZEKAZAĆ DANE OSOBOWE DO PAŃSTWA TRZECIEGO (W TYM WIELKIEJ BRYTANII)?

- a) prawnie wiążący i egzekwowalny instrument między organami lub podmiotami publicznymi; Chodzi w tym miejscu o szeroko rozumiane umowy międzynarodowe oraz inne uzgodnienia o wiążącym charakterze. Przesłanka ta będzie mieć jednak zastosowanie tylko w przypadku transferu danych pomiędzy podmiotami publicznymi, którego podstawą jest przepis prawa.
- b) wiążące reguły korporacyjne zgodnie z art. 47;
Wyjaśnienie w pkt 3
- c) zatwierdzony kodeks postępowania zgodnie z art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Aby podmioty polskie mogły zastosować tę przesłankę jako podstawę transferu danych do Wielkiej Brytanii konieczne jest opracowanie takich kodeksów po stronie brytyjskiej. Po 29 marca w przypadku zamiaru transferu do określonego podmiotu konieczne będzie upewnienie się czy odbiorca danych w Wielkiej Brytanii podjął wiążące zobowiązanie do stosowania postanowień tego kodeksu w trybie, o którym mowa w art. 40 ust. 3 RODO.
- d) zatwierdzony mechanizm certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą. Podobnie jak w przypadku kodeksów postępowania, również w przypadku zatwierdzonego mechanizmu certyfikacji aby podmioty polskie mogły zastosować tę przesłankę jako podstawę transferu danych do Wielkiej Brytanii konieczne jest ich ustanowienie po stronie brytyjskiej. Po 29 marca w przypadku zamiaru transferu do określonego podmiotu konieczne będzie upewnienie się czy odbiorca danych w Wielkiej Brytanii podjął wiążące zobowiązanie do stosowania tego zabezpieczenia w trybie, o którym mowa w art. 42 ust. 2 RODO

PRZEDSIĘBIORCO, WYKORZYSTAJ STANDARDOWE KLAUZULE UMOWNE!

Urząd Ochrony Danych Osobowych zaleca, aby w pierwszej kolejności przedsiębiorcy pomyśleli o zastosowaniu standardowych klauzul umownych ochrony danych, które zostały zatwierdzone przez Komisję Europejską (KE).

Obecnie obowiązują trzy decyzje KE:

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>



3. NA PODSTAWIE WIĄŻĄCYCH REGUŁ KORPORACYJNYCH (ZGODNIE Z ART. 47)

PYTANIE: CZY POZOSTAJĄ W MOCY
WIĄŻĄCE REGUŁY KORPORACYJNE
ZAAKCEPTOWANE PRZEZ URZĄD
OCHRONY DANYCH (POLSKI
I BRYTYJSKI) PRZED 25 MAJA BR.
I CZY STANOWIĄ ONE
WYSTARCZAJĄCĄ PODSTAWĘ
PRAWNĄ DO PRZEKAZANIA DANYCH
OSOBOWYCH DO UK? [1]

„Wiążące reguły korporacyjne” (WRK) oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą.

Zgodnie z dotychczasowymi procedurami przyjętymi przez Grupę Roboczą Art. 29 ds. ochrony danych osobowych w odniesieniu do Wiążących Reguł Korporacyjnych organem wiodącym był brytyjski urząd ochrony danych.

Zgodnie z art. 46 ust. 5 RODO, zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylecia w razie potrzeby przez ten organ. Brytyjski organ ochrony danych zezwolenia o takim charakterze wydawał w odniesieniu do Wiążących Reguł Korporacyjnych na podstawie Data Protection Act 1998. Takie zezwolenia nie stanowią formalnego zatwierdzenia, lecz wyrażenie zgody na przekazanie danych osobowych przez administratorów działających w zakresie właściwości brytyjskiego urzędu ochrony danych.

Biorąc to pod uwagę należy stwierdzić, że art. 46 ust. 5 RODO w tym zakresie będzie miał ograniczony zakres zastosowania, gdyż formalnie decyzje brytyjskiego urzędu ochrony danych osobowych dotyczące Wiążących Reguł Korporacyjnych nie obejmowały wszystkich transferów danych ze wszystkich państw członkowskich. Niemniej duża część Wiążących Reguł Korporacyjnych, które obejmowały podmioty działające na terenie Polski, była przedmiotem postępowań i decyzji Generalnego Inspektora Ochrony Danych Osobowych (obecnie Urzędu Ochrony Danych Osobowych).

W kwestii dalszego stosowania Wiążących Reguł Korporacyjnych należy zauważyć, że ten instrument prawny nie był regulowany wprost przepisami dyrektywy 95/46/WE, a procedura jego zatwierdzenia nie miała charakteru prawnie wiążącego. W szczególności przyjęta w ramach Grupy Roboczej Art. 29 procedura wzajemnego uznawania miała charakter nieformalnego zobowiązania się poszczególnych organów ochrony danych do respektowania ustaleń organu wiodącego i organów współoceniających projekt Wiążących Reguł Korporacyjnych w toku krajowych procedur zatwierdzenia transferów danych osobowych do państw trzecich. Tym samym w świetle większości dotychczasowych przepisów krajowych zatwierdzenie Reguł nie miało charakteru formalnego. Taki charakter miało dopiero zezwolenie na transfer danych w ramach przygotowanego WRK i dopiero taki akt należy traktować jako zezwolenie w rozumieniu art. 26 ust. 2 dyrektywy 95/46/WE, do którego odwołuje się art. 46 ust. 5 RODO.



CZY MOŻLIWE JEST PRZEKAZANIE DANYCH

w przypadku, gdy nie jest spełniony żaden z opisanych wcześniej warunków?

Tak, pod warunkiem, że:

a) Poinformujemy osobę, której dane dotyczą, o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie i uzyskamy od niej zgodę. Taka zgoda musi:

- być wyraźna,
- dotyczyć konkretnego jednorazowego lub wielokrotnego przekazania danych,
- być świadoma, czyli osoba udzielająca zgody musi zdawać sobie sprawę z ewentualnego ryzyka, z którym może się wiązać przekazanie.

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

Przykład: Firma działająca w Polsce podpisuje umowę z dostawcą usług informatycznych w Wielkiej Brytanii. Do realizacji umowy konieczne jest przekazanie danych osobowych klientów.



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

Przykład 1: Klient w biurze podróży wykupuje wycieczkę do Wielkiej Brytanii (albo innego państwa trzeciego np. Egiptu). Podpisuje w związku z tym umowę z biurem podróży. Biuro podróży, działając w imieniu klienta, kontaktuje się z hotelem w Wielkiej Brytanii, przekazując dane osobowe swojego klienta – np. imię i nazwisko, preferencje dietetyczne.

Przykład 2: Polski pracodawca wysyła do pracy w Wielkiej Brytanii ekipę budowlaną w związku z umową podpisaną z brytyjskim klientem. Pracownicy są ubezpieczeni. Dochodzi do wypadku na placu budowy. Dla potrzeb wypłaty odszkodowania konieczna jest wymiana danych poszkodowanych pracowników pomiędzy podmiotami w PL i UK.

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

Przykład: Klient banku w Wielkiej Brytanii zaciągnął zobowiązanie kredytowe, którego nie spłacał, po czym wyjechał do Polski. Jeśli sąd w Wielkiej Brytanii zwróci się do organu polskiego o podanie danych na potrzeby tego postępowania podanie danych będzie uprawnione

e) Przekazanie jest 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.

Przykład: Obywatel Polski podczas wakacji w Wielkiej Brytanii (lub innym państwie trzecim) trafił do szpitala. Pacjent pozostaje nieprzytomny. Krewny poszkodowanego informuje szpital, że cierpi on na chorobę przewlekłą. W związku z tym szpital z Wielkiej Brytanii zwraca się do polskiej placówki posiadającej pełną dokumentację medyczną chorego o przekazanie danych, które mogą być kluczowe dla ochrony jego życia bądź zdrowia.

f) Przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

Przykłady: Chodzi zarówno o rejestry, w których zawarte dane są powszechnie dostępne np. Centralna Ewidencja i Informacja Działalności Gospodarczej czy Księgi wieczyste online, jak też i o takie, w których dostęp do danych możliwy jest tylko dla podmiotów uprawnionych np. dostęp do Krajowego Rejestru Karnego, który może uzyskać pracodawca (tylko w zakresie niezbędnym dla zatrudnienia pracownika, jeżeli z ustawy wynika wymóg niekaralności, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej)



„OSTATNIA DESKA RATUNKU”



Jeżeli przekazanie nie może się opierać na żadnej z wcześniej omówionych przesłanek, przekazanie do państwa trzeciego może nastąpić wyłącznie, gdy spełnia ono wszystkie poniższe warunki jednocześnie (art. 49 ust. 1 akapit drugi RODO):

- nie jest ono powtarzalne,
- dotyczy tylko ograniczonej liczby osób, których dane dotyczą,
- jest niezbędne ze względu na ważne prawnie uzasadnione interesy administratora, o ile charakteru nadrzędnego nie mają interesy lub prawa i wolności osoby, której dane dotyczą.
- administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych.

W powyższym przypadku o przekazaniu administrator informuje organ nadzorczy.

Motyw 113 - Przekazanie, które można uznać za niepowtarzające się i dotyczące tylko ograniczonej liczby osób, których dane dotyczą, może być także dopuszczalne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, o ile charakteru nadrzędnego nie mają interesy lub prawa i wolności osoby, której dane dotyczą, i administrator ocenił wszelkie okoliczności związane z przekazaniem danych. Administrator powinien zwrócić szczególną uwagę na charakter danych osobowych, cel i czas trwania proponowanej operacji przetwarzania lub proponowanych operacji przetwarzania oraz na sytuację w państwie pochodzenia, państwie trzecim i państwie ostatecznego przeznaczenia, a także powinien zapewnić odpowiednie zabezpieczenia poszanowania podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych. Takie przekazanie powinno być dopuszczalne w nielicznych przypadkach – gdy nie ma zastosowania żadna z pozostałych podstaw umożliwiających przekazanie. Gdy chodzi o cele badań naukowych lub historycznych lub cele statystyczne, należy wziąć pod uwagę uzasadnione oczekiwania społeczne co do rozwoju wiedzy. Administrator powinien informować o przekazaniu organ nadzorczy oraz osobę, której dane dotyczą.

W JAKIEJ SYTUACJI BĘDZIE KONIECZNA ZMIANA KLAUZULI INFORMACYJNEJ I PONOWNE SPEŁNIENIE OBOWIĄZKU INFORMACYJNEGO?

Aktualizacja klauzul informacyjnych nie musi być dokonywana automatycznie tylko w związku z Brexitem. Potrzebę dokonania aktualizacji tej informacji należy przeanalizować przede wszystkim pod kątem czy można uznać, że osoba, której dane dotyczą jest już w posiadaniu niezbędnej informacji.

Przykład: Jeśli w dotychczasowej klauzuli informacyjnej poinformowano, że dane mogą być udostępniane podmiotom w Wielkiej Brytanii i jednocześnie, że mogą one być przekazywane do państwa trzeciego (z uwagi na ich udostępnianie jeszcze przed Brexitem do innego państwa trzeciego niż Wielka Brytania) to wówczas aktualizacja klauzuli informacyjnej nie jest niezbędna. Inaczej będzie w sytuacji jeśli przed Brexitem dane nie były przekazywane do państwa trzeciego. Nawet jeśli w klauzuli znalazła się akurat informacja, że dane będą przekazywane do Wielkiej Brytanii. Brak informacji o przekazywaniu do państwa trzeciego mógłby zostać potraktowany jako naruszenie obowiązku informacyjnego. Ocena potrzeby rewizji klauzuli zależy to od sposobu sformułowania obecnej klauzuli. Ważne natomiast, aby nie wprowadzała ona w błąd.



CO JEŚLI JESTEM PRZEDSIĘBIORCĄ DZIAŁAJĄCYM W WIELKIEJ BRYTANII I ŚWIADCZĘ SVOJE USŁUGI W POLSCE?

W opisanej sytuacji nadal bezpośrednio zastosowanie ma RODO, bowiem stosuje się je także do przetwarzania danych dotyczących osób przebywających w UE w przypadku firm, które nie mają jednostek organizacyjnych w Unii.

Gdy administrator lub podmiot przetwarzający nie ma jednostki organizacyjnej w Unii Europejskiej, a przetwarza dane osób znajdujących się w UE i czynności przetwarzania wiążą się z:

- oferowaniem towarów lub usług tym osobom w Unii (niezależnie od tego, czy wymaga od tych osób płatności) lub
- monitorowaniem ich zachowania (o ile ma ono miejsce w Unii)

to taki administrator lub podmiot przetwarzający powinien wyznaczyć na piśmie swojego przedstawiciela w kraju członkowskim UE. Przedstawiciel ten – działający w imieniu administratora lub podmiotu przetwarzającego – będzie adresatem ewentualnych działań organu nadzorczego.

Przedstawiciela nie trzeba wyznaczać, gdy:

- przetwarzanie ma charakter sporadyczny,
- nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa,
- jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele przetwarzanie powodowało ryzyko naruszenia praw lub wolności osób fizycznych,
- jeżeli administrator jest organem lub podmiotem publicznym.



WPROST O TAKIEJ SYTUACJI MÓWI MOTYW 80 RODO.

Gdy administrator lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii przetwarza dane osobowe osób, których dane dotyczą, znajdujących się w Unii, a jego czynności przetwarzania wiążą się z oferowaniem towarów lub usług tym osobom w Unii (niezależnie od tego, czy wymaga od tych osób płatności) lub z monitorowaniem ich zachowania (o ile ma ono miejsce w Unii), to taki administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela, chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli administrator jest organem lub podmiotem publicznym. Przedstawiciel powinien działać w imieniu administratora lub podmiotu przetwarzającego i może być adresatem ewentualnych działań organu nadzorczego.

Administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela w wyraźny sposób za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków administratora lub podmiotu przetwarzającego wynikających z niniejszego rozporządzenia. Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z niniejszego rozporządzenia. Przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania niniejszego rozporządzenia. W razie jego nieprzestrzegania przez administratora lub podmiot przetwarzający wyznaczony przedstawiciel powinien zostać poddany działaniom egzekucyjnym.



ŚCIEŻKA POSTĘPOWANIA DLA PRZEDSIĘBIORCY.

Jeśli jesteś przedsiębiorcą, który przekazuje dane do Wielkiej Brytanii, podejmij poniższe działania:



sprawdź, jakie dane przekazujesz do UK



zdecyduj, czy po Brexicie nadal będziesz chciał je przekazywać



sprawdź, która z opisanych wcześniej podstaw prawnych będzie miała zastosowanie w Twoim przypadku



zmień swoją klauzulę informacyjną



uzupełniaj rejestr czynności przetwarzania przy okazji przekazania danych



monitoruj kwestię wydania decyzji przez KE opisanej w punkcie 1



w razie jej braku takiej decyzji KE monitoruj też istnienie innych instrumentów uprawniających do przekazania danych do państwa trzeciego takich jak np. zatwierdzony po stronie odbiorcy danych w Wielkiej Brytanii kodeks postępowania, który uprawniałby do przekazania danych osobowych

