Europejska Rada Ochrony Danych

Zalecenia 1/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE

Przyjęte 10 listopada 2020 r.

(tłumaczenie robocze: w przypadku jakichkolwiek wątpliwości ostatecznie rozstrzygającym jest oficjalny tekst zaleceń, dostępny w języku angielskim na stronie Europejskiej Rady Ochrony Danych pod adresem: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_pl)

Streszczenie

Ogólne rozporządzenie UE o ochronie danych (RODO) zostało przyjęte, aby spełniać dwa cele: ułatwiać swobodny przepływ danych osobowych w Unii Europejskiej, przy jednoczesnym zachowaniu podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych.

W swoim niedawnym wyroku C-311/18 (Schrems II) Trybunał Sprawiedliwości Unii Europejskiej (TSUE) przypomina nam, że ochrona danych osobowych w Europejskim Obszarze Gospodarczym (EOG) musi „podróżować" razem z danymi wszędzie tam, gdzie są przekazywane. Przekazywanie danych osobowych do państw trzecich nie może być sposobem podważenia lub osłabienia ochrony zapewnianej w EOG. Trybunał potwierdza to również, wyjaśniając, że stopień ochrony w państwach trzecich nie musi być identyczny ze stopniem gwarantowanym w EOG, ale powinien być merytorycznie równoważny. Trybunał podtrzymuje również ważność standardowych klauzul umownych, jako narzędzia przekazywania, które może służyć umownemu zapewnieniu merytorycznie równoważnego stopnia ochrony danych przekazywanych do państw trzecich.

Standardowe klauzule umowne i inne narzędzia przekazywania, o których mowa w art. 46 RODO, nie działają w próżni. Trybunał stwierdził, że administratorzy lub podmioty przetwarzające, działając jako podmioty przekazujące, są odpowiedzialni za sprawdzenie, w każdym konkretnym przypadku i, w stosownych przypadkach, we współpracy z podmiotami odbierającymi w państwie trzecim, czy prawo lub praktyka państwa trzeciego wpływa na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO. W tych sprawach Trybunał nadal pozostawia podmiotom przekazującym otwartą możliwość wdrożenia środków uzupełniających, które wypełnią luki w ochronie i podniosą ją do stopnia wymaganego przez prawo UE. Trybunał nie określa, jakie mogłyby to być środki. Trybunał podkreśla jednak, że podmioty przekazujące będą musiały identyfikować je indywidualnie dla każdego przypadku. Jest to zgodne z zasadą rozliczalności określoną w art. 5 ust. 2 RODO, która wymaga, aby administratorzy byli odpowiedzialni za przestrzeganie zasad RODO dotyczących przetwarzania danych osobowych i byli w stanie wykazać ich przestrzeganie.

Aby pomóc podmiotom przekazującym (administratorom lub podmiotom przetwarzającym, podmiotom prywatnym lub organom publicznym, przetwarzającym dane osobowe w zakresie stosowania RODO) w złożonym zadaniu oceny państw trzecich i określeniu w razie potrzeby odpowiednich środków uzupełniających, Europejska Rada Ochrony Danych (EROD) przyjęła niniejsze zalecenia. W zaleceniach tych przedstawiono podmiotom przekazującym szereg kroków, które należy podjąć, potencjalne źródła informacji oraz kilka przykładów środków uzupełniających, które można zastosować.

Jako **pierwszy krok** EROD radzi Wam, jako podmiotom przekazującym, abyście **mieli świadomość prowadzonych przez siebie operacji przekazywania**. Identyfikowanie wszystkich przypadków przekazywania danych osobowych do państw trzecich może być trudnym zadaniem. Świadomość tego, dokąd trafiają dane osobowe, jest jednak konieczna, aby zapewnić merytorycznie równoważny stopień ochrony wszędzie tam, gdzie dane są przetwarzane. Musisz również zweryfikować, czy przekazane przez Ciebie dane są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane i przetwarzane w państwie trzecim.

Drugim krokiem jest **weryfikacja narzędzia przekazywania, na którym opiera się Twoje przekazywanie**, spośród tych wymienionych w rozdziale V RODO. Jeśli Komisja Europejska już stwierdziła, że państwo trzecie, terytorium lub określony sektor, do którego przekazujesz dane, jest odpowiednie, w drodze jednej ze swoich decyzji stwierdzających odpowiedni stopień ochrony na podstawie art. 45 RODO lub poprzedniej Dyrektywy 95/46, i o ile decyzja nadal obowiązuje, nie będziesz musiał podejmować żadnych dalszych kroków poza monitorowaniem, czy decyzja stwierdzająca odpowiedni stopień ochrony pozostaje ważna. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony, musisz polegać na jednym z narzędzi przekazywania wymienionych w art. 46 RODO dla operacji przekazywania, które są systematyczne i powtarzające się. Tylko w niektórych sporadycznych i niepowtarzalnych przypadkach przekazywania danych możesz skorzystać z jednego z wyjątków przewidzianych w artykule 49 RODO, jeśli spełniasz warunki.

Trzecim krokiem jest **ocena**, czy w **prawie lub praktyce państwa trzeciego** istnieje cokolwiek, co może mieć wpływ na skuteczność odpowiednich zabezpieczeń narzędzi przekazywania, na których polegasz, w kontekście twojego konkretnego przekazywania danych. Twoja ocena powinna skupiać się przede wszystkim na przepisach państwa trzeciego, które są istotne dla twojego przekazywania danych, oraz na narzędziu przekazywania wymienionym w artykule 46 RODO, na którym się opierasz i które może zmniejszyć stopień jego ochrony. W celu oceny elementów, które należy wziąć pod uwagę podczas oceny prawa państwa trzeciego dotyczącego dostępu organów publicznych do danych do celów nadzoru, należy zapoznać się z zaleceniami EROD w zakresie niezbędnych gwarancji europejskich. W szczególności należy dokładnie rozważyć, kiedy przepisy regulujące dostęp organów publicznych do danych są niejednoznaczne lub nie są publicznie dostępne. W przypadku braku przepisów regulujących okoliczności, w których organy publiczne mogą uzyskać dostęp do danych osobowych, jeśli nadal chcesz kontynuować przekazywanie, powinieneś przyjrzeć się innym istotnym i obiektywnym czynnikom i nie polegać na czynnikach subiektywnych, takich jak prawdopodobieństwo, że organy publiczne będą miały dostęp do danych osobowych w sposób niezgodny z normami UE. Powinieneś przeprowadzić tę ocenę z należytą starannością i dokładnie ją udokumentować, ponieważ będziesz odpowiedzialny za decyzję, którą możesz podjąć na tej podstawie.

Czwartym krokiem jest **zidentyfikowanie i przyjęcie środków uzupełniających**, które są konieczne, aby stopień ochrony przekazywanych danych osobowych osiągnął unijny merytorycznie równoważny stopień. Ten krok jest konieczny tylko wtedy, gdy Twoja ocena wykaże, że przepisy państwa trzeciego mają wpływ na skuteczność narzędzia przekazywania wymienionego w art. 46 RODO, na którym polegasz lub na którym zamierzasz polegać w kontekście Twojego przekazywania danych. Zalecenia te zawierają (w Załączniku 2) niewyczerpującą listę przykładów dodatkowych środków wraz z niektórymi warunkami, jakie musiałyby spełniać, aby były skuteczne. Podobnie jak w przypadku odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46, niektóre środki uzupełniające mogą być skuteczne w niektórych państwach, ale niekoniecznie w innych. Będziesz odpowiedzialny za ocenę ich skuteczności w kontekście przekazywania danych oraz w świetle prawa państwa trzeciego i narzędzia przekazywania, na którym polegasz, i będziesz odpowiedzialny za podjętą decyzję. Może to również wymagać połączenia kilku środków uzupełniających. Ostatecznie może się okazać, że żaden środek uzupełniający nie zapewni merytorycznie równoważnego stopnia ochrony Twojego konkretnego przekazywania danych. W przypadkach, w których żadne środki uzupełniające nie są odpowiednie, należy unikać przekazywania danych, zawiesić lub zakończy je, aby uniknąć naruszenia stopnia ochrony danych osobowych. Powinieneś również przeprowadzić tę ocenę uzupełniających środków z należytą starannością i udokumentować ją.

Piątym krokiem jest **podjęcie** wszelkich **formalnych kroków proceduralnych**, których może wymagać przyjęcie środka uzupełniającego, w zależności od narzędzia przekazywania na podstawie art. 46 RODO, na którym się opierasz. Niniejsze zalecenia precyzują te formalności. W przypadku niektórych z nich może być konieczne skonsultowanie się z właściwymi organami nadzorczymi.

Szóstym i ostatnim krokiem będzie ponowna ocena w odpowiednich odstępach czasu stopnia ochrony danych, które przekazujesz do państw trzecich, oraz monitorowanie, czy nastąpiły lub będą jakiekolwiek zmiany, które mogą na ten stopień ochrony wpłynąć. Zasada rozliczalności wymaga ciągłego czuwania nad stopniem ochrony danych osobowych.

Organy nadzorcze będą nadal wykonywać swoje uprawnienia w zakresie monitorowania stosowania RODO i egzekwowania go. Organy nadzorcze zwrócą należytą uwagę na działania podejmowane przez podmioty przekazujące w celu zapewnienia, aby przekazywane przez nich dane objęte były merytorycznie równoważnym stopniem ochrony. Jak przypomina Trybunał, organy nadzorcze zawieszą lub zabronią przekazywania danych w przypadkach, gdy w wyniku dochodzenia lub skargi stwierdzą, że nie można zapewnić merytorycznie równoważnego stopnia ochrony.

Organy nadzorcze będą nadal opracowywać wytyczne dla podmiotów przekazujących i koordynować swoje działania w EROD, aby zapewnić spójność w stosowaniu unijnych przepisów o ochronie danych.

Spis treści

1 ROZLICZALNOŚĆ PRZY PRZEKAZYWANIU DANYCH 7

2 PLAN DZIAŁAŃ: STOSOWANIE ZASADY ROZLICZALNOŚCI W ODNIESIENIU DO PRZEKAZYWANIA DANYCH W PRAKTYCE.....8

2.1 Krok 1: Świadomość prowadzonych przez Ciebie operacji przekazywania.....8

2.2 Krok 2: Określ narzędzia przekazywania, na których polegasz 10

2.3 Krok 3: Ocena, czy narzędzie przekazywania danych z art. 46 RODO, na którym polegasz, jest skuteczne w świetle wszystkich okoliczności przekazania danych 12

2.4 Krok 4: Przyjmij środki uzupełniające 15

2.5 Krok 5: Kroki proceduralne, jeśli zidentyfikowano skutecznie środki uzupełniające 18

2.6 Krok 6: Ponowna ocena w odpowiednich odstępach czasu 20

3 Wnioski 20

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), w szczególności jego załącznik XI i protokół 37, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018r.[1],

Uwzględniając art. 12 i 22 Regulaminu wewnętrznego EROD,

Mając na uwadze, iż:

(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 standardowych klauzul umownych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii przez to rozporządzenie, interpretowane w świetle Karty praw podstawowych Unii Europejskiej.[2]

(2) Jak podkreślił Trybunał, stopień ochrony osób fizycznych merytorycznie równoważny temu gwarantowanemu w Unii przez RODO w świetle Karty musi być zagwarantowany niezależnie od przepisu Rozdziału V na podstawie którego następuje 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, odpowiednie zabezpieczenia, administrator danych lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Administrator lub podmiot przetwarzający może zapewnić odpowiednie zabezpieczenia, bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego, korzystając z jednego z narzędzi przekazywania wymienionych w art. 46 ust. 2 RODO, takich jak standardowe klauzule ochrony danych.

(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, a zatem niezależnie od stopnia ochrony gwarantowanego w każdym z tych państw. Ze względu na swój umowny charakter, standardowe klauzule ochrony danych nie mogą wiązać organów władzy publicznej państw trzecich, ponieważ nie są stroną umowy. W konsekwencji może

---

[1] Odniesienia do „państw członkowskich" występujące w tym dokumencie, należy rozumieć jako odniesienia do „państw członkowskich EOG".

[2] Wyrok TSUE z dnia 16 lipca 2020 r., Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximillianowi Schremsowi, (dalej: C-311/18 (Schrems II)), drugie stwierdzenie.

[3] C-311/18 (Schrems II), pkt 92 i 93.

okazać się konieczne, aby podmioty przekazujące dane uzupełnili zabezpieczenia zawarte w tych standardowych klauzulach ochrony danych o środki uzupełniające w celu zapewnienia przestrzegania stopnia ochrony wymaganego na mocy prawa UE w danym państwie trzecim. Trybunał odsyła do motywu 109 RODO, który wspomina o takiej możliwości i zachęca administratorów i podmioty przetwarzające do korzystania z niej.[4]

(5) Trybunał stwierdził, że 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 docelowego państwa trzeciego zapewnia właściwą, w świetle prawa Unii, ochronę 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 administratora danych lub podmiot przetwarzający dodatkowych środków odpowiednich dla zagwarantowania takiej ochrony, podmioty te lub, pomocniczo, właściwy organ nadzorczy, są zobowiązane do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego.[6]

(7) RODO ani Trybunał nie definiują ani nie precyzują „zabezpieczeń dodatkowych", „środków dodatkowych" ani „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 zgodność ze stopniem ochrony wymaganym przez prawo UE w danym państwie trzecim.

(8) EROD postanowiła z własnej inicjatywy zbadać tę kwestię i przekazać administratorom i podmiotom przetwarzającym, działającym jako podmioty przekazujące zalecenia dotyczące procesu, który mogą zastosować w celu określenia i przyjęcia środków uzupełniających. Zalecenia te mają na celu dostarczenie podmiotom przekazującym metodologii umożliwiającej określenie, czy i jakie dodatkowe środki należałoby wprowadzić w celu przekazywania danych do państw trzecich. Podstawowym obowiązkiem podmiotów przekazujących dane jest zapewnienie, aby przekazywane dane były objęte w państwie trzecim stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w Unii. Za pomocą tych zaleceń EROD stara się zachęcać do spójnego stosowania RODO i orzeczenia Trybunału, zgodnie z właściwością EROD.[7]

PRZYJĘŁA NASTĘPUJĄCE 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] Artykuł 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, a ograniczania można wprowadzać tylko, jeżeli są one przewidziane prawem, nie naruszają istoty prawa, są proporcjonalne, niezbędne i rzeczywiście spełniają cele interesu ogólnego uznane przez Unię lub potrzebę ochrony praw i wolności innych osób.[9] Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności.[10]

2. Stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE musi być zagwarantowany dla danych, gdy są one przekazywane do państw trzecich poza EOG, w celu zapewnienia, by nie został naruszony stopień ochrony danych zagwarantowany przez RODO.

3. Prawo do ochrony danych ma czynny charakter. Wymaga ono od podmiotów przekazujących i podmiotów odbierających (niezależnie od tego czy są oni administratorami i/lub podmiotami przetwarzającymi) wyjścia poza uznanie tego prawa lub pasywną zgodność z tym prawem.[11] Administratorzy i podmioty przetwarzające muszą dążyć do przestrzegania prawa do ochrony danych w aktywny i ciągły sposób, wdrażając środki prawne, techniczne i organizacyjne zapewniające jego skuteczność. Administratorzy i podmioty przetwarzające muszą być w stanie wykazać te wysiłki w odniesieniu do osób, których dane dotyczą, ogółu społeczeństwa i organów nadzorczych do spraw ochrony danych. Jest to tak zwana zasada rozliczalności.[12]

4. Zasada rozliczalności, która jest niezbędna do zapewnienia skutecznego stosowania stopnia ochrony danych przewidzianego w RODO dotyczy również operacji przekazywania danych do państw trzecich[13], ponieważ stanowią one formę przetwarzania danych same w sobie[14]. Jak podkreślił Trybunał, stopień ochrony merytorycznie równoważny temu gwarantowanemu na terytorium Unii Europejskiej przez RODO odczytywany w świetle Karty powinien być zapewniony niezależnie od podstawy, na jakiej dokonywane jest przekazywanie danych osobowych do państwa trzeciego.[15]

5. W wyroku w sprawie Schrems II, Trybunał podkreśla zobowiązania podmiotów przekazujących i podmiotów odbierających do zapewnienia, że przetwarzanie danych osobowych odbywało się i będzie nadal się odbywać zgodnie ze stopniem ochrony przewidzianym prawem UE w zakresie ochrony danych, oraz do zawieszenia przekazywania danych lub rozwiązania umowy w przypadku, gdy podmiot odbierający dane nie jest lub przestał być w stanie przestrzegać standardowych klauzul ochrony danych zawartych we właściwej umowie między podmiotem przekazującym a podmiotem odbierającym[16]. Administrator lub podmiot przetwarzający pełniący funkcję podmiotu przekazującego musi zapewnić, aby podmioty

---

[8] Artykuł 8 ust. 1 Karty praw podstawowych oraz artykuł 16 ust. 1 TFUE, preambuła 1, artykuł 1 ust. 2 RODO.

[9] Artykuł 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 oraz C-93/02, Volker und Markus Schecke GbR przeciwko Land Hessen, Opinia rzecznika generalnego Sharpstona, 17 czerwca 2010 r., pkt 71.

[12] Artykuł 5 ust. 2 i artykuł 28 ust. 3 lit. h) RODO.

[13] Artykuł 44 i motyw 101 RODO, jak również artykuł 47 ust. 2 lit. d) RODO.

[14] Wyrok TSUE z 6 października 2015 r., *Maximillian Schrems przeciwko Data Protection Commissioner,* (dalej C-362/14 (Schrems I), pkt 45.

[15] C-311/18 (Schrems II), pkt 92 i 93.

[16] C-311/18 (Schrems II), pkt 134, 135, 139, 140, 142, 142.

odbierające współpracowały z podmiotem przekazującym, w stosownych przypadkach, w wykonywaniu przez niego jego zobowiązań, informując go, np. o wszelkich wydarzeniach mających wpływ na stopień ochrony danych osobowych zapewniany w państwie podmiotu odbierającego.[17] Zobowiązania te stanowią stosowanie zasady rozliczalności przewidzianej w RODO w odniesieniu do operacji przekazywania danych.[18]

2 PLAN DZIAŁAŃ: STOSOWANIE ZASADY ROZLICZALNOŚCI W ODNIESIENIU DO PRZEKAZYWANIA DANYCH W PRAKTYCE

6. Wynikiem jest plan działań, jakie należy podjąć, aby ustalić, czy Ty (jako podmiot przekazujący dane) musisz wdrożyć środki uzupełniające, aby być w stanie przekazywać dane zgodnie z prawem poza EOG. „Ty"* w niniejszym dokumencie oznacza administratora lub podmiot przetwarzający, który pełni rolę podmiotu przekazującego dane, przetwarzającego dane osobowe w zakresie stosowania RODO – w tym przetwarzania przez podmioty prywatne i organy publiczne przy przekazywaniu danych do podmiotów prywatnych.[19] Jeżeli chodzi o przekazywanie danych osobowych prowadzone między organami publicznymi, konkretne wskazówki zapewnione są w Wytycznych 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) Rozporządzenia 2016/679 do celów przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG.[20]

7. Będziesz musiał odpowiednio udokumentować tę ocenę i środki uzupełniające, które wybierzesz i wdrożysz, oraz udostępnić taką dokumentację właściwemu organowi nadzorczemu na wniosek.[21]

2.1 Krok 1: Świadomość prowadzonych przez Ciebie operacji przekazywania

8. Pierwszym krokiem, dzięki któremu będziesz wiedział, co może być od Ciebie (jako podmiotu przekazującego dane) wymagane, abyś był w stanie kontynuować lub prowadzić nowe operacje przekazywania danych osobowych[22], jest zapewnienie, żebyś miał pełną świadomość prowadzonych przez Ciebie operacji przekazywania. Rejestrowanie i identyfikowanie (ang. *mapping*) wszystkich operacji przekazywania może być złożonym zadaniem dla podmiotów zaangażowanych w liczne, zróżnicowane i regularne operacje przekazywania z państwami trzecimi i korzystających z usług szeregu podmiotów przetwarzających i podmiotów podprzetwarzających. Świadomość prowadzonych przez Ciebie operacji przekazywania jest niezbędnym pierwszym krokiem w kierunku wypełnienia Twoich

---

[17] C-311/18 (Schrems II), pkt 134.

[18] Artykuł 5 ust. 2 oraz artykuł 28 ust. 3 lit. h) RODO.

* *Przypis tłumacza: zaimek „Ty" – odpowiednik „You" w wersji angielskiej dokumentu – w wersji polskiej dokumentu jest zazwyczaj pomijany z uwagi na charakterystykę języka polskiego, zatem na odniesienie do słowa „Ty" (ang. „You") wskazuje użycie czasownika w 2. osobie liczby pojedynczej (np. musisz) bądź użycie form odmiennych zaimka „Ty" (np. Ciebie, Tobie, Tobą, Twoich).*

[19] Zob. Wytyczne EROD 3/2018 w sprawie zakresu terytorialnego RODO (artykuł 3) https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_pl.

[20] Wytyczne 2/2020 w sprawie stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) Rozporządzenia 2016/679 do celów przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_pl.

[21] Artykuł 5 ust. 2 RODO i artykuł 24 ust. 1 RODO.

[22] Proszę zauważyć, że zdalny dostęp przez podmiot z państwa trzeciego do danych znajdujących się w EOG również uważany jest za przekazywanie.

zobowiązań w ramach zasady rozliczalności.

9. Aby zyskać pełną świadomość prowadzonych przez Ciebie operacji przekazywania, możesz oprzeć się na rejestrach czynności przetwarzania, które możesz mieć obowiązek prowadzić jako administrator lub podmiot przetwarzający na mocy artykułu 30 RODO.[23] Pomocne mogą być również wcześniejsze działania podejmowane w celu przekazywania osobom, których dane dotyczą, na mocy artykułu 13 ust. 1 lit. f) oraz artykułu 14 ust. 1 lit. f) RODO, informacji na temat Twoich operacji przekazywania danych osobowych do państwa trzecich.[24]

10. Podczas identyfikowania operacji przekazywania nie zapomnij również wziąć pod uwagę dalszego przekazywania, na przykład gdy Twoje podmioty przetwarzające spoza EGO przekazują dane osobowe, które im powierzyłeś, do podmiotu podprzetwarzającego w innym państwie trzecim lub w tym samym państwie trzecim.[25]

11. Zgodnie z zasadą „minimalizacji danych"[26] z RODO, musisz zweryfikować, czy dane, które przekazujesz, są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane do i przetwarzane w państwie trzecim.

12. Działania te muszą być dokonane przed każdym przekazaniem i aktualizowane przed ponownym podjęciem operacji przekazywania danych po ich zawieszeniu: musisz wiedzieć, gdzie dane osobowe, które przekazałeś, mogą się znajdować lub mogą być przetwarzane przez podmioty odbierające (mapa miejsc docelowych).

13. Pamiętaj, że zdalny dostęp z państwa trzeciego (na przykład w sytuacjach wsparcia) i/lub przechowywanie w chmurze znajdującej się poza EOG również uznawane są za przekazywanie.[27] A dokładniej, jeżeli korzystasz z międzynarodowej infrastruktury chmury, musisz oszacować, czy Twoje dane będą przekazywane do państw trzecich i gdzie, chyba że dostawca chmury wyraźnie stwierdzi w swojej umowie, że dane nie będą w ogóle przetwarzane w państwach trzecich.

---

[23] Zob. artykuł 30 RODO, a w szczególności ust. 1 lit. e) i ust. 2 lit. c). Ponadto Twoje rejestry przetwarzania powinny zawierać opis Twoich czynności przetwarzania (w tym, ale nie tylko, kategorie osób, których dane dotyczą, kategorie danych osobowych oraz cele przetwarzania i konkretne informacje na temat operacji przetwarzania danych. Niektórzy administratorzy i podmioty przetwarzające są zwolnieni z obowiązku prowadzenia rejestrów przetwarzania (artykuł 30 ust. 5 RODO). Wskazówki dotyczące tego odstępstwa zawiera dokument Grupy Roboczej Artykułu 29 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 wyjątków od obowiązku prowadzenia rejestrów czynności przetwarzania na mocy art. 30 ust. 5 RODO) (zatwierdzony przez RODO 25 maja 2018 r.).

[24] Zgodnie z zasadami przejrzystości RODO, musisz przekazywać osobom, których dane dotyczą, informacje na temat operacji przekazywania danych osobowych do państw trzecich (artykuł 13 ust. 1 lit. f) oraz artykuł 14 ust. 1 lit. f) RODO). W szczególności musisz przekazać im informacje o stwierdzeniu lub braku stwierdzenia przez Komisję 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 podawane osobie, której dane dotyczą, muszą być prawidłowe i aktualne, szczególnie w świetle orzecznictwa Trybunału dotyczącego przekazywania.

[25] Gdy administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.

[26] Artykuł 5 ust. 1 lit. c) RODO.

[27] Zob. Często zadawane pytanie nr 11: *„należy pamiętać, że nawet udzielenie dostępu do danych z państwa trzeciego, na przykład 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, 23 lipca 2020 r.

2.2 Krok 2: Określ narzędzia przekazywania, na których polegasz

14. Drugim krokiem, jaki musisz podjąć, jest określenie narzędzi przekazywania, na których polegasz, spośród tych wymienionych i przewidzianych w Rozdziale V RODO.

Decyzje stwierdzające odpowiedni stopień ochrony

15. Komisja Europejska może uznać poprzez swoje decyzje stwierdzające odpowiedni stopień ochrony dotyczące niektórych lub wszystkich państw trzecich, do których przekazujesz dane osobowe, że zapewniają one odpowiedni stopień ochrony danych osobowych.[28]

16. Skutkiem takiej decyzji stwierdzającej odpowiedni stopień ochrony jest to, że możliwy jest przepływ danych osobowych z EOG do danego państwa trzeciego bez konieczności wykorzystania żadnego z narzędzi przekazywania z artykułu 46 RODO.

17. Decyzje stwierdzające odpowiedni stopień ochrony mogą obejmować państwo jako całość lub być ograniczone do jego części. Decyzje takie mogą obejmować wszystkie operacje przekazywania danych do państwa lub być ograniczone do określonych rodzajów przekazywania (np. w jednym sektorze).[29]

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

19. Jeżeli przekazujesz dane osobowe do państw trzecich, regionów lub sektorów objętych decyzją Komisji stwierdzającą odpowiedni stopień ochrony (w mającym zastosowanie zakresie), **nie musisz podejmować żadnych dalszych kroków opisanych w niniejszych zaleceniach.**[31] Jednakże musisz nadal monitorować, czy decyzje stwierdzające odpowiedni stopień ochrony odnoszące się do Twoich operacji przekazywania nie zostały uchylone lub unieważnione.[32]

20. Jednakże decyzje stwierdzające odpowiedni stopień ochrony danych nie uniemożliwiają osobom, których dane dotyczą, składania skarg. Nie uniemożliwiają także organom nadzorczym wniesienia sprawy do sądu krajowego, jeżeli mają one wątpliwości co do ważności decyzji, tak aby sąd krajowy mógł skierować wniosek o wydanie orzeczenia w trybie prejudycjalnym do TSUE w celu zbadania tej ważności.[33]

---

[28] Komisja Europejska ma prawo do ustalenia, na podstawie artykułu 45 RODO, czy państwo spoza UE zapewnia odpowiedni stopień ochrony danych. Podobnie Komisja Europejska ma prawo do ustalenia, czy organizacja międzynarodowa zapewnia odpowiedni stopień ochrony.

[29] Artykuł 45 ust. 1 RODO.

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

[31] Pod warunkiem, że Ty i podmiot odbierający dane, wdrożyliście środki w celu zapewnienia zgodności z innymi zobowiązaniami wynikającymi z RODO; w przeciwnym razie wdróżcie te środki.

[32] Komisja Europejska musi dokonywać okresowych przeglądów wszystkich decyzji stwierdzających odpowiedni stopień ochrony oraz monitorować, czy państwa trzecie korzystające z takich decyzji nadal zapewniają odpowiedni stopień ochrony (zob. art. 45 ust. 3 i art. 45 ust. 4 RODO). Ponadto TSUE może unieważnić decyzje stwierdzające odpowiedni stopień ochrony (zob. wyroki TSUE w sprawach C-362/14 (Schrems I) i C-311/18 (Schrems II).

[33] C-311/18 (Schrems II), punkty 118 - 120. Organy nadzorcze nie mogą zignorować decyzji stwierdzającej odpowiedni stopień ochrony i zawiesić lub wstrzymać operacje przekazywania danych osobowych do takich państw wskazując jedynie na nieodpowiedni stopień ochrony. Mogą one jedynie skorzystać ze swojego uprawnienia do zawieszenia lub zakazania przekazywania danych osobowych do tego państwa trzeciego na innych podstawach (np. niewystarczające środki bezpieczeństwa z naruszeniem artykułu 32 RODO, brak podstawy prawnej jest ważnym czynnikiem do uznania przetwarzania jako takiego za naruszenie art. 6 RODO). Organy nadzorcze mogą zbadać, z zachowaniem całkowitej niezależności, czy przekazanie danych jest zgodne

Przykład: Obywatel UE, Pan Schrems, w czerwcu 2013 r. złożył skargę do Irlandzkiej Komisji Ochrony Danych (Irish Data Protection Commission - DPC) i zwrócił się do tego organu nadzorczego o zakazanie lub zawieszenie przekazywania jego danych osobowych z Facebook Ireland do Stanów Zjednoczonych, ponieważ uznał, że prawo i praktyka obowiązujące w tym państwie nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi w nim przez władze publiczne. DPC oddaliła skargę, w szczególności ze względu na to, że Komisja Europejska w decyzji 2000/520 stwierdziła, iż, w ramach programu 'bezpiecznej przystani' Stany Zjednoczone zapewniają odpowiedni stopień ochrony przekazywanych danych osobowych (decyzja w sprawie 'bezpiecznej przystani'). Pan Schrems zaskarżył decyzję DPC i Irlandzki Wysoki Trybunał skierował kwestię ważności decyzji 2000/520 do Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Następnie TSUE wydał decyzję o unieważnieniu decyzji Komisji 2000/520 w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach 'bezpiecznej przystani'.[34]

Instrumenty przekazywania z artykułu 46 RODO

21. W art. 46 RODO wymieniono szereg narzędzi przekazywania danych zawierających *„odpowiednie zabezpieczenia", które podmioty przekazujące dane* mogą wykorzystywać w celu przekazywania danych osobowych do państw trzecich w przypadku braku odpowiednich decyzji stwierdzających odpowiedni stopień ochrony. Głównymi rodzajami narzędzi przekazywania danych z art. 46 RODO są:

- standardowe klauzule ochrony danych (SCC);
- wiążące reguły korporacyjnych (BCR);
- kodeksy postępowania;
- mechanizmy certyfikacji;
- klauzule umowne ad hoc.

22. Niezależnie od wybranego przez Ciebie narzędzia przekazywania zgodnie z art. 46 RODO, należy zapewnić, że przekazywane dane osobowe będą objęte merytorycznie równoważnym stopniem ochrony.

23. Narzędzia przekazywania danych z art. 46 RODO w głównej mierze zawierają odpowiednie zabezpieczenia o charakterze umownym, które mogą być stosowane w celu przekazywania danych do wszystkich państw trzecich. Sytuacja w państwie trzecim, do którego przekazujesz dane, może nadal wymagać uzupełnienia tych narzędzi oraz zawartych w nich zabezpieczeń o dodatkowe środki („środki uzupełniające") w celu zapewnienia merytorycznie równoważnego stopnia ochrony.[35]

Wyjątki

24. Poza decyzjami stwierdzającymi odpowiedni stopień ochrony i narzędziami przekazywania danych z art. 46, RODO zawiera trzecią drogę umożliwiającą przekazywanie danych osobowych w określonych sytuacjach. Z zastrzeżeniem określonych warunków, nadal możesz mieć

---

z wymogami określonymi w RODO, oraz, w stosownych przypadkach, wnieść sprawę do sądu krajowego, jeżeli mają wątpliwości co do ważności decyzji Komisji stwierdzającej odpowiedni stopień ochrony, skierować wniosek o wydanie orzeczenia w trybie prejudycjalnym do TSUE w celu zbadania tej ważności.

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

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

możliwość przekazywania danych osobowych na podstawie wyjątków wymienionych w art. 49 RODO.

25. Artykuł 49 RODO ma wyjątkowy charakter. Zawarte w nim wyjątki muszą być interpretowane w sposób restrykcyjny i odnosić się głównie do okazjonalnych i niepowtarzających się czynności przetwarzania danych. EROD wydała Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679.[36]

26. Przed skorzystaniem z wyjątków określonych w art. 49 RODO, musisz sprawdzić, czy przekazanie danych spełnia rygorystyczne warunki określone w tym przepisie dla każdego z nich.

***

27. Jeżeli przekazanie danych nie może być prawnie oparte na decyzji stwierdzającej odpowiedni stopień ochrony, ani na wyjątkach zgodnie z art. 49 RODO, należy kontynuować Krok 3.

2.3 Krok 3: Ocena, czy narzędzie przekazywania danych z art. 46 RODO, na którym polegasz, jest skuteczne w świetle wszystkich okoliczności przekazania danych

28. Samo wybranie narzędzia przekazywania na podstawie art. 46 RODO może nie być wystarczające. Narzędzie przekazywania musi zapewniać, że stopień ochrony gwarantowany przez RODO nie zostanie naruszony.[37] Innymi słowy, narzędzie przekazywania musi być skuteczne w praktyce.

29. "*Skuteczne*" oznacza zapewnienie, że przekazywane dane osobowe są chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w EOG.[38] Nie dzieje się tak, jeżeli podmiot odbierający dane nie jest w stanie wywiązać się ze swoich zobowiązań wynikających z wybranego narzędzia przekazywania na podstawie art. 46 RODO ze względu na przepisy i praktyki państwa trzeciego mające zastosowanie do przekazywania danych.

30. W związku z tym musisz ocenić, w stosownych przypadkach we współpracy z podmiotem odbierającym dane, czy w prawie lub praktyce państwa trzeciego istnieje coś, co może mieć wpływ na skuteczność odpowiednich zabezpieczeń narzędzia przekazywania z art. 46 RODO, na którym się opierasz, w kontekście konkretnego przekazania. W stosownych przypadkach podmiot odbierający dane powinien dostarczyć Ci odpowiednich źródeł i informacji dotyczących państwa trzeciego, w którym ma jednostkę organizacyjną, oraz przepisów mających zastosowanie do przekazywania danych. Można również odnieść się do innych źródeł informacji, takich jak te wymienione niewyczerpująco w Załączniku 3.[39]

31. Twoja ocena powinna uwzględniać wszystkie podmioty uczestniczące w przekazywaniu danych (np. administratorów, podmioty przetwarzające i podmioty podprzetwarzające w państwie trzecim), jak wskazano przy identyfikowaniu (ang. *mapping*) operacji przekazywania. Im więcej zaangażowanych administratorów, podmiotów przetwarzających lub podmiotów odbierających dane, tym bardziej skomplikowana będzie Twoja ocena. Należy w niej również uwzględnić wszelkie dalsze przekazanie, które może nastąpić.

---

[36] Więcej informacji na ten temat można znaleźć na stronie https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_pl.

[37] Artykuł 44 RODO.

[38] C-311/18 (Schrems II), pkt 105 i drugie stwierdzenie.

[39] Zob. również pkt 43 poniżej.

32. W tym celu należy zapoznać się z charakterystyką każdego przekazania i określić, w jaki sposób krajowy porządek prawny państwa, do którego dane są przekazywane (lub przekazywane dalej), ma zastosowanie do tego przekazania.

33. Ramy prawne mające zastosowanie będą zależały od okoliczności przekazywania, w szczególności od:

- Celów, dla których dane są przekazywane i przetwarzane (np. marketing, HR, przechowywanie, wsparcie informatyczne, badania kliniczne);
- Rodzajów podmiotów zaangażowanych w przetwarzanie (publiczne/prywatne; administrator/podmiot przetwarzający);
- Sektora, w którym następuje przekazywanie (np. sektor adtech, telekomunikacja, finanse itp.);
- Kategorii przekazywanych danych osobowych (np. dane osobowe dotyczące dzieci mogą wchodzić w zakres szczególnego ustawodawstwa państwa trzeciego);
- Tego, czy dane będą przechowywane w państwie trzecim lub czy istnieje tylko zdalny dostęp do danych przechowywanych w UE/EOG;
- Formatu przekazywanych danych (tj. w prostym /spseudonimizowanym lub zaszyfrowanym tekście[40]);
- Możliwości dalszego przekazywania danych z państwa trzeciego do innego państwa trzeciego.[41]

34. Spośród obowiązujących przepisów będziesz musiał ocenić, czy mają one jakikolwiek wpływ na zobowiązania zawarte w wybranym przez Ciebie narzędziu przekazywania danych na podstawie 46 RODO. Należy sprawdzić, czy zobowiązania umożliwiające osobom, których dane dotyczą, wykonywanie ich praw w kontekście międzynarodowego przekazywania danych (takie jak wnioski o dostęp, poprawienie i usunięcie przekazanych danych) mogą być skutecznie stosowane w praktyce i nie są udaremniane przez prawo w docelowym państwie trzecim.

35. Będziesz musiał ocenić odpowiednie przepisy o charakterze ogólnym w zakresie, w jakim mają one wpływ na skuteczne stosowanie zabezpieczeń zawartych w narzędziu przekazywania z art. 46 RODO oraz na prawa podstawowe osób fizycznych (w szczególności prawo do środka zaskarżenia przysługujące osobie, której dane dotyczą, w przypadku dostępu organów publicznych państw trzecich do przekazanych danych).

36. W każdym przypadku należy zwrócić szczególną uwagę na wszelkie odpowiednie przepisy, w szczególności określające wymogi udostępniania danych osobowych organom publicznym lub przyznające takim organom publicznym uprawnienia dostępu do danych osobowych (np. do celów egzekwowania prawa karnego, nadzoru regulacyjnego i bezpieczeństwa narodowego). Jeżeli te wymogi lub uprawnienia są ograniczone do tego, co jest niezbędne i proporcjonalne w demokratycznym społeczeństwie[42], nie mogą one wpływać na zobowiązania zawarte w narzędziu przekazywania z art. 46 RODO, na którym się opierasz.

37. Normy UE, takie jak art. 47 i 52 Karty praw podstawowych UE, muszą być stosowane jako odniesienie do oceny, czy taki dostęp władz publicznych jest ograniczony do tego, co jest

---

[40] Niektóre państwa trzecie nie zezwalają na odbieranie zaszyfrowanych danych.

[41] Jeżeli administrator udzielił uprzedniej szczegółowej lub ogólnej pisemnej zgody zgodnie z art. 28 ust. 2 RODO.

[42] Zob. art. 47 i 52 Karty praw podstawowych UE, 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_pl.

niezbędne i proporcjonalne w demokratycznym społeczeństwie oraz czy osobom, których dane dotyczą, zapewnia się skuteczne sądowe środki zaskarżenia.

38. Przy przeprowadzaniu tej oceny istotne są również różne aspekty systemu prawnego państwa trzeciego, np. elementy wymienione w art. 45 ust. 2 RODO.[43] Na przykład sytuacja w zakresie praworządności w państwie trzecim może mieć znaczenie dla oceny skuteczności dostępnych mechanizmów uzyskiwania przez osoby fizyczne (sądowych) środków zaskarżenia na bezprawny dostęp rządu do danych osobowych. Istnienie kompleksowego prawa o ochronie danych lub niezależnego organu ochrony danych, jak również przestrzeganie międzynarodowych instrumentów zapewniających zabezpieczenia w zakresie ochrony danych, może przyczynić się do zapewnienia proporcjonalnej ingerencji rządu.[44]

***

39. Zalecenia EROD w sprawie niezbędnych gwarancji europejskich zawierają elementy, które należy ocenić w celu ustalenia, czy ramy prawne regulujące dostęp organów publicznych w państwie trzecim do danych osobowych, będących agencjami bezpieczeństwa narodowego lub organami egzekwowania prawa, można uznać za uzasadnioną ingerencję (a zatem nie wpływającą na zobowiązania podjęte w ramach narzędzi przekazywania na podstawie art. 46 RODO) czy też nie. W szczególności należy to dokładnie rozważyć, gdy przepisy regulujące dostęp organów publicznych do danych są niejednoznaczne lub nie są dostępne publicznie.

40. W przypadku przekazywania danych w oparciu o narzędzia z art. 46, zalecenia EROD w sprawie niezbędnych gwarancji europejskich mogą stanowić wskazówkę dla podmiotu przekazującego i podmiotu odbierającego dane przy ocenie, czy takie uprawnienia w nieuzasadniony sposób ingerują w obowiązki podmiotu odbierającego dane w zakresie zapewnienia niezbędnej równoważności.

41. Brak merytorycznie równoważnego stopnia ochrony będzie szczególnie widoczny w przypadku, gdy ustawodawstwo lub praktyka państwa trzeciego, mające znaczenie dla Twojego przekazywania, nie spełniają wymogów niezbędnych gwarancji europejskich.

42. Twoja ocena musi opierać się przede wszystkim na publicznie dostępnym ustawodawstwie. Jednak w niektórych sytuacjach to nie wystarczy, ponieważ ustawodawstwo w państwach trzecich może być niewystarczające. W takim przypadku, jeśli nadal chcesz przewidzieć przekazanie danych, powinieneś przyjrzeć się innym istotnym i obiektywnym czynnikom[45], a nie polegać na subiektywnych czynnikach, takich jak prawdopodobieństwo dostępu organów publicznych do Twoich danych w sposób niezgodny z normami UE. Należy przeprowadzić tę ocenę z należytą starannością i dokładnie ją udokumentować, ponieważ zostaniesz rozliczony z decyzji, którą możesz podjąć na tej podstawie.[46]

43. Możesz uzupełnić swoją ocenę informacjami uzyskanymi z innych źródeł[47], takich jak:

- Elementy wykazujące, że organ państwa trzeciego będzie starał się uzyskać dostęp do

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

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

[45] Zob. pkt 43 poniżej oraz Załącznik 3.

[46] Art. 5 ust. 2 RODO.

[47] Zob. również Załącznik 3.

danych za wiedzą podmiotu odbierającego dane lub bez niej, w świetle zgłoszonych precedensów, przepisów i praktyk;

- Elementy wykazujące, że organ państwa trzeciego będzie mógł uzyskać dostęp do danych za pośrednictwem podmiotu odbierającego dane lub poprzez bezpośrednie przechwycenie kanału komunikacyjnego w świetle zgłoszonych precedensów, uprawnień oraz zasobów technicznych, finansowych i ludzkich, którymi dysponuje.

44. Twoja ocena może ostatecznie ujawnić, że narzędzie przekazywania z art. 46 RODO, na którym się opierasz, oraz odpowiednie zabezpieczenia w nim zawarte:

- Skutecznie zapewniają, aby przekazywane dane osobowe były chronione w państwie trzecim w stopniu merytorycznie równoważnym temu gwarantowanemu w EOG. Ustawodawstwo i praktyki państwa trzeciego mające zastosowanie do przekazania sprawiają, że podmiot odbierający dane jest w stanie wywiązać się ze swoich zobowiązań wynikających z wybranego narzędzia przekazywania. Należy dokonać ponownej oceny w odpowiednich odstępach czasu lub w przypadku pojawienia się znaczących zmian (zob. Krok 6).
- Nie zapewniają skutecznie merytorycznie równoważnego stopnia ochrony. Podmiot odbierający dane nie może wywiązać się ze swoich zobowiązań ze względu na ustawodawstwo lub praktyki państwa trzeciego mające zastosowanie do przekazywania danych. TSUE podkreślił, że w przypadku gdy narzędzia przekazywania danych zawarte w art. 46 RODO są niewystarczające, obowiązkiem podmiotu przekazującego dane jest wprowadzenie skutecznych środków uzupełniających lub nieprzekazywanie danych osobowych.[48]

TSUE orzekł na przykład, że art. 702 FISA nie odpowiada minimalnym wymogom związanym w prawie Unii z zasadą proporcjonalności i nie może być traktowany jako ograniczony do tego, co ściśle konieczne. Oznacza to, że stopień ochrony programów dozwolonych na mocy art. 702 FISA nie jest merytorycznie równoważny z zabezpieczeniami wymaganymi na mocy prawa UE. W konsekwencji, jeśli podmiot odbierający dane lub jakikolwiek dalszy odbiorca, któremu podmiot odbierający może je ujawnić, podlega art. 702 FISA[49], w przypadku takiego przekazywania można polegać na standardowych klauzulach ochrony danych lub innych narzędziach przekazywania z art. 46 RODO jedynie, jeżeli dodatkowe uzupełniające środki techniczne sprawiają, że dostęp do przekazanych danych jest niemożliwy lub nieskuteczny.

2.4 Krok 4: Przyjmij środki uzupełniające

45. Jeżeli ocena przeprowadzona przez Ciebie w ramach Kroku 3. wykaże, że Twoje narzędzie przekazywania danych wskazane w art. 46 RODO nie jest skuteczne, wówczas będziesz musiał

[48] C-311/18 (Schrems II), pkt 134-135.

[49] Art. 702 FISA 702 ma zastosowanie, jeżeli dane są uzyskiwane "od lub za pomocą dostawcy usług łączności elektronicznej" (art. 702 FISA = 50 USC § 1881a, lit. h) pkt 2 A ppkt (vi))), który z kolei jest zdefiniowany w 50 USC § 1881 lit. b) pkt 4) jako:

"(A) operator telekomunikacyjny, zgodnie z definicją tego terminu zawartą w sekcji 153 tytułu 47;

(B) dostawca usług łączności elektronicznej, zgodnie z definicją tego terminu zawartą w tytule 18 sekcja 2510;

(C) dostawca zdalnej usługi informatycznej, zgodnie z definicją tego terminu zawartą w sekcji 2711 tytułu 18;

(D) każdy inny podmiot świadczący usługi łączności, który ma dostęp do usług łączności przewodowej lub elektronicznej w formie, w jakiej taka komunikacja jest przekazywana lub w jakiej jest przechowywana; lub

(E) członek kadry kierowniczej, pracownik lub przedstawiciel podmiotu opisanego w punkcie (A), (B), (C) lub (D)".

rozważyć, w stosownych przypadkach we współpracy z podmiotem odbierającym dane, czy istnieją środki uzupełniające, które, dodane do zabezpieczeń zawartych w narzędziach przekazywania danych, mogłyby zapewnić, że przekazywane dane są chronione w państwie trzecim w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii.[50] "Środki uzupełniające" z definicji mają charakter uzupełniający w stosunku do zabezpieczeń przewidzianych dotychczasowo w art. 46 RODO.[51]

46. Przy stosowaniu konkretnego narzędzia przekazywania określonego w art. 46 RODO musisz określić w każdym indywidualnym przypadku, jakie środki uzupełniające mogłyby być skuteczne w odniesieniu do zbioru operacji przekazania danych do określonego państwa trzeciego. W oparciu o wcześniejsze oceny przeprowadzone w ramach Kroków 1, 2 i 3 powyżej, będziesz w stanie sprawdzić, na podstawie ich wyników, potencjalną skuteczność środków uzupełniających w zakresie zagwarantowania wymaganego stopnia ochrony.

47. Co do zasady, środki uzupełniające mogą mieć charakter umowny, techniczny lub organizacyjny. Połączenie różnych środków w sposób, w którym będą się nawzajem wspierać i wzmacniać, może zwiększyć stopień ochrony i w związku z tym przyczynić się do osiągnięcia unijnych standardów.

48. Same środki umowne i organizacyjne na ogół nie rozwiążą problemu dostępu do danych osobowych przez organy publiczne państwa trzeciego (w przypadku gdy w sposób nieuzasadniony koliduje to z obowiązkiem zapewnienia równoważności stopnia ochrony przez podmiot odbierający dane). Będą bowiem istniały sytuacje, w których jedynie środki techniczne mogą utrudniać lub uniemożliwiać organom publicznym państw trzecich skuteczny dostęp do danych osobowych, w szczególności do celów nadzoru.[52] W takich sytuacjach środki umowne lub organizacyjne mogą uzupełniać środki techniczne i wzmacniać ogólny stopień ochrony danych, np. poprzez tworzenie utrudnień dla prób uzyskania przez organy publiczne dostępu do danych w sposób niezgodny ze standardami UE.

49. W stosownych przypadkach, we współpracy z podmiotem odbierającym dane, możesz przyjrzeć się następującej (niewyczerpującej) liście czynników, aby określić, które środki uzupełniające byłyby najbardziej skuteczne w ochronie przekazywanych danych:

- Format przekazywanych danych (tj. w postaci zwykłego tekstu/ tekstu spseudonimizowanego lub zaszyfrowanego);
- Charakter danych;
- Długość i złożoność procesu przetwarzania danych, liczba podmiotów zaangażowanych w przetwarzanie oraz relacje między nimi (np. czy przekazywanie danych dotyczy wielu administratorów danych lub zarówno administratorów, jak i podmiotów przetwarzających dane, czy też udział podmiotów przetwarzających, które będą przekazywać dane od Ciebie do podmiotu odbierającego dane (z uwzględnieniem

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

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

[52] Tam, gdzie taki dostęp wykracza poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym; zob. art. 47 i 52 Karty Praw Podstawowych UE, art. 23 ust. 1 RODO oraz 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_pl.

odpowiednich przepisów mających do nich zastosowanie na mocy ustawodawstwa docelowego państwa trzeciego));[53]

– możliwość dalszego przekazywania danych w tym samym państwie trzecim lub nawet do innych państw trzecich (np. zaangażowanie podmiotów podprzetwarzających podmiotów odbierających dane[54]).

Przykłady środków uzupełniających

50. Niektóre przykłady środków technicznych, umownych i organizacyjnych, które można rozważyć, można znaleźć w niewyczerpujących wykazach w Załączniku 2.

***

51. Jeżeli wdrożyłeś skuteczne środki uzupełniające, które w połączeniu z wybranym narzędziem przekazywania, zgodnie z art. 46 RODO osiągają stopień ochrony, w stopniu merytorycznie równoważnym temu gwarantowanemu w ramach EOG: przekazywanie danych do państwa trzeciego może być kontynuowane.

52. Jeżeli nie jesteś w stanie znaleźć lub wdrożyć skutecznych środków uzupełniających, które zapewnią stopnień ochrony merytorycznie równoważny temu gwarantowanemu w ramach Unii[55], nie możesz rozpoczynać przekazywania danych osobowych do danego państwa trzeciego na podstawie narzędzia przekazywania z art. 46 RODO, na którym się opierasz. Jeżeli już przekazujesz dane, musisz zawiesić lub zakończyć przekazywanie danych osobowych.[56] Zgodnie z zabezpieczeniami zawartymi w narzędziu przekazywania z art. 46 RODO, na którym się opierasz, dane, które już zostały przekazane do tego państwa trzeciego, oraz ich kopie powinny zostać zwrócone lub zniszczone w całości przez podmiot odbierający dane.[57]

Przykład: prawo państwa trzeciego zabrania stosowania określonych przez Ciebie środków uzupełniających (np. zakazuje stosowania szyfrowania) lub w inny sposób uniemożliwia ich skuteczne stosowanie. Nie możesz rozpocząć przekazywania danych osobowych do tego państwa, lub musisz zakończyć dalsze przekazywanie danych do tego państwa.

53. Jeżeli zdecydujesz się na to, by kontynuować przekazywanie danych pomimo tego, że podmiot odbierający dane nie jest w stanie wywiązać się z zobowiązań wynikających z narzędzia przekazywania z art. 46 RODO, powinieneś powiadomić właściwy organ nadzorczy zgodnie ze szczegółowymi przepisami zawartymi w odpowiednim narzędziu przekazywania

[53] RODO nakłada odrębne zobowiązania na administratorów i podmioty przetwarzające. Przekazywanie może odbywać się od administratora do administratora, pomiędzy współadministratorami, od administratora do podmiotu przetwarzającego oraz, pod warunkiem uzyskania zgody administratora, od podmiotu przetwarzającego do administratora lub pomiędzy podmiotami przetwarzającymi.

[54] Por. przypis 25

[55] Tam, gdzie taki dostęp wykracza poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym; zob. art. 47 i 52 Karty praw podstawowych UE, art. 23 ust. 1 RODO oraz 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_pl.

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

[57] Por. Klauzula 12 w załączniku Decyzji Komisji 87/2010 w sprawie standardowych klauzul umownych; por. (opcjonalnie) Dodatkową klauzulę dot. wypowiedzenia w Załączniku B w Decyzji 2004/915/WE w sprawie standardowych klauzul umownych

z art. 46 RODO.[58] Właściwy organ nadzorczy zawiesi lub zabroni przekazywania danych w przypadkach, w których uzna, że nie można zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w Unii.[59]

54. Właściwy organ nadzorczy może nałożyć wszelkie inne środki naprawcze (np. administracyjną karę pieniężną), jeżeli rozpoczniesz lub będziesz kontynuował l przekazywanie danych, pomimo tego, że nie możesz w państwie trzecim wykazać stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w Unii.

2.5 Krok 5: Kroki proceduralne, jeśli zidentyfikowano skutecznie środki uzupełniające

55. Kroki proceduralne, które być może będziesz musiał podjąć w przypadku stwierdzenia, że skuteczne środki uzupełniające, które należy wprowadzić, mogą się różnić w zależności od narzędzia przekazywania z art. 46 RODO, którego używasz lub zamierzasz użyć.

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

56. Jeżeli masz zamiar wprowadzić środki uzupełniające poza standardowymi klauzulami ochrony danych, nie ma potrzeby zwracania się do właściwego organu nadzorczego o zezwolenie na dodanie tego rodzaju klauzul lub dodatkowych zabezpieczeń, o ile określone środki uzupełniające nie są sprzeczne, bezpośrednio lub pośrednio, ze standardowymi klauzulami i są wystarczające, aby zapewnić, że stopień ochrony gwarantowany przez RODO nie zostanie naruszony.[60] Podmioty przekazujący i odbierający dane muszą zapewnić, że dodatkowe klauzule nie mogą być interpretowane w żaden sposób ograniczający prawa i obowiązki w standardowych klauzulach ochrony danych ani w żaden inny sposób obniżający stopień ochrony danych. Musisz być w stanie to wykazać, w tym jednoznaczność wszystkich klauzul, zgodnie z zasadą rozliczalności i obowiązkiem zapewnienia wystarczającego stopnia ochrony danych. Właściwe organy nadzorcze są uprawnione do przeglądu tych klauzul dodatkowych w razie potrzeby (np. w przypadku skargi lub zapytania z własnej inicjatywy.

57. Jeżeli masz zamiar zmienić same standardowe klauzule ochrony danych lub jeżeli środki uzupełniające dodane są „sprzeczne" bezpośrednio lub pośrednio ze standardowymi klauzulami umownymi, nie uważa się już, że opierasz się na standardowych klauzulach umownych[61] i musisz wystąpić o zezwolenie do właściwego organu nadzorczego zgodnie z art. 46 ust. 3 lit. a) RODO.

---

[58] Por. Często zadawane pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-311/18 — Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillianowi Schremsowi przyjęte 23 lipca 2020 r., a w szczególności pytania 5, 6 i 9. Por. także Klauzulę 4(g) Decyzji Komisji 2010/87/UE; Klauzulę 5(a) Decyzji Komisji 2001/497/WE i Załącznik „Pakiet II" klauzulę II(c) Decyzji Komisji 2004/915/WE.

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

[60] Motyw 109 RODO stanowi, że "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 zostały zawarte standardowych klauzulach umownych przyjętych przez Komisję Europejską na mocy dyrektywy 95/45/WE.

[61] Por. analogicznie, przyjętą Opinię EROD 17/2020 w sprawie projektu standardowych klauzul umownych przedłożonego przez organ nadzorczy Słowenii (art. 28 ust. 8 RODO), która zawiera podobne postanowienie

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

58. Uzasadnienie przedstawione w wyroku w sprawie Schrems II ma również zastosowanie do innych instrumentów przekazywania zgodnie z art. 46 ust. 2 RODO, ponieważ wszystkie te instrumenty mają zasadniczo charakter umowny, a zatem przewidziane w nich gwarancje i zobowiązania podjęte przez strony nie mogą być wiążące dla organów publicznych państw trzecich.[62]

59. The Wyrok w sprawie Schrems II ma znaczenie dla przekazywania danych osobowych na podstawie wiążących reguł korporacyjnych, ponieważ przepisy krajów trzecich mogą wpływać na ochronę zapewnianą przez takie instrumenty. Dokładny wpływ wyroku w sprawie Schrems II na wiążące reguły korporacyjne jest nadal przedmiotem dyskusji. EROD przekaże bardziej szczegółowe informacje na temat tego, czy konieczne może być uwzględnienie dodatkowych zobowiązań w wiążących regułach korporacyjnych, odnosząc się do WP256/257, tak szybko jak będzie to możliwe.[63]

60. Trybunał podkreślił, że do obowiązków podmiotu przekazującego i podmiotu odbierającego dane należy ocena, czy stopień ochrony wymagany przez prawo UE jest przestrzegany w danym państwie trzecim, w celu ustalenia, czy gwarancje udzielone przez standardowe klauzule umowne lub wiążące reguły korporacyjne mogą być przestrzegane w praktyce. Jeśli tak nie jest, należy ocenić, czy można zapewnić środki uzupełniające w celu zapewnienia stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w ramach EOG, oraz czy prawo lub praktyka państwa trzeciego nie naruszy tych środków uzupełniających, pozbawiając je ich skuteczności.

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

61. Uzasadnienie przedstawione w wyroku w sprawie Schrems II ma również zastosowanie do innych instrumentów przekazywania zgodnie z art. 46 ust. 2 RODO, ponieważ wszystkie te instrumenty mają zasadniczo charakter umowny, a zatem przewidziane w nich gwarancje i zobowiązania podjęte przez strony nie mogą być wiążące dla organów publicznych państw trzecich.[64] Wyrok w sprawie Schrems II ma zatem znaczenie dla przekazywania danych osobowych na podstawie klauzul umownych ad hoc, ponieważ ustawodawstwa państw trzecich mogą wpływać na ochronę zapewnianą przez takie instrumenty. Dokładny wpływ wyroku w sprawie Schrems II na klauzule ad hoc jest nadal przedmiotem dyskusji. EROD przekaże w tej sprawie więcej szczegółów jak najszybciej będzie to możliwe.

(„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_pl.pdf.

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

[63] Dokument Roboczy Grupy Roboczej Art. 29 ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, ostatnio zmieniony i przyjęty w dniu 6 lutego 2018r., WP 256 rev.01; Dokument roboczy Grupy Roboczej Art. 29 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] C-311/18 (Schrems II), pkt 132.

2.6 Krok 6: Ponowna ocena w odpowiednich odstępach czasu

62. Musisz na bieżąco monitorować, w stosownych przypadkach we współpracy z podmiotami odbierającymi dane, rozwój sytuacji w państwie trzecim, do którego dane osobowe zostały przekazane, która może mieć wpływ na wstępną ocenę stopnia ochrony oraz decyzje, jakie zostały podjęte w związku z przekazaniem. Rozliczalność jest obowiązkiem o charakterze ciągłym (art. 5 ust. 2 RODO).

63. Powinieneś wprowadzić wystarczająco stabilne mechanizmy, aby zapewnić szybkie zawieszenie lub zakończenie przekazywania danych w sytuacji, gdy:

- podmiot odbierający dane naruszył lub nie jest w stanie uczynić zadość zobowiązaniom, które podjął w ramach narzędzia przekazywania określonego w art. 46 RODO; lub
- środki uzupełniające nie są już skuteczne w tym państwie trzecim.

3 WNIOSKI

64. RODO określa zasady przetwarzania danych osobowych w EOG, co pozwala na swobodne przemieszczanie danych osobowych w EOG. Rozdział V RODO reguluje przekazywanie danych osobowych do państw trzecich i stawia wysokie wymagania: przekazywanie nie może naruszać stopnia ochrony osób fizycznych zagwarantowanego w RODO (art. 44 RODO). Wyrok TSUE C-311/18 (Schrems II) podkreśla potrzebę zapewnienia ciągłości stopnia ochrony zapewnianej w ramach RODO, gdy dane osobowe są przekazywane do państwa trzeciego.[65]

65. Aby zapewnić merytorycznie równoważny stopień ochrony danych, musisz przede wszystkim być świadomy prowadzonych przez Ciebie operacji przekazywania. Musisz również sprawdzić, czy dane, które przekazujesz, są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane do i przetwarzane w państwie trzecim.

66. Musisz również określić narzędzia przekazywania, na których polegasz do celów Twoich operacji przekazywania danych. Jeśli narzędzie przekazywania nie jest objęte decyzją stwierdzającą odpowiedni stopień ochrony, musisz sprawdzić w każdym konkretnym przypadku, czy prawo lub praktyka docelowego państwa trzeciego nie narusza zabezpieczeń zawartych w art. 46 RODO w kontekście Twoich operacji przekazywania. W przypadku gdy samo narzędzie przekazywania danych z art. 46 RODO nie zapewnia, aby dane osobowe były chronione w stopniu merytorycznie równoważnym, środki uzupełniające mogą wypełnić tę lukę.

67. Jeżeli nie jesteś w stanie znaleźć lub wdrożyć skutecznych środków uzupełniających, które zapewnią, że przekazane dane będą chronione w stopniu merytorycznie równoważnym, nie możesz rozpoczynać przekazywania danych osobowych do danego państwa trzeciego na podstawie wybranego przez Ciebie narzędzia. Jeżeli już przekazujesz dane, musisz natychmiast zawiesić lub zakończyć przekazywanie danych osobowych.

68. Właściwy organ nadzorczy jest uprawniony do zawieszenia lub zakończenia przekazywania danych osobowych do państwa trzeciego, jeżeli ochrona przekazywanych danych wymagana przez prawo UE, w szczególności w art. 45 i 46 RODO oraz Karcie praw podstawowych, nie jest zapewniona.

W imieniu Europejskiej Rady Ochrony Danych
Przewodnicząca
(Andrea Jelinek)

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