Zalecenia

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

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

Przyjęte w dniu 10 listopada 2020 r.

Streszczenie

Przyjęcie ogólnego rozporządzenia UE o ochronie danych (RODO) miało służyć dwóm celom: ułatwieniu swobodnego przepływu danych osobowych na terytorium Unii Europejskiej, przy jednoczesnej ochronie podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych.

W niedawno wydanym wyroku w sprawie C-311/18 (Schrems II) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) przypomniał, że ochrona przyznana danym osobowym w Europejskim Obszarze Gospodarczym (EOG) musi towarzyszyć tym danym w każdym miejscu, do którego są przekazywane. Przekazanie danych osobowych do państwa trzeciego nie może prowadzić do rozluźnienia lub osłabienia ochrony zagwarantowanej w EOG. Trybunał wyjaśnił również, iż nie jest wymagane, aby państwa trzecie zapewniały stopień ochrony identyczny jak ten zagwarantowany w EOG, lecz jedynie merytorycznie równoważny. Trybunał potwierdził także ważność standardowych klauzul umownych jako narzędzia przekazywania, dzięki któremu można zapewnić na poziomie umownym merytorycznie równoważny stopień ochrony danych przekazywanych do państw trzecich.

Standardowe klauzule umowne i inne narzędzia przekazywania, o których mowa w art. 46 RODO, nie funkcjonują w próżni. Trybunał stwierdził, że administratorzy lub podmioty przetwarzające pełniący rolę podmiotów przekazujących dane są zobowiązani do sprawdzenia w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane w państwie trzecim, czy prawo lub praktyki państwa trzeciego mają negatywny wpływ na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO. W takich przypadkach Trybunał wciąż pozostawia podmiotom przykazującym dane otwartą możliwość wdrożenia środków uzupełniających, które wypełniłyby luki w ochronie i podniosłyby ją do stopnia wymaganego przez prawo UE. Trybunał nie sprecyzował, jakie mogą to być środki. Wskazał jednak, że podmioty przekazujące dane będą musiał określać je w każdym konkretnym przypadku. Jest to zgodne z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, stanowiącą, że administrator jest odpowiedzialny za przestrzeganie zasad RODO dotyczących przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie.

Żeby wesprzeć podmioty przekazujące dane (niezależnie czy będą nimi administratorzy, podmioty przetwarzające, podmioty prywatne czy urzędy publiczne, które przetwarzają dane osobowe w zakresie zastosowania RODO) w skomplikowanym zadaniu polegającym na przeprowadzeniu oceny państw trzecich i w razie potrzeby określeniu odpowiednich środków uzupełniających, Europejska Rada Ochrony Danych (EROD) przyjęła niniejsze zalecenia. Przedstawiają one podmiotom przekazującym dane schemat działań, jakie należy podjąć, potencjalne źródła informacji, a także pewne przykłady środków uzupełniających, jakie można wprowadzić.

Pierwszym krokiem, jaki zdaniem EROD podmioty przekazujące dane powinny podjąć, jest **rozpoznanie przeprowadzanych operacji przekazywania**. Zidentyfikowanie wszystkich operacji przekazywania danych osobowych do państw trzecich może być bardzo trudnym zadaniem. Uświadomienie sobie, gdzie dane osobowe trafiają, jest niemniej jednak konieczne, żeby zapewnić merytorycznie równoważny stopień ochrony wszędzie tam, gdzie dane są przetwarzane. Należy także sprawdzić, czy dane, jakie zostaną przekazane, są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przekazywane i przetwarzane w państwie trzecim.

Drugi krok polega na **sprawdzeniu, czy wykorzystywane narzędzie przekazywania**, jest wymienione w rozdziale V RODO. Jeśli Komisja Europejska w drodze decyzji stwierdzającej odpowiedni stopień ochrony wydanej na podstawie art. 45 RODO lub poprzednio obowiązującej dyrektywy 95/46

stwierdziła już, że dane państwo, region lub sektor, do którego dane są przesyłane, oferuje odpowiedni stopień ochrony, to do momentu, aż decyzja taka przestanie obowiązywać, nie będzie trzeba podejmować żadnych dalszych działań poza monitorowaniem, czy taka decyzja stwierdzająca odpowiedni stopień ochrony pozostaje ważna. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony konieczne będzie skorzystanie z jednego z narzędzi przekazywania, wymienionych w art. 46 RODO, jeśli operacje przekazywania są regularne i powtarzalne. Jedynie w przypadku sporadycznych i niepowtarzających się operacji przetwarzania możliwe będzie skorzystanie z jednego z wyjątków przewidzianych w art. 49 RODO, jeśli spełniono określone tam warunki.

Trzecim krokiem jest **ocena**, czy w **prawie lub praktyce państwa trzeciego** funkcjonuje cokolwiek, co w kontekście danej operacji przekazywania mogłoby negatywnie wpłynąć na skuteczność odpowiednich zabezpieczeń wykorzystywanych narzędzi przekazywania. Ocena powinna skupiać się przede wszystkim na przepisach państwa trzeciego, które znajdują zastosowanie do danej operacji przetwarzania i do wykorzystywanego narzędzia przetwarzania z art. 46 RODO, a które może doprowadzić do zmniejszenia stopnia jego ochrony. Przy analizie elementów, które trzeba uwzględnić w ocenie przepisów państwa trzeciego dotyczących dostępu organów publicznych do danych do celów nadzoru, należy odwołać się do zaleceń EROD w sprawie niezbędnych gwarancji europejskich. W szczególności należy dokładnie rozważyć, czy przepisy dotyczące dostępu organów publicznych do danych są niejednoznaczne lub nie są publicznie dostępne. Jeśli nie ma przepisów określających przypadki, gdy organy publiczne mogą uzyskać dostęp do danych osobowych, i niezależnie od tego operacja przekazywania ma się odbyć, należy przyjrzeć się innym istotnym i obiektywnym czynnikom, a nie polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne uzyskają dostęp do danych w sposób niezgodny z normami UE. Ocenę tę należy przeprowadzić z należytą starannością i dokładnie ją udokumentować, jako że podmiot będzie rozliczany z decyzji, jaką może podjąć na tej podstawie.

Czwartym krokiem jest **określenie i przyjęcie środków uzupełniających**, jakie są konieczne, żeby stopień ochrony przekazywanych danych był merytorycznie równoważny temu gwarantowanemu na podstawie norm UE. Krok ten jest niezbędny tylko wtedy, gdy przeprowadzona ocena wykaże, iż przepisy państwa trzeciego mają w kontekście danej operacji przekazywania negatywny wpływ na skuteczność wykorzystywanego lub planowanego narzędzia przekazywania z art. 46 RODO. Zalecenia te zawierają (w załączniku nr 2) również niewyczerpujący wykaz przykładowych środków uzupełniających oraz niektórych warunków, które byłyby niezbędne do zapewnienia skuteczności. Podobnie jak w przypadku odpowiednich zabezpieczeń zawartych w narzędziach przekazywania wymienionych w art. 46 niektóre środki uzupełniające mogą być skuteczne w jednych państwach, ale niekoniecznie w innych. Będą Państwo odpowiedzialni za ocenę ich skuteczności w kontekście danej operacji przetwarzania, w świetle przepisów obowiązujących w państwie trzecim i wykorzystywanego narzędzia przekazywania, i rozliczani z podjętej decyzji. Może to także pociągnąć za sobą konieczność połączenia różnych środków uzupełniających. Ostatecznie może okazać się, że żaden środek uzupełniający nie zapewni merytorycznie równoważnego stopnia ochrony na potrzeby danej operacji przekazywania. W takim przypadku, gdy żaden środek uzupełniający nie będzie odpowiedni, należy odstąpić od przekazania danych, zawiesić lub zakończyć je, żeby uniknąć naruszenia stopnia ochrony danych osobowych. Powinni Państwo przeprowadzić tę ocenę z należytą starannością i udokumentować ją.

Piątym krokiem jest **podjęcie** wszelkich **formalnych kroków proceduralnych**, jakich wymagać może przyjęcie środka uzupełniającego w zależności od wykorzystywanego narzędzia przekazywania z art. 46 RODO. Niniejsze zalecenia wskazują, jakie są to formalności. W niektórych przypadkach koniecznie może być także skonsultowanie się z właściwym organem nadzorczym.

Szóstym i ostatnim krokiem będzie dokonanie ponownej oceny, w odpowiednich odstępach czasu, stopnia ochrony danych przekazywanych do państw trzecich i monitorowanie, czy wystąpiły lub wystąpią jakiekolwiek zmiany w tym zakresie. Zasada rozliczalności wymaga zachowania stałej czujności w odniesieniu do stopnia ochrony danych osobowych.

Organy nadzorcze będą nadal wykonywać swoje uprawnienia w zakresie monitorowania stosowania RODO i egzekwowania go. Będą one zwracać należytą uwagę na działania podejmowane przez podmioty przekazujące w celu zapewnienia, że przekazywane dane są objęte merytorycznie równoważnym stopniem ochrony. Jak przypomina Trybunał, organy nadzorcze są zobowiązane do zawieszenia lub zakazania przekazywania danych w przypadku, gdy po przeprowadzeniu dochodzenia lub na podstawie skargi stwierdzą, że nie można zapewnić merytorycznie równoważnego stopnia ochrony.

Organy nadzorcze będą nadal opracowywać wytyczne dla podmiotów przekazujących i koordynować swoje działania w ramach EROD w celu zapewnienia spójności w stosowaniu unijnych przepisów o ochronie danych.

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 (zwanego dalej „RODO"),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym (EOG), a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

mając również na uwadze, co następuje:

(1) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w swoim wyroku z dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland LTD i Maximillianowi Schremsowi stwierdził, że art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO należy interpretować w ten sposób, że wymagane przez te przepisy odpowiednie zabezpieczenia, egzekwowalne prawa oraz skuteczne środki ochrony prawnej powinny zapewniać, by prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie klauzul ochrony danych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii przez to rozporządzenie, interpretowane w świetle Karty praw podstawowych Unii Europejskiej[2].

(2) Jak Trybunał podkreślił, stopień ochrony osób fizycznych merytorycznie równoważny temu gwarantowanemu w Unii Europejskiej przez RODO interpretowane w świetle Karty powinien być zapewniony niezależnie od przepisu rozdziału V dotyczącego podstawy, na jakiej dokonywane jest przekazywanie danych osobowych do państwa trzeciego. Przepisy rozdziału V RODO mają na celu zapewnienie ciągłości stopnia tej ochrony w sytuacji, gdy dane te są przekazywane do państwa trzeciego[3].

(3) Motyw 108 i art. 46 ust. 1 RODO stanowią, że w razie braku unijnej decyzji stwierdzającej odpowiedni stopień ochrony administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Administrator lub podmiot przetwarzający mogą zapewnić odpowiednie zabezpieczenia bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego poprzez zastosowanie jednego z narzędzi przekazywania wymienionych w art. 46 ust. 2 RODO, np. standardowych klauzul ochrony danych.

[1] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Wyrok TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland LTD i Maximillianowi Schremsowi (dalej: C-311/18 (Schrems II)), drugie ustalenie.
[3] C-311/18 (Schrems II), pkt 92 i 93.

(4) Trybunał wyjaśnił, że standardowe klauzule ochrony danych przyjęte przez Komisję mają na celu wyłącznie ustanowienie dla mających siedzibę w Unii administratorów danych lub podmiotów przetwarzających zabezpieczeń umownych znajdujących jednolite zastosowanie we wszystkich państwach trzecich. Ze względu na ich umowny charakter standardowe klauzule ochrony danych nie mogą wiązać organów władzy publicznej państw trzecich, ponieważ nie są one stronami zawartej umowy. W związku z powyższym może okazać się konieczne uzupełnienie tych zabezpieczeń zawartych w standardowych klauzulach ochrony danych poprzez podjęcie przez podmioty przekazujące dane środków uzupełniających mających na celu zapewnienie przestrzegania stopnia ochrony wymaganego na podstawie przepisów UE w państwie trzecim. Trybunał przywołuje motyw 109 RODO, który wspomina o takiej możliwości i zachęca administratorów i podmioty przetwarzające do korzystania z niej[4].

(5) Trybunał wskazał, że to przede wszystkim do podmiotu przekazującego dane należy sprawdzenie w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane, czy prawo państwa trzeciego przeznaczenia zapewnia merytorycznie równoważny, w świetle prawa Unii, stopień ochrony danych osobowych przekazywanych na podstawie standardowych klauzul ochrony danych, udzielając w razie potrzeby zabezpieczeń dodatkowych w stosunku do tych zapewnianych w tych klauzulach[5].

(6) W przypadku braku możliwości podjęcia przez mających siedzibę w Unii Europejskiej administratora danych lub podmiot przetwarzający środków uzupełniających odpowiednich dla zagwarantowania merytorycznie równoważnego stopnia ochrony w świetle prawa UE, podmioty te lub, pomocniczo, właściwy organ nadzorczy, są zobowiązane do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego[6].

(7) Ani RODO, ani Trybunał nie podają definicji ani nie precyzują pojęć „zabezpieczeń dodatkowych", „dodatkowych środków" czy „środków uzupełniających" w stosunku do zabezpieczeń narzędzi przekazywania wymienionych w art. 46 ust. 2 RODO, które administratorzy i podmioty przetwarzające mogą przyjąć w celu zapewnienia przestrzegania wymaganego przez prawo UE stopnia ochrony w danym państwie trzecim.

(8) EROD z własnej inicjatywy podjęła decyzję o przeanalizowaniu tej kwestii i przedstawieniu zaleceń dla administratorów i podmiotów przetwarzających działających jako podmiot przekazujące w zakresie procedury, którą można zastosować w celu określenia i przyjęcia środków uzupełniających. Niniejsze zalecenia mają na celu dostarczenie podmiotom przekazującym metodologii, dzięki której możliwe będzie ustalenie, czy w odniesieniu do operacji przekazywania należy podjąć jakiekolwiek dodatkowe środki, a jeśli tak – jakie. Podstawowym obowiązkiem podmiotów przekazujących jest zapewnienie, że przekazywane dane są objęte w państwie trzecim merytorycznie równoważnym stopniem ochrony do tego gwarantowanego w UE. Za pomocą tych zaleceń EROD zgodnie ze swoją właściwością zachęca do konsekwentnego stosowania zarówno RODO, jak i orzeczenia Trybunału[7].

PRZYJMUJE NINIEJSZE ZALECENIA:

[4] C-311/18 (Schrems II), pkt 132 i 133.
[5] C-311/18 (Schrems II), pkt 134.
[6] C-311/18 (Schrems II), pkt 135.
[7] Art. 70 ust. 1 lit. e) RODO.

1 ROZLICZALNOŚĆ PRZY PRZEKAZYWANIU DANYCH

1. Prawo pierwotne UE uznaje prawo do ochrony danych za prawo podstawowe[8]. W związku z tym prawu do ochrony danych przyznaje się wysoki stopień ochrony, zaś wszelkie ograniczenia tego prawa można wprowadzać tylko wtedy, gdy są one przewidziane ustawą, szanują jego istotę, są proporcjonalne, niezbędne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób[9]. Prawo do ochrony danych osobowych nie jest jednak prerogatywą o charakterze absolutnym, lecz powinno być rozpatrywane w kontekście jego funkcji społecznej i wyważone względem innych praw podstawowych w myśl zasady proporcjonalności[10].

2. Stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE musi być zagwarantowany w odniesieniu do danych przekazywanych do państwa trzeciego spoza EOG, żeby zapewnić, iż nie naruszono stopnia ochrony gwarantowanego na podstawie RODO.

3. Prawo do ochrony danych ma czynny charakter. Wymaga ono od podmiotów przekazujących i podmiotów odbierających (zarówno administratorów, jak i podmiotów przetwarzających) czegoś więcej niż tylko uznania, że takie prawo istnieje, lub pasywnej zgodności z nim[11]. Administratorzy i podmioty przetwarzające są w obowiązku dążyć do przestrzegania prawa do ochrony danych w czynny i ciągły sposób poprzez wprowadzanie środków prawnych, technicznych i organizacyjnych, które zapewniają jego skuteczność. Administratorzy i podmioty przetwarzające muszą także być w stanie udowodnić osobom, których dane dotyczą, ogółowi społeczeństwa i organom nadzorczym odpowiedzialnym za ochronę danych, że takie działania są faktycznie podejmowane. Jest to tak zwana zasada rozliczalności[12].

4. Zasada rozliczalności, która jest konieczna do zapewnienia skutecznego stosowania stopnia ochrony przewidzianego w RODO, dotyczy również przekazywania danych do państw trzecich[13], jako że operacje tego rodzaju stanowią same w sobie formę przetwarzania danych[14]. Jak Trybunał podkreślił w wydanym wyroku, stopień ochrony merytorycznie równoważny temu zagwarantowanemu w Unii Europejskiej przez RODO, interpretowany w świetle Karty, musi być zapewniony niezależnie od przepisu rozdziału V, na podstawie którego dokonywane jest przekazywanie danych osobowych do państwa trzeciego[15].

5. W wyroku w sprawie Schrems II Trybunał podkreślił obowiązek podmiotów przekazujących i podmiotów odbierających do zapewnienia, iż przetwarzanie danych osobowych odbywało się i będzie się nadal odbywało zgodnie ze stopniem ochrony przewidzianym w prawie UE w zakresie ochrony danych, do zawieszenia przekazywania danych czy też rozwiązania umowy w przypadku, gdy podmiot odbierający dane nie jest lub przestał być w stanie przestrzegać standardowych klauzul ochrony danych wprowadzonych do stosownej umowy zawartej między podmiotem przekazującym a podmiotem

[8] Art. 8 ust. 1 Karty praw podstawowych oraz art. 16 ust. 1 TFUE, preambuła 1, art. 1 ust. 2 RODO.
[9] Art. 52 ust. 1 Karty praw podstawowych UE.
[10] Motyw 4 RODO i C-507/17, Google LLC, następca prawny Google Inc., przeciwko Commission nationale de l'informatique et des libertés (CNIL), pkt 60.
[11] C-92/09 i C-93/02, Volker und Markus Schecke GbR przeciwko Land Hessen, opinia rzecznika generalnego E. Sharpston, 17 czerwca 2010 r., pkt 71.
[12] Art. 5 ust. 2 i art. 28 ust. 3 lit. h) RODO.
[13] Art. 44 i motyw 101 RODO, a także art. 47 ust. 2 lit. d) RODO.
[14] Wyrok TSUE z dnia 6 października 2015 r. Maximillian Schrems przeciwko Data Protection Commissioner, (dalej: C-362/14 (Schrems I)), pkt45.
[15] C-311/18 (Schrems II), pkt 92 i 93.

odbierającym[16]. Administrator lub podmiot przetwarzający działający jako podmiot przekazujący muszą zapewnić, że podmioty odbierające będą w stosownych przypadkach współpracować z podmiotem przekazującym w realizacji powyższych obowiązków, informując go np. o wszelkich zmianach wpływających na stopień ochrony otrzymanych danych osobowych w państwie podmiotu odbierającego[17]. Obowiązki te stanowią wyraz ustanowionej w RODO zasady rozliczalności w odniesieniu do przekazywania danych[18].

2 PLAN DZIAŁANIA: STOSOWANIE ZASADY ROZLICZALNOŚCI DO PRZEKAZYWANIA DANYCH W PRAKTYCE

6. Poniżej znaleźć można plan działań przedstawiający kroki, jakie należy podjąć, żeby dowiedzieć się, czy jako podmiot przekazujące dane muszą Państwo podjąć środki uzupełniające, aby móc zgodnie z prawem przekazywać dane poza EOG. Termin „Państwo" w niniejszym dokumencie odnosi się do administratora lub podmiotu przetwarzającego działających w roli podmiotu przekazującego, przetwarzającego dane osobowe w zakresie zastosowania RODO – w tym przetwarzania przez podmioty prywatne lub organy publiczne przy przekazywaniu danych do podmiotów prywatnych[19]. Jeśli chodzi o przekazywanie danych osobowych między organami publicznymi, konkretne wskazówki określono w Wytycznych 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 na potrzeby przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG[20].

7. Dokonaną ocenę oraz podjęte i wdrożone środki uzupełniające należy odpowiednio dokumentować i udostępnić taką dokumentację na wniosek właściwego organu nadzorczego[21].

2.1 Krok 1: Rozpoznanie przeprowadzanych operacji przekazywania

8. Pierwszym krokiem, jaki należy wykonać, żeby dowiedzieć się o nałożonych na Państwo obowiązkach jako podmiotu przekazującego dane na potrzeby kontynuowania lub przeprowadzenia nowych operacji przekazywania danych osobowych[22], jest zapewnienie pełnej wiedzy o przeprowadzanych operacjach przekazywania (rozpoznanie przeprowadzanych operacji przekazywania). Rejestrowanie i zidentyfikowanie wszystkich operacji przetwarzania może być bardzo skomplikowanym przedsięwzięciem dla podmiotów zaangażowanych w liczne, zróżnicowane i regularne operacje przekazywania z państwami trzecimi i korzystających z usług szeregu podmiotów przetwarzających i podmiotów podprzetwarzających. Rozpoznanie przeprowadzanych operacji przekazywania jest koniecznym pierwszym etapem, żeby zrealizować Państwa obowiązki w ramach zasady rozliczalności.

[16] C-311/18 (Schrems II), pkt 134, 135, 139, 140, 141, 142.
[17] C-311/18 (Schrems II), pkt 134.
[18] Art. 5 ust. 2 i art. 28 ust. 3 lit. h) RODO.
[19] Zob. Wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[20] Wytyczne EROD 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 na potrzeby przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG; zob. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[21] Art. 5 ust. 2 RODO i art. 24 ust. 1 RODO.
[22] Należy zwrócić uwagę, że zdalny dostęp przez podmiot z państwa trzeciego do danych znajdujących się w EOG również uznawany jest za przekazywanie.

9. Aby w pełni rozpoznać przeprowadzane operacje przekazywania, mogą Państwo oprzeć się na rejestrach czynności przetwarzania, które mogą mieć Państwo obowiązek prowadzić jako administrator lub podmiot przetwarzający na podstawie art. 30 RODO[23]. Pomocne mogą okazać się także uprzednio przeprowadzone czynności zgodnie z art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO dla celów powiadomienia osób, których dane dotyczą, o przekazywaniu ich danych osobowych do państw trzecich[24].

10. W procesie identyfikowania operacji przekazywania nie można zapominać o uwzględnieniu dalszego przekazywania, np. gdy Państwa podmioty przetwarzające spoza EOG przekazują powierzone im dane osobowe do podmiotów podprzetwarzających w innym lub tym samym państwie trzecim[25].

11. Zgodnie z zasadą „minimalizacji danych" na podstawie RODO[26] należy zweryfikować, czy wszystkie przekazywane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane do państwa trzeciego i tam przetwarzane.

12. Czynności tych należy dokonać przed przeprowadzeniem operacji przekazywania i aktualizować je przed ponownym podjęciem przekazywania po tym, jak zostało ono zawieszone: muszą Państwo wiedzieć, gdzie przekazane dane osobowe mogą się znajdować lub być przetwarzane przez podmioty odbierające (mapa miejsc przeznaczenia).

13. Należy pamiętać, że zdalny dostęp z państwa trzeciego (np. w sytuacji wsparcia) lub przechowywanie w chmurze zlokalizowanej poza EOG również uważa się za przekazywanie[27]. Innymi słowy, jeśli korzystają Państwo z międzynarodowej infrastruktury chmury, będą musieli Państwo ocenić, czy dane będą przekazywane do państw trzecich i do których, chyba że dostawca usług chmury wyraźnie stwierdzi w swojej umowie, że dane nie będą przetwarzane w państwach trzecich.

[23] Zob. art. 30 RODO, w szczególności ust. 1 lit. e) i ust. 2 lit. c). Ponadto prowadzone rejestry czynności przetwarzania powinny zawierać opis czynności przetwarzania, w tym m.in. kategorie osób, których dane dotyczą, kategorie danych i cele przetwarzania, a także konkretne informacje na temat operacji przetwarzania. Niektórzy administratorzy i niektóre podmioty przetwarzające są zwolnieni z obowiązku prowadzenia rejestrów czynności przetwarzania (art. 30 ust. 5 RODO). Dodatkowe informacje na temat powyższego zwolnienia można znaleźć w dokumencie Grupy Roboczej Artykułu 29 pt. „Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR" (dokument przedstawiający stanowisko w sprawie zwolnienia z obowiązku prowadzenia rejestru czynności przetwarzania na podstawie art. 30 ust. 5 RODO) (zatwierdzonym przez EROD dnia 25 maja 2018 r.).

[24] Zgodnie z zasadą przejrzystości na podstawie RODO należy poinformować osoby, których dane dotyczą, o przekazywaniu danych osobowych do państw trzecich (art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) RODO). Trzeba w szczególności powiadomić te osoby o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych. Informacje przekazane osobom, których dane dotyczą, muszą być prawidłowe i aktualne, zwłaszcza w świetle orzecznictwa Trybunału dotyczącego przekazywania.

[25] W przypadku, gdy administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.

[26] Art. 5 ust. 1 lit. c) RODO.

[27] Zob. Często zadawane pytanie nr 11: „należy pamiętać, że nawet udzielanie dostępu do danych z państwa trzeciego, np. w celach administracyjnych, również stanowi przekazanie danych", Często zadawane pytania EROD dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej wydanego w sprawie C- 311/18 – Data Protection Commissioner przeciwko Facebook Ireland i Maximillianowi Schremsowi, z dnia 23 lipca 2020 r.

2.2 Krok 2: Określenie wykorzystywanych narzędzi przekazywania

14. Drugim koniecznym krokiem jest określenie, czy wykorzystywane narzędzia przekazywania, są wymienione i przewidziane w rozdziale V RODO.

Decyzje stwierdzające odpowiedni stopień ochrony

15. Komisja Europejska na podstawie **decyzji stwierdzającej odpowiedni stopień ochrony** dotyczącej niektórych lub wszystkich państw trzecich, do których przekazują Państwo dane, może uznać, że państwa takie zapewniają odpowiedni stopień ochrony danych osobowych[28].

16. Taka decyzja stwierdzająca odpowiedni stopień ochrony skutkuje tym, że możliwy jest przepływ danych osobowych z EOG do takiego państwa trzeciego bez konieczności zastosowania któregokolwiek z narzędzi przekazywania z art. 46 RODO.

17. Decyzja stwierdzająca odpowiedni stopień ochrony może odnosić się do całego państwa lub jego części. Decyzja taka może dotyczyć wszystkich operacji przekazywania danych do danego państwa lub ograniczać się do wybranych rodzajów przekazywania (np. w jednym sektorze)[29].

18. Komisja Europejska publikuje listę decyzji stwierdzających odpowiedni stopień ochrony na swojej stronie internetowej[30].

19. Jeśli przekazują Państwo dane osobowe do państw trzecich, regionów lub sektorów, których dotyczy decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony (w stosownym zakresie), **nie ma potrzeby podejmowania jakichkolwiek dalszych kroków wskazanych w niniejszych zaleceniach[31]**. Konieczne będzie jednak nadal monitorowanie, czy decyzje stwierdzające odpowiedni stopień ochrony nie zostały uchylone lub unieważnione[32].

20. Należy pamiętać, że decyzje stwierdzające odpowiedni stopień ochrony nie uniemożliwiają osobom, których dane dotyczą, składania skarg. Nie stanowią one również przeszkody dla organów nadzorczych dla wniesienia sprawy do sądu krajowego w przypadku wątpliwości dotyczących ważności decyzji stwierdzającej odpowiedni stopień ochrony, żeby sąd krajowy mógł skierować odesłanie prejudycjalne mające doprowadzić do przeanalizowania tej ważności[33].

---

[28] Komisja Europejska władna jest określać na podstawie art. 45 RODO, czy dane państwo spoza UE zapewnia odpowiedni stopień ochrony danych. Komisja Europejska posiada również prawo do określenia, czy organizacja międzynarodowa zapewnia odpowiedni stopień ochrony.

[29] Art. 45 ust. 1 RODO.

[30] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[31] Pod warunkiem, że zarówno Państwo, jak i podmiot odbierający dane wdrożyliście środki mające na celu przestrzeganie innych zobowiązań na podstawie RODO; w przeciwnym wypadku takie środki należy wdrożyć.

[32] Komisja Europejska musi dokonywać okresowych przeglądów wszystkich decyzji stwierdzających odpowiedni stopień ochrony i monitorować, czy państwa trzecie, których takie decyzje dotyczą, nadal zapewniają odpowiedni stopień ochrony (zob. art. 45 ust. 3 i art. 45 ust. 4 RODO). Decyzje stwierdzające odpowiedni stopień ochrony mogą być także unieważnione przez TSUE (zob. wyroki w sprawach C-362/14 (Schrems I) i C-311/18 (Schrems II).

[33] C-311/18 (Schrems II), pkt 118 - 120. Organy nadzorcze nie mogą zignorować decyzji stwierdzającej odpowiedni stopień ochrony i zawiesić przekazywanie danych do takiego państwa lub zakazać go, powołując się wyłącznie na nieodpowiedni stopień ochrony. Mogą jedynie skorzystać ze swoich uprawnień do zawieszenia lub zakazania przekazywania danych osobowych do takiego państwa trzeciego na innej podstawie (np. niewystarczające środki bezpieczeństwa z naruszeniem art. 32 RODO czy też brak ważnej podstawy prawnej, na której bazuje przetwarzanie danych, z naruszeniem art. 6 RODO). Organy nadzorcze mogą zbadać w sposób całkowicie niezależny, czy przekazywanie tych danych spełnia wymogi ustanowione w RODO oraz, w odpowiednim

Przykład: Obywatel UE, Pan Schrems, w czerwcu 2013 r. wniósł do Irish Data Protection Commission (irlandzkiego komisarza ds. ochrony danych) skargę, w której zwrócił się o zawieszenie i zakazanie spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych; w tej skardze podniósł on, że prawo i praktyka obowiązujące w tym państwie nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi przez władze publiczne. Data Protection Commission odrzucił tę skargę w szczególności na tej podstawie, że w decyzji 2000/520 Komisja Europejska uznała, że w ramach programu „bezpiecznej przystani" Stany Zjednoczone zapewniają odpowiedni stopień ochrony przekazywanych danych osobowych. Pan Schrems zaskarżył decyzję Data Protection Commission i High Court (wysoki trybunał, Irlandia) zwrócił się do Trybunał Sprawiedliwości Unii Europejskiej (TSUE) z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie ważności decyzji 2000/520. Następnie TSUE unieważnił decyzję 2000/520 Komisji w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani[34].

Narzędzia przekazywania z art. 46 RODO

21. Art. 46 RODO wymienia szereg narzędzi przekazywania, cechujących się „odpowiednimi zabezpieczeniami", które podmioty przekazujące mogą wykorzystać dla celów przekazywania danych osobowych do państw trzecich w przypadku braku decyzji stwierdzających odpowiedni stopień ochrony. Główne rodzaje narzędzi przekazywania wymienione w art. 46 RODO są następujące:

- standardowe klauzule ochrony danych (SCC);
- wiążące reguły korporacyjne (WRK).
- kodeksy postępowania;
- mechanizmy certyfikacji;
- klauzule umowne *ad hoc*.

22. Niezależnie od wybranego narzędzia przekazywania wskazanego w art. 46 RODO, należy zapewnić, że zasadniczo przekazywane dane osobowe będą objęte merytorycznie równoważnym stopniem ochrony.

23. Narzędzia przekazywania wskazane w art. 46 RODO obejmują przede wszystkim odpowiednie zabezpieczenia o charakterze umownym, które mogą być stosowane w przypadku przekazywania danych do wszystkich państw trzecich. Sytuacja panująca w państwie trzecim, do którego dane są przekazywane, może jednak wymagać uzupełnienia tych narzędzi przekazywania i zawartych w nich zabezpieczeń dodatkowymi środkami („środkami uzupełniającymi") w celu zapewnienia merytorycznie równoważnego stopnia ochrony[35].

przypadku, mają możliwość wniesienia do sądów krajowych skargi mającej na celu skierowanie przez te sądy, jeśli podzielą one wątpliwości tego organu co do ważności tej decyzji Komisji stwierdzającej odpowiedni stopień ochrony, odesłania prejudycjalnego mającego doprowadzić do przeanalizowania tej ważności przez Trybunał Sprawiedliwości Unii Europejskiej.

[34] Sprawa C-362/14 (Schrems I).

[35] C-311/18 (Schrems II), pkt 130 i 133. Zob. również pkt 2.3 poniżej.

Wyjątki

24. W dodatku do decyzji stwierdzających odpowiedni stopień ochrony i narzędzi przekazywania z art. 46 RODO rozporządzenie przewiduje trzecią drogę dopuszczającą przekazywanie danych osobowych w określonych przypadkach. Z zastrzeżeniem podanych warunków możliwe będzie przekazanie danych osobowych na podstawie wyjątku wskazanego w art. 49 RODO.

25. Art. 49 GDPR ma wyjątkowy charakter. Zawarte w nim wyjątki muszą być interpretowane w sposób zawężający i odnosić się głównie do czynności przetwarzania, które są sporadyczne i niepowtarzające się. EROD wydała Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679. [36]

26. Przed skorzystaniem z któregokolwiek wyjątku przewidzianego w art. 49 RODO należy sprawdzić, czy przekazanie spełnia rygorystyczne wymogi, jakie zostały określone dla każdego z tych wyjątków.

***

27. Jeśli przekazanie danych nie może być w sposób zgodny z prawem oparte na decyzji stwierdzającej odpowiedni stopień ochrony ani na wyjątku z art. 49, należy przejść do Kroku 3.

2.3 Krok 3: Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania

28. Wykorzystanie narzędzia przekazywania z art. 46 RODO może okazać się niewystarczające. Takie narzędzie przekazywania musi bowiem zapewnić, że w wyniku przekazania nie dojdzie do uszczuplenia stopnia ochrony gwarantowanego na podstawie RODO[37]. Innymi słowy, narzędzie przekazywania musi być skuteczne w praktyce.

29. „Skuteczne" oznacza, że przekazane dane osobowe będą w państwie trzecim chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w EOG[38]. Nie będzie mieć to miejsca, jeśli podmiot odbierający dane nie jest w stanie wywiązać się ze swoich zobowiązań wynikających z wybranego narzędzia przekazywania z art. 46 RODO ze względu na obowiązujące w państwie trzecim przepisy lub praktyki dotyczące przekazywania.

30. Należy zatem ocenić, w stosownych przypadkach we współpracy z podmiotem odbierającym, czy w prawie lub praktyce państwa trzeciego funkcjonuje cokolwiek, co w kontekście danej operacji przekazywania mogłoby negatywnie wpłynąć na skuteczność odpowiednich zabezpieczeń wykorzystywanych narzędzi przekazywania z art. 46 RODO. W stosownych przypadkach podmiot odbierający dane powinien przekazać właściwe źródła i informacje dotyczące państwa trzeciego, w którym prowadzi działalność gospodarczą, i przepisów mających zastosowanie do przekazywania. Można także odwołać się do innych źródeł informacji, wymienionych na zasadzie przykładu w załączniku 3[39].

[36] Dodatkowe informacje w tym zakresie znaleźć można pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.
[37] Art. 44 RODO.
[38] C-311/18 (Schrems II), pkt 105 i drugie ustalenie.
[39] Zob. również pkt 43 poniżej.

31. Przeprowadzona ocena powinna uwzględnić wszystkie podmioty biorące udział w przekazaniu (np. administratorów, podmioty przetwarzające, podmioty podprzetwarzające w państwie trzecim), które zidentyfikowano w wyniku mapowania operacji przekazywania. Im więcej uczestniczących administratorów, podmiotów przetwarzających i podmiotów odbierających, tym bardziej złożona będzie ta ocena. Trzeba także wziąć pod uwagę dalsze przekazanie, jakie może mieć miejsce.

32. W tym celu należy zapoznać się z charakterystyką każdej przeprowadzanej operacji przekazywania i ustalić, w jaki sposób porządek prawny panujący w państwie, do którego dane są przekazywane (lub przekazywane dalej), stosuje się do takiego przekazywania.

33. Stosowny kontekst prawny będzie zależeć od okoliczności przekazywania, w szczególności od:

- celów, w jakich dane są przekazywane i przetwarzane (np. marketing, HR, przechowywanie, wsparcie informatyczne, badania kliniczne);
- rodzajów podmiotów zaangażowanych w przetwarzanie (prywatne czy publiczne; administrator czy podmiot przetwarzający);
- sektora, w którym przekazywanie ma miejsce (np. adtech, telekomunikacja, sektor finansowy itd.);
- kategorii przekazywanych danych osobowych (np. dane osobowe dotyczące dzieci mogą być objęte zakresem stosowania przepisów szczególnych w państwie trzecim);
- tego, czy dane będą przechowywane w państwie trzecim i czy do danych przechowywanych w UE/EOG możliwy będzie tylko dostęp zdalny;
- formatu danych, które będą przekazywane (tj. czy dane będą w formie zwykłego tekstu, spseudonimizowane lub zaszyfrowane[40]);
- możliwości dalszego przekazywania danych z jednego państwa trzeciego do innego państwa trzeciego[41].

34. Należy ocenić, czy którykolwiek z obowiązujących przepisów może negatywnie wpłynąć na zobowiązania zawarte w wybranym narzędziu przekazywania z art. 46 RODO. Konieczna będzie weryfikacja, czy zobowiązania, dzięki którym osoby, których dane dotyczą, mogą w praktyce skutecznie wykonać swoje prawa w kontekście międzynarodowego przekazania danych (takie jak wnioski u udostępnienie, sprostowanie lub usunięcie przekazywanych danych), nie są niwelowane przez przepisy w docelowym państwie trzecim.

35. Trzeba również ocenić stosowne przepisy o charakterze ogólnym w takim zakresie, w jakim wpływają one na skuteczne stosowanie zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO i na prawa podstawowe osób fizycznych (w szczególności prawo do środka zaskarżenia przyznane osobie, której dane dotyczą, w przypadku dostępu organów publicznych państwa trzeciego do przekazywanych danych).

36. W każdym przypadku należy zwrócić szczególną uwagę na odpowiednie przepisy, w tym przepisy określające wymogi udostępnienia danych osobowych organom publicznym lub przyznające takim organom publicznym prawo dostępu do danych osobowych (np. dla celów egzekwowania prawa karnego, nadzoru regulacyjnego i bezpieczeństwa narodowego). Jeżeli te wymogi lub uprawnienia są

[40] Niektóre państwa trzecie nie zezwalają na odbieranie zaszyfrowanych danych.
[41] W przypadku, gdy administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.

ograniczone do tego, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie[42], nie mogą one negatywnie wpływać na zobowiązania zawarte w wybranym narzędziu przekazywania z art. 46 RODO.

37. Normy UE, takie jak art. 47 i 52 Karty praw podstawowych Unii Europejskiej, należy stosować jako punkt odniesienia w celu oceny, czy taki dostęp przez organy publiczne jest ograniczony do tego, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie, oraz czy osobom, których dane dotyczą, zapewnia się skuteczne środki zaskarżenia.

38. Przy przeprowadzaniu tej oceny istotne mogą być również inne aspekty systemu prawa tego państwa trzeciego, np. czynniki wymienione w art. 45 ust. 2 RODO[43]. Przykładowo, sytuacja praworządności w państwie trzecim może mieć znaczenie dla oceny skuteczności zapewnionych osobom fizycznym mechanizmów zaskarżenia (do sądu) bezprawnego dostępu organów rządowych do danych osobowych. Istnienie kompleksowego prawa ochrony danych lub niezależnego urzędu ochrony danych, a także przestrzeganie międzynarodowych instrumentów przewidujących zabezpieczenia danych, może przyczynić się do zapewnienia proporcjonalności ingerencji rządu[44].

***

39. Zalecenia EROD w sprawie niezbędnych gwarancji europejskich wskazują elementy, które należy ocenić w celu ustalenia, czy ramy prawne państwa trzeciego dotyczące dostępu władz publicznych, tzn. krajowych służb bezpieczeństwa i organów ścigania, do danych osobowych, uznać można za uzasadnioną ingerencję (nie naruszającą zobowiązań podjętych w ramach narzędzi przekazywania z art. 46 RODO). W szczególności należy dokładnie rozważyć, czy przepisy dotyczące dostępu organów publicznych do danych są niejednoznaczne lub nie są publicznie dostępne.

40. W przypadku operacji przekazywania danych przy wykorzystaniu narzędzi przekazywania z art. 46 zalecenia EROD w sprawie niezbędnych gwarancji europejskich mogą dać wskazówki podmiotowi przekazującemu dane i podmiotowi odbierającemu dane na potrzeby oceny, czy takie uprawnienia w nieuzasadniony sposób ingerują w obowiązek podmiotu odbierającego dane do zapewnienia niezbędnej równoważności.

41. Brak merytorycznie równoważnego stopnia ochrony będzie szczególnie widoczny w przypadku, gdy przepisy lub praktyka państwa trzeciego znajdujące zastosowanie do danej operacji przetwarzania nie spełniają wymogów wynikających z niezbędnych gwarancji europejskich.

[42] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[43] C-311/18 (Schrems II), pkt 104.

[44] Dla przykładu: Konwencja Nr 108 Rady Europy (Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, ETS nr 108) lub Konwencja nr 108+ Rady Europy (Protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, CETS nr 223) zapewniają egzekwowalne, międzynarodowe środki zaskarżenia w przypadku naruszenia ochrony danych i przyczyniają się do zapewnienia minimalnego stopnia ochrony danych osobowych i poszanowania życia prywatnego.

42. Ocena musi być oparta przede wszystkim na publicznie dostępnych przepisach. Niekiedy może się to jednak okazać niewystarczające, ponieważ prawo państwa trzeciego może zawierać braki. W takiej sytuacji, jeśli nadal planują Państwo przekazanie danych, należy przyjrzeć się innym istotnym i obiektywnym czynnikom[45], a nie polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne uzyskają dostęp do danych w sposób niezgodny z normami UE. Ocenę tę należy przeprowadzić z należytą starannością i dokładnie ją udokumentować, jako że podmiot będzie rozliczany z decyzji, jaką może podjąć na tej podstawie[46].

43. Ocenę można uzupełnić informacjami uzyskanymi z innych źródeł[47], takimi jak:

- czynniki dowodzące na podstawie zgłoszonych precedensów, przepisów i praktyki, że organ państwa trzeciego będzie domagał się dostępu do danych za wiedzą podmiotu odbierającego dane lub bez niej;
- czynniki dowodzące na podstawie zgłoszonych precedensów, uprawnień oraz zasobów technicznych, finansowych i ludzkich, którymi dysponuje, że organ państwa trzeciego będzie mógł uzyskać dostęp do danych za pośrednictwem podmiotu odbierającego dane lub drogą bezpośredniego przechwycenia kanału komunikacji.

44. Przeprowadzona ocena może ostatecznie wykazać, że wykorzystywane narzędzie przekazywania z art. 46 RODO wraz z właściwymi mu odpowiednimi zabezpieczeniami:

- skutecznie zapewnia, że przekazane dane osobowe objęte są stopniem ochrony w państwie trzecim, który jest merytorycznie równoważny temu gwarantowanemu w EOG. Przepisy i praktyki państwa trzeciego znajdujące zastosowanie do danej operacji przekazywania umożliwiają podmiotowi odbierającemu realizację zobowiązań wynikających z wybranego narzędzia przekazywania. Ocenę należy przeprowadzić ponownie w stosownych odstępach czasu lub w razie, gdy wystąpią istotne zmiany (zob. krok 6).
- nie zapewnia w sposób skuteczny merytorycznie równoważnego stopnia ochrony. Podmiot odbierający dane nie może spełnić leżących na nim zobowiązań ze względu na przepisy lub praktyki państwa trzeciego znajdujące zastosowanie do danej operacji przekazywania. TSUE podkreślił, że w przypadku, gdy narzędzia przekazywania z art. 46 RODO okażą się niewystarczające, obowiązkiem podmiotu przekazującego dane jest wdrożenie skutecznych środków uzupełniających lub zaniechanie przekazania danych osobowych[48].

[45] Zob. pkt 43 poniżej, a także załącznik 3.
[46] Art. 5 ust. 2 RODO.
[47] Zob. także załącznik 3.
[48] C-311/18 (Schrems II), pkt 134-135.

TSUE orzekł na przykład, że art. 702 FISA nie zapewnia minimalnych wymogów wynikających z zasady proporcjonalności na podstawie prawa UE, w związku z czym nie można uznać, że jest ograniczony do tego, co jest ściśle niezbędne. Oznacza to, że stopień ochrony programów zatwierdzonych na podstawie art. 702 FISA nie jest merytorycznie równoważny zabezpieczeniom wymaganym na podstawie prawa UE. W konsekwencji jeśli podmiot odbierający dane lub jakikolwiek dalszy odbiorca, któremu podmiot odbierające dane może udostępnić dane, podlega art. 702 FISA[49], na potrzeby danej operacji przekazywania będzie można wykorzystać standardowe klauzule ochrony danych lub inne narzędzia przekazywania z art. 46 RODO pod warunkiem, że dodatkowe, uzupełniające środki techniczne sprawiają, że dostęp do przekazanych danych będzie niemożliwy lub nieskuteczny.

2.4 Krok 4: Przyjęcie środków uzupełniających

45. Jeśli ocena przeprowadzona w kroku 3 wykazała, że wybrane narzędzie przekazywania z art. 46 RODO nie jest skuteczne, konieczne będzie rozważenie, w stosownych przypadkach we współpracy z podmiotem odbierającym dane, czy dostępne są jakiekolwiek środki uzupełniające, które po dodaniu do zabezpieczeń zawartych już w narzędziach przekazywania mogłyby zapewnić, że przekazywane dane są objęte w państwie trzecim stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE[50]. „Środki uzupełniające" z definicji mają charakter uzupełniający w stosunku do zabezpieczeń zawartych już w narzędziach przekazywania z art. 46 RODO[51].

46. Należy określić w każdym konkretnym przypadku, które środki uzupełniające mogłyby okazać się skuteczne w odniesieniu do zestawu operacji przekazywania do danego państwa trzeciego przy wykorzystaniu konkretnego narzędzia przekazywania z art. 46 RODO. Można oprzeć się na wynikach poprzednich ocen (z kroków 1, 2 i 3 powyżej) w celu sprawdzenia potencjalnej skuteczności środków uzupełniających w zakresie zagwarantowania wymaganego stopnia ochrony.

47. Co do zasady środki uzupełniające mają charakter umowny, techniczny lub organizacyjny. Połączenie różnych środków w taki sposób, że będą się one wzajemnie wspierać i uzupełniać, może doprowadzić do zwiększenia stopnia ochrony i przyczynić się do osiągnięcia standardów unijnych.

48. Same środki umowne i organizacyjne nie będą w większości przypadków w stanie rozwiązać problemu dostępu organów publicznych państwa trzeciego do danych osobowych (w przypadku, gdy dostęp taki w nieuzasadniony sposób ingeruje w zobowiązanie podmiotu odbierającego dane do zapewnienia równoważności stopnia ochrony). W rzeczy samej pojawią się sytuacje, gdy jedynie środki techniczne będą mogły ograniczyć lub uniemożliwić dostęp organów publicznych państwa trzeciego do danych

[49] Art. 702 FISA znajduje zastosowanie, jeśli dane zostały uzyskane „od lub przy pomocy dostawcy usług łączności elektronicznej" (art. 702 FISA = 50 USC § 1881a, lit. h) pkt 2 ppkt A tiret (vi)), który z kolei zdefiniowany jest w 50 USC § 1881 lit. b) pkt 4) jako
„(A) operator telekomunikacyjny zgodnie z definicją w sekcji 153 tytułu 47;
(B) dostawca usług łączności elektronicznej zgodnie z definicją w sekcji 2510 tytułu 18;
(C) dostawca zdalnych usług obliczeniowych zgodnie z definicją w sekcji 2711 tytułu 18;
(D) każdy inny dostawca usług łączności, który ma dostęp do usług łączności przewodowej lub elektronicznej podczas przekazywania lub przechowywania takich informacji; lub
(E) członek kadry zarządzającej, pracownik lub przedstawiciel podmiotu, o którym mowa w podpunktach (A), (B), (C) lub (D)".

[50] C-311/18 (Schrems II), pkt 96.

[51] Motyw 109 RODO i C-311/18 (Schrems II), pkt 133.

osobowych, w szczególności dla celów nadzoru[52]. W takich przypadkach środki umowne lub organizacyjne mogą uzupełniać środki techniczne i wzmacniać ogólny stopień ochrony danych, np. tworząc przeszkody dla prób uzyskania przez organy publiczne dostępu do danych w sposób, który nie jest zgodny ze standardami UE.

49. W stosownych przypadkach we współpracy z podmiotem odbierającym dane można odwołać się do poniższej niewyczerpującej listy czynników, aby określić, które środki uzupełniające byłyby najbardziej skuteczne w ochronie przekazywanych danych:

- format danych, które będą przekazywane (tj. w formie zwykłego tekstu, spseudonimizowanego lub zaszyfrowanego);
- charakter danych;
- długość i złożoność procesu przetwarzania danych, liczba podmiotów uczestniczących w przetwarzaniu i relacje między nimi (np. czy przekazywanie obejmuje wielu administratorów i wiele podmiotów przetwarzających, czy też udział podmiotów przetwarzających, które będą przekazywać otrzymane dane do podmiotu odbierającego dane (uwzględniając stosowne przepisy znajdujące zastosowanie do nich na podstawie prawa państwa trzeciego przeznaczenia));[53]
- możliwość dalszego przekazywania danych w ramach danego państwa trzeciego lub nawet do innych państw trzecich (np. zaangażowanie podmiotów podprzetwarzających podmiotu odbierającego dane[54]).

Przykłady środków uzupełniających

50. Wybrane przykłady środków technicznych, umownych i organizacyjnych, które można rozważyć, podane zostały w niewyczerpującym wykazie zawartym w załączniku 2.

***

51. Jeśli wdrożono skuteczne środki uzupełniające, które w połączeniu z wybranym narzędzie przekazywania z art. 46 RODO, osiągają stopień ochrony merytorycznie równoważny temu zagwarantowanemu w EOG, operacja przekazywania może się odbyć.

[52] W przypadku gdy taki dostęp wykracza poza to, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie; zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[53] RODO nakłada na administratorów i podmioty przetwarzające różne obowiązki. Przekazywanie może mieć miejsce od administratora do administratora, pomiędzy współadministratorami, od administratora do podmiotu przetwarzającego oraz – pod warunkiem uzyskania zgody administratora – od podmiotu przetwarzającego do administratora i od podmiotu przetwarzającego do podmiotu przetwarzającego.

[54] Zob. przypis 25.

52. Jeśli jednak nie znaleziono lub nie wdrożono skutecznego środka uzupełniającego, który by zapewnił, że przekazywane dane osobowe cieszą się merytorycznie równoważnym stopniem ochrony[55], nie wolno rozpoczynać przekazywania danych osobowych do danego państwa trzeciego przy wykorzystaniu narzędzia przekazywania z art. 46 RODO. Jeśli operacja przekazywania już ma miejsce, należy zawiesić lub zakończyć przekazywanie danych osobowych[56] . Zgodnie z zabezpieczeniami zawartymi w wykorzystywanym narzędziu przekazywania z art. 46 RODO dane, które już zostały przekazane do takiego państwa trzeciego, oraz ich kopie powinny zostać zwrócone lub zniszczone w całości przez podmiot odbierający dane[57].

Przykład: prawo państwa trzeciego zakazuje określonych środków uzupełniających (np. szyfrowania) lub w inny sposób niweczy ich skuteczność. W takim wypadku nie można rozpocząć przekazywania danych osobowych lub należy wstrzymać dalsze przekazywanie do tego państwa.

53. Jeśli podjęta zostanie decyzja o kontynuowania przekazywania mimo tego, że podmiot odbierający nie jest w stanie wywiązać się z zobowiązań wynikających z narzędzia przekazywania z art. 46 RODO, należy powiadomić właściwy organ nadzorczy zgodnie ze szczegółowymi przepisami dotyczącymi danego narzędzia przekazywania z art. 46 RODO[58]. Właściwy organ nadzorczy zawiesi przekazywanie danych lub zakaże go, gdy uzna, że nie można zapewnić merytorycznie równoważnego stopnia ochrony[59].

54. Właściwy organ nadzorczy może zastosować wszelkie inne środki naprawcze (np. nałożyć grzywnę), gdy przekazywanie zostanie rozpoczęte lub będzie kontynuowane mimo tego, że nie można udowodnić merytorycznie równoważnego stopnia ochrony w państwie trzecim.

2.5 Krok 5: Podjęcie kroków proceduralnych w przypadku, gdy zidentyfikowano skuteczne środki uzupełniające

55. Proceduralne kroki, które być może będzie trzeba podjąć, gdy zidentyfikowano skuteczne środki uzupełniające do wdrożenia, mogą się różnić w zależności od wykorzystywanego lub planowanego do wykorzystania narzędzia przekazywania z art. 46 RODO.

2.5.1 Standardowe klauzule ochrony danych („SCC") (art. 46 ust. 2 lit. c) i d) RODO)

56. Jeśli zamierzają Państwo wprowadzić środki uzupełniające w dodatku do standardowych klauzul umownych, nie ma potrzeby składania wniosku do właściwego organu nadzorczego o pozwolenia na dodanie tego rodzaju klauzul lub dodatkowych zabezpieczeń, o ile określone środki uzupełniające nie są w bezpośredniej lub pośredniej sprzeczności ze standardowymi klauzulami umownymi i są

[55] W przypadku gdy taki dostęp wykracza poza to, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie; zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

[56] C-311/18 (Schrems II), pkt 135.

[57] Zob. klauzulę 12 w załączniku do decyzji Komisji 87/2010 w sprawie standardowych klauzul umownych; zob. (dobrowolną) dodatkową klauzulę o wypowiedzeniu w załączniku B do decyzji Komisji 2004/915/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych.

[58] Zob. Często zadawane pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej wydanego w sprawie C-311/18 – Data Protection Commissioner przeciwko Facebook Ireland i Maximillianowi Schremsowi, przyjęte dnia 23 lipca 2020 r., w szczególności pytanie nr 5, 6 i 9. Zob. klauzulę 4 lit. g) decyzji Komisji 2010/87/UE, jak również klauzulę 5 lit. a) decyzji Komisji 2001/497/WE i załącznik – Pakiet II klauzula II lit. c) decyzji Komisji 2004/915/WE.

[59] C-311/18 (Schrems II), pkt 113 i 121.

wystarczające, żeby zapewnić, iż stopień ochrony gwarantowany przez RODO nie ulegnie uszczupleniu[60]. Podmiot przekazujący i podmiot odbierający muszą zapewnić, że takie dodatkowe klauzule nie będą mogły być zinterpretowane w sposób ograniczający prawa i obowiązki wskazane w standardowych klauzulach umownych ani w żaden inny sposób obniżający stopień ochrony danych. Muszą być Państwo w stanie wykazać powyższe, w tym jednoznaczność wszystkich klauzul, zgodnie z zasadą rozliczalności i obowiązkiem zapewnienia wystarczającego stopnia ochrony. Właściwy organ nadzorczy ma w razie potrzeby prawo do przeglądu tych uzupełniających klauzul (np. w przypadku skargi lub dochodzenia wszczętego z własnej inicjatywy).

57. W przypadku gdy zamierzają Państwo zmienić same standardowe klauzule ochrony danych lub jeżeli dodane środki uzupełniające pozostają w bezpośredniej lub pośredniej sprzeczności ze standardowymi klauzulami umownymi, uznaje się, że nie opierają się już Państwo na standardowych klauzulach umownych[61], w związku z czym należy wystąpić o zezwolenie właściwego organu nadzorczego zgodnie z art. 46 ust. 3 lit. a) RODO.

2.5.2 Wiążące reguły korporacyjne (art. 46 ust. 2 lit. b) RODO)

58. Tok rozumowania wskazany w wyroku w sprawie Schrems II stosuje się również do innych narzędzi przekazywania z art. 46 ust. 2 RODO, jako że wszystkie te narzędzia mają charakter zasadniczo umowny, w związku z czym gwarancje przewidziane i zobowiązania przyjęte przez ich strony nie mogą być wiążące dla organów publicznych państwa trzeciego[62].

59. Wyrok w sprawie Schrems II znajduje zastosowanie do przekazywania danych osobowych na podstawie wiążących reguł korporacyjnych, ponieważ przepisy państwa trzeciego mogą mieć wpływ na ochronę zapewnianą przez takie narzędzia. Nadal trwają dyskusję dotyczące dokładnego wpływu wyroku w sprawie Schrems II na wiążące reguły korporacyjne. EROD w najkrótszym możliwym terminie przekaże bardziej szczegółowe informacje na temat tego, czy konieczne może być uwzględnienie w wiążących regułach korporacyjnych dodatkowych zobowiązań zgodnie z listami referencyjnymi WP256/257.[63]

---

[60] Motyw 109 RODO stanowi: „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". Podobne postanowienia zawarte są w standardowych klauzulach umownych przyjętych przez Komisję Europejską na mocy dyrektywy 95/45/WE.

[61] Zob. analogicznie przyjętą już Opinię 17/2020 EROD w sprawie projektu standardowych klauzul umownych przedłożonego przez organ nadzorczy Słowenii (art. 28 ust. 8 RODO), która zawiera podobne postanowienie („Ponadto Rada przypomina, że możliwość stosowania standardowych klauzul umownych przyjętych przez organ nadzorczy nie uniemożliwia stronom dodawania innych klauzul lub dodatkowych gwarancji, pod warunkiem że nie są one sprzeczne, bezpośrednio lub pośrednio z przyjętymi standardowymi klauzulami umownymi, ani nie naruszają podstawowych praw i wolności osób, których dane dotyczą. Dodatkowo, w przypadku zmiany standardowych klauzul ochrony danych, strony nie będą dłużej uznawane za podmioty, które wdrożyły standardowe klauzule umowne"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pd .

[62] CJEU, C-311/18 (Schrems II), pkt 132.

[63] Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, ostatnio zmieniony i przyjęty w dniu 6 lutego 2018

60. Trybunał podkreślił, że obowiązkiem podmiotu przekazującego dane i podmiotu odbierającego dane jest dokonanie oceny, czy poziom ochrony wymagany prawem Unii jest przestrzegany w danym państwie trzecim, co pozwoli ustalić, czy gwarancje przewidziane w standardowych klauzulach umownych lub wiążących regułach korporacyjnych mogą być przestrzegane w praktyce. Jeżeli tak nie jest, należy ocenić, czy możliwe jest zastosowanie dodatkowych środków w celu zapewnienia merytorycznie równoważnego stopnia ochrony do tego przewidzianego w EOG, jak również, czy prawo lub praktyka państwa trzeciego nie wpłynie niekorzystnie na takie dodatkowe środki w taki sposób, że pozbawi je skuteczności.

2.5.3 Klauzule umowne *ad hoc* (art. 46 ust. 3 lit. a) RODO)

61. Tok rozumowania wskazany w wyroku w sprawie Schrems II stosuje się również do innych narzędzi przekazywania z art. 46 ust. 2 RODO, jako że wszystkie te narzędzia mają charakter zasadniczo umowny, w związku z czym gwarancje przewidziane i zobowiązania przyjęte przez ich strony nie mogą być wiążące dla organów publicznych państwa trzeciego[64]. Wyrok w sprawie Schrems II znajduje zatem zastosowanie do przekazywania danych osobowych na podstawie klauzul umownych *ad hoc*, ponieważ przepisy państwa trzeciego mogą mieć wpływ na ochronę zapewnianą przez takie narzędzia. Nadal trwają dyskusję dotyczące dokładnego wpływu wyroku w sprawie Schrems II na klauzule umowne *ad hoc*. EROD w najkrótszym możliwym terminie przekaże bardziej szczegółowe informacje na ten temat.

2.6 Krok 6: Ponowna ocena w odpowiednich odstępach czasu

62. Należy na bieżąco monitorować, w stosownych przypadkach we współpracy z podmiotami odbierającymi dane, zmiany w państwie trzecim, do którego dane osobowe są przekazywane, jakie mogą mieć wpływ na dokonaną uprzednio ocenę stopnia ochrony i na decyzje, które podjęto na jej podstawie w związku z przekazywaniem. Rozliczalność jest obowiązkiem o charakterze ciągłym (art. 5 ust. 2 RODO).

63. Zaleca się wdrożenie dostatecznie solidnych mechanizmów w celu zapewnienia, że przekazywanie można natychmiast zawiesić lub zakończyć, jeśli:

- podmiot odbierający naruszył zobowiązania, jakie podjął na podstawie narzędzia przekazywania z art. 46 RODO, lub nie jest w stanie spełnić tych zobowiązań; lub
- środki uzupełniający utraciły swoją skuteczność w takim państwie trzecim.

r., WP 256 rev.01; Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, ostatnio zmieniony i przyjęty w dniu 6 lutego 2018 r., WP 257 rev.01.

[64] CJEU, C-311/18 (Schrems II), pkt 132.

3 WNIOSKI

64. RODO ustanawia zasady dotyczące przetwarzania danych osobowych w EOG, umożliwiając w ten sposób swobodny przepływ danych osobowych na terytorium EOG. Rozdział V RODO reguluje przekazywanie danych osobowych do państw trzecich i stawia wysoko poprzeczkę: przekazywanie nie może naruszać stopnia ochrony osób fizycznych zagwarantowanego w RODO (art. 44 RODO). Wyrok TSUE w sprawie C-311/18 (Schrems II) podkreśla potrzebę zapewnienia ciągłości stopnia ochrony gwarantowanej na podstawie RODO w odniesieniu do danych osobowych przekazywanych do państwa trzeciego[65].

65. W celu zapewnienia merytorycznie równoważnego stopnia ochrony danych konieczne jest przede wszystkim dokładne rozpoznanie przeprowadzanych operacji przekazywania. Należy zweryfikować, czy przekazywane dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane i przetwarzane w państwie trzecim.

66. Trzeba również określić wykorzystywane narzędzie przekazywania. Jeśli nie jest ono objęte decyzją stwierdzającą odpowiedni stopień ochrony, należy sprawdzić w każdym konkretnym przypadku, czy prawo lub praktyka państwa trzeciego przeznaczenia nie narusza zabezpieczeń zawartych w narzędziu przekazywania z art. 46 RODO w kontekście przeprowadzanych operacji przekazywania. W przypadku gdy samo narzędzie przekazywania z art. 46 RODO nie zapewnia merytorycznie równoważnego stopnia ochrony przekazywanych danych osobowych, lukę tę wypełnić mogą środki uzupełniające.

67. Jeśli znalezienie lub wdrożenie środków uzupełniających, które zapewniałyby, że przekazywane dane osobowe objęte są merytorycznie równoważnym stopniem ochrony, nie jest możliwe, nie wolno rozpocząć operacji przekazywania danych osobowych do takiego państwa trzeciego przy wykorzystaniu wybranego narzędzia przekazywania. Jeśli operacja przekazywania już się rozpoczęła, są Państwo zobowiązani natychmiast zawiesić lub zakończyć przekazywanie danych osobowych.

68. Właściwy organ nadzorczy ma prawo do zawieszenia lub zakończenia przekazywania danych osobowych do państwa trzeciego, jeśli nie zapewniono ochrony przekazywanych danych, jaka wymagana jest na podstawie prawa UE, w szczególności art. 45 i 46 RODO oraz Karty praw podstawowych.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[65] C-311/18 (Schrems II), pkt 93.

ZAŁĄCZNIK 1: DEFINICJE

- „Państwo trzecie” oznacza każde państwo niebędące państwem członkowskim EOG.
- „EOG” oznacza Europejski Obszar Gospodarczy i obejmuje państwa członkowskie Unii Europejskiej, a także Islandię, Norwegię i Liechtenstein. RODO stosuje się do tych trzech ostatnich państw na mocy Porozumienia o EOG, w szczególności Załącznika XI i Protokołu 37 do tego porozumienia.
- „RODO” oznacza Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych).
- „Karta” oznacza Kartę praw podstawowych Unii Europejskiej, Dz.U. C 326 z 26.10.2012, s. 391–407.
- „TSUE” lub „Trybunał” oznacza Trybunał Sprawiedliwości Unii Europejskiej. Jest on organem sądowym Unii Europejskiej, który we współpracy z sądami i trybunałami państw członkowskich zapewnia jednolite stosowanie i jednolitą wykładnię prawa UE.
- „Podmiot przekazujący dane” oznacza administratora lub podmiot przetwarzający w EOG, który przekazuje dane osobowe administratorowi lub podmiotowi przetwarzającemu w państwie trzecim.
- „Podmiot odbierający dane” oznacza administratora lub podmiot przetwarzający w państwie trzecim, który otrzymuje dane osobowe przekazywane z EOG lub uzyskuje do nich dostęp.
- „Narzędzie przekazywania z art. 46” odnosi się do odpowiednich zabezpieczeń na podstawie art. 46 RODO, jakie podmioty przekazujące dane mają obowiązek zastosować przy przekazywaniu danych osobowych do państwa trzeciego w razie braku decyzji stwierdzającej odpowiedni stopień ochrony zgodnie z art. 45 ust. 3 RODO. Art. 46 ust. 2 i ust. 3 RODO zawierają listę narzędzi przekazywania z art. 46, z których administratorzy lub podmioty przetwarzające mogą korzystać.
- „SCC” oznacza standardowe klauzule ochrony danych (lub standardowe klauzule umowne) przyjęte przez Komisję Europejską dla potrzeb przekazywania danych między administratorami i podmiotami przetwarzającymi w EOG a administratorami i podmiotami przetwarzającymi spoza EOG. Standardowe klauzule umowne przyjęte przez Komisję Europejską stanowią narzędzie przekazywania na podstawie RODO, zgodnie z art. 46 ust. 2 lit. c) i art. 46 ust. 5 RODO.

ZAŁĄCZNIK 2: PRZYKŁADY ŚRODKÓW UZUPEŁNIAJĄCYCH

69. Poniżej wskazano przykładowe środki uzupełniające, jakie można uwzględnić, jeśli dojdą Państwo do Kroku 4 „Przyjęcie środków uzupełniających". Lista ta nie jest wyczerpująca. Wybór i wdrożenie jednego z lub kilku tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE. Należy wybrać te środki uzupełniające, które mogą skutecznie zagwarantować taki stopień ochrony w odniesieniu do przeprowadzanych operacji przekazywania.

70. Dany środek uzupełniający uznać można za skuteczny w rozumieniu wyroku TSUE w sprawie Schrems II, jeśli prowadzi on – i w zakresie, w jakim prowadzi on – do usunięcia konkretnych uchybień określonych w wyniku przeprowadzonej oceny sytuacji prawnej w państwie trzecim. Jeśli ostatecznie nie będzie możliwe zapewnienie merytorycznie równoważnego stopnia ochrony, przekazywanie danych nie może mieć miejsca.

71. Jako administrator lub podmiot przetwarzający mogą być Państwo już zobowiązani do wdrożenia niektórych środków opisanych w niniejszym załączniku, nawet jeśli podmiot odbierający, z którego usług Państwo korzystają, objęty jest decyzją stwierdzającą odpowiedni stopień ochrony, podobnie jak mogą być Państwo zobowiązani do ich wdrożenia podczas przetwarzania danych w ramach EOG[66].

Środki techniczne

72. W niniejszej sekcji wskazano w sposób niewyczerpujący przykładowe środki techniczne, które mogą uzupełniać zabezpieczenia zawarte w narzędziach przekazywania z art. 46 RODO w celu zapewnienia przestrzegania wymaganego przez prawo UE stopnia ochrony w kontekście przekazywania danych osobowych do państwa trzeciego. Środki te będą konieczne zwłaszcza wtedy, gdy przepisy państwa trzeciego nakładają na podmiot odbierający dane wymagania, które są sprzeczne z zabezpieczeniami zawartymi w narzędziach przekazywania z art. 46 RODO i które w szczególności mogą mieć negatywny wpływ na udzielone umownie gwarancje merytorycznie równoważnego stopnia ochrony przed dostępem organów władz publicznych tego państwa trzeciego do tych danych[67].

73. W celu osiągnięcia jeszcze większej jasności niniejsza sekcja najpierw określi środki techniczne, które mogą być potencjalnie skuteczne w pewnych okolicznościach/scenariuszach w zapewnianiu merytorycznie równoważnego stopnia ochrony. W następnej kolejności opisane zostaną okoliczności/scenariusze, dla których nie znaleziono żadnego środka technicznego zapewniającego taki stopień ochrony.

Scenariusze, dla których znaleziono *skuteczne* środki

74. Środki wymienione poniżej mają na celu zagwarantować, że dostęp organów publicznych państw trzecich do przekazywanych danych nie wpływa negatywnie na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO. Środki te znajdują zastosowanie nawet wtedy, gdy dostęp organów publicznych dokonany jest z poszanowaniem prawa państwa

[66] Art. 5 ust. 2 RODO, art. 32 RODO.
[67] C-311/18 (Schrems II), pkt 135.

podmiotu odbierającego, jeśli dostęp tego rodzaju wykracza poza to, co jest niezbędne i proporcjonalne w społeczeństwie demokratycznym[68]. Ich celem jest zapobieganie potencjalnym naruszeniom w zakresie dostępu poprzez uniemożliwienie organom określenia osób, których dane dotyczą, wywnioskowania informacji na ich temat, odnalezienia ich w innym kontekście lub powiązania przekazywanych danych z innymi zestawami danych będących w posiadaniu tych organów, a które mogą obejmować m.in. identyfikatory internetowe generowane przez urządzenia, aplikacje, narzędzia i protokoły, jakie osoby, których dane dotyczą, wykorzystują w innych kontekstach.

75. Organy publiczne państw trzecich mogą podejmować starania, żeby uzyskać dostęp do przekazywanych danych:

    a) w tranzycie poprzez dostęp do kanałów komunikacji wykorzystywanych do przekazywania danych do państwa otrzymującego. Dostęp ten może przyjąć formę bierną, kiedy treści komunikatu, czasem po przeprowadzeniu procesu selekcji, zostaną po prostu skopiowane. Dostęp może być jednak również bardziej czynny w takim znaczeniu, że organy publiczne przejmą proces łączności, nie tylko czytając komunikat, ale także manipulując lub zatajając jego części;

    b) przechowywanych przez zamierzonego odbiorcę poprzez uzyskanie dostępu do samych zakładów przetwarzania lub poprzez nałożenie na odbiorcę danych obowiązku zlokalizowania i ekstrakcji istotnych danych oraz przekazania ich do władz.

76. Niniejsza sekcja uwzględnia przypadki, gdy zastosowano środki skuteczne w obu tych scenariuszach. Różne środki uzupełniające mogą być wykorzystywane i wystarczające w okolicznościach danej operacji przetwarzania, jeśli przepisy państwa otrzymującego przewidują tylko jedną formę dostępu. Podmiot przekazujący dane musi zatem dokładnie przeanalizować, przy wsparciu podmiotu odbierającego dane, jakie obowiązki nałożono na podmiot odbierający dane.

Dla przykładu amerykańskie podmioty odbierające dane, o których mowa w 50 USC § 1881a (art. 702 FISA), mają bezpośredni obowiązek zapewnić dostęp do odebranych danych osobowych będących w ich posiadaniu, przechowywanych przez nich lub znajdujących się pod ich kontrolą oraz przekazać takie dane do władz. Może to dotyczyć również kluczy kryptograficznych służących do odszyfrowania danych.

77. Scenariusze opisują konkretne okoliczności i podjęte środki. Wszelkie zmiany do scenariuszy mogą doprowadzić do odmiennych wniosków.

78. Administratorzy być może będą musieli zastosować niektóre lub wszystkie opisane tutaj środki niezależnie od stopnia ochrony przewidzianego przez przepisy obowiązujące podmiot odbierający dane, ponieważ mają oni obowiązek spełnienia wymogów na nich nałożonych na podstawie art. 25 i 32 RODO w konkretnych okolicznościach, w jakich dochodzi do przekazywania. Innymi słowy, podmioty przekazujące mogą być zobowiązane do wdrożenia środków opisanych w tym dokumencie, nawet jeśli podmiot odbierający, z którego usług korzystają, objęty jest decyzją stwierdzającą odpowiedni stopień ochrony, podobnie jak administratorzy i podmioty przetwarzające mogą być zobowiązani do ich wdrożenia podczas przetwarzania danych w ramach EOG.

[68] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD w sprawie niezbędnych gwarancji europejskich dla środków nadzoru.

Scenariusz nr 1: Przechowywanie danych w celach wykonania kopii zapasowej i w innych celach, które nie wymagają dostępu do niezakodowanych danych

79. Podmiot przekazujące dane korzysta z usług dostawcy usług hostingowych w państwie trzecim w celu przechowywania danych osobowych, np. na potrzeby kopii zapasowej.

Jeżeli

1. dane osobowe są przetwarzane przy wykorzystaniu mocnego szyfrowania przed wysyłaniem,
2. algorytm szyfrowania i jego parametryzacja (np. długość klucza, tryb działania, jeśli dotyczy) są zgodne z aktualnym stanem wiedzy i można je uznać za zaawansowaną ochronę przed analizą kryptograficzną przeprowadzaną przez organy publiczne w państwie otrzymującym, uwzględniając dostępne tym organom zasoby i środki techniczne (np. moc obliczeniową na potrzeby ataków brute-force),
3. siła szyfrowania uwzględnia okres, przez jaki należy zachować poufność zaszyfrowanych danych osobowych,
4. algorytm szyfrowania jest perfekcyjnie wdrażany przez odpowiednio aktualizowane programy, których zgodność ze specyfikacją wybranego algorytmu została potwierdzona, np. w formie certyfikacji,
5. klucze są odpowiednio zarządzane (generowane, przydzielane, przechowywane, w razie konieczności powiązane z tożsamością docelowego odbiorcy i blokowane), oraz
6. klucze są przechowywane wyłącznie pod kontrolą podmiotu przekazującego dane lub innych podmiotów, którym powierzono to zadanie, mających siedzibę w EOG lub państwie trzecim, na terytorium lub w określonym sektorze lub określonych sektorach w państwie trzecim, bądź organizacji międzynarodowej, w stosunku do których Komisja zgodnie z art. 45 RODO stwierdziła, że zapewniają odpowiedni stopień ochrony,

EROD uznaje, że przeprowadzone operacje szyfrowania stanowią skuteczny środek uzupełniający.

Scenariusz nr 2: Przekazywanie danych spseudonimizowanych

80. Podmiot przekazujący dane najpierw pseudonimizuje posiadane dane, a następnie przekazuje je do państwa trzeciego w celach analizy, np. na potrzeby badań.

Jeżeli

1. podmiot przekazujący dane przekazuje dane osobowe przetworzone w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, ani wykorzystać w celu odnalezienia osoby, której dane dotyczą, w ramach większej grupy, bez użycia dodatkowych informacji[69],
2. takie dodatkowe informacje znajdują się w wyłącznym posiadaniu podmiotu przekazującego dane i przechowywane są osobno w państwie członkowskim lub w państwie trzecim, terytorium, określonym sektorze lub określonych sektorach w państwie trzecim, bądź organizacji międzynarodowej, w stosunku do których Komisja zgodnie z art. 45 RODO stwierdziła, że zapewniają odpowiedni stopień ochrony,

[69] Zgodnie z art. 4 ust. 5 RODO: „Pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

3. ujawnienie lub nieupoważnione wykorzystanie takich dodatkowych informacji nie jest możliwe ze względu na odpowiednie zabezpieczenia techniczne i organizacyjne i zapewniono, że podmiot przekazujący dane zachowuje wyłączną kontrolę nad algorytmem lub archiwum umożliwiającymi ponowną identyfikację przy wykorzystaniu dodatkowych informacji, oraz
4. administrator, przeprowadziwszy dogłębną analizę określonych danych przy uwzględnieniu wszelkich informacji, jakie mogą znajdować się w posiadaniu organów publicznych państwa otrzymującego, ustalił, że nie można przypisać spseudonimizowanych danych osobowych zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, nawet po przeprowadzeniu porównania z takimi informacjami,

EROD uznaje, że przeprowadzona pseudonimizacja stanowi skuteczny środek uzupełniający.

81. Należy zwrócić uwagę, że w wielu przypadkach czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, jej lokalizację lub korzystanie z usług internetowych w określonym czasie[70] mogą umożliwić identyfikację takiej osoby, nawet jeśli pomięto jej nazwisko, adres czy inne zwykłe identyfikatory.

82. Odnosi się to przede wszystkim do przypadków, gdy dane dotyczą wykorzystania usług informacyjnych (data dostępu, kolejność użytych funkcji, charakterystyka użytego sprzętu itd.). Usługi te mogą równie dobrze podlegać, podobnie jak podmiot odbierający dane osobowe, obowiązkowi przyznania dostępu tym samym organom publicznym w ich jurysdykcji, które z dużym prawdopodobieństwem będą wtedy posiadać dane o wykorzystaniu tych usług informacyjnych przez osobę docelową.

83. Ponadto, zważywszy, że wykorzystanie niektórych usług informacyjnych ma charakter publiczny, i uwzględniając możliwość ich wykorzystania przez podmioty posiadające znaczne zasoby, administratorzy będą musieli zachować szczególną ostrożność, biorąc pod uwagę, że organy publiczne w ich jurysdykcji z dużym prawdopodobieństwem posiadają dane o wykorzystaniu usług informacyjnych przez osobę docelową.

Scenariusz nr 3: Zaszyfrowane dane jedynie przechodzą przez państwo trzecie

84. Podmiot przekazujący dane chce przekazać dane do państwa docelowego uznanego za gwarantujące odpowiednią ochronę zgodnie z art. 45 RODO. Dane przesyłane są przez państwo trzecie.

Jeżeli

1. podmiot przekazujący dane przekazuje dane osobowe do podmiotu odbierającego dane w jurysdykcji zapewniającej odpowiednią ochronę, a dane są przesyłane przez internet i mogą geograficznie przechodzić przez państwo trzecie, które nie zapewnia merytorycznie równoważnego stopnia ochrony,
2. zastosowano szyfrowanie transmisji i zapewniono, że protokoły szyfrowania są najnowocześniejsze i zapewniają skuteczną ochronę przeciwko aktywnym i pasywnym atakom za pomocą zasobów, o których wiadomo, że są dostępne dla organów publicznych państwa trzeciego,
3. odszyfrowanie możliwe jest tylko poza danym państwem trzecim,

[70] Art. 4 ust. 1 RODO: „Dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoba, której dane dotyczą); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

4. podmioty zaangażowane w proces komunikacji wspólnie wybiorą wiarygodny organ lub infrastrukturę certyfikacji klucza publicznego,
5. wykorzystano konkretne najnowocześniejsze środki ochronne przeciwko aktywnym i pasywnym atakom na zaszyfrowaną transmisję,
6. w przypadku gdy szyfrowanie transmisji samo przez się nie zapewnia odpowiedniego bezpieczeństwa ze względu na wcześniejsze przypadki podatności infrastruktury lub wykorzystanego oprogramowania, dane osobowe zaszyfrowano na całej drodze przesyłu danych na warstwie aplikacji dzięki zastosowaniu najnowocześniejszych metod szyfrowania,
7. algorytm szyfrowania i jego parametryzacja (np. długość klucza, tryb działania, jeśli dotyczy) są zgodne z aktualnym stanem wiedzy i można je uznać za zaawansowaną ochronę przed analizą kryptograficzną przeprowadzoną przez organy publiczne w państwie tranzytu, uwzględniając dostępne tym organom zasoby i środki techniczne (np. moc obliczeniową na potrzeby ataków brute-force),
8. siła szyfrowania uwzględnia okres, przez jaki należy zachować poufność zaszyfrowanych danych osobowych,
9. algorytm szyfrowania jest perfekcyjnie wdrażany przez odpowiednio aktualizowane programy, których zgodność ze specyfikacją wybranego algorytmu została potwierdzona, np. w formie certyfikacji,
10. wykluczono istnienie luk (backdoor) w oprogramowaniu i sprzęcie,
11. klucze są odpowiednio zarządzane (generowane, przydzielane, przechowywane, w razie konieczności powiązane z tożsamością docelowego odbiorcy i blokowane), przez podmiot przekazujący lub inny zaufany podmiot podmiotu przekazującego działający w jurysdykcji oferującej merytorycznie równoważny stopień ochrony,

EROD uznaje, że szyfrowanie transmisji, w razie konieczności w połączeniu z szyfrowaniem na całej drodze przesyłu danych, stanowi skuteczny środek uzupełniający.

Scenariusz nr 4: Chroniony odbiorca

85. Podmiot przekazujący dane przekazuje dane osobowe do podmiotu odbierającego dane w państwie trzecim, podlegającego szczególnej ochronie na podstawie przepisów tego państwa, np. w celu wspólnego świadczenia usług medycznych dla pacjenta lub usług prawnych dla klienta.

Jeżeli

1. przepisy państwa trzeciego zwalniają będący rezydentem podmiot odbierający z potencjalnego naruszenia dostępu do danych posiadanych przez tego odbiorcę we wskazanym celu, np. na podstawie obowiązku zachowania tajemnicy zawodowej, który stosuje się do podmiotu odbierającego dane,
2. takie zwolnienie dotyczy wszystkich informacji posiadanych przez podmiot odbierający dane, które mogą być wykorzystane w celu obejścia ochrony informacji uprzywilejowanych (klucze kryptograficzne, hasła, inne dane uwierzytelniające itp.),
3. podmiot odbierający dane nie korzysta z usług podmiotu przetwarzającego w takim zakresie, który umożliwiłby organom publicznym uzyskanie dostępu do danych, kiedy znajdują się one w posiadaniu podmiotu przekazującego, ani podmiot odbierający dane nie przekazuje danych innemu podmiotowi, który nie podlega ochronie na podstawie narzędzi przekazywania z art. 46 RODO,

4. dane osobowe zostały przed wysyłką zaszyfrowane metodą zgodną z najnowocześniejszymi rozwiązaniami i gwarantującą, że odszyfrowanie nie będzie możliwe bez znajomości klucza do deszyfrowania (szyfrowanie na całej drodze przesyłu danych) przez cały okres, kiedy dane muszą być chronione,
5. klucz do deszyfrowania jest na wyłącznym przechowaniu chronionego podmiotu odbierającego dane i jest należycie zabezpieczony środkami technicznymi i organizacyjnymi zgodnymi z najnowocześniejszymi rozwiązaniami przed nieupoważnionym wykorzystaniem lub ujawnieniem, oraz
6. podmiot przekazujący dane w sposób wiarygodny ustalił, że klucz do szyfrowania, z którego zamierza skorzystać, odpowiada kluczowi do deszyfrowania znajdującemu się w posiadaniu odbiorcy,

EROD uznaje, że wykonane szyfrowanie transmisji stanowi skuteczny środek uzupełniający.

Scenariusz nr 5: Przetwarzanie dzielone lub przetwarzanie przez wiele podmiotów

86. Podmiot przekazujący dane chce, żeby dane były przetwarzane łącznie przez co najmniej dwa niezależne podmioty przetwarzające mające siedziby w dwóch różnych jurysdykcjach, bez jednoczesnego ujawnienia im treści danych. Przed transmisją dzieli dane w taki sposób, że żadna z części otrzymanych przez podmioty przetwarzające nie wystarcza do odtworzenia danych osobowych w części lub całości. Podmiot przekazujący dane otrzymuje wyniki przetwarzania w sposób niezależny od każdego z podmiotów przetwarzających i łączy otrzymane części, tworząc w ten sposób końcowy rezultat, który może stanowić dane osobowe lub dane zagregowane.

Jeżeli

1. podmiot przekazujący dane przetwarza dane osobowe w taki sposób, że dzieli je na dwie lub więcej części, które nie mogą zostać zinterpretowane lub przypisane do konkretnej osoby, której dane dotyczą, bez wykorzystania dodatkowych informacji,
2. każda z części przekazana zostaje do innych podmiotów przetwarzających, które mają siedziby w różnych jurysdykcjach,
3. podmioty przetwarzające mogą przetwarzać dane wspólnie, np. w przy wykorzystaniu obliczeń wielopodmiotowych, w taki sposób, że żadne informacje nie zostają ujawnione któremukolwiek z tych podmiotów, za wyjątkiem tych informacji, które podmioty te posiadały przed obliczeniem,
4. algorytm wykorzystywany na potrzeby wspólnych obliczeń jest zabezpieczony przed aktywnymi agresorami,
5. nie ma dowodów na współpracę między organami publicznymi zlokalizowanymi w odpowiednich jurysdykcjach, w których siedziby mają podmioty przetwarzające, co dałoby im dostęp do wszystkich zestawów danych osobowych znajdujących się w posiadaniu podmiotów przetwarzających i pozwoliłoby im na odtworzenie i wykorzystanie treści danych osobowych w czystej postaci w przypadku, gdy takie wykorzystanie naruszyłoby istotę podstawowych praw i wolności osób, których dane dotyczą. Podobnie organy publiczne któregokolwiek z państw nie powinny mieć prawa dostępu do danych osobowych znajdujących się w posiadaniu podmiotów przetwarzających we wszystkich właściwych jurysdykcjach.
6. administrator, przeprowadziwszy dogłębną analizę określonych danych przy uwzględnieniu wszelkich informacji, jakie mogą znajdować się w posiadaniu organów publicznych państw otrzymujących, ustalił, że nie można przypisać żadnej części danych osobowych, jakie przekazywane są przez niego podmiotom przetwarzającym, zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, nawet po przeprowadzeniu porównania z takimi informacjami,

EROD uznaje, że przetwarzanie dzielone stanowi skuteczny środek uzupełniający.

Scenariusze, w których nie znaleziono *skutecznego* środka

87. Środki opisane poniżej w określonych okolicznościach nie zapewniałyby w skuteczny sposób merytorycznie równoważnego stopnia ochrony danych przekazywanych do państwa trzeciego. Z tego względu nie można by ich uznać za środki uzupełniające.

Scenariusz nr 6: Przekazanie do dostawców usług chmury obliczeniowej lub innych podmiotów przetwarzających, wymagające dostępu do niezakodowanych danych

88. Podmiot przekazujący dane korzysta z usług dostawcy chmury obliczeniowej lub innych podmiotów przetwarzających w celu przetworzenia danych osobowych w państwie trzecim zgodnie z otrzymanymi instrukcjami.

Jeżeli

1. administrator przekazuje dane do dostawcy chmury obliczeniowej lub innego podmiotu przetwarzającego,
2. dostawca usług chmury lub inny podmiot przetwarzający potrzebuje dostępu do niezakodowanych danych na potrzeby realizacji powierzonego zadania, oraz
3. uprawnienia przyznane organom publicznym państwa otrzymującego w zakresie dostępu do przekazywanych danych wykraczają poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie[71],

EROD, uwzględniając obecny stan wiedzy, nie jest w stanie przewidzieć skutecznego środka technicznego, dzięki któremu taki dostęp nie naruszałby praw osób, których dane dotyczą. EROD nie wyklucza, że dalszy rozwój technologiczny może zapewnić środki, które osiągną zamierzony cel biznesowy, i nie będą wymagać dostępu do niezakodowanych danych.

89. W takim scenariuszu, gdy niezaszyfrowane dane osobowe są technicznie konieczne podmiotowi przetwarzającemu do świadczenia usług, szyfrowanie transmisji i szyfrowanie danych w spoczynku, nawet zastosowane jednocześnie, nie stanowią środka uzupełniającego, który zapewniałby merytorycznie równoważny stopień ochrony, jeśli podmiot odbierający dane jest w posiadaniu kluczy kryptograficznych.

Scenariusz nr 7: Dostęp zdalny do danych w celach biznesowych

90. Podmiot przekazujący dane udostępnia dane osobowe podmiotom w państwie trzecim na potrzeby realizacji wspólnych celów biznesowych. Typowy układ może obejmować mających siedzibę w państwie członkowskim administratora lub podmiot przetwarzający, które przekazują dane osobowe administratorowi lub podmiotowi przetwarzającemu w państwie trzecim, w ramach tej samej grupy przedsiębiorstw, lub grupę przedsiębiorstw prowadzących wspólną działalność gospodarczą. Podmiot odbierający dane może przykładowo wykorzystać dane, jakie otrzyma, żeby świadczyć na rzecz

[71] Zob. art. 47 i 52 Karty praw podstawowych Unii Europejskiej, art. 23 ust. 1 RODO i zalecenia EROD w sprawie niezbędnych gwarancji europejskich dla środków nadzoru.

podmiotu przekazującego dane profesjonalne usługi kadrowe, do których potrzebuje danych dotyczących zasobów ludzkich, albo żeby prowadzić komunikację telefoniczną lub e-mailową z klientami podmiotu przekazującego dane, którzy mieszkają w Unii Europejskiej.

Jeżeli

1. podmiot przekazujący dane przekazuje dane podmiotowi odbierającemu dane w państwie trzecim, udostępniając je w powszechnie wykorzystywanym systemie informacyjnym w sposób, dzięki któremu podmiot odbierający będzie mógł uzyskać bezpośredni dostęp do danych wedle jego wyboru, albo przekazując je bezpośrednio pojedynczo lub masowo przy wykorzystaniu usług łączności,
2. podmiot odbierający wykorzystuje niezakodowane dane na własne potrzeby,
3. uprawnienia przyznane organom publicznym państwa otrzymującego w zakresie dostępu do przekazywanych danych wykraczają poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie,

EROD nie jest w stanie przewidzieć skutecznego środka technicznego, dzięki któremu taki dostęp nie naruszałby praw osób, których dane dotyczą.

91. W takim scenariuszu, gdy niezaszyfrowane dane osobowe są technicznie konieczne podmiotowi przetwarzającemu do świadczenia usług, szyfrowanie transmisji i szyfrowanie danych w spoczynku, nawet zastosowane jednocześnie, nie stanowią środka uzupełniającego, który zapewniałby merytorycznie równoważny stopień ochrony, jeśli podmiot odbierający dane jest w posiadaniu kluczy kryptograficznych.

Dodatkowe środki umowne

92. Środki te zasadniczo obejmują zobowiązania umowne[72] o charakterze jednostronnym, dwustronnym lub wielostronnym[73]. W przypadku wykorzystania narzędzia przekazywania z art. 46 RODO narzędzie takie będzie w większości przypadków już obejmować pewne zobowiązania (przede wszystkim o charakterze umownym) podejmowane przez podmiot przekazujący dane i podmiot odbierający dany, pełniące funkcję zabezpieczeń danych osobowych[74].

93. W niektórych wypadkach środki te mogą uzupełniać i wzmacniać zabezpieczenia wynikające z narzędzia przekazywania i właściwych przepisów państwa trzeciego, gdy, uwzględniając okoliczności przekazywania, te narzędzia i przepisy nie spełniają wszystkich warunków wymaganych do zapewnienia stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. W świetle charakteru środków umownych, które zasadniczo nie są w stanie wiązać władz takiego państwa trzeciego, gdy nie są one stronami umowy[75], środki te należy połączyć z innymi środkami technicznymi i organizacyjnymi, żeby zapewnić wymagany stopień ochrony. Wybór i wdrożenie jednego z lub kilku

[72] Np. w ramach wiążących reguł korporacyjnych, które w każdym przypadku powinny regulować niektóre ze środków wskazanych poniżej.

[73] Będą mieć prywatny charakter i nie będą uważane za umowy międzynarodowe na podstawie prawa międzynarodowego publicznego. Nie będą w związku z tym wiązać organów publicznych państwa trzeciego, bowiem nie są one stronami tej umowy zawartej między prywatnymi podmiotami w państwach trzecich, jak Trybunał podkreślił w swoim wyroku w sprawie C-311/18 (Schrems II), pkt 125.

[74] Zob. wyrok w sprawie C-311/18 (Schrems II), pkt 137 w którym Trybunał uznał, że SCC przewidują „skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony i czy odbywające się na podstawie takich klauzul przekazywanie danych osobowych zostanie w przypadku ich naruszenia lub niemożności ich przestrzegania zawieszone lub zakazane", zob. także pkt 148).

[75] C-311/18 (Schrems II), pkt 125.

tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE.

94. W zależności od tego, jakie środki umowne zawarte są już w wykorzystywanym narzędziu przekazywania z art. 46 RODO, pomocne mogą okazać się również dodatkowe środki umowne, dzięki którym posiadające siedzibę w EOG podmioty przekazujące dane dowiedzą się o nowych rozwiązaniach mających wpływ na ochronę danych przekazywanych do państw trzecich.

95. Jak wskazano powyżej, środki umowne nie będą w stanie wyłączyć stosowania przepisów państwa trzeciego niespełniających standardów niezbędnych gwarancji europejskich EROD w przypadku, gdy przepisy te nakładają na podmioty odbierające dane obowiązek stosowania się do nakazów od organów publicznych[76].

96. Poniżej znaleźć można przykładowe potencjalne środki umowne, pogrupowane zgodnie z ich charakterem:

Nałożenie obowiązku umownego do stosowania określonych środków technicznych

97. ***W zależności od konkretnych okoliczności danej operacji przekazywania umowa może przewidywać, że na potrzeby przekazywania należy wprowadzić określone środki techniczne (patrz powyżej proponowane środki techniczne).***

98. ***Warunki skuteczności:***

- Klauzula ta może być skuteczna w sytuacji, gdy podmiot przekazujący stwierdził potrzebę zastosowania środków technicznych. Należy nadać jej formę prawną, żeby zapewnić, iż podmiot odbierający również zobowiąże się do wprowadzenia koniecznych środków technicznych.

Obowiązki w zakresie przejrzystości:

99. ***Podmiot przekazujący może uzupełnić umowę załącznikami zawierającymi informacje przekazane przez podmiot odbierający wedle jego najlepszych starań dotyczące dostępu do danych przez organy publiczne, w tym w dziedzinie wywiadu, pod warunkiem że przepisy w państwie docelowym są zgodne z niezbędnymi gwarancjami europejskimi EROD. Może to pomóc podmiotowi przekazującemu dane wywiązać się ze swojego obowiązku udokumentowania oceny stopnia ochrony w państwie trzecim.***

100. Przykładowo, podmiot odbierający może być zobowiązany do:

(1) określenia przepisów i regulacji w państwie docelowym, znajdujących zastosowanie do podmiotu odbierającego lub jego (dalszych) podmiotów przetwarzających, które dają prawo organom publicznym do dostępu do przekazywanych danych osobowych, w szczególności w dziedzinie wywiadu, egzekwowania prawa oraz nadzoru administracyjnego i regulacyjnego w odniesieniu do przekazywanych danych;

[76] Wyrok TSUE w sprawie C-311/18 (Schrems II), pkt 132.

(2) w braku przepisów regulujących dostęp organów publicznych do danych, podania informacji i danych statystycznych, w oparciu o doświadczenia podmiotu odbierającego lub raporty z różnych źródeł (np. od partnerów, z otwartych źródeł, krajowego orzecznictwa i decyzji krajowych wydanych przez organy nadzoru), dotyczących dostępu organów publicznych do danych osobowych w sytuacjach analogicznych do okoliczności danej operacji przekazywania danych (tj. w określonym obszarze regulacyjnym; w odniesieniu do rodzaju podmiotów, do których należy podmiot odbierający dane itd.);
(3) wskazania podjętych środków dla celu uniemożliwienia dostępu do przekazywanych danych (jeśli dotyczy);
(4) podania dostatecznie szczegółowych informacji o wszystkich otrzymanych przez podmiot odbierający w określonym czasie[77] żądaniach dostępu organów publicznych do danych osobowych, w szczególności w obszarach wymienionych w podpunkcie (1) powyżej, w tym informacji o otrzymanych żądaniach, żądanych danych, organie, który wysunął żądanie, podstawie prawnej ujawnienia i zakresie, w jakim podmiot odbierający ujawnił żądane dane[78];
(5) określenia, czy i w jakim zakresie podmiot odbierający ma prawny zakaz przekazania informacji wymienionych w podpunktach (1) – (5) powyżej.

101. Informację tę można przekazać w formie ustrukturyzowanych kwestionariuszy, które podmiot odbierający wypełni i podpisze, z zastrzeżeniem zobowiązania umownego podmiotu odbierającego do zadeklarowania w określonym terminie wszelkich możliwych zmian w odniesieniu do tych informacji, zgodnie z obowiązującą praktyką w zakresie procesów należytej staranności.

102. ***Warunki skuteczności:***

- Podmiot odbierający musi być w stanie przekazać, wedle swojej najlepszej wiedzy i dołożywszy należytej staranności w celu ich uzyskania, podmiotowi przekazującemu informacje tego rodzaju[79].
- Obowiązek ten nałożony na podmiot odbierający służy zapewnieniu, iż podmiot przekazujący będzie w każdym czasie wiedział o zagrożeniach, z jakimi wiąże się przekazywanie danych do państwa trzeciego. Pozwoli on zatem podmiotowi przekazującemu odstąpić od zawarcia umowy lub w przypadku zmian informacji po jej zawarciu spełnić obowiązek zawieszenia operacji przekazywania lub rozwiązania umowy, jeśli przepisy państwa trzeciego, zabezpieczenia zawarte w narzędziu przekazywania z art. 46 RODO i wszelkie dodatkowe zabezpieczenia, które zostały wdrożone, nie są już w stanie zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. Obowiązek ten nie może jednak uzasadnić ujawnienia danych osobowych przez podmiot odbierający ani dawać podstaw do oczekiwania, że nie będzie dalszych żądań dostępu.

***

[77] Długość okresu powinna zależeć od poziomu zagrożenia dla praw i wolności osób, których dane są przekazywane, np. ostatni rok przed zakończeniem używania narzędzia przekazywania danych przez podmiot przekazujący dane

[78] Wywiązanie się z tego obowiązku samo przez się nie oznacza zapewnienia odpowiedniego stopnia ochrony. Jednocześnie niewłaściwe ujawnienie, które miało miejsce, prowadzi do konieczności podjęcia środków uzupełniających.

[79] Zob. pkt 32.5 powyżej.

103. ***Podmiot przekazujący może również dodać klauzulę, zgodnie z którą podmiot odbierający oświadczy, iż 1) nie stworzył celowo luk typu back door lub podobnych rozwiązań programistycznych, które mogłyby być wykorzystane w celu uzyskania dostępu do systemu lub danych osobowych, (2) nie stworzył celowo ani nie zmienił procesów biznesowych w taki sposób, który umożliwiłby dostęp do systemu lub danych osobowych, i 3) że prawo krajowe lub polityka państwowa nie wymagają od podmiotu odbierającego stworzenia lub utrzymania luk typu back door ani umożliwienia dostępu do danych osobowych lub systemów, ani nie wymagają od podmiotu odbierającego posiadania lub przekazania klucza do szyfrowania[80].***

104. ***Warunki skuteczności:***

- Istnienie przepisów lub polityki państwowej, które uniemożliwiają podmiotom odbierającym ujawnienie informacji, może sprawić, że klauzula ta będzie nieskuteczna. Podmiot odbierający być może nie będzie mógł zatem zawrzeć umowy lub będzie musiał powiadomić podmiot przekazujący o braku możliwości dalszej realizacji swoich zobowiązań umownych[81].
- Umowa musi przewidywać kary lub prawo podmiotu przekazującego do rozwiązania umowy z krótkim wyprzedzeniem w przypadku, gdy podmiot odbierający nie powiadomi o istnieniu luki typu back door czy podobnego rozwiązania programistycznego, zmanipulowanych procesach biznesowych lub wymogu wprowadzenia powyższych lub nie powiadomi podmiotu przekazującego niezwłocznie po tym, jak dowie się o istnieniu powyższych.

***

105. ***Podmiot przekazujący może wzmocnić swoje uprawnienie do przeprowadzenia audytu[82] lub inspekcji urządzeń przetwarzania danych podmiotu odbierającego, na miejscu lub zdalnie, w celu weryfikacji, czy dane zostały ujawnione organom publicznym i na jakich warunkach (dostęp niewykraczający poza to, co niezbędne i proporcjonalne w demokratycznym społeczeństwie), np. poprzez zawiadomienie z krótkim wyprzedzeniem, wprowadzenie mechanizmów zapewniających niezwłoczne działanie organów kontrolujących czy wzmocnienie autonomii podmiotu przekazującego w zakresie wyboru organu kontrolującego.***

106. ***Warunki skuteczności:***

- Żeby osiągnąć pełną skuteczność, zakres audytu powinien pod względem prawnym i technicznym obejmować przetwarzanie przez podmioty przetwarzające i podmioty podprzetwarzające podmiotu odbierającego danych osobowych przekazywanych do państwa trzeciego.
- Rejestry dostępu i inne podobne ślady powinny być zabezpieczone przed fałszowaniem, żeby audytorzy mogli znaleźć dowody ujawnienia. Rejestry dostępu i inne podobne ślady powinny również rozróżniać dostęp wynikający ze zwykłych czynności biznesowych i dostęp wynikający z nakazów lub żądań dostępu.

[80] Klauzula ta jest istotną gwarancją odpowiedniego stopnia ochrony przekazywanych danych osobowych i powinna być wymagana w większości przypadków.
[81] Zob. pkt 32.5 powyżej.
[82] Zob. np. Klauzula 5 lit. f) standardowych klauzul umownych między administratorami i podmiotami przetwarzającymi w decyzji 2010/87/UE, audyty mogłyby być również przeprowadzane na podstawie kodeksów postępowania lub poprzez certyfikację.

***

107. ***W przypadku gdy pierwotna ocena przepisów i praktyki państwa trzeciego wykazała stopień ochrony merytorycznie równoważny temu w UE dla danych przekazywanych przez podmiot przekazujący, podmiot przekazujący może wzmocnić obowiązek podmiotu odbierającego dane do niezwłocznego informowania podmiot przekazujący dane o niemożliwości wywiązania się z zobowiązań umownych i w efekcie zapewnienia wymaganego standardu „merytorycznie równoważnego stopnia ochrony danych.[83].”***

108. Brak takiej możliwości może wynikać ze zmian w przepisach lub praktykach państwa trzeciego[84]. Klauzule mogą przewidywać określone i sztywne terminy i procedury zapewniające szybkie zawieszenie przekazywania danych lub rozwiązanie umowy, a także zwrot lub usunięcie otrzymanych danych przez podmiot odbierający. Prowadzenie rejestru otrzymanych żądań, ich zakresu i skuteczności środków przyjętych w celu przeciwdziałania takim żądaniom powinno zapewnić podmiotowi przekazującemu wystarczające dowody, żeby wypełnić obowiązek zawieszenia lub zakończenia operacji przekazywania lub rozwiązania umowy.

109. ***Warunki skuteczności:***

- Powiadomienie musi mieć miejsce przed przyznaniem dostępu do danych. W przeciwnym razie, zanim podmiot przekazujący otrzyma powiadomienie, prawa jednostki mogły zostać już naruszone, jeśli żądanie opiera się na obowiązujących w takim państwie trzecim przepisach, które nie zapewniają stopnia ochrony wymaganego na podstawie prawa UE. Powiadomienie może służyć również do przeciwdziałania przyszłym naruszeniom i pozwolić podmiotowi przekazującemu zawiesić przekazywanie danych osobowych do państwa trzeciego lub rozwiązać umowę.
- Podmiot odbierający dane musi monitorować zmiany prawne i w polityce, które mogą doprowadzić do braku możliwości wywiązania się z obowiązków przez podmiot odbierający dane, i niezwłocznie powiadomić podmiot przekazujący dane o takich zmianach przed ich wejściem w życie (jeśli to możliwe), żeby pozwolić podmiotowi przekazującemu dane odzyskać dane od podmiotu odbierającego dane.
- Klauzule powinny przewidywać szybki mechanizm, za pomocą którego podmiot przekazujący dane zezwoli podmiotowi odbierającemu dane na niezwłoczne zabezpieczenie lub zwrócenie danych podmiotowi przekazującemu dane, a jeśli nie jest to możliwe – usunięcie lub bezpieczne zaszyfrowanie danych bez oczekiwania na instrukcje podmiotu przekazującego, jeśli zostanie osiągnięty określony próg uzgodniony między podmiotem przekazującym dane a podmiotem odbierającym dane. Podmiot odbierający dane powinien wdrożyć ten mechanizm od samego początku operacji przekazywania danych i regularnie przeprowadzać jego testy, żeby zapewnić, iż można go zastosować z krótkim wyprzedzeniem.

[83] Klauzula 5 lit. a) i lit. d) ppkt (i) standardowych klauzul umownych w decyzji 2010/87/UE.

[84] Zob. C-311/18 (Schrems II), pkt 139, gdzie Trybunał stwierdził, że „choć ta klauzula 5 lit. d) ppkt (i) pozwala podmiotowi odbierającemu dane osobowe w przypadku istnienia ustawodawstwa, które może on powołać na swoją obronę, takiego jak mający karny charakter zakaz mający na celu zachowanie tajemnicy dochodzenia policyjnego, na nieprzekazywanie mającemu siedzibę w Unii administratorowi danych prawnie wiążącego wniosku o ujawnienie danych osobowych ze strony organów ścigania, o tyle jest on jednak zobowiązany, zgodnie z zawartą w załączniku do decyzji w sprawie klauzul standardowych klauzulą 5 lit. a), do poinformowania tego administratora danych o swej niemożności spełnienia tego warunku zgodnie ze standardowymi klauzulami ochrony danych”.

- Inne klauzule mogą pozwolić podmiotowi przekazującemu na monitorowanie przestrzegania tych obowiązków przez podmiot odbierający za pomocą audytów, inspekcji i innych środków weryfikacji, a także egzekwowanie ich za pomocą kar nałożonych na podmiot odbierający czy prawa podmiotu przekazującego do zawieszenia przekazywania lub rozwiązania umowy ze skutkiem natychmiastowym.

***

110. ***O ile jest to dozwolone na podstawie prawa krajowego państwa trzeciego, umowa może wzmacniać obowiązki w zakresie przejrzystości nałożone na podmiot odbierający poprzez wykorzystanie metody „Warrant Canary", zgodnie z którą podmiot odbierający przyjmuje na siebie zobowiązanie do regularnej wysyłki (np. przynajmniej co 24 godziny) kryptograficznie podpisanej wiadomości informującej podmiot przekazujący, że na dany dzień i daną godzinę nie otrzymał żadnego nakazu ujawnienia danych osobowych lub podobnego. Brak aktualizacji w tym zakresie może wskazywać podmiotowi przekazującemu, że podmiot odbierający mógł otrzymać nakaz.***

111. ***Warunki skuteczności:***

- Przepisy państwa trzeciego muszą pozwalać podmiotowi odbierającemu dane wysyłać takie bierne powiadomienia podmiotowi przekazującemu.
- Podmiot przekazujący musi automatycznie monitorować powiadomienia typu warrant canary.
- Podmiot odbierający musi zapewnić, że jego prywatny klucz wykorzystywany do podpisywania Warrant Canary przechowywany jest w bezpiecznym miejscu i że przepisy państwa trzeciego nie mogą zmusić podmiotu odbierającego do wysłania fałszywych powiadomień typu Warrant Canary. W tym celu użyteczne może być ustanowienie wymogu podpisu przez różne osoby lub wysyłki powiadomienia typu Warrant Canary przez osobę poza jurysdykcją państwa trzeciego.

Obowiązek podjęcia konkretnych działań

112. ***Podmiot odbierający może zobowiązać się do przeprowadzenia kontroli, zgodnie z prawem państwa docelowego, legalności nakazu ujawnienia danych, w szczególności w zakresie tego, czy znajduje się on w ramach właściwości żądającego organu publicznego, i zaskarżenia nakazu, jeśli po dogłębnej analizie dojdzie do wniosku, że zgodnie z prawem państwa docelowego są do tego podstawy. Zaskarżając nakaz, podmiot odbierający dane powinien złożyć wniosek o zastosowanie środków tymczasowych w celu wstrzymania skuteczności nakazu, dopóki sąd nie rozpatrzy sprawy co do istoty. Podmiot odbierający miałby zakaz ujawniania żądanych danych osobowych, dopóki nie będzie do tego zobowiązany na podstawie obowiązujących przepisów proceduralnych. Podmiot odbierający dane zobowiązałby się również do przekazania minimalnej dozwolonej ilości informacji w odpowiedzi na nakaz, zgodnie z zasadną interpretacją nakazu.***

113. ***Warunki skuteczności:***

- Porządek prawny państwa trzeciego musi oferować skuteczne środki prawne do zaskarżenia nakazów ujawnienia danych.
- Klauzula ta zawsze będzie zapewniać bardzo ograniczoną dodatkową ochronę, ponieważ nakaz ujawnienia danych może być zgodny z prawem w ramach porządku prawnego państwa

trzeciego, ale ten porządek prawny może nie spełniać standardów UE. Ten środek umowny będzie musiał być wsparty innymi środkami uzupełniającymi.

- Zaskarżenie nakazu musi mieć, na podstawie prawa państwa trzeciego, skutek zawieszający. W przeciwnym razie organy publiczne będą nadal mieć dostęp do danych osób fizycznych i wszelkie dalsze działania podjęte na rzecz osoby fizycznej będą mieć tylko ten skutek, że pozwolą jej dochodzić odszkodowania za negatywne konsekwencje wynikające z ujawnienia danych.
- Podmiot odbierający będzie musiał dokumentować i udowodnić podmiotowi przekazującemu, jakie działania podjął, dokładając wszelkich starań, w celu wywiązania się z tego zobowiązania.

***

114. ***W przypadku opisanym powyżej podmiot odbierający może zobowiązać się do powiadomienia żądającego organu publicznego o niezgodności nakazu z zabezpieczeniami zawartymi w narzędziu przekazywania z art. 46 RODO[85] i wynikającym z tego konflikcie obowiązków podmiotu odbierającego. Podmiot odbierający powiadomi jednocześnie i niezwłocznie podmiot przekazujący lub właściwy organ nadzorczy z EOG, jeśli jest to możliwe na podstawie porządku prawnego państwa trzeciego.***

115. ***Warunki skuteczności:***

- Takie informacje dotyczące ochrony zapewnianej przez prawo UE i konfliktu obowiązków powinny mieć jakiś skutek prawny na podstawie porządku prawnego państwa trzeciego, np. prowadzić do kontroli sądowej lub administracyjnej nakazu lub żądania dostępu, wymogu uzyskania nakazu sądowego lub tymczasowego zawieszenia wykonania nakazu w celu zapewnienia dodatkowej ochrony danych.
- System prawny państwa trzeciego nie może uniemożliwić podmiotowi odbierającemu powiadomienia podmiotu przekazującego lub chociaż właściwego organu nadzorczego w UE o nakazie lub żądaniu dostępu, jakie podmiot odbierający otrzymał.
- Podmiot odbierający będzie musiał dokumentować i udowodnić podmiotowi przekazującemu, jakie działania podjął, dokładając wszelkich starań, w celu wywiązania się z tego zobowiązania.

Przyznanie osobom, których dane dotyczą, dodatkowych uprawnień

116. ***Umowa może przewidywać, że dane osobowe przekazane w formie zwykłego tekstu w normalnym toku działalności (w tym w przypadku wsparcia) mogą być udostępnione wyłącznie za wyraźną lub dorozumianą zgodą podmiotu przekazującego lub osoby, której dane dotyczą.***

[85] Przykładowo standardowe klauzule umowne przewidują, że przetwarzanie i przekazywanie danych odbywało się i będzie się nadal odbywało zgodnie z „odpowiednimi przepisami właściwego prawa o ochronie danych". Prawo definiuje się jako „prawodawstwo chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, właściwe dla administratora danych w państwie członkowskim, w którym podmiot przekazujący dane prowadzi działalność gospodarczą". TSUE potwierdza, że przepisy RODO, odczytywane w świetle Karty praw podstawowych UE, stanowią część tego prawodawstwa, zob. wyrok TSUE w sprawie C-311/18 (Schrems II), pkt 138.

117. ***Warunki skuteczności:***

- Klauzula ta może być skuteczna w tych przypadkach, gdy podmioty odbierające dane otrzymują od organów publicznych żądania dobrowolnej współpracy, w przeciwieństwie do przypadków dostępu do danych przez organy publiczne bez wiedzy podmiotu odbierającego lub wbrew jego woli.
- W pewnych sytuacjach osoba, której dane dotyczą, może nie być w stanie przeciwstawić się dostępowi lub udzielić zgody, która spełniałaby wszystkie warunki określone prawem UE (dobrowolna, świadoma i jednoznaczna) (np. w przypadku pracowników)[86].
- Przepisy lub polityki krajowe nakładające na podmiot odbierający zakaz ujawniania nakazu dostępu mogą sprawić, że klauzula ta nie będzie skuteczna, chyba że zostanie ona wsparta metodami technicznymi wymagającymi działania ze strony podmiotu przekazującego lub osoby, której dane dotyczą, żeby można było uzyskać dostęp do danych w zwykłym tekście. Takie środki techniczne ograniczające dostęp mogą być przewidziane w szczególności wtedy, gdy dostęp przyznawany jest wyłącznie w konkretnych przypadkach wsparcia lub świadczenia usług, a same dane są przechowywane w EOG.

***

118. ***Umowa mogłaby nakładać na podmiot odbierający lub podmiot przekazujący obowiązek niezwłocznego powiadomienia osoby, której dane dotyczą, o żądaniu lub nakazie otrzymanym od organów publicznych państwa trzeciego lub o tym, że podmiot odbierający nie jest w stanie spełnić zobowiązań umownych w celu umożliwienia osobie, której dane dotyczą, uzyskania informacji lub złożenia skutecznego środka odwoławczego (np. poprzez wniesienie skargi do właściwego organu nadzorczego lub organu sądowego i wykazanie legitymacji czynnej w sądach państwa trzeciego).***

119. ***Warunki skuteczności:***

- Powiadomienie to może ostrzec osobę, której dane dotyczą, o potencjalnym dostępie do jej danych przez organy publiczne w państwie trzecim. Dzięki niemu osoba, której dane dotyczą, może uzyskać dodatkowe informacje od podmiotów przekazujących i wnieść skargę do właściwego organu nadzorczego. Klauzula ta może rozwiązać także niektóre problemy, jakie osoba fizyczna może mieć z wykazaniem legitymacji czynnej *(locus standi)* przed sądami państwa trzeciego w zakresie zaskarżenia dostępu organów publicznych do jej danych.
- Przepisy lub polityki krajowe mogą uniemożliwić powiadomienie osoby, której dane dotyczą. Podmiot przekazujący i podmiot odbierający mogą jednak zobowiązać się powiadomić osobę, której dane dotyczą, jak tylko ograniczenia ujawnienia danych zostaną zniesione, i dołożyć wszelkich starań, żeby uzyskać odstępstwo od zakazu ujawnienia. Jako niezbędne minimum podmiot przekazujący lub właściwy organ nadzorczy mogą powiadomić osobę, której dane dotyczą, o zawieszeniu lub zakończeniu przekazywania jej danych osobowych z tego względu, że podmiot odbierający nie jest w stanie wywiązać się ze swoich zobowiązań umownych w wyniku otrzymania żądania dostępu.

***

[86] Art. 4 ust. 11 RODO.

120. ***Umowa mogłaby nakładać na podmiot odbierający lub podmiot przekazujący obowiązek wsparcia osoby, której dane dotyczą, w wykonaniu przysługujących jej praw w ramach jurysdykcji państwa trzeciego za pomocą mechanizmów dochodzenia roszczeń ad hoc i doradztwa prawnego.***

121. ***Warunki skuteczności***

- Przepisy lub polityki krajowe mogą nałożyć warunki, które zniweczą skuteczność mechanizmów dochodzenia roszczeń *ad hoc*.
- Doradztwo prawne może być pomocne dla osoby, której dane dotyczą, biorąc zwłaszcza pod uwagę, jak skomplikowane i kosztowne może być zapoznanie się z systemem prawnym państwa trzeciego przez osobę, której dane dotyczą, i podjęcie działań prawnych z zagranicy, czasem w obcym języku. Klauzula ta zawsze będzie zapewniać bardzo ograniczoną dodatkową ochronę, ponieważ udzielanie wsparcia i świadczenie doradztwa prawnego na rzecz osób, których dane dotyczą, nie może samo w sobie zaradzić temu, że porządek prawny państwa trzeciego nie zapewnia stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w UE. Ten środek umowny będzie musiał być wsparty innymi środkami uzupełniającymi.

Ten środek uzupełniający będzie skuteczny tylko wtedy, gdy przepisy państwa trzeciego przewidują możliwość dochodzenia roszczeń przed sądami krajowymi lub gdy istnieją mechanizmu dochodzenia roszczeń *ad hoc*. W każdym razie nie będzie to skuteczny środek uzupełniający chroniący przed narzędziami nadzoru, jeśli mechanizm dochodzenia roszczeń nie został przewidziany.

Środki organizacyjne

122. Dodatkowe środki organizacyjne mogą obejmować polityki wewnętrzne, metody organizacyjne i standardy, jakie administratorzy i podmioty przetwarzające stosują w ramach swojej organizacji i nakładają na podmioty odbierające dane w państwach trzecich. Mogą one przyczynić się do zapewnienia spójności ochrony danych osobowych w czasie całego cyklu przetwarzania. Środki organizacyjne mogą również podnosić świadomość podmiotów przekazujących o zagrożeniu i próbach uzyskania dostępu do danych w państwach trzecich oraz o możliwościach reakcji na takie okoliczności. Wybór i wdrożenie jednego z lub kilku tych środków nie zapewni w sposób pewny i systematyczny, że przeprowadzona operacja przekazywania spełni standard merytorycznie równoważnego stopnia ochrony wymaganego na podstawie prawa UE. W zależności od konkretnych okoliczności danej operacji przekazywania i przeprowadzonej oceny przepisów państwa trzeciego środki organizacyjne mogą być konieczne jako uzupełnienie środków prawnych lub technicznych w celu zapewnienia stopnia ochrony danych osobowych merytorycznie równoważnego temu gwarantowanemu w UE.

123. Ocenę najbardziej stosownych środków należy przeprowadzić osobno dla każdego przypadku, biorąc pod uwagę, że administratorzy i podmioty przetwarzające mają obowiązek przestrzegać zasady rozliczalności. EROD podaje poniżej listę przykładowych środków organizacyjnych, jakie podmioty przekazujące mogą wdrożyć, przy czym lista ta nie jest wyczerpująca i może nie obejmować wszystkich odpowiednich środków:

Polityki wewnętrzne w zakresie zarządzania przekazywaniem, zwłaszcza w grupach przedsiębiorstw

124. ***Przyjęcie adekwatnych polityk wewnętrznych przewidujących jasny podział obowiązków w zakresie przekazywania danych, kanały informacyjne i standardowe procedury operacyjne w przypadkach niejawnych lub oficjalnych żądań urzędów publicznych o dostęp do danych. W szczególności w przypadku przekazywania w ramach grupy przedsiębiorstw polityki te mogą przewidywać m.in.: powołanie specjalnego zespołu mającego siedzibę w EOG, złożonego z ekspertów z dziedziny IT, ochrony danych i prawa prywatności, który będzie obsługiwał żądania dotyczące danych osobowych przekazywanych z UE; powiadomienie kierownictwa prawnego i korporacyjnego wyższego szczebla i podmiotu przekazującego dane o otrzymaniu takich żądań; działania proceduralne zmierzające do zaskarżenia nieproporcjonalnych lub niezgodnych z prawem żądań oraz przekazanie osobom, których dane dotyczą, przejrzystych informacji.***

125. Opracowanie specjalnych procedur szkoleniowych dla pracowników odpowiedzialnych za obsługę żądań dostępu od organów publicznych, które należy okresowo aktualizować w celu uwzględnienia nowych zmian legislacyjnych i orzeczniczych w państwie trzecim i w EOG. Procedury szkoleniowe powinny uwzględniać wymogi prawa UE w zakresie dostępu organów publicznych do danych osobowych, w szczególności wynikające z art. 52 ust. 1 Karty praw podstawowych. Należy podnosić świadomość personelu w szczególności poprzez ocenę praktycznych przykładów żądań dostępu wystosowanych przez organy publiczne i poprzez zastosowanie do takich praktycznych przykładów standardu wynikającego z art. 52 ust. 1 Karty praw podstawowych. Szkolenia takie powinny brać pod uwagę szczególną sytuację podmiotu odbierającego dane, np. ustawodawstwo i uregulowania państwa trzeciego, którym podlega podmiot odbierający dane, i być w miarę możliwości opracowane we współpracy z podmiotem przekazującym dane.

126. ***Warunki skuteczności:***

- Polityki te mogą być przewidziane tylko w tych przypadkach, gdy żądanie dostępu wystosowane przez organy publiczne w państw trzecim jest zgodne z prawem UE[87]. Jeżeli jest niezgodne, polityki te nie będą wystarczające, żeby zapewnić równoważny stopień ochrony danych osobowych, w związku z czym - o czym była mowa powyżej - należy zaprzestać wszelkich operacji przekazywania lub wprowadzić odpowiednie środki uzupełniające w celu uniemożliwienia dostępu.

Środki związane z przejrzystością i rozliczalnością

127. ***Udokumentowanie i prowadzenie rejestru żądań dostępu otrzymanych od organów publicznych i udzielonych odpowiedzi, wraz z uzasadnieniem prawnym i zaangażowanymi podmiotami (np. jeżeli podmiot przekazujący został powiadomiony - również jego odpowiedzi i oceny zespołu ds. obsługi takich żądań itd.). Rejestry te należy udostępnić podmiotowi przekazującemu dane, który z kolei w razie potrzeby powinien przekazać je zainteresowanym osobom, których dane dotyczą.***

128. ***Warunki skuteczności:***

- Ustawodawstwo krajowe państwa trzeciego może uniemożliwić ujawnienie żądań lub istotnych informacji na ich temat, a tym samym sprawić, że środki te będą nieskuteczne.

[87] Zob. wyrok w sprawie C-362/14 („Schrems I"), pkt 94; C-311/18 (Schrems II), pkt 168, 174, 175 i 176.

Podmiot odbierający dane powinien powiadomić podmiot przekazujący o tym, że nie jest w stanie dostarczyć takich dokumentów i rejestrów, oferując tym samym podmiotowi przekazującemu możliwość zawieszenia przekazywania danych, jeżeli taka niezdolność prowadziłaby do obniżenia stopnia ochrony.

***

129. ***Regularna publikacja sprawozdań dotyczących przejrzystości lub streszczeń dotyczących żądań państwowych o dostęp do danych oraz rodzaju udzielonej odpowiedzi, w zakresie, w jakim publikacja jest dozwolona na mocy prawa lokalnego.***

130. ***Warunki skuteczności:***

- Przekazane informacje powinny być odpowiednie, jasne i możliwie jak najbardziej szczegółowe. Przepisy krajowe w państwie trzecim mogą uniemożliwiać ujawnienie szczegółowych informacji. W takim wypadku podmiot odbierający dane powinien dołożyć wszelkich starań, aby opublikować informacje statystyczne lub informacje zagregowane podobnego rodzaju.

Metody organizacyjne i środki minimalizacji danych

131. ***Uprzednie wymogi organizacyjne w ramach zasady rozliczalności, takie jak przyjęcie surowych i szczegółowych polityk i najlepszych praktyk w zakresie dostępu do danych i poufności, opartych na ścisłej zasadzie ograniczonego dostępu, monitorowanych za pomocą regularnych audytów i egzekwowanych za pomocą środków dyscyplinarnych, mogą być również użytecznymi środkami w kontekście przekazywania danych. W takich okolicznościach należy uwzględnić zasadę minimalizacji danych, aby ograniczyć narażenie danych osobowych na nieupoważniony dostęp. Przykładowo niekiedy może nie być potrzeby przekazania niektórych danych (np. w przypadku zdalnego dostępu do danych EOG, choćby w przypadkach wsparcia, gdy zamiast pełnego dostępu przyznaje się ograniczony dostęp; lub gdy świadczenie usługi wymaga jedynie przekazania ograniczonego zestawu danych, a nie całej bazy danych).***

132. ***Warunki skuteczności:***

- Należy prowadzić regularne audyty i podjąć zdecydowane środki dyscyplinarne w celu monitorowania i egzekwowania zgodności ze środkami minimalizacji danych również w kontekście przekazywania.
- Podmiot przekazujący dane powinien przed przekazaniem przeprowadzić ocenę posiadanych danych osobowych w celu zidentyfikowania tych zestawów danych, które nie są niezbędne dla celów przekazania, w związku z czym nie zostaną udostępnione podmiotowi odbierającemu dane.
- Środkom minimalizacji danych powinny towarzyszyć środki techniczne w celu zapewnienia, że dane nie są przedmiotem nieuprawnionego dostępu. Przykładowo, ustanowienie bezpiecznych mechanizmów obliczeń wielopodmiotowych i przekazanie zaszyfrowanych zestawów danych różnym zaufanym podmiotom może zapobiec w fazie projektowania jednostronnemu dostępowi prowadzącemu do ujawnienia danych umożliwiających identyfikację.

***

133. ***Opracowanie najlepszych praktyk w celu odpowiedniego i terminowego powiadomienia inspektora ochrony danych (jeżeli istnieje) oraz zespołów prawnych i zespołów ds. audytów wewnętrznych zapewnienia im dostępu do informacji dotyczących spraw związanych z międzynarodowym przekazywaniem danych osobowych.***

134. ***Warunki skuteczności:***

- Inspektor ochrony danych, jeżeli istnieje, oraz zespół prawny i zespół ds. audytów wewnętrznych otrzymają przed przekazaniem wszystkie stosowne informacje, a także będą konsultowani w sprawie niezbędności przekazania oraz ewentualnych dodatkowych zabezpieczeń.
- Stosowne informacje powinny obejmować m.in. ocenę niezbędności przekazania konkretnych danych osobowych, przegląd obowiązujących przepisów prawa państwa trzeciego oraz zabezpieczeń, do których wdrożenia podmiot odbierający się zobowiązał.

Przyjęcie norm i najlepszych praktyk

135. ***Przyjęcie surowszych polityk ochrony danych i prywatności danych, opartych na certyfikacji UE lub kodeksach postępowania bądź standardach międzynarodowych (np. normy ISO) i najlepszych praktykach (np. ENISA) z należytym uwzględnieniem aktualnego stanu wiedzy, zgodnie z ryzykiem związanym z kategoriami przetwarzanych danych i prawdopodobieństwem prób dostępu do nich ze strony organów publicznych.***

Inne

136. ***Przyjęcie i regularna weryfikacja wewnętrznych polityk dla celów oceny stosowności wdrożonych środków uzupełniających oraz w razie konieczności określenia i wdrożenia dodatkowych lub alternatywnych rozwiązań, aby zapewnić stopień ochrony przekazywanych danych osobowych równoważny temu gwarantowanemu w UE.***

***

137. ***Zobowiązanie podmiotu odbierającego dane do powstrzymania się od dalszego przekazania danych osobowych w tym samym lub innym państwie trzecim lub do zawieszenia ciągłego przekazywania, jeśli nie można zapewnić w państwie trzecim stopnia ochrony przekazywanych danych osobowych równoważnemu temu gwarantowanemu w UE.***[88]

[88] C-311/18 (Schrems II), pkt 135 i 137.

ZAŁĄCZNIK 3: MOŻLIWE ŹRÓDŁA INFORMACJI NA POTRZEBY OCENY PAŃSTWA TRZECIEGO

138. Podmiot odbierający dane powinien być w stanie podać stosowne źródła i informacje dotyczące państwa trzeciego, w którym prowadzi działalność, i przepisów, które znajdują do niego zastosowanie. Można także odwołać się do innych źródeł informacji, wymienionych na zasadzie przykładu poniżej:

- Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE) i Europejskiego Trybunału Praw Człowieka (ETPC)[89], wymienione w zaleceniach w sprawie niezbędnych gwarancji europejskich;[90]
- Decyzje stwierdzające odpowiedni stopień ochrony w państwie docelowym, jeśli przekazywanie odbywa się na innej podstawie prawnej[91];
- Rezolucje i sprawozdania organizacji międzyrządowych, np. Rady Europy[92], innych instytucji regionalnych[93]; oraz organów i agencji ONZ (np. Rady Praw Człowieka ONZ[94], Komitetu Praw Człowieka[95]);
- Orzecznictwo krajowe i decyzje podjęte przez niezależne organy sądowe lub administracyjne właściwe ds. prywatności i ochrony danych w państwie trzecim;
- Raporty instytucji akademickich i organizacji społeczeństwa obywatelskiego (np. organizacji pozarządowych i organizacji branżowych).

[89] Zob. arkusz informacyjny dotyczący orzecznictwa ETPC w sprawie masowej inwigilacji: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[90] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[91] C-311/18 (Schrems II), pkt 141; zob. decyzje stwierdzające odpowiedni stopień ochrony https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[92] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[93] Zob. np. raporty krajowe Międzyamerykańskiej Komisji Praw Człowieka (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[94] Zob. https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[95] Zob.: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5