Wytyczne

Wytyczne 07/2022 dotyczące certyfikacji jako narzędzia do przekazywania danych

Wersja 2.0

Przyjęte 14 lutego 2023 r.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

HISTORIA WERSJI

Wersja 1.0	14 czerwca 2022 r.	Przyjęcie wytycznych do konsultacji publicznych
Wersja 2.0	14 lutego 2023 r.	Przyjęcie wytycznych po konsultacjach publicznych

STRESZCZENIE

W art. 46 RODO wymaga się, aby podmioty przekazujące dane wprowadziły odpowiednie zabezpieczenia w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. W tym celu w RODO różnicuje się odpowiednie zabezpieczenia, które mogą zastosować podmioty przekazujące dane na podstawie art. 46 do określenia ram przekazywania danych do państw trzecich, i wprowadza się między innymi certyfikację jako nowy mechanizm przekazywania (art. 42 ust. 2 i art. 46 ust. 2 lit. f) RODO).

Niniejszy dokument zawiera wytyczne dotyczące stosowania art. 46 ust. 2 lit. f) RODO w odniesieniu do przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na podstawie certyfikacji. Składa się z czterech sekcji i załącznika.

W części pierwszej niniejszego dokumentu („INFORMACJE OGÓLNE") wyjaśniono, że niniejsze wytyczne uzupełniają już istniejące ogólne Wytyczne 1/2018 w sprawie certyfikacji i odnoszą się do szczegółowych wymogów określonych w rozdziale V RODO, jeżeli certyfikacja jest wykorzystywana jako narzędzie do przekazywania danych. Zgodnie z art. 44 RODO wszelkie przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych musi nie tylko spełniać warunki przewidziane w przepisach zawartych w rozdziale V RODO, ale również spełniać warunki określone w pozostałych przepisach RODO. W związku z tym w pierwszej kolejności należy zapewnić zgodność z przepisami ogólnymi RODO, a następnie z przepisami rozdziału V RODO. W sekcji tej opisano zaangażowane podmioty i ich główne role w tym kontekście, ze szczególnym uwzględnieniem roli podmiotu odbierającego dane, któremu zostanie udzielona certyfikacja, oraz podmiotu przekazującego dane, który wykorzysta tę certyfikację jako narzędzie do kształtowania ram przekazywania przez siebie danych (biorąc pod uwagę, że odpowiedzialność za przetwarzanie danych pozostaje po stronie podmiotu przekazującego dane). Certyfikacja może również obejmować w tym kontekście środki uzupełniające w stosunku do narzędzi do przekazywania danych służące zapewnieniu zgodności ze stopniem ochrony danych osobowych mającym zastosowanie w UE. Część pierwsza wytycznych zawiera również informacje na temat procesu uzyskiwania certyfikacji, która ma być wykorzystywana jako narzędzie do przekazywania danych.

W drugiej części niniejszych wytycznych („WYTYCZNE DOTYCZĄCE WDROŻENIA WYMOGÓW AKREDYTACJI") przypomina się, że wymogi akredytacji podmiotu certyfikującego znajdują się w normie ISO 17065 oraz są dostępne w drodze interpretacji Wytycznych 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 RODO i załącznika do nich w kontekście rozdziału V. W niniejszych wytycznych natomiast doprecyzowano, w kontekście przekazywania danych, niektóre wymogi akredytacji mające zastosowanie do podmiotu certyfikującego.

Trzecia część niniejszych wytycznych („SZCZEGÓLNE KRYTERIA CERTYFIKACJI") zawiera wytyczne dotyczące kryteriów certyfikacji już wymienionych w Wytycznych 1/2018. Ponadto sformułowano w niej dodatkowe kryteria szczegółowe do uwzględnienia w mechanizmie certyfikacji, który ma być stosowany jako narzędzie do przekazywania danych do państw trzecich. Kryteria te obejmują ocenę ustawodawstwa państwa trzeciego, ogólne obowiązki podmiotów przekazujących i odbierających, przepisy dotyczące dalszego przekazywania, środków zaskarżenia i działań egzekucyjnych, procedury i działania w sytuacjach, w których krajowe przepisy i praktyki uniemożliwiają przestrzeganie zobowiązań podjętych w ramach certyfikacji i wykonanie wniosków o udostępnienie danych składanych przez organy państw trzecich.

W części czwartej niniejszych wytycznych („WIĄŻĄCE I EGZEKWOWALNE ZOBOWIĄZANIA DO WDROŻENIA”) przedstawiono elementy do uwzględnienia w wiążących i egzekwowalnych zobowiązaniach, które administratorzy lub podmioty przetwarzające, niepodlegający RODO, powinni podjąć w celu zapewnienia odpowiednich zabezpieczeń w odniesieniu do danych przekazywanych do państw trzecich. Zobowiązania te mogą być określone w różnych instrumentach, w tym w umowach, i obejmują w szczególności gwarancję, że podmiot odbierający nie ma powodów, by sądzić, że przepisy i praktyki obowiązujące w państwie trzecim mające zastosowanie do danego przypadku przetwarzania, w tym wszelkie wymogi dotyczące ujawniania danych osobowych lub środki zezwalające organom publicznym na dostęp do tych danych, uniemożliwiają mu wypełnienie zobowiązań wynikających z certyfikacji.

W ZAŁĄCZNIKU do niniejszych wytycznych zawarto kilka przykładów środków uzupełniających zgodnych ze środkami wymienionymi w załączniku II do Zaleceń 01/2020 (Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych) w kontekście stosowania certyfikacji jako narzędzia do przekazywania danych. Przytoczone w tej części przykłady służą zwróceniu uwagi na najważniejsze sytuacje.

SPIS TREŚCI

Europejska Rada Ochrony Danych,

uwzględniając art. 70 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

1 INFORMACJE OGÓLNE

1.1 Cel i zakres

1. Niniejszy dokument ma na celu zapewnienie wytycznych dotyczących stosowania art. 46 ust. 2 lit. f) RODO w odniesieniu do przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na podstawie certyfikacji. EROD opublikowała już ogólne wytyczne dotyczące certyfikacji[2] i akredytacji[3] w ramach RODO. Niniejsze nowe wytyczne odnoszą się zatem jedynie do szczególnych aspektów certyfikacji jako narzędzia do przekazywania danych. Określono w nich stosowanie art. 46 ust. 2 lit. f) i art. 42 ust. 2 RODO, zapewniając praktyczne wytyczne w tym zakresie i wprowadzając nowe elementy w stosunku do już opublikowanych wytycznych.

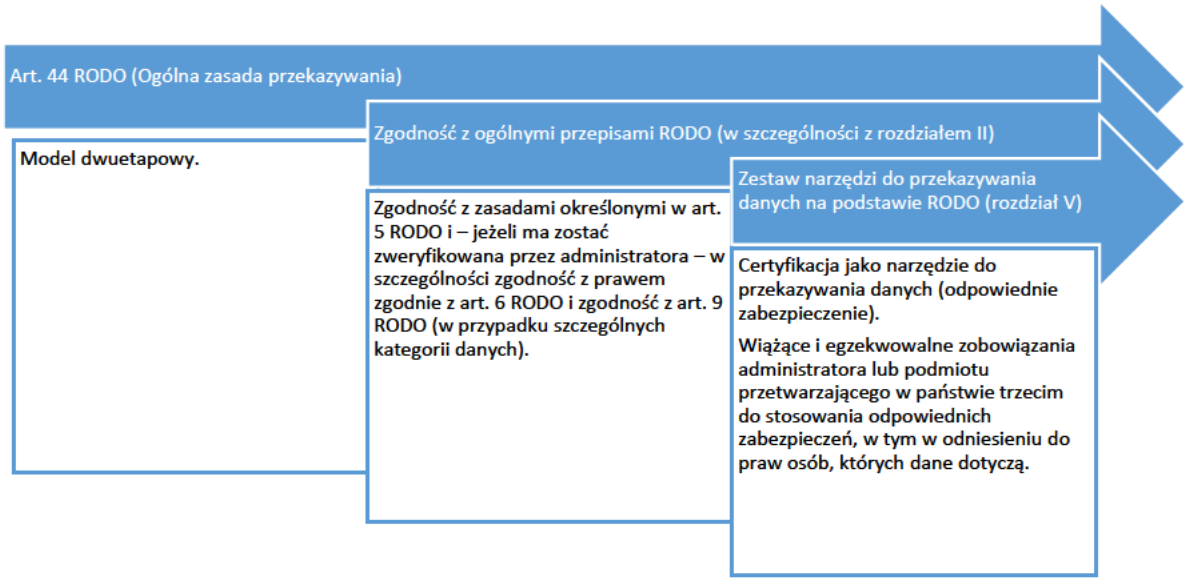
2. EROD oceni funkcjonowanie niniejszych wytycznych w świetle doświadczeń zdobytych podczas ich stosowania w praktyce i przedstawi dalsze wytyczne w celu wyjaśnienia stosowania elementów wymienionych poniżej, w tym roli umowy o certyfikacji w odniesieniu do wiążących i egzekwowalnych zobowiązań, o których mowa w art. 46 ust. 2 lit. f) RODO.

1.2 Zasady ogólne mające zastosowanie do międzynarodowego przekazywania danych

3. Zgodnie z art. 44 RODO wszelkie przekazywanie danych osobowych do państw trzecich[4] lub organizacji międzynarodowych musi nie tylko spełniać warunki przewidziane w przepisach zawartych w rozdziale V RODO, ale również spełniać warunki określone w pozostałych przepisach RODO. Każde przekazanie musi być zatem zgodne między innymi z zasadami ochrony danych określonymi w art. 5 RODO, zgodne z prawem, jak określono w art. 6 RODO, oraz zgodne z art. 9 RODO w przypadku szczególnych kategorii danych. 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.

---

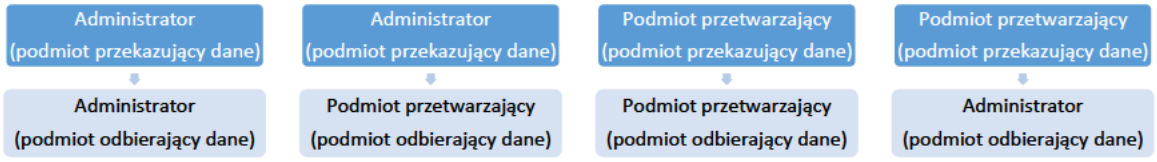
[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679.
[3] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679).
[4] Wytyczne 05/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO, s. 4.



4. Art. 46 RODO stanowi, że „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". Zgodnie z art. 46 ust. 2 lit. f) RODO takie odpowiednie zabezpieczenia mogą być przewidziane w zatwierdzonym mechanizmie certyfikacji 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.

5. Dzięki temu podmiot przekazujący dane może podjąć decyzję o powołaniu się na certyfikację uzyskaną przez podmiot odbierający dane w ramach wykazywania zgodności ze swoimi 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.

6. Zarówno podmiot przekazujący dane, jak i podmiot odbierający dane mogą mieć różne role (na przykład rolę administratora lub podmiotu przetwarzającego)[5], w zależności od przypadku przetwarzania w ramach rozdziału V, z którymi wiążą się różne obowiązki:



7. Oprócz stosowania certyfikacji lub innych narzędzi lub mechanizmów przekazywania danych, o których mowa w art. 45 i 46, art. 49 RODO stanowi, że w ograniczonej liczbie szczególnych sytuacji międzynarodowe przekazywanie danych może mieć miejsce, jeżeli nie jest przestrzegany żaden inny mechanizm określony w rozdziale V[6]. Jak jednak wyjaśniono w poprzednich opublikowanych przez

[5] Zob. poniżej: WYTYCZNE DOTYCZĄCE WDROŻENIA KRYTERIÓW CERTYFIKACJI

[6] Więcej informacji na temat art. 49 i jego wzajemnych zależności z art. 46 w ogóle można znaleźć w Wytycznych 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679.

EROD wytycznych, wyjątki przewidziane w art. 49 RODO należy interpretować w sposób zawężający i muszą one dotyczyć głównie przetwarzania, które jest sporadyczne i niepowtarzające się[7].

1.3 Kim są podmioty zaangażowane w certyfikację, która ma służyć jako narzędzie do przekazywania danych, i jaka jest ich rola?

8. **Europejska Rada Ochrony Danych (EROD)** jest uprawniona do zatwierdzania kryteriów certyfikacji obejmujących cały EOG (europejski znak jakości ochrony danych) oraz do wydawania opinii na temat projektów decyzji organów nadzorczych w sprawie kryteriów certyfikacji i wymogów akredytacji podmiotów certyfikujących, co ma na celu zapewnienie spójności. Jest również organem właściwym do gromadzenia w rejestrze wszystkich mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych i udostępniania ich opinii publicznej[8].

9. **Organy nadzorcze** zatwierdzają kryteria certyfikacji, jeżeli mechanizmem certyfikacji nie jest europejski znak jakości ochrony danych[9]. Mogą również akredytować podmiot certyfikujący, opracowywać kryteria certyfikacji i udzielać certyfikacji, jeżeli tak stanowi prawo krajowe ich państwa członkowskiego[10].

10. **Krajowa jednostka akredytująca** może akredytować podmioty certyfikujące będące stronami trzecimi, korzystając z normy ISO 17065 i dodatkowych wymogów akredytacji ustanowionych przez organy nadzorcze, w sposób zgodny z sekcją 2 niniejszych wytycznych. W niektórych państwach członkowskich akredytację może również oferować właściwy organ nadzorczy, a także krajowa jednostka akredytująca lub oba te podmioty.

11. **Właścicielem systemu** jest organizacja, która określiła kryteria certyfikacji i wymogi w zakresie metodyki, zgodnie z którymi dokonuje się oceny zgodności. Organizacja dokonująca oceny może być tą samą organizacją, która opracowała system i jest jej właścicielem. Mogą jednak istnieć ustalenia, zgodnie z którymi jedna organizacja jest właścicielem systemu, inna zaś (lub kilka innych organizacji) dokonuje oceny jako podmiot certyfikujący.

12. W zależności od prawa krajowego certyfikacji może udzielać – jest to rozwiązanie alternatywne w stosunku do udzielania certyfikacji przez organy nadzorcze – **podmiot certyfikujący** akredytowany zgodnie z powyższym opisem[11]. Może on opracować kryteria certyfikacji, a tym samym być właścicielami systemu (zob. pkt 11 powyżej). Taki podmiot musi mieć siedzibę w EOG, w szczególności w celu umożliwienia skutecznego wykonywania uprawnień naprawczych zapisanych w art. 58 ust. 2 lit. f) RODO. Podmiot certyfikujący może jednak zlecić podwykonawstwo działań lokalnym ekspertom lub oddziałom spoza EOG, którzy będą przeprowadzać czynności audytowe w jego imieniu[12]. Podmiot certyfikujący nie zleca jednak podwykonawcom czynności podejmowania decyzji dotyczącej udzielenia lub nieudzielenia certyfikacji.

13. **Podmiot odbierający dane** to podmiot (administrator lub podmiot przetwarzający) w państwie trzecim otrzymujący dane od podmiotu przekazującego dane.

---

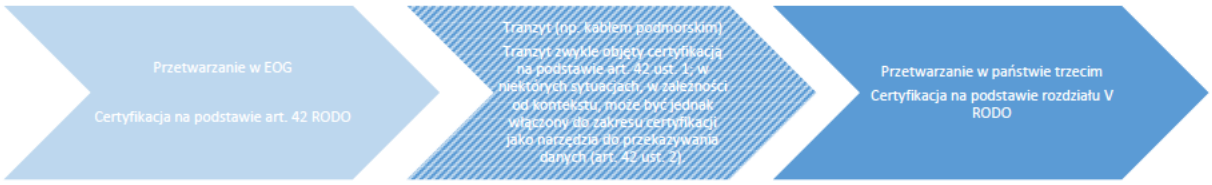
[7] Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 5.
[8] Art. 42 ust. 8 RODO.
[9] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679, pkt 2.2.
[10] Art. 42 ust. 5 i 43 ust. 1 RODO.
[11] Art. 42 ust. 5 RODO.
[12] Podmioty certyfikujące muszą ocenić swoich lokalnych ekspertów zgodnie z normą ISO 17065 i dodatkowymi wymogami akredytacji ustanowionymi przez organ nadzorczy (art. 43 ust. 1 lit. b) RODO).

14. **Podmiot przekazujący dane** to podmiot (administrator lub podmiot przetwarzający) przekazujący dane z EOG do podmiotu odbierającego dane. Podmiot przekazujący dane musi zapewnić zgodność z rozdziałem V.

1.4 Jaki jest zakres i przedmiot certyfikacji jako narzędzia do przekazywania danych?

15. Mechanizm certyfikacji jako narzędzie do przekazywania danych na podstawie art. 42 ust. 2 musi mieć na celu zapewnienie odpowiednich zabezpieczeń w odniesieniu do przetwarzania danych osobowych zgodnie z warunkami określonymi w art. 46 ust. 2 lit. f). Certyfikacja ma 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.

16. Ogólnie rzecz biorąc, operacja polegająca na przekazywaniu danych osobowych z państwa członkowskiego do państwa trzeciego stanowi jako taka przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO, dokonywane na terytorium państwa członkowskiego[13], i w związku z tym podlega certyfikacji na podstawie art. 42 ust. 1 RODO. W niektórych sytuacjach, w zależności od kontekstu, zakres certyfikacji jako narzędzia do przekazywania danych może jednak obejmować tranzyt. W związku z tym przedmiotem certyfikacji – który pokrywa się podczas certyfikacji z przedmiotem oceny[14] – powinny zasadniczo być przetwarzanie danych otrzymanych z EOG przez podmiot odbierający dane w państwie trzecim oraz tranzyt, jeżeli odbywa się pod kontrolą podmiotu odbierającego.



17. Przedmiotem certyfikacji może być pojedyncza operacja przetwarzania lub zestaw operacji. Wspomniane operacje lub zestawy operacji mogą obejmować procesy zarządzania w rozumieniu środków organizacyjnych, a zatem mogą stanowić integralne części operacji przetwarzania[15].

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

1.5 Jaką rolę powinien odgrywać podmiot przekazujący w stosowaniu certyfikacji jako narzędzia do przekazywania?

19. Przekazywanie danych przez podmiot przekazujący dane jako takie podlega zasadniczo bezpośrednio RODO. Oznacza to, że podmiot przekazujący dane jest zobowiązany do wypełnienia swoich

---

[13] Wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems, pkt 83.
[14] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679, s. 17.
[15] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679, s. 16 (np. mechanizm rozpatrywania skarg).

obowiązków wynikających z RODO, a w szczególności do zapewnienia, aby dane były przekazywane w bezpieczny sposób zgodnie z art. 32 i rozdziałem V z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w tym rozporządzeniu (art. 44 RODO)[16]. Powyższe podlega oczywiście certyfikacji zgodnie z art. 42 ust. 1.

20. 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 sprawdzenia, czy certyfikacja, na której zamierza polegać, jest skuteczna w świetle cech planowanego przetwarzania. W tym celu podmiot przekazujący dane musi sprawdzić w odniesieniu do udzielonej certyfikacji, czy certyfikat jest ważny i nie wygasł, czy obejmuje konkretne przekazanie, które ma zostać dokonane, czy w zakres certyfikacji wchodzi tranzyt danych osobowych, a także czy będzie mieć miejsce dalsze przekazywanie danych oraz czy dostarczono odpowiednią dokumentację na ten temat. Ponadto podmiot przekazujący musi sprawdzić, czy podmiot certyfikujący udzielający certyfikacji jest akredytowany przez krajową jednostkę akredytującą lub właściwy organ nadzorczy. Co więcej, podmiot przekazujący dane 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 przez administratora do podmiotu przetwarzającego lub w umowie o udostępnianiu danych zawartej z podmiotem odbierającym dane w przypadku przekazywania danych przez administratora do administratora.

21. Biorąc pod uwagę, że podmiot przekazujący jest odpowiedzialny za stosowanie wszystkich przepisów rozdziału V, musi on również ocenić, czy certyfikacja, którą zamierza wykorzystać jako narzędzie do przekazywania danych, jest skuteczna w świetle prawa i praktyk obowiązujących w państwie trzecim, które są istotne dla odnośnego przypadku przekazania. Do celów tej oceny i jako ważny element służący wykazaniu spełnienia tego obowiązku podmiot przekazujący dane może polegać na przeprowadzonej przez podmiot certyfikujący weryfikacji udokumentowanej oceny przepisów i praktyk państwa trzeciego dokonanej przez podmiot odbierający.

22. 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.

23. Jeżeli warunki te nie są spełnione, podmiot przekazujący dane będzie musiał wymagać od podmiotu odbierającego dane wprowadzenia dostosowanych środków uzupełniających lub ustanowienia ich samodzielnie.

---

[16] Należy zauważyć w tym względzie, że w art. 44 RODO wyraźnie przewidziano, że przekazania może dokonać nie tylko administrator, ale również podmiot przetwarzający. W związku z tym dojdzie do sytuacji przekazania, w której podmiot przetwarzający przesyła dane innemu podmiotowi przetwarzającemu lub nawet administratorowi w państwie trzecim zgodnie z poleceniem administratora (art. 28 ust. 3 lit. a) RODO). W takich przypadkach podmiot przetwarzający działa jako podmiot przekazujący dane w imieniu administratora danych i musi zapewnić przestrzeganie przepisów rozdziału V w odniesieniu do tego przekazania danych zgodnie z poleceniami administratora, w tym zapewnić wykorzystanie odpowiedniego narzędzia do przekazywania danych. Biorąc pod uwagę, że przekazanie danych jest czynnością przetwarzania prowadzoną w imieniu administratora, administrator jest również odpowiedzialny i może ponosić odpowiedzialność na mocy rozdziału V, a także musi zapewnić, aby podmiot przetwarzający zapewniał wystarczające gwarancje na mocy art. 28.

1.6 Na czym polega proces certyfikacji jako narzędzia do przekazywania danych?

24. Certyfikacja jest dobrowolna, ale w przypadku ubiegania się o nią musi być udzielana w drodze przejrzystego procesu opartego na bezwzględnie obowiązujących przepisach. W RODO pokłada się duże zaufanie w prywatnych mechanizmach certyfikacji jako „regulowanej samoregulacji". W związku z tym mechanizmy te muszą zapewniać, aby certyfikaty spełniały zasadniczo wymogi dotyczące odpowiednich zabezpieczeń określone w art. 46 RODO.

25. Certyfikacja musi się zatem opierać się na ocenie kryteriów certyfikacji zgodnie z wiążącą metodyką audytu. Kryteria te zostaną zatwierdzone przez krajowe organy nadzorcze lub EROD, jak opisano w art. 42 ust. 5 RODO. Kryteria certyfikacji obejmują wymogi dotyczące oceny przetwarzania dokonywanego przez podmiot odbierający dane, w tym dalszego przekazywania danych, oraz oceny odpowiednich ram prawnych państwa trzeciego, aby uniknąć sytuacji, w której przepisy i praktyki państwa trzeciego uniemożliwiają podmiotowi odbierającemu dane wywiązanie się z obowiązków wynikających z certyfikacji.

26. 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[17].

27. Zgodnie z art. 43 ust. 1 RODO podmioty certyfikujące, które dysponują odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych, dokonują certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h) RODO.

28. Zgodnie z art. 43 ust. 5 RODO podmioty certyfikujące przedstawiają właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji. Nie oznacza to, że podmiot certyfikujący potrzebuje upoważnienia organu nadzorczego do wydania certyfikacji. Podmiot ten będzie monitorować przestrzeganie kryteriów certyfikacji przez swoich klientów.

29. Organ nadzorczy ma uprawnienie naprawcze do cofnięcia certyfikacji lub nakazania cofnięcia certyfikacji wydanej na podstawie art. 42 i 43 RODO, lub nakazania podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.

30. W odniesieniu do międzynarodowego przekazywania danych europejski znak jakości ochrony danych może służyć jako narzędzie obejmujące przekazywanie danych do państw trzecich wraz z wiążącymi i egzekwowalnymi zobowiązaniami[18].

31. Certyfikacje, które mają być wykorzystywane jako narzędzie do przekazywania danych, mogą być jednak również udzielane zgodnie z krajowymi zatwierdzonymi systemami certyfikacji w państwach EOG. W związku z tym są one ważne jedynie w odniesieniu do przypadków przekazania do państw trzecich przez podmioty przekazujące w państwie członkowskim EOG, w którym system certyfikacji został zatwierdzony, ponieważ nie istnieje wzajemne uznawanie różnych certyfikacji wydanych przez

[17] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych (2016/679), s. 9.
[18] Zob. art. 42 ust. 5 RODO i pkt 35 Wytycznych 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia.

państwa EOG. Organy nadzorcze w różnych państwach EOG mogą jednak zatwierdzić ten sam mechanizm certyfikacji w odniesieniu do przekazywania danych[19].

2 WYTYCZNE DOTYCZĄCE WDROŻENIA WYMOGÓW AKREDYTACJI

32. Wymogi dotyczące akredytacji podmiotu certyfikującego w odniesieniu do certyfikacji jako narzędzia do przekazywania danych zawarto w normie ISO 17065 oraz są dostępne w drodze interpretacji Wytycznych 4/2018[20] w kontekście rozdziału V, jak wyjaśniono poniżej.

33. Zdaniem EROD dodatkowe wymogi akredytacji 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. W scenariuszu dotyczącym przekazania niektóre wymogi wymagają jednak pewnych udoskonaleń pod względem uwag wyjaśniających i interpretacji.

34. W odniesieniu do wymogów dotyczących zasobów (zob. wymóg 6 Wytycznych 4/2018 – załącznik 1) podmiot certyfikujący zapewnia sobie zasoby niezbędne do sprawdzenia, czy zgodnie z kryteriami certyfikacji podmiot odbierający należycie i prawidłowo przeprowadził niezbędną ocenę sytuacji prawnej i praktyk państwa trzeciego lub państw trzecich, w których ma siedzibę lub prowadzi działalność[21]. Ocenę tę należy przeprowadzić w odniesieniu do czynności przetwarzania, które mają być certyfikowane w ramach przedmiotu oceny w odniesieniu do odpowiednich zabezpieczeń przewidzianych w art. 46 RODO, i obejmuje ona w razie potrzeby środki uzupełniające określone i wdrożone przez podmiot odbierający. Wymaga to również np. znacznej znajomości odpowiednich lokalnych przepisów i praktyk oraz adekwatnych kompetencji językowych w odniesieniu do państw trzecich.

35. W odniesieniu do wymogów dotyczących procesów (zob. wymóg 7 Wytycznych 4/2018 – załącznik 1) podmiot certyfikujący zapewnia, aby proces certyfikacji mógł być poparty ewentualnymi audytami na miejscu, był przeprowadzany w odniesieniu do przetwarzania, które będzie się odbywać w państwach trzecich, oraz aby ocena obejmowała również praktyczne wdrożenie obowiązujących przepisów i polityk w państwach trzecich.

36. W odniesieniu do wymogów dotyczących zmian mających wpływ na certyfikację (zob. wymóg 7.10 Wytycznych 4/2018 – załącznik 1) podmiot certyfikujący monitoruje zmiany w prawodawstwie państw trzecich lub w ich orzecznictwie, mogące mieć wpływ na przetwarzanie objęte zakresem przedmiotu oceny.

---

[19] Jeżeli organ nadzorczy kieruje przyjęciem kryteriów certyfikacji X w ramach inicjatywy krajowej, a następnie inne państwa – przy uwzględnieniu kryteriów systemu i swoich mających zastosowanie szczególnych przepisów krajowych – chcą przyjąć te same kryteria certyfikacji, mogą je przyjąć bez konieczności wydania przez EROD opinii na podstawie art. 64 RODO, w oparciu o opinię wydaną pierwszemu organowi nadzorczemu zgodnie z art. 64 ust. 3 RODO (zob. w tym względzie odniesienie do addendum do wytycznych – (załącznik do Wytycznych nr 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia), pkt 66.

[20] Wytyczne 4/2018 w sprawie akredytacji podmiotów certyfikujących na podstawie art. 43 ogólnego rozporządzenia o ochronie danych wraz z załącznikiem.

[21] Zob. pkt 12 powyżej.

3 SZCZEGÓLNE KRYTERIA CERTYFIKACJI

37. W kontekście uwzględnienia szczególnych kryteriów certyfikacji niniejsze wytyczne opierają się na Wytycznych 1/2018 w sprawie certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia (wersja 3. 0), odnośnym załączniku 2 dotyczącym przeglądu i oceny kryteriów certyfikacji zgodnie z art. 42 ust. 5 oraz addendum do wytycznych dotyczących oceny kryteriów certyfikacji.

38. W opinii EROD kryteria certyfikacji opracowane na podstawie Wytycznych 1/2018, załącznik 2, oraz addendum do wytycznych dotyczących oceny kryteriów certyfikacji, obejmują już większość kryteriów certyfikacji, które należy wziąć pod uwagę przy opracowywaniu systemu certyfikacji do wykorzystywania jako narzędzie do przekazywania danych. Może jednak zaistnieć potrzeba doprecyzowania niektórych z tych istniejących kryteriów, aby dostosować je do konkretnego scenariusza przekazania danych (zob. pkt 3.1). Ponadto może zaistnieć potrzeba sformułowania dodatkowych kryteriów do celów stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą (zob. pkt 3.2).

3.1 WYTYCZNE DOTYCZĄCE WDROŻENIA KRYTERIÓW CERTYFIKACJI

39. Zakres mechanizmu certyfikacji i przedmiotu oceny (zob. sekcja 2.a w załączniku 2) powinien być jasno opisany w odpowiedniej dokumentacji, w tym w przypadku przekazywania danych osobowych do państwa trzeciego. Ponadto w dokumentacji tej należy wskazać, czy zakres ten obejmuje również tranzyt danych osobowych.

40. W odniesieniu do zakresu mechanizmu certyfikacji i przedmiotu oceny (zob. sekcja 2.b w załączniku 2) w odpowiedniej dokumentacji powinno się znaleźć konkretne wskazanie, do jakiego rodzaju podmiotu (np. administratora lub podmiotu przetwarzającego) ten mechanizm certyfikacji ma zastosowanie.

41. W odniesieniu do zakresu mechanizmu certyfikacji i przedmiotu oceny (zob. sekcja 2.f w załączniku 2) kryteria powinny wymagać konkretnego określenia – w celu uniknięcia nieporozumień – przedmiotu oceny. Powinny one obejmować przynajmniej:

42. W odniesieniu do operacji przetwarzania, w tym w przypadku gdy przewiduje się dalsze przekazywanie danych:

    a) cel

    b) rodzaj podmiotu (np. administrator lub podmiot przetwarzający)

    c) rodzaj przekazywanych danych ze wskazaniem, czy chodzi o szczególne kategorie danych osobowych określone w art. 9 RODO

    d) kategorie osób, których dane dotyczą

    e) państwa, w których odbywa się przetwarzanie danych.

43. W odniesieniu do przejrzystości i praw osób, których dane dotyczą (zob. sekcja 8 w załączniku 2), kryteria certyfikacji powinny:

    a) 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);

b) przewidywać wymóg zapewnienia osobie, której dane dotyczą, prawa dostępu, sprostowania, usunięcia, ograniczenia, powiadomienia o sprostowaniu, usunięciu lub ograniczeniu, sprzeciwu wobec przetwarzania, prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, zasadniczo równoważnych prawom przewidzianym w art. 15–19, art. 21 i 22 RODO;
c) przewidywać wymóg, aby podmiot odbierający dane posiadający certyfikację ustanowił odpowiednią procedurę rozpatrywania skarg w celu zapewnienia skutecznego wykonywania praw osób, których dane dotyczą;
d) 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.

44. W odniesieniu do środków technicznych i organizacyjnych gwarantujących ochronę (załącznik 2 sekcja 10.q) 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.

3.2 DODATKOWE SZCZEGÓLNE KRYTERIA CERTYFIKACJI

45. W świetle zabezpieczeń określonych w odniesieniu do innych instrumentów przekazywania danych na podstawie art. 46 RODO (takich jak wiążące reguły korporacyjne lub kodeksy postępowania) oraz w celu zapewnienia spójnego stopnia ochrony, a także biorąc pod uwagę wyrok TSUE w sprawie Schrems II, EROD jest zdania, że mechanizm certyfikacji, który ma być stosowany jako narzędzie do przekazywania danych do państw trzecich, powinien obejmować również kryteria wymienione poniżej.

1. Ocena przepisów państwa trzeciego

a) Czy w kryteriach nakłada się na podmiot odbierający 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?
b) Czy w kryteriach nakłada się na podmiot odbierający wymóg udokumentowania oceny przepisów i praktyk państwa trzeciego, w którym prowadzi działalność, oraz do prowadzenia i przechowywania dokumentacji do dyspozycji podmiotu certyfikującego oraz udostępniania jej na żądanie organowi nadzorczemu w EOG właściwemu dla podmiotu przekazującego dane i podmiotowi przekazującemu dane?
c) Czy w kryteriach nakłada się na podmiot odbierający wymóg określenia i wdrożenia środków organizacyjnych i technicznych w celu zapewnienia odpowiednich zabezpieczeń przewidzianych w art. 46 RODO, z uwzględnieniem „Zaleceń 01/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych”?

d) Czy w kryteriach nakłada się na podmiot odbierający wymóg dokumentowania skutecznie wdrożonych środków organizacyjnych i technicznych służących zapewnieniu odpowiednich zabezpieczeń przewidzianych w art. 46 RODO oraz przechowywania tej dokumentacji do dyspozycji podmiotu certyfikującego oraz udostępniania jej na żądanie właściwym organom ochrony danych i podmiotowi przekazującemu dane?
e) Czy w kryteriach nakłada się na podmiot odbierający wymóg określenia i wdrożenia środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa przekazywania danych osobowych, z uwzględnieniem „Zaleceń 01/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych", jeżeli zakresem certyfikacji jako narzędzia do przekazywania danych objęty jest tranzyt danych?
f) Czy w kryteriach nakłada się wymóg zagwarantowania podmiotowi certyfikującemu i podmiotowi przekazującemu, że podmiot odbierający nie ma powodów, by sądzić, że mające do niego zastosowanie przepisy i praktyki mogą uniemożliwić mu wypełnienie obowiązków wynikających z certyfikacji?

2. Ogólne obowiązki podmiotów przekazujących i odbierających

a) Czy w kryteriach nakłada się 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?

b) Czy w zakresie, w jakim w kryteriach nałożono 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?

3. Przepisy dotyczące dalszego przekazywania danych

a) Czy w kryteriach nakłada się 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?

4. Środki zaskarżenia i egzekwowanie przepisów

a) 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?
b) 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?

c) 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?

d) 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?

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

a) 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?

b) 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)?

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

a) 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?

b) 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?

7. Dodatkowe zabezpieczenia dotyczące podmiotu przekazującego

46. 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?

4 WIĄŻĄCE I EGZEKWOWALNE ZOBOWIĄZANIA DO WDROŻENIA

47. 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[22] – do stosowania odpowiednich zabezpieczeń przewidzianych w mechanizmie certyfikacji, w tym w odniesieniu do praw osób, których dane dotyczą.

48. Jak określono w RODO, takie zobowiązania można podjąć w drodze umowy, co wydaje się najprostszym rozwiązaniem. Można również wykorzystać inne instrumenty, pod warunkiem że administrator/podmioty przetwarzające przestrzegający mechanizmu certyfikacji są w stanie wykazać wiążący i egzekwowalny charakter tych innych środków.

49. W każdym razie taki wiążący i egzekwowalny charakter musi być zagwarantowany zgodnie z prawem Unii, a odnośne zobowiązania również powinny być wiążące i możliwe do wyegzekwowania przez osoby, których dane dotyczą, jako prawa przysługujące im jako beneficjentom będącym stronami trzecimi.

50. Prostym wariantem byłoby włączenie wiążących i egzekwowalnych zobowiązań do umowy między podmiotem przekazującym dane a podmiotem odbierającym dane. W praktyce strony mogą wykorzystać istniejącą umowę (np. umowę o świadczenie usług między podmiotem przekazującym a podmiotem odbierającym dane lub umowę o przetwarzaniu danych między administratorami a podmiotami przetwarzającymi zawartą zgodnie z art. 28 RODO, lub umowę o udostępnianiu danych pomiędzy różnymi administratorami), w której można zawrzeć wiążące i egzekwowalne zobowiązania. Zobowiązania te należy wyraźnie odróżnić od wszelkich innych klauzul. Inną opcją mogłoby być wykorzystanie odrębnej umowy, na przykład przez dodanie do mechanizmu certyfikacji przeznaczonego do przekazywania danych wzoru umowy, która musiałaby być następnie podpisana przez administratorów/podmioty przetwarzające w państwie trzecim i wszystkie podmioty przekazujące.

51. Powinna istnieć możliwość wyboru najbardziej odpowiedniego wariantu w zależności od konkretnej sytuacji.

52. Jeżeli mechanizm certyfikacji ma służyć do przekazywania oraz dalszego przekazywania danych przez podmiot przetwarzający podwykonawcom przetwarzania, w umowie z podmiotem przetwarzającym podpisanej przez podmiot przetwarzający i jego administratora należy również zamieścić odniesienie do mechanizmu certyfikacji oraz instrumentu przewidującego wiążące i egzekwowalne zobowiązania.

Przykład wiążących i egzekwowalnych zobowiązań włączonych do umowy między podmiotem przekazującym dane a podmiotem odbierającym dane:

[22] Taki prawnie wiążący instrument nie może być innym narzędziem określonym w rozdziale V (takim jak np. szczególne kryteria certyfikacji), ponieważ te wiążące i egzekwowalne zobowiązania, o których mowa w art. 46 ust. 2 lit. f), muszą być skonstruowane w taki sposób, aby zagwarantować przestrzeganie przez podmiot odbierający kryteriów certyfikacji.

53. Ogólnie rzecz biorąc, umowa lub inny prawnie wiążący instrument musi określać, że posiadający certyfikację administrator/podmiot przetwarzający działający w charakterze podmiotu odbierającego zobowiązuje się do przestrzegania zasad określonych w certyfikacji na potrzeby przekazywania danych podczas przetwarzania odpowiednich danych otrzymanych z EOG i deklaruje, że nie ma powodów, by sądzić, że przepisy i praktyki obowiązujące w państwie trzecim mające zastosowanie do danego przypadku przetwarzania, w tym jakiekolwiek wymogi dotyczące ujawniania danych osobowych lub środki zezwalające organom publicznym na dostęp do tych danych, uniemożliwiają mu wypełnienie zobowiązań wynikających z certyfikacji, oraz że będzie informować podmiot przekazujący o wszelkich istotnych zmianach w przepisach lub praktykach w tym zakresie.

54. Ponadto w umowie lub innym instrumencie należy przewidzieć mechanizmy pozwalające egzekwować takie zobowiązania w przypadku nieprzestrzegania przepisów wynikających z certyfikacji przez administratora/podmiot przetwarzający działającego w charakterze podmiotu odbierającego, w szczególności w odniesieniu do praw osób, których dane dotyczą, a których dane są przekazywane na podstawie certyfikacji.

55. W szczególności w umowie lub innym instrumencie należy odnieść się do:

- Istnienia prawa osób, których dane dotyczą, a których dane są przekazywane w ramach certyfikacji, do egzekwowania zobowiązań podjętych przez certyfikowany podmiot odbierający dane w ramach certyfikacji jako beneficjenci będący stronami trzecimi.

- Kwestii odpowiedzialności w przypadku nieprzestrzegania zasad określonych w certyfikacji przez posiadający certyfikację poza EOG podmiot odbierający dane. W przypadku nieprzestrzegania zasad certyfikacji przez posiadający certyfikację poza EOG podmiot odbierający dane osoby, których dane dotyczą, mają możliwość wytoczenia powództwa, powołując się na przysługujące im jako beneficjentowi będącemu stroną trzecią prawo, w tym o odszkodowanie, przeciwko temu podmiotowi przed organy nadzorcze EOG i sąd EOG właściwy dla miejsca zwykłego pobytu osoby, której dane dotyczą. Posiadający certyfikację podmiot odbierający akceptuje decyzję osoby, której dane dotyczą, o podjęciu takiego działania. Osoby, których dane dotyczą, mają również możliwość – w przypadku gdy nieprzestrzeganie przez podmiot odbierający wspomnianych zasad może prowadzić do odpowiedzialności podmiotu przekazującego dane – wytoczenia powództwa przeciwko podmiotowi przekazującemu dane przed organ nadzorczy lub sąd właściwym dla siedziby podmiotu przekazującego dane lub miejsca zwykłego pobytu osoby, której dane dotyczą23. Podmiot odbierający dane i podmiot przekazujący dane powinny również przyjąć, że

[23] Odpowiedzialność ta powinna pozostawać bez uszczerbku dla mechanizmów, które mają być wdrożone na podstawie certyfikacji wraz z podmiotem certyfikującym, który także może podejmować działania wobec

osoba, której dane dotyczą, może być reprezentowana przez podmiot, organizację lub zrzeszenie, które nie mają charakteru zarobkowego, na warunkach określonych w art. 80 ust. 1 RODO.

- Istnienia prawa podmiotu przekazującego do egzekwowania – w charakterze beneficjenta będącego stroną trzecią – od posiadającego certyfikację podmiotu odbierającego dane przestrzegania zasad wynikających z certyfikacji.
- Istnienia obowiązku posiadającego certyfikację podmiotu odbierającego do powiadamiania podmiotu przekazującego i organu nadzorczego podmiotu przekazującego dane o wszelkich środkach zastosowanych przez podmiot certyfikujący w odpowiedzi stwierdzone nieprzestrzeganie zasad certyfikacji przez ten podmiot odbierający dane.

administratorów/podmiotów przetwarzających zgodnie z certyfikacją w drodze zastosowania środków naprawczych.

ZAŁĄCZNIK

A. PRZYKŁADY ŚRODKÓW UZUPEŁNIAJĄCYCH, KTÓRE PODMIOT ODBIERAJĄCY MA OBOWIĄZEK WDROŻYĆ W PRZYPADKU, GDY ZAKRESEM CERTYFIKACJI OBJĘTY JEST TRANZYT DANYCH

Przypadek użycia 1: Przechowywanie danych do celów tworzenia kopii zapasowych i innych celów, które nie wymagają dostępu do danych niezaszyfrowanych

Należy ustanowić kryteria dotyczące norm szyfrowania i bezpieczeństwa klucza deszyfrującego, w szczególności kryteria dotyczące sytuacji prawnej w państwie trzecim. Jeżeli podmiot odbierający może być zmuszony do przekazania kluczy deszyfrujących, ten dodatkowy środek nie może być uznany za skuteczny[24].

Przypadek użycia 2: Przekazywanie danych spseudonimizowanych

W przypadku danych spseudonimizowanych ustanawia się kryteria dotyczące bezpieczeństwa dodatkowych informacji niezbędnych do przypisania przekazanych danych zidentyfikowanej lub możliwej do zidentyfikowania osobie, w szczególności:

— Kryteria dotyczące sytuacji prawnej w państwie trzecim. Jeżeli podmiot odbierający może być zmuszony do uzyskania dostępu do dodatkowych danych lub wykorzystania ich w celu przypisania danych do zidentyfikowanej lub możliwej do zidentyfikowania osobie, środek ten nie może być uznany za skuteczny[25].

— Kryteria dotyczące definicji dodatkowych informacji dostępnych organom państw trzecich, które to informacje mogą być wystarczające do przypisania danych do zidentyfikowanej lub możliwej do zidentyfikowania osoby.

Przypadek użycia 3: Szyfrowanie danych w celu ich ochrony przed dostępem organów publicznych państwa trzeciego podmiotu odbierającego w przypadku tranzytu między podmiotem przekazującym a podmiotem odbierającym

W przypadku zaszyfrowanych danych uwzględnia się wszelkie kryteria dotyczące bezpieczeństwa tranzytu. Jeżeli podmiot odbierający może być zmuszony do przekazania kluczy kryptograficznych w celu odszyfrowania lub uwierzytelnienia, lub modyfikacji komponentu wykorzystywanego do tranzytu w taki sposób, że właściwości tego komponentu w zakresie bezpieczeństwa zostaną naruszone, ten dodatkowy środek nie może być uznany za skuteczny[26].

Przypadek użycia 4: Odbiorca chroniony

W przypadku odbiorców chronionych należy określić kryteria dotyczące granic tego przywileju. Przetwarzanie danych musi pozostawać w granicach prawniczej tajemnicy zawodowej. Dotyczy to

[24] Załącznik 2, Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0, przypadek użycia 1: Przechowywanie danych do celów tworzenia kopii zapasowych i innych celów, które nie wymagają dostępu do danych niezaszyfrowanych, s. 85; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[25] Tamże, pkt 86–89.

[26] Tamże, pkt 90.

również przetwarzania przez podmioty przetwarzające (podwykonawców przetwarzania) i dalszego przekazywania, którego odbiorcy również muszą być objęci tym przywilejem[27].

B. PRZYKŁADY ŚRODKÓW UZUPEŁNIAJĄCYCH W PRZYPADKU, GDY TRANZYT NIE JEST OBJĘTY CERTYFIKACJĄ, A PODMIOT PRZEKAZUJĄCY MUSI ZAPEWNIĆ TAKIE ŚRODKI

Przypadek użycia 2: Przekazywanie danych spseudonimizowanych

Należy przewidzieć kryteria dotyczące dodatkowych informacji dostępnych organom państw trzecich, które to informacje mogą być wystarczające do przypisania danych do zidentyfikowanej lub możliwej do zidentyfikowania osoby.

Przypadek użycia 3: Szyfrowanie danych w celu ich ochrony przed dostępem organów publicznych państwa trzeciego podmiotu odbierającego w przypadku tranzytu między podmiotem przekazującym a podmiotem odbierającym

Należy przewidzieć kryteria dotyczące wiarygodności organu certyfikacji zapewniającego certyfikację klucza publicznego lub wykorzystywanej infrastruktury, bezpieczeństwa kluczy kryptograficznych stosowanych do uwierzytelniania lub odszyfrowywania oraz niezawodności zarządzania kluczami, a także korzystania z odpowiednio utrzymywanego oprogramowania bez znanych podatności.

Jeżeli podmiot odbierający może być zmuszony do ujawnienia kluczy kryptograficznych umożliwiających odszyfrowanie lub uwierzytelnienie, lub modyfikację komponentu wykorzystywanego do tranzytu w celu naruszenia jego właściwości w zakresie bezpieczeństwa, środek ten nie może być uznany za skuteczny[28].

Przypadek użycia 4: Odbiorca chroniony

W przypadku odbiorców chronionych należy określić kryteria dotyczące granic tego przywileju. Przetwarzanie danych musi pozostawać w granicach prawniczej tajemnicy zawodowej. Dotyczy to również przetwarzania przez podmioty przetwarzające (podwykonawców przetwarzania) i dalszego przekazywania, którego odbiorcy również muszą być objęci tym przywilejem[29].

[27] Tamże, pkt 91.
[28] Tamże, pkt 90.
[29] Tamże, pkt 91.