URZĄD OCHRONY DANYCH OSOBOWYCH

CERTYFIKACJA JAKO NARZĘDZIE DO PRZEKAZYWANIA DANYCH

OGÓLNA CHARAKTERYSTYKA NARZĘDZI TRANSFEROWYCH PRZEWIDZIANYCH W ART. 46 RODO

WEBINARIUM - 24.04.2024 r.

Michał Utych
Główny Specjalista
Departament Orzecznictwa i Legislacji
Wydział Kodeksów i Certyfikacji

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH (OGÓLNE ZASADY)

URZĄD OCHRONY DANYCH OSOBOWYCH

- Art. 44 RODO:

Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy - **z zastrzeżeniem innych przepisów niniejszego rozporządzenia** - administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. **Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu.**

PRZEKAZYWANIE Z ZASTRZEŻENIEM ODPOWIEDNICH ZABEZPIECZEŃ

KOMISJA EUROPEJSKA NIE PRZYJĘŁA DECYZJI STWIERDZAJĄCEJ ODPOWIEDNI POZIOM OCHRONY

ART. 46 RODO (PRZEKAZYWANIE Z ZASTRZEŻENIEM ODPOWIEDNICH ZABEZPIECZEŃ)

„W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.” (ART. 46 UST. 1 RODO)

ODPOWIEDNIE ZABEZPIECZENIA – BEZ ZEZWOLENIA WŁAŚCIWEGO ORGANU (ART. 46 UST. 2 RODO)

URZĄD OCHRONY DANYCH OSOBOWYCH

- Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić - bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego - za pomocą:

  a) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;

  b) wiążących reguł korporacyjnych zgodnie z art. 47;

  c) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

  d) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

  e) zatwierdzonego kodeksu 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; lub

  f) zatwierdzonego mechanizmu 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.

ODPOWIEDNIE ZABEZPIECZENIA – Z ZASTRZEZENIEM ZEZWOLENIA WŁAŚCIWEGO ORGANU (ART. 46 UST. 3 RODO)

URZĄD OCHRONY DANYCH OSOBOWYCH

- Pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą:

  a) klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; lub

  b) postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

ŚRODKI UZUPEŁNIAJĄCE

URZĄD OCHRONY DANYCH OSOBOWYCH

Zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych

Wersja 2.0

przyjęta 18 czerwca 2021 r.

WIĄŻĄCE REGUŁY KORPORACYJNE

DEFINICJA:

- "wiążące reguły korporacyjne" 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

  (ART. 4 PKT 20 RODO)

WIĄŻĄCE REGUŁY KORPORACYJNE (ELEMENTY) – ART. 47 RODO

1. Właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne zgodnie z mechanizmem spójności przewidzianym w art. 63, pod warunkiem że:

a) są one prawnie wiążące oraz mają zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników, i są przez każdego z tych członków egzekwowane;

b) wyraźnie przyznają osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych; oraz

c) spełniają wymogi określone w ust. 2.

WIĄŻĄCE REGUŁY KORPORACYJNE (ELEMENTY) – ART. 47 RODO – C.D.

URZĄD OCHRONY DANYCH OSOBOWYCH

- 2. W wiążących regułach korporacyjnych, o których mowa w ust. 1, określone zostają co najmniej:
- a) struktura i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków;
- b) jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą, oraz nazwa danego państwa trzeciego lub danych państw trzecich;
- c) ich prawnie wiążący charakter, wewnętrzny i zewnętrzny;
- d) zastosowanie ogólnych zasad ochrony danych - w szczególności ograniczenia celu, minimalizacji danych, ograniczonych okresów przechowywania, jakości danych, uwzględnianie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podstawa prawna przetwarzania, przetwarzanie szczególnych kategorii danych osobowych, środki zapewniające bezpieczeństwo danych, wymogi w zakresie dalszego przekazywania podmiotom niezwiązanym wiążącymi regułami korporacyjnymi;

WIĄŻĄCE REGUŁY KORPORACYJNE (ELEMENTY) – ART. 47 RODO – C.D.

URZĄD OCHRONY DANYCH OSOBOWYCH

- e) prawa osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw, w tym z prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu - w tym profilowaniu - zgodnie z art. 22, prawa do wnoszenia skarg do właściwego organu nadzorczego i właściwych sądów państw członkowskich zgodnie z art. 79 oraz prawa do środka zaskarżenia, a w stosownych przypadkach - odszkodowania za naruszenie wiążących reguł korporacyjnych;
- f) przyjęcie przez administratora lub podmiot przetwarzający posiadających jednostki organizacyjnej na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego jednostki organizacyjne w Unii; administrator lub podmiot przetwarzający są zwolnieni z tej odpowiedzialności - w całości lub w części - wyłącznie, gdy udowodni, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody;
- g) sposób, w jaki osobom, których dane dotyczą, podaje się - oprócz informacji, o których mowa w art. 13 i 14 - informacje o wiążących regułach korporacyjnych, w szczególności o postanowieniach, o których mowa w lit. d), e) i f) niniejszego ustępu;

WIĄŻĄCE REGUŁY KORPORACYJNE (ELEMENTY) – ART. 47 RODO – C.D.

URZĄD OCHRONY DANYCH OSOBOWYCH

- h) zadania inspektora ochrony danych wyznaczonego zgodnie z art. 37 lub innej osoby lub podmiotu odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz monitorowanie szkoleń i rozpatrywanie skarg;
- i) procedury dotyczące skarg;
- j) stosowane w grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych. Mechanizmy takie obejmują audyty w zakresie ochrony danych oraz metody zapewniania działań naprawczych mających chronić prawa osób, których dane dotyczą. Wyniki takiej weryfikacji powinny być przekazywane osobie lub podmiotowi, o których mowa w lit. h), oraz zarządowi przedsiębiorstwa sprawującego kontrolę w grupie przedsiębiorstw lub organowi kierującemu grupą przedsiębiorców prowadzących wspólną działalność gospodarczą i powinny być dostępne na żądanie właściwego organu nadzorczego;

WIĄŻĄCE REGUŁY KORPORACYJNE (ELEMENTY) – ART. 47 RODO – C.D.

URZĄD OCHRONY DANYCH OSOBOWYCH

- k) mechanizmy zgłaszania i rejestrowania zmian w zasadach i zgłaszania tych zmian organowi nadzorczemu;
- l) mechanizm współpracy z organem nadzorczym zapewniający przestrzeganie zasad przez wszystkich członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w szczególności poprzez udostępnianie organowi nadzorczemu wyników weryfikacji środków, o której mowa w lit. j);
- m) mechanizm zgłaszania właściwemu organowi nadzorczemu wszelkich wymogów prawnych, którym podlega w państwie trzecim członek grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i które mogą mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych; oraz
- n) właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych.

STANDARDOWE KLAUZULE OCHRONY DANYCH (ART. 46 UST. 2 LIT. C RODO)

URZĄD OCHRONY DANYCH OSOBOWYCH

- **DECYZJA WYKONAWCZA KOMISJI (UE) 2021/914 z dnia 4 czerwca 2021 r.** w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679
- Podejście modułowe

STANDARDOWE KLAUZULE OCHRONY DANYCH (ART. 46 UST. 2 LIT. C RODO)

URZĄD OCHRONY DANYCH OSOBOWYCH

Motyw 109 preambuły RODO:

„Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony.”

KODEKS POSTĘPOWANIA (ART. 46 UST. 2 LIT. E RODO)

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

CERTYFIKACJA (ART. 46 UST. 2 LIT. F RODO)

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

WSPARCIE DLA PODMIOTÓW PRZEKAZUJĄCYCH DANE POZA EOG

URZĄD OCHRONY DANYCH OSOBOWYCH

WYTYCZNE, ZALECENIA, REKOMENDACJE EUROPEJSKIEJ RADY OCHRONY DANYCH

URZĄD OCHRONY DANYCH OSOBOWYCH

DZIĘKUJĘ ZA UWAGĘ

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

URZĄD OCHRONY DANYCH OSOBOWYCH

CERTYFIKACJA JAKO NARZĘDZIE DO PRZEKAZYWANIA DANYCH

WSKAZÓWKI DOTYCZĄCE OPRACOWANIA KRYTERIÓW CERTYFIKACJI

WEBINARIUM - 24.04.2024 r.

Agnieszka Kociełkiewicz
Starszy Specjalista
Departament Orzecznictwa i Legislacji
Wydział Kodeksów i Certyfikacji

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 1

URZĄD OCHRONY DANYCH OSOBOWYCH

AGENDA

1. Certyfikacja jako narzędzie transferu.
2. Rodzaje mechanizmów certyfikacji.
3. Zakres i przedmiot certyfikacji, o której mowa w art. 46 ust. 2 lit. f RODO.
4. Elementy kryteriów certyfikacji.
5. Zatwierdzanie kryteriów certyfikacji jako narzędzia transferu – procedura.
6. Podmioty, które będą mogły udzielać certyfikacji, o której mowa w art. 46 ust. 2 lit. f RODO – zasady akredytacji.

URZĄD OCHRONY DANYCH OSOBOWYCH

Certyfikacja jako narzędzie transferu

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 3

URZĄD OCHRONY DANYCH OSOBOWYCH

Brak w RODO definicji „certyfikacji”.

CERTYFIKACJA – to:

- niezależna ocena dowodów
- przeprowadzona przez akredytowany podmiot certyfikujący lub organ nadzorczy,
- w której zostanie stwierdzone, że spełniono kryteria certyfikacji

(więcej: p.15-18 Wytycznych 1/2018 EROD).

Ta ocena dowodów odbywa się podstawie **mechanizmu certyfikacji**, na który składają się: **kryteria certyfikacji** i **procedury certyfikacji**.

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 4

URZĄD OCHRONY DANYCH OSOBOWYCH

Cel certyfikacji.

Dla podmiotów podlegających RODO:

Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych osobowych **mają świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające** (**art. 42 ust. 1 RODO**).

Dla podmiotów nie podlegających RODO:

Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych, które mają zastosowanie do administratorów lub podmiotów przetwarzających podlegających RODO, **mogą być ustanowione do wykazania odpowiednich zabezpieczeń przez administratorów lub podmioty przetwarzające, którzy zgodnie z art. 3 RODO mu nie podlegają, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. f)**. Tacy administratorzy lub takie podmioty przetwarzające **podejmują wiążące i egzekwowalne zobowiązania** - w drodze umowy lub poprzez inne prawnie wiążące instrumenty - **do stosowania tych odpowiednich zabezpieczeń,** w tym w odniesieniu do praw osób, których dane dotyczą (**art. 42 ust. 2 RODO**)

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 5

URZĄD OCHRONY DANYCH OSOBOWYCH

Ogólna zasada przekazywania danych

(art. 44 RODO)

W związku z tym każde przekazanie musi spełniać dwa warunki:

- w pierwszej kolejności należy zapewnić zgodność z przepisami ogólnymi RODO,
- a następnie – z przepisami rozdziału V RODO.

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 6

URZĄD OCHRONY DANYCH OSOBOWYCH

Art. 46 ust. 1 i ust. 2 lit. f RODO

W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej:

- wyłącznie, **gdy zapewnią odpowiednie zabezpieczenia,**
- **i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.** (**art. 46 ust. 1 RODO**)

Odpowiednie zabezpieczenia, o których mowa powyżej, można zapewnić - bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego - za pomocą **zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 RODO 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.** (**art. 46 ust.2 lit. f RODO**)

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 7

URZĄD OCHRONY DANYCH OSOBOWYCH

Podmiot przekazujący dane (eksporter danych) może podjąć decyzję o powołaniu się na certyfikację uzyskaną przez podmiot odbierający dane w celu wykazania zgodności z jego obowiązkami, np. zgodnie z art. 24 ust. 3 lub art. 28 ust. 5 RODO.

Podmiot odbierający dane może podjąć decyzję o złożeniu wniosku o certyfikację w celu wykazania, że wdrożono odpowiednie zabezpieczenia.

Zarówno podmiot przekazujący dane, jak i podmiot odbierający dane mogą pełnić role (np. rolę administratora lub podmiotu przetwarzającego), w zależności od przetwarzania, którego dokonują, co prowadzi do różnych obowiązków.

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 8

URZĄD OCHRONY DANYCH OSOBOWYCH

Podmiot przekazujący dane zobowiązany jest do wypełnienia swoich obowiązków wynikających z RODO – może to podlegać certyfikacji na mocy art. 42 ust. 1 RODO.

Ponadto podmiot przekazujący dane, który chce skorzystać z certyfikacji jako odpowiedniego zabezpieczenia zgodnie z art. 46 ust. 2 lit. f) RODO, jest w szczególności zobowiązany do:

1. sprawdzenia, czy certyfikacja, na której zamierza polegać, jest skuteczna w świetle cech planowanego przetwarzania. W tym celu podmiot przekazujący dane musi sprawdzić:

- certyfikat - czy jest ważny,
- czy przedmiot certyfikacji w nim wskazany obejmuje konkretne przekazanie, które ma zostać przeprowadzone,
- czy tranzyt danych osobowych jest objęty zakresem certyfikacji,
- a także czy certyfikat obejmuje dalsze przekazywanie oraz czy dostarczono odpowiednią dokumentację w tym zakresie;

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 9

2. sprawdzenia, czy podmiot certyfikujący, który wydał certyfikat, posiada akredytację zgodną z RODO;

3. powinien odnieść się do stosowania certyfikacji jako narzędzia do przekazywania danych

- **w umowie o przetwarzanie danych na podstawie art. 28 RODO** (w przypadku przekazywania danych od administratora do podmiotu przetwarzającego)
- lub w **umowie o udostępnieniu danych** zawartej z podmiotem odbierającym dane (w przypadku przekazania danych od administratora do administratora).

CERTYFIKACJA JAKO NARZĘDZIE TRANSFERU - 10

URZĄD OCHRONY DANYCH OSOBOWYCH

4. ocenić, czy certyfikacja, na której zamierza polegać jako narzędzie przekazywania danych, jest skuteczna w świetle prawa i praktyk obowiązujących w państwie trzecim.

Do celów tej oceny i jako ważny element służący wykazu spełnienie tego obowiązku, podmiot przekazujący dane **może polegać na przeprowadzonej przez podmiot certyfikujący weryfikacji**, udokumentowanej oceny przepisów i praktyk państwa trzeciego dokonanej przez podmiot odbierający dane.

Jeżeli z oceny dokonanej przez podmioty przekazujące wynika, że podmiot odbierający dane lub podmiot przekazujący dane może być zmuszony do wprowadzenia dodatkowych środków przewidzianych w certyfikacji w celu zapewnienia zasadniczo równoważnego stopnia ochrony jak w EOG

- podmiot przekazujący dane musi zweryfikować środki uzupełniające zapewnione przez podmiot odbierający dane posiadający certyfikację
- oraz to, czy jest w stanie zapewnić środki techniczne i (w stosownych przypadkach) uzupełniające, o które zwrócił się podmiot odbierający dane.

URZĄD OCHRONY DANYCH OSOBOWYCH

Rodzaje mechanizmów certyfikacji

URZĄD OCHRONY DANYCH OSOBOWYCH

RODZAJE MECHANIZMÓW CERTYFIKACJI - przypomnienie:

- **ogólny mechanizm certyfikacji** – dotyczy **różnych operacji** przetwarzania przeprowadzanych przez administratora danych/podmiot przetwarzający dane **z różnych sektorów działalności**;
- **specyficzny mechanizm certyfikacji** – ukierunkowany na **konkretne operacje** przetwarzania przeprowadzane przez administratora danych/podmiot przetwarzający dane i/lub dla **określonego sektora działalności**.

Powyższe mechanizmy mogą być:

- **krajowymi** (obowiązujące w jednym kraju EOG, w którym zatwierdzone zostały kryteria certyfikacji), **wielonarodowymi** (obowiązują w krajach EOG, w których organy nadzorcze zatwierdziły kryteria certyfikacji), **ogólnoeuropejskimi** (obowiązujące w całym EOG, kryteria certyfikacji są zatwierdzane przez EROD)

RODZAJE MECHANIZMÓW CERTYFIKACJI - 13

Certyfikacje, które mają być wykorzystywane jako narzędzie do przekazywania danych, mogą być udzielane zgodnie z:

- **krajowymi mechanizmami certyfikacji**
- **oraz mechanizmami ogólnoeuropejskimi.**

Mechanizmy krajowe są ważne jedynie w odniesieniu do przypadków przekazania do państw trzecich przez podmioty przekazujące w państwie członkowskim EOG, w którym mechanizm certyfikacji został zatwierdzony.

W tej chwili nie ma dostępnego żadnego mechanizmu certyfikacji jako narzędzia do przekazywania danych, **którego kryteria zostałyby zaopiniowanie/zatwierdzone przez EROD** – por. rejestr mechanizmów certyfikacji EROD (https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_pl)

URZĄD OCHRONY DANYCH OSOBOWYCH

Zakres i przedmiot certyfikacji jako narzędzia do przekazywania danych

ZAKRES I PRZEDMIOT CERTYFIKACJI JAKO NARZĘDZIA TRANSFERU - 14

URZĄD OCHRONY DANYCH OSOBOWYCH

Certyfikacja, jako narzędzie przekazywania danych zgodnie z art. 42 ust. 2 RODO, musi mieć na celu wykazanie, że istnieją odpowiednie zabezpieczenia zapewnione **przez administratorów lub podmioty przetwarzające spoza EOG lub organizacje międzynarodowe otrzymujące dane od administratorów lub podmiotów przetwarzających z EOG, służące przeciwdziałaniu szczególnemu ryzyku związanemu z przekazywaniem danych osobowych.**

Przedmiotem certyfikacji jako narzędzie przekazywania danych zgodnie z art. 42 ust. 2 RODO powinno zasadniczo być przetwarzanie danych otrzymanych od EOG przez podmiot odbierający dane w państwie trzecim,

a tranzyt - jeżeli znajduje się pod kontrolą podmiotu odbierającego dane.

Przedmiotem certyfikacji może być **pojedyncza operacja przetwarzania lub zestaw operacji**.

Podmiot składający wniosek o certyfikację byłby zatem podmiotem odbierającym dane w państwie trzecim w odniesieniu do jego przedmiotu certyfikacji.

URZĄD OCHRONY DANYCH OSOBOWYCH

ELEMENTY KRYTERIÓW CERTYFIKACJI JAKO NARZĘDZIA DO PRZEKAZYWANIA DANYCH

KRYTERIA CERTYFIKACJI - 16

Opracowując
kryteria certyfikacji jako narzędzia do przekazywania danych
należy wziąć pod uwagę **wskazówki wynikające z niżej wymienionych dokumentów wydanych przez Europejską Radę Ochrony Danych**:

- **Wytyczne 1/2018** w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia,
- **Wytyczne 7/2022** w sprawie certyfikacji jako narzędzia do przekazywania danych,
- **Uzupełnienie do Wytycznych 1/2018** – Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation).

Ww. dokumenty dostępne są na stronie internetowej EROD i UODO.

URZĄD OCHRONY DANYCH OSOBOWYCH

Kryteria certyfikacji jako narzędzia do przekazywania danych - obejmują wymogi dotyczące oceny:

- **przetwarzania dokonywanego przez podmiot odbierający dane**, w tym dalsze przekazywanie danych,
- **oraz ram prawnych państwa trzeciego**, aby uniknąć sytuacji, w której przepisy i praktyki stosowane w państwie trzecim uniemożliwiają importerowi wypełnianie jego obowiązków wynikających z certyfikacji.

W trakcie procesu certyfikacji przedmiot oceny jest sprawdzany na podstawie kryteriów certyfikacji przez podmiot certyfikujący akredytowany przez krajową jednostkę akredytującą lub przez właściwy organ nadzorczy.

URZĄD OCHRONY DANYCH OSOBOWYCH

W opinii EROD kryteria certyfikacji opracowane na podstawie Wytycznych 1/2018 oraz uzupełnienia do Wytycznych 1/2018 **obejmują już większość kryteriów certyfikacji, które należy wziąć pod uwagę przy opracowywaniu mechanizmu certyfikacji, o którym mowa w art. 46 ust. 2 lit. f RODO**.

Może jednak zaistnieć potrzeba **doprecyzowania niektórych z tych istniejących** kryteriów w celu dostosowania ich do konkretnego scenariusza transferu.

Ponadto może zaistnieć potrzeba sformułowania **dodatkowych kryteriów do celów stosowania odpowiednich zabezpieczeń**, w tym w odniesieniu do praw osób, których dane dotyczą.

URZĄD OCHRONY DANYCH OSOBOWYCH

Doprecyzowanie niektórych kryteriów certyfikacji określonych w załączniku 2 do Wytycznych 1/2018 w celu dostosowania ich do konkretnego scenariusza transferu:

dot. **ZAKRESU MECHANIZMU CERTYFIKACJI I PRZEDMIOTU OCENY** – kryteria powinny wymagać szczegółowego opisania przedmiotu oceny, w tym czy tranzyt też jest przedmiotem certyfikacji, państwa, w których odbywa się przetwarzanie danych, czy dochodzi do dalszego przekazywania danych (p. 39-42 Wytycznych 7/2022);

URZĄD OCHRONY DANYCH OSOBOWYCH

Doprecyzowanie niektórych kryteriów certyfikacji określonych w załączniku 2 do Wytycznych 1/2018 w celu dostosowania ich do konkretnego scenariusza transferu:

dot. **PRZEJRZYSTOŚCI i PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ** – kryteria powinny m.in.:

- **przewidywać wymóg udzielania osobom, których dane dotyczą, informacji** na temat czynności przetwarzania, w tym, w stosownych przypadkach, na temat przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (zob. art. 12, 13 i 14 RODO);
- **przewidywać wymóg zapewnienia osobie, której dane dotyczą, jej praw** zasadniczo równoważnych prawom przewidzianym w art. 15–19, art. 21 i 22 RODO;
- przewidywać wymóg, aby podmiot odbierający dane posiadający certyfikację ustanowił odpowiednią **procedurę rozpatrywania skarg** w celu zapewnienia skutecznego wykonywania praw osób, których dane dotyczą;

URZĄD OCHRONY DANYCH OSOBOWYCH

Doprecyzowanie niektórych kryteriów certyfikacji określonych w załączniku 2 do Wytycznych 1/2018 w celu dostosowania ich do konkretnego scenariusza transferu:

dot. **PRZEJRZYSTOŚCI i PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ** – kryteria powinny m.in.:

- **przewidywać wymóg przeprowadzenia oceny, czy i w jakim zakresie prawa te są możliwe do wyegzekwowania dla osób, których dane dotyczą, w odnośnym państwie trzecim oraz oceny wszelkich dodatkowych odpowiednich środków, które mogą być konieczne w celu wyegzekwowania tych praw**, np. wymogu, aby podmiot odbierający wyraził zgodę na poddanie się jurysdykcji organu nadzorczego właściwego dla podmiotu przekazującego lub podmiotów przekazujących i współpracę z tym organem w ramach wszelkich procedur mających na celu zapewnienie przestrzegania tych praw, a w szczególności aby zgodził się odpowiadać na zapytania, poddać się audytowi i zastosować się do środków przyjętych przez wspomniany organ nadzorczy, w tym środków zaradczych i odszkodowawczych (p. 43 Wytycznych 7/2022).

URZĄD OCHRONY DANYCH OSOBOWYCH

Doprecyzowanie niektórych kryteriów certyfikacji określonych w załączniku 2 do Wytycznych 1/2018 w celu dostosowania ich do konkretnego scenariusza transferu:

- dot. **ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH** - kryteria certyfikacji powinny nakładać **na podmiot odbierający obowiązek poinformowania podmiotu przekazującego** oraz, jeżeli ten pierwszy działa w charakterze administratora danych, **powiadomienia organu nadzorczego w EOG** właściwego dla podmiotu przekazującego lub podmiotów przekazujących dane o naruszeniu ochrony danych oraz poinformowania o tym osób, których dane dotyczą, w przypadku gdy takie naruszenie może spowodować wysokie ryzyko naruszenia ich praw i wolności, zgodnie z wymogami art. 34 RODO (p. 44 Wytycznych 7/2022),

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

1. Ocena przepisów państwa trzeciego - w kryteriach nakłada się na podmiot odbierający, **np.**:

- **wymóg dokonania oceny przepisów i praktyk państwa trzeciego**, w którym prowadzi działalność, oraz czy te przepisy i praktyki **uniemożliwiają** podmiotowi odbierającemu wywiązanie się ze zobowiązań wynikających z certyfikacji,
- **wymóg udokumentowania** powyższego, **przechowywania dokumentacji** do dyspozycji podmiotu certyfikującego oraz udostępniania jej na żądanie organowi nadzorczemu w EOG właściwemu dla podmiotu przekazującego dane i podmiotowi przekazującemu dane,

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

2. **Ogólne obowiązki podmiotów przekazujących i odbierających** - w kryteriach nakłada się na podmiot odbierający:

- wymóg określenia w postanowieniach umownych (np. w istniejącej umowie o świadczenie usług) między podmiotami przekazującymi a podmiotami odbierającymi **opisu konkretnego przypadku przekazania, do którego ma zastosowanie certyfikacja, oraz uznania praw przysługujących osobom, których dane dotyczą, jako beneficjentom będącym stronami trzecimi,**
- **wymóg przewidujący szczególną treść tych umów lub instrumentów umownych** oraz w zakresie, w jakim przedstawiono wzór, w kryteriach przewidziano wymóg, aby ta treść i ten wzór zostały również poddane ocenie.

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

3. **Przepisy dotyczące dalszego przekazywania danych** - w kryteriach nakłada się na podmiot odbierający:

   - wymóg, aby dalsze przekazywanie danych **podlegało szczególnym zabezpieczeniom zgodnie z wymogami określonymi w rozdziale V RODO**, służącym zagwarantowaniu, aby stopień ochrony zapewniony w EOG nie został naruszony, oraz czy nakłada się w nich wymóg prowadzenia odpowiedniej dokumentacji do dyspozycji podmiotu certyfikującego i organu nadzorczego w EOG właściwego dla podmiotu przekazującego lub podmiotów przekazujących dane oraz udostępniania jej na żądanie podmiotowi przekazującemu dane?

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

4. Środki zaskarżenia i egzekwowanie przepisów:

- Czy w kryteriach przewidziano, że osoby, których dane dotyczą, **mogą egzekwować prawa przysługujące im jako beneficjentom będącym stronami trzecimi w stosunku do podmiotu odbierającego dane przed sądem EOG właściwym dla miejsca zwykłego pobytu osoby, której dane dotyczą**, lub w ramach organizacji międzynarodowej, w tym w odniesieniu do odszkodowania za szkody poniesione przez osobę, której dane dotyczą, w przypadku nieprzestrzegania przez podmiot odbierający wymogów odpowiedniego systemu certyfikacji.

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

4. Środki zaskarżenia i egzekwowanie przepisów:

- Czy kryteria **umożliwiają odpowiednią ocenę odpowiedzialności podmiotu odbierającego w EOG** za szkodę poniesioną przez osobę, której dane dotyczą, w przypadku nieprzestrzegania wymogów odpowiedniego systemu certyfikacji,
- Czy w kryteriach nakłada się wymóg, **aby osoby, których dane dotyczą, mogły wnieść skargę przeciwko podmiotowi odbierającemu do organu nadzorczego w EOG**, w szczególności w państwie EOG, w którym mają miejsce zwykłego pobytu lub miejsce pracy, lub do organu nadzorczego właściwego dla podmiotu przekazującego lub podmiotów przekazujących dane

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

4. Środki zaskarżenia i egzekwowanie przepisów:

- Czy w kryteriach nakłada się wymóg, aby **podmiot odbierający współpracował z organem nadzorczym w EOG** właściwym dla podmiotu przekazującego (podmiotów przekazujących) dane i wyraził zgodę na poddanie się audytowi i kontroli przez ten podmiot przekazujący (te podmioty przekazujące) dane, brał pod uwagę jego (ich) porady i stosował się do jego (ich) decyzji?

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

5. Procedury i działania w sytuacjach, w których krajowe przepisy i praktyki uniemożliwiają przestrzeganie zobowiązań podjętych w ramach certyfikacji:

- Czy w kryteriach nakłada się wymóg, że w przypadku gdy podmiot odbierający dane w państwie trzecim lub organizacja międzynarodowa ma powody, by sądzić, że zmiany w mających do niego (lub do niej) zastosowanie przepisach i praktykach mogą uniemożliwić mu (lub jej) wypełnienie obowiązków wynikających z certyfikacji, **ten podmiot odbierający dane lub ta organizacja międzynarodowa muszą niezwłocznie powiadomić o tym podmiot certyfikujący i podmiot przekazujący dane, tak aby ten ostatni mógł ocenić, czy należy natychmiast zaprzestać przekazywania danych?**

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

5. Procedury i działania w sytuacjach, w których krajowe przepisy i praktyki uniemożliwiają przestrzeganie zobowiązań podjętych w ramach certyfikacji:

- Czy w kryteriach nakłada się **wymóg przedstawienia opisu działań**, jakie należy podjąć (w tym powiadomienia podmiotu przekazującego w EOG i wprowadzenia odpowiednich dodatkowych środków), jeżeli podmiot odbierający dane dowie się o przepisach lub praktykach państwa trzeciego, które uniemożliwiają wypełnienie obowiązków wynikających z certyfikacji, a także opisu środków, jakie należy wprowadzić w przypadku wniosków o udzielenie informacji wystosowanych przez organy państwa trzeciego (w tym o obowiązku zweryfikowania i, w razie potrzeby, zakwestionowania zgodności z prawem takiego wniosku oraz minimalizacji wszelkich ujawnionych informacji)?

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

6. **Rozpatrywanie wniosków o dostęp do danych wystosowanych przez organy państw trzecich:**

- Czy w kryteriach nakłada się wymóg, aby podmiot odbierający dane **niezwłocznie informował** podmiot przekazujący dane w przypadku wniosków o dostęp do danych wystosowanych przez organy państwa trzeciego oraz wprowadził odpowiednie dodatkowe środki?
- Czy w kryteriach nakłada się wymóg, **aby nie dochodziło do przekazywania danych w wyniku nieproporcjonalnych żądań o dostęp** wystosowanych przez organy publiczne państw trzecich, w szczególności wniosków, w których żąda się masowego i niezróżnicowanego przekazania danych osobowych?

URZĄD OCHRONY DANYCH OSOBOWYCH

Dodatkowe szczególne kryteria certyfikacji do celów stosowania odpowiednich zabezpieczeń:

(p. 45-46 Wytycznych 7/2022),

7. **Dodatkowe zabezpieczenia dotyczące podmiotu przekazującego**:

- Czy w kryteriach nakłada się wymóg, aby podmiot odbierający dane, o ile tak przewidziano, zapewniał, również w drodze wiążących wymogów w tym zakresie nałożonych na podmiot przekazujący dane, **aby środki uzupełniające określone przez podmiot odbierający odpowiadały odpowiednim środkom uzupełniającym po stronie podmiotu przekazującego dane,** z uwzględnieniem Zaleceń 01/2020 i przypadków użycia, w celu zapewnienia skutecznego wdrożenia środków uzupełniających podmiotu odbierającego?

URZĄD OCHRONY DANYCH OSOBOWYCH

WIĄŻĄCE I MOŻLIWE DO WYEGZEKWOWANIA ZOBOWIĄZANIA

W art. 42 ust. 2 RODO wymaga się, aby administratorzy i podmioty przetwarzające, niepodlegający RODO i przestrzegający mechanizmu certyfikacji przeznaczonego do przekazywania danych, **podjęli ponadto wiążące i egzekwowalne zobowiązania** – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – **do stosowania odpowiednich zabezpieczeń przewidzianych w mechanizmie certyfikacji, w tym w odniesieniu do praw osób, których dane dotyczą**.

URZĄD OCHRONY DANYCH OSOBOWYCH

ZATWIERDZANIE KRYTERIÓW CERTYFIKACJI JAKO NARZĘDZIA TRANSFERU

ZATWIERDZANIE KRYTERIÓW CERTYFIKACJI JAKO NARZĘDZIA TRANSFERU - 35

URZĄD OCHRONY DANYCH OSOBOWYCH

Kryteria certyfikacji są zatwierdzane odpowiednio przez organ nadzorczy lub EROD.

Etap krajowy:

1. WNIOSEK do właściwego organu nadzorczego.
2. OCENA MECHANIZMU CERTYFIKACJI przez właściwy organ nadzorczy (**pierwsza ocena**).
3. **PODJĘCIE DECYZJI O PRZEKAZANIU DOKUMENTÓW DO SEKRETARIATU EROD**.

Etap na poziomie EROD:

1. ETAP NIEFORMALNY – ocena przez współrecenzentów (**druga ocena**).
2. ETAP NIEFORMALNY – ocena przez podgrupę EROD (CEH) (**trzecia ocena**).
3. ETAP NIEFORMALNY – SESJA CERTYFIKACYJNA.
4. ETAP FORMALNY – OPINIA EROD (**czwarta ocena).**

Etap krajowy (dot. krajowych kryteriów certyfikacji):

1. Zatwierdzenie kryteriów certyfikacji (zgodnie z opinią EROD) przez właściwy organ nadzorczy – w przypadku krajowego mechanizmu certyfikacji.

URZĄD OCHRONY DANYCH OSOBOWYCH

PODMIOTY, KTÓRE BĘDĄ MOGŁY UDZIELAĆ CERTYFIKACJI,

O KTÓREJ MOWA

W ART. 46 UST. 2 LIT. F RODO.

ZASADY AKREDYTACJI

URZĄD OCHRONY DANYCH OSOBOWYCH

p. 32-35 Wymogów 7/2022

Zdaniem EROD dodatkowe wymogi akredytacji podmiotów certyfikujących opracowane na podstawie Wytycznych 4/2018 i normy ISO 17065, przyjęte zgodnie z art. 64 ust. 1 lit. c) RODO, **obejmują już szczegółowe wymogi niezbędne do akredytacji podmiotu certyfikującego w odniesieniu do certyfikacji jako narzędzia do przekazywania danych -** niektóre wymogi wymagają jednak pewnych uzupełnień, tzn.:

- **wymogi dotyczące zasobów** (zob. wymóg 6 Wytycznych 4/2018 – załącznik 1),
- **wymogi dotyczące procesów** (zob. wymóg 7 Wytycznych 4/2018 – załącznik 1),
- **wymogi dotyczące zmian mających wpływ na certyfikację** (zob. wymóg 7.10 Wytycznych 4/2018 – załącznik 1).

URZĄD OCHRONY DANYCH OSOBOWYCH

DZIĘKUJĘ ZA UWAGĘ

SESJA PYTAŃ I ODPOWIEDZI

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl