Wytyczne 2/2020 w sprawie art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) rozporządzenia 2016/679 dotyczącego przekazywania danych osobowych między organami i podmiotami publicznymi z EOG i spoza EOG

Wersja 2.0

przyjęte 15 grudnia 2020 r.

Historia wersji

Wersja 2.0	15 grudnia 2020 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	18 lutego 2020 r.	Przyjęcie wytycznych do konsultacji publicznych

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

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

[1] Odniesienia do „państw członkowskich” zawarte w niniejszych wytycznych należy rozumieć jako odniesienia do „państw należących do EOG”.

1 UWAGI OGÓLNE

1.1 Cel

1. Niniejszy dokument ma na celu przedstawienie wytycznych dotyczących stosowania art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) ogólnego rozporządzenia o ochronie danych (RODO) w odniesieniu do przekazywania danych osobowych przez organy lub podmioty publiczne z EOG (zwane dalej „podmiotami publicznymi") do podmiotów publicznych w państwach trzecich lub organizacji międzynarodowych w zakresie, w jakim te podmioty lub organizacje nie są objęte przyjętą przez Komisję Europejską decyzją stwierdzającą odpowiedni stopień ochrony danych [2]. Podmioty publiczne mogą zdecydować się na skorzystanie z tych mechanizmów, które uznano w RODO za bardziej odpowiednie do ich sytuacji, ale mają również możliwość korzystania z innych stosownych narzędzi zapewniających odpowiednie zabezpieczenia zgodnie z art. 46 RODO.

2. Celem wytycznych jest przedstawienie oczekiwań Europejskiej Rady Ochrony Danych (EROD) w kwestii zabezpieczeń, które należy wprowadzić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi zgodnie z art. 46 ust. 2 lit. a) RODO, lub pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego za pomocą postanowień uzgodnień administracyjnych między podmiotami publicznymi zgodnie z art. 46 ust. 3 lit. b) RODO[3]. EROD zdecydowanie zaleca, aby strony stosowały wytyczne jako punkt odniesienia na wczesnym etapie, gdy planują podpisanie lub zmianę takich instrumentów lub uzgodnień[4].

3. Wytyczne należy odczytywać w związku z innymi wcześniejszymi pracami EROD (w tym z dokumentami zatwierdzonymi przez podmiot będący jej poprzednikiem, Grupę Roboczą Art. 29[5]) na temat głównych kwestii dotyczących zakresu terytorialnego i przekazywania danych osobowych do państw trzecich[6]. Wytyczne zostaną poddane przeglądowi i, w razie konieczności, zaktualizowane w oparciu o praktyczne doświadczenia zdobyte w wyniku stosowania RODO.

4. Niniejsze wytyczne obejmują międzynarodowe przekazywanie danych między podmiotami publicznymi odbywające się w różnych celach związanych ze współpracą administracyjną wchodzących w zakres RODO. W związku i zgodnie z art. 2 ust. 2 RODO wytyczne te nie obejmują przekazywania danych w obszarze bezpieczeństwa publicznego, obrony lub bezpieczeństwa państwa. Nie dotyczą one również przetwarzania i przekazywania danych przez właściwe organy w celu ścigania przestępstw, ponieważ takie przetwarzanie i przekazywanie danych jest regulowane odrębnym szczegółowym instrumentem prawnym– dyrektywą 2016/680[7]. Ponadto, w wytycznych skoncentrowano się

[2] Na przykład japońskie podmioty publiczne, które nie są objęte decyzją stwierdzającą odpowiedni stopień ochrony w Japonii, ponieważ dotyczy ona wyłącznie organizacji sektora prywatnego.
[3] W niniejszych wytycznych termin „umowy międzynarodowe" oznacza prawnie wiążące i egzekwowalne instrumenty, o których mowa w art. 46 ust. 2 lit. a) RODO, oraz uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b) RODO.
[4] Art. 96 RODO stanowi, że umowy, które zostały zawarte przed 24 maja 2016 r., pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.
[5] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych ustanowiona na mocy art. 29 dyrektywy o ochronie danych 95/46/WE.
[6] Zob. dokument Grupy Roboczej Art. 29 zatytułowany „Odpowiedni stopień ochrony przekazywanych danych osobowych" (WP 254 rev. 01, zatwierdzony przez EROD w dniu 25 maja 2018 r.), wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679 oraz wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO (art. 3).
[7] Dyrektywa (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości,

wyłącznie na przekazywaniu danych między podmiotami publicznymi i nie obejmują one przekazywania danych osobowych z podmiotu publicznego do podmiotu prywatnego lub z podmiotu prywatnego do podmiotu publicznego.

1.2 Zasady ogólne mające zastosowanie do międzynarodowego przekazywania danych

5. Zgodnie z art. 44 RODO podmiot przekazujący dane osobowe do państw trzecich lub organizacji międzynarodowych musi nie tylko przestrzegać przepisów zawartych w rozdziale V RODO, ale również spełniać warunki określone w pozostałych przepisach RODO. W szczególności każda czynność przetwarzania musi być zgodna z zasadami ochrony danych określonymi w art. 5 RODO, zgodna z prawem, jak określono w art. 6 RODO, oraz zgodna z art. 9 RODO w przypadku szczególnych kategorii danych. W związku z tym każda czynność musi spełniać dwa warunki: po pierwsze, podstawa prawna musi mieć zastosowanie do przetwarzania danych jako takiego wraz ze wszystkimi właściwymi przepisami RODO; a po drugie, należy przestrzegać przepisów rozdziału V RODO.

6. Art. 46 RODO stanowi, że „w razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że dostępne są egzekwowalne prawa osób, których dane dotyczą oraz skuteczne środki ochrony prawnej.” Takie odpowiednie zabezpieczenia można zapewnić za pomocą prawnie wiążącego i egzekwowalnego instrumentu między podmiotami publicznymi (art. 46 ust. 2 lit. a) RODO) lub – pod warunkiem uzyskania zezwolenia właściwego organu nadzorczego – za pomocą postanowień uzgodnień administracyjnych między podmiotami publicznymi, w których przewidziane będą skuteczne i egzekwowalne prawa osób, których dane dotyczą (art. 46 ust. 3 lit. b) RODO). Jak wyjaśnił Trybunał Sprawiedliwości Unii Europejskiej (TSUE), takie odpowiednie zabezpieczenia powinny gwarantować, by prawa przysługujące osobom, których dane są przekazywane, korzystały ze stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w EOG[8].

7. Niezależnie od tego rozwiązania jak i w przypadku jego niestosowania, w art. 49 RODO określono również ograniczoną liczbę szczególnych sytuacji, w których międzynarodowe przekazywanie danych może mieć miejsce, w przypadku braku stwierdzenia przez Komisję Europejską zapewniania odpowiedniego poziomu ochrony[9]. W szczególności jeden z wyjątków dotyczy przekazania niezbędnego ze względu na ważne względy interesu publicznego uznanego w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, w tym w duchu zasady wzajemności w ramach współpracy międzynarodowej[10]. Jak jednak wyjaśniono w poprzednich opublikowanych przez EROD wytycznych, wyjątki przewidziane w art. 49 RODO należy interpretować w sposób zawężający i muszą one dotyczyć głównie przetwarzania, które jest sporadyczne i niepowtarzające się[11].

1.3 Definicja organu lub podmiotu publicznego

prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych.

[8] Wyrok TSUE w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II”), pkt 96.

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

[10] Zob. Wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 10.

[11] Zob. Wytyczne EROD w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, s. 5.

8. W RODO nie zdefiniowano pojęcia „organ lub podmiot publiczny”. EROD uważa, że pojęcie to jest wystarczająco szerokie, aby mogło objąć zarówno podmioty publiczne w państwach trzecich, jak i organizacje międzynarodowe[12]. W przypadku podmiotów publicznych w państwach trzecich pojęcie to należy rozumieć zgodnie z prawem krajowym. W związku z tym do podmiotów publicznych zaliczają się organy rządowe różnych szczebli (np. władze krajowe, regionalne i lokalne), ale mogą to być również inne podmioty prawa publicznego (np. agencje wykonawcze, uniwersytety, szpitale itp.)[13]. Zgodnie z art. 4 pkt 26 RODO „organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

9. EROD przypomina, że RODO stosuje się, nie naruszając przepisów prawa międzynarodowego, takich jak przepisy regulujące przywileje i immunitety organizacji międzynarodowych. Jednocześnie należy pamiętać, że każdy podmiot publiczny z EOG przekazujący dane organizacjom międzynarodowym musi przestrzegać przepisów RODO dotyczących przekazywania danych do państw trzecich lub organizacji międzynarodowych[14].

2 OGÓLNE ZALECENIA DOTYCZĄCE ODPOWIEDNICH ZABEZPIECZEŃ ZAPEWNIANYCH NA MOCY ART. 46 UST. 2 LIT. a) I ART. 46 UST. 3 LIT. b) RODO

10. W przeciwieństwie do art. 26 ust. 2 dyrektywy 95/46/WE w art. 46 RODO przewidziano dodatkowe odpowiednie zabezpieczenia jako narzędzia przekazywania danych między podmiotami publicznymi, mianowicie:

    (i) prawnie wiążący i egzekwowalny instrument, zgodnie z art. 46 ust. 2 lit. a) RODO, lub
    (ii) postanowienia uzgodnień administracyjnych, zgodnie z art. 46 ust. 3 lit. b) RODO.

    Takie instrumenty i uzgodnienia mogą mieć charakter dwustronny lub wielostronny.

11. W poniższej sekcji przedstawiono pewne ogólne zalecenia, które mają pomóc w zapewnieniu zgodności z RODO prawnie wiążących instrumentów lub uzgodnień administracyjnych (zwanych dalej „umowami międzynarodowymi”) między podmiotami publicznymi.

12. Chociaż art. 46 i motyw 108 RODO nie zawierają konkretnych wskazówek dotyczących gwarancji, które należy zawrzeć w takich umowach międzynarodowych, uwzględniając art. 44 RODO[15] i najnowsze orzecznictwo TSUE[16], EROD opracowała wykaz minimalnych zabezpieczeń, które należy zawrzeć w umowach międzynarodowych między podmiotami publicznymi objętymi zakresem art. 46 ust. 2 lit. a) lub art. 46 ust. 3 lit. b) RODO. Zabezpieczenia te mają na celu zapewnienie, aby nie został naruszony stopień ochrony osób fizycznych przewidziany w RODO, gdy ich dane osobowe są

[12] Zob. również motyw 108 RODO.
[13] Zob. np. definicje „organu sektora publicznego” „podmiotu prawa publicznego” w art. 2 pkt 1 i 2 dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).
[14] Zob. Wytyczne EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO, s. 23.
[15] Art. 44 RODO stanowi: „Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu.”
[16] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II”).

przekazywane poza EOG, oraz aby stopień ochrony osób, których dane dotyczą, był merytorycznie równoważny temu zagwarantowanemu w UE przez RODO[17].

13. Zgodnie z najnowszym orzecznictwem TSUE[18] obowiązkiem przekazującego podmiotu publicznego w państwie członkowskim jest przeprowadzenie oceny, w razie potrzeby z pomocą otrzymującego podmiotu publicznego, czy w państwie trzecim zachowany jest stopień ochrony wymagany prawem Unii, celem ustalenia, czy przestrzeganie wykazu zabezpieczeń zawartego w umowie międzynarodowej będzie możliwe w praktyce, uwzględniając ewentualny wpływ prawodawstwa państwa trzeciego na przestrzeganie tych zabezpieczeń.

14. W tym względzie należy również zauważyć, że w celu zagwarantowania zabezpieczeń wymienionych w niniejszych wytycznych, umowy międzynarodowe mogą opierać się na już istniejących elementach prawa krajowego państwa trzeciego lub na przepisach wewnętrznych/ramach regulacyjnych organizacji międzynarodowej.

2.1 Cel i zakres

15. W umowach międzynarodowych należy zdefiniować ich zakres, a cele tych umów należy określić jednoznacznie i szczegółowo. Ponadto, należy jasno określić kategorie danych osobowych, których umowy te dotyczą, oraz rodzaj przetwarzania danych osobowych, które są przekazywane i przetwarzane na podstawie umowy.

2.2 Definicje

16. Umowy międzynarodowe powinny zawierać zgodne z RODO definicje podstawowych pojęć i praw dotyczących danych osobowych, które są istotne dla danej umowy. Przykładowo, takie umowy powinny zawierać definicje następujących istotnych terminów, jeżeli takie terminy w nich występują: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający", „odbiorca" i „dane wrażliwe".

2.3 Zasady ochrony danych

17. Umowy międzynarodowe muszą zawierać konkretne sformułowania zobowiązujące obie strony do zapewnienia przestrzegania podstawowych zasad ochrony danych.

2.3.1 Zasada ograniczenia celu

18. W umowach międzynarodowych należy określić cele, w których dane osobowe mają być przekazywane i przetwarzane, w tym cele dalszego przetwarzania zgodne z celami, w których dane osobowe zostały pierwotnie zebrane, a także należy w nich zapewnić, aby dane nie były przetwarzane dalej w celach niezgodnych z pierwotnymi celami. Cele zgodne z pierwotnymi celami mogą obejmować przechowywanie danych do celów archiwalnych w interesie publicznym, jak również przetwarzanie danych do celów badań naukowych lub historycznych lub do celów statystycznych. Dla większej jasności zaleca się, by konkretne cele przetwarzania i przekazywania danych zostały wymienione w treści umowy międzynarodowej.

[17] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 105.
[18] Tamże.

19. Aby uniknąć ryzyka „zmiany celu”, w takich umowach należy również sprecyzować, że przekazywanych danych nie można wykorzystywać do żadnych innych celów niż te wyraźnie wymienione w umowie, z wyjątkiem przypadków określonych w poniższym punkcie.

20. Jeżeli obie strony umowy międzynarodowej chcą zezwolić otrzymującemu podmiotowi publicznemu na inne, zgodne z przepisami wykorzystywanie przekazanych danych osobowych, dalsze wykorzystywanie przez otrzymujący podmiot publiczny jest dozwolone jedynie wtedy, gdy jest zgodne z pierwotnym wykorzystywaniem i zostało wcześniej zgłoszone przekazującemu podmiotowi publicznemu, który może wyrazić sprzeciw z określonych powodów.

2.3.2 Zasady prawidłowości i minimalizacji danych

21. Umowa międzynarodowa musi określać, że przekazywane i dalej przetwarzane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przekazywane i dalej przetwarzane.

22. W praktyce istotnym celem tej zasady minimalizacji danych jest uniknięcie przekazywania danych osobowych, gdy są one nieadekwatne lub nadmierne.

23. Ponadto, dane powinny być prawidłowe i aktualne, z uwzględnieniem celów, w których są przetwarzane. Umowa międzynarodowa musi zatem stanowić, że strona przekazująca zapewni, aby dane osobowe przekazywane na mocy umowy były prawidłowe i, w stosownych przypadkach, aktualne. Ponadto umowa powinna stanowić, że jeżeli jedna ze stron zauważy, że przekazano lub przetwarza się nieprawidłowe lub nieaktualne dane, musi bezzwłocznie powiadomić o tym drugą stronę. Ponadto umowa powinna zapewniać, aby w przypadku potwierdzenia, że przekazane lub przetwarzane dane są nieprawidłowe, każda ze stron przetwarzających dane podjęła wszelkie zasadne działania w celu sprostowania lub usunięcia tych informacji.

2.3.3 Zasada ograniczenia przechowywania

24. Strony muszą zapewnić, aby umowa międzynarodowa zawierała klauzulę dotyczącą zatrzymywania danych. W klauzuli tej należy w szczególności sprecyzować, że danych osobowych nie zatrzymuje się na czas nieokreślony, ale przechowuje się je w formie umożliwiającej identyfikację osób, których dane dotyczą, jedynie przez okres niezbędny do celów, w których dane te zostały przekazane, a następnie przetwarzane. Może to obejmować przechowywanie danych tak długo, jak jest to konieczne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, pod warunkiem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą, takie jak dodatkowe środki techniczne (np. środki bezpieczeństwa, pseudonimizacja) i ograniczenia dostępu. Jeżeli w prawodawstwie krajowym lub w przepisach wewnętrznych/ramach regulacyjnych organizacji międzynarodowej nie określono jeszcze maksymalnego okresu zatrzymywania, należy go określić w tekście umowy.

2.3.4 Bezpieczeństwo i poufność danych

25. Strony powinny zobowiązać się do zapewnienia bezpieczeństwa i poufności prowadzonego przez siebie przetwarzania i przekazywania danych osobowych.
W szczególności strony powinny zobowiązać się do wprowadzenia odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem dostępem, zniszczeniem, utratą, modyfikacją lub nieuprawnionym ujawnieniem. Środki te mogą obejmować na przykład szyfrowanie, w tym w trakcie przekazywania,

pseudonimizację, oznaczanie informacji jako danych osobowych przekazywanych z EOG, ograniczenie zakresu osób mających dostęp do danych osobowych, zapewnienie bezpiecznego przechowywania danych osobowych lub wdrożenie zasad mających na celu zapewnienie, aby dane osobowe były przechowywane w sposób bezpieczny i poufny.
Poziom bezpieczeństwa powinien uwzględniać zagrożenia, stan wiedzy technicznej oraz związane z tym koszty.

26. Umowa międzynarodowa może ponadto stanowić, że jeśli jedna ze stron dowie się o naruszeniu ochrony danych osobowych, poinformuje o tym jak najszybciej drugą stronę (lub pozostałe strony) oraz zastosuje rozsądne i odpowiednie środki w celu zaradzenia naruszeniu ochrony danych osobowych i zminimalizowania potencjalnych niekorzystnych skutków, w tym poprzez zawiadomienie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeśli to naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw i wolności osoby fizycznej.
Zaleca się, aby w umowie międzynarodowej określono termin zgłoszenia naruszenia ochrony danych osobowych, a także procedury zawiadomienia osoby, której dane dotyczą.

2.4 Prawa osób, których dane dotyczą

27. Umowa międzynarodowa musi gwarantować egzekwowalne i skuteczne prawa osób, których dane dotyczą, jak określono w art. 46 ust. 1 i motywie 108 RODO.

28. W umowie należy wymienić prawa przysługujące osobom, których dane dotyczą, w tym konkretne zobowiązania podjęte przez strony w celu zapewnienia takich praw. Aby umowa międzynarodowa była skuteczna, musi przewidywać mechanizmy zapewniające stosowanie ich w praktyce. Ponadto każde naruszenie praw osób, których dane dotyczą, musi pociągać za sobą odpowiedni środek zaradczy.

2.4.1 Prawo do przejrzystości

29. Strony muszą zadbać o to, aby umowa międzynarodowa zawierała jasne sformułowania opisujące obowiązki stron w zakresie przejrzystości.

30. Obowiązki te powinny obejmować m.in. ogólną informację wskazującą co najmniej, jak i dlaczego podmioty publiczne mogą przetwarzać i przekazywać dane osobowe, dane narzędzie wykorzystywane do przekazywania danych, podmioty, do których dane te można przekazywać, prawa przysługujące osobom, których dane dotyczą, i obowiązujące ograniczenia, dostępne mechanizmy zaskarżenia oraz dane kontaktowe służące do zgłaszania sporów lub roszczeń.

31. Należy jednak pamiętać, że w przypadku przekazującego podmiotu publicznego nie wystarczy ogólna informacja umieszczona na stronie internetowej tego podmiotu publicznego. Przekazujący podmiot publiczny powinien podawać odpowiednie informacje każdej osobie, której dane dotyczą, zgodnie z obowiązkami informacyjnymi określonymi w art. 13 i 14 RODO[19].
W umowie międzynarodowej można również wskazać pewne wyjątki od podawania takich informacji. Wyjątki te są ograniczone i powinny być zgodne z wyjątkami przewidzianymi w art. 14 ust. 5 RODO – na przykład mogą dotyczyć sytuacji, w której osoba, której dane dotyczą, dysponuje już tymi informacjami lub gdy udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

[19] Zob. Wytyczne EROD w sprawie przejrzystości na podstawie rozporządzenia 2016/679, GR 260 rev. 01, s. 13–22.

32. Strony muszą się zobowiązać do udostępnienia umowy międzynarodowej osobom, których dane dotyczą, na ich wniosek oraz do podania umowy międzynarodowej lub odpowiednich postanowień przewidujących odpowiednie zabezpieczenia do wiadomości publicznej na swojej stronie internetowej. W zakresie niezbędnym do ochrony informacji szczególnie chronionych lub innych informacji poufnych, przed przekazaniem kopii umowy lub jej publicznym udostępnieniem, z tekstu umowy międzynarodowej można usunąć odpowiednie informacje. W stosownych przypadkach, aby umożliwić osobie, której dane dotyczą, zrozumienie treści umowy międzynarodowej, strony muszą przedstawić zrozumiałe streszczenie tej umowy.

2.4.2 Prawo dostępu do danych, ich sprostowania, usunięcia i ograniczenia przetwarzania danych oraz prawo do sprzeciwu

33. Umowa międzynarodowa powinna zabezpieczać prawo osoby, której dane dotyczą, do uzyskania informacji o wszystkich przetwarzanych danych osobowych, które jej dotyczą, i dostępu do tych danych, prawo do sprostowania i usunięcia tych danych, prawo do ograniczenia przetwarzania danych oraz, w stosownych przypadkach, prawo do sprzeciwu wobec przetwarzania danych z przyczyn związanych z jej szczególną sytuacją.

34. W kwestii prawa dostępu, w umowie międzynarodowej należy sprecyzować, że osoby fizyczne są uprawnione do uzyskania od otrzymującego podmiotu publicznego potwierdzenia, czy przetwarzane są dane osobowe, które ich dotyczą, a jeżeli ma to miejsce, są uprawnione do uzyskania dostępu do tych danych; a także do uzyskania konkretnych informacji dotyczących przetwarzania, takich jak cel przetwarzania, kategorie przetwarzanych danych osobowych, odbiorcy, którym dane osobowe są ujawniane, przewidywany okres przechowywania i dostępne środki zaskarżenia.

35. W umowie należy ponadto wskazać, kiedy można powołać się na te prawa, oraz określić tryb wykonywania praw przez osoby, których dane dotyczą, wobec obu stron, a także sposób postępowania stron w przypadku otrzymania takich wniosków. Na przykład w odniesieniu do usuwania, umowa międzynarodowa może stanowić, że dane należy usunąć, jeżeli informacje były przetwarzane niezgodnie z prawem lub nie są już niezbędne do celów przetwarzania. Ponadto, w umowie międzynarodowej należy określić, że strony odpowiedzą na żądania osób, których dane dotyczą, w rozsądny i terminowy sposób. W umowie międzynarodowej można również wskazać, że strony mogą podjąć odpowiednie działania, w tym pobrać opłatę w rozsądnej wysokości w celu pokrycia kosztów administracyjnych, jeżeli żądania osoby, której dane dotyczą, są w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swoją powtarzalność.

36. W umowie międzynarodowej należy również określić obowiązek przekazującego podmiotu publicznego udzielenia bez zbędnej zwłoki informacji osobie, której dane dotyczą – po przekazaniu dotyczących jej danych osobowych – na temat działań podjętych w związku z jej żądaniem na podstawie praw przewidzianych w tejże umowie międzynarodowej, a w tym celu należy określić w niej odpowiedni termin (np. jeden miesiąc). Ponadto, jeżeli strony nie podejmą działań w związku z żądaniem osoby, której dane dotyczą, wówczas taką osobę należy niezwłocznie – tj. w określonym odpowiednim terminie (np. w terminie miesiąca od otrzymania żądania) – poinformować o powodach niepodjęcia działań oraz o możliwości wniesienia skargi oraz skorzystania ze środków ochrony prawnej przed sądem.

37. W umowie międzynarodowej można również przewidzieć wyjątki od tych praw. Na przykład można określić wyjątki od prawa dostępu i prawa do usunięcia danych, takie jak te przewidziane w art. 15 ust. 4 i art. 17 ust. 3 RODO. Podobnie można przewidzieć wyjątki od praw indywidualnych w przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych, do celów

statystycznych lub do celów archiwalnych, o ile prawdopodobne jest, że takie prawa uniemożliwią lub poważnie utrudnią realizację celów takiego przetwarzania, oraz pod warunkiem zapewnienia odpowiednich zabezpieczeń (np. środków technicznych i organizacyjnych, w tym pseudonimizacji). Co więcej, umowa może stanowić, że strony mogą odmówić podjęcia działania w związku z żądaniem, które jest ewidentnie nieuzasadnione lub nadmierne.

2.4.3 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

38. W stosownych przypadkach w odniesieniu do przedmiotowej umowy, umowy międzynarodowe zasadniczo powinny zawierać klauzulę stanowiącą, że otrzymujący podmiot publiczny nie podejmie decyzji wyłącznie na podstawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, która to decyzja wywołuje wobec danej osoby, której dane dotyczą, skutki prawne lub w podobny sposób istotnie na nią wpływa. Jeżeli cel przekazywania danych wiąże się z możliwością podejmowania przez otrzymujący podmiot publiczny decyzji wyłącznie w oparciu o zautomatyzowane przetwarzanie w rozumieniu art. 22 RODO, powinno to nastąpić wyłącznie na określonych warunkach wskazanych w danej umowie międzynarodowej, na przykład konieczności uzyskania wyraźnej zgody osoby, której dane dotyczą. Jeżeli dana decyzja nie spełnia określonych warunków, osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać takiej decyzji. Jeżeli w danej umowie międzynarodowej dopuszcza się zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, wówczas w każdym przypadku w takiej umowie należy zapewnić niezbędne zabezpieczenia, w tym prawo do uzyskania informacji o konkretnych powodach wydania decyzji i zasadach jej podjęcia, prawo do poprawienia nieprawidłowych informacji lub uzupełnienia niekompletnych informacji oraz prawo do zakwestionowania decyzji i prawo do uzyskania interwencji ludzkiej.

2.4.4 Prawo dochodzenia roszczeń

39. Chronione prawa osoby, której dane dotyczą, muszą być egzekwowalne i skuteczne. Z tego względu osoba, której dane dotyczą, musi mieć dostęp do środków zaskarżenia. Poniżej, w sekcji 2.7 i 3, przedstawiono różne przykładowe sposoby zapewnienia mechanizmów zaskarżenia.

2.4.5 Ograniczenia praw osób, których dane dotyczą

40. W umowie międzynarodowej należy również przewidzieć ograniczenia praw osób, których dane dotyczą. Ograniczenia te powinny być zgodnie z ograniczeniami przewidzianymi w art. 23 RODO. Takie ograniczenie musi być środkiem niezbędnym i proporcjonalnym w demokratycznym społeczeństwie służącym ważnym celom leżącym w interesie publicznym zgodnym z celami wymienionymi w art. 23 ust. 1 RODO, takimi jak prawa i wolności innych osób, bezpieczeństwo narodowe, obrona lub zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych. Ograniczenie musi być określone w prawie lub, w przypadku organizacji międzynarodowych, w mających zastosowanie przepisach wewnętrznych/ramach regulacyjnych i obowiązywać wyłącznie przez okres, w którym istnieje powód jego stosowania.

2.5 Ograniczenia dotyczące dalszego przekazywania i udostępniania danych (w tym ujawniania i dostępu administracji rządowej)

41. W umowie międzynarodowej należy co do zasady wyraźnie wykluczyć dalsze przekazywanie danych przez otrzymujący podmiot publiczny lub otrzymującą organizację międzynarodową odbiorcom

niezwiązanym daną umową. W zależności od przedmiotu sprawy i konkretnych okoliczności strony mogą uznać, że dalsze przekazywanie danych jest konieczne. W takim przypadku, jeżeli spełniona jest zasada ograniczenia celu[20], umowa międzynarodowa powinna stanowić, że takie dalsze przekazywanie jest możliwe wyłącznie wówczas, gdy przekazujący podmiot publiczny udzielił uprzednio wyraźnej zgody, a otrzymujące strony trzecie zobowiązały się do przestrzegania zasad i zabezpieczeń w zakresie ochrony danych odpowiadających zasadom i zabezpieczeniom określonym w danej umowie międzynarodowej. Obejmuje to zobowiązanie do zapewnienia osobom, których dane dotyczą, tych samych praw i gwarancji w zakresie ochrony danych co w danej umowie międzynarodowej w celu dopilnowania, aby w przypadku dalszego przekazywania danych nie doszło do obniżenia stopnia ochrony.

42. Zasadniczo w odniesieniu do udostępniania danych osobowych w tym samym państwie zastosowanie powinny mieć te same zabezpieczenia co w przypadku dalszego przekazywania, tj. w umowie międzynarodowej należy wykluczyć takie dalsze udostępnianie, a odstępstwa zasadniczo należy dopuścić wyłącznie wówczas, gdy przekazujący podmiot publiczny udzielił uprzednio wyraźnej zgody, a otrzymujące strony trzecie zobowiązały się do przestrzegania zasad i zabezpieczeń w zakresie ochrony danych odpowiadających zasadom i zabezpieczeniom określonym w danej umowie międzynarodowej.

43. Zaleca się, aby przed zwróceniem się do przekazującego podmiotu publicznego z wnioskiem o udzielenie wyraźnej zgody otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa przedstawiły wystarczające informacje na temat rodzaju danych osobowych, które zamierzają przekazać/udostępnić, przyczyn i celów, ze względu na które uznały, że niezbędne jest przekazanie/udostępnienie danych osobowych oraz w przypadku dalszego przekazywania – informacje na temat państw lub organizacji, do których zamierzają dalej przekazać dane osobowe, co ma umożliwić ocenę przepisów danego państwa trzeciego lub, w przypadku organizacji międzynarodowych, mających zastosowanie przepisów wewnętrznych/ram regulacyjnych.

44. Jeżeli niezbędne jest dopuszczenie udostępnienia danych osobowych stronie trzeciej w państwie otrzymującego podmiotu publicznego lub innej organizacji międzynarodowej, w określonych okolicznościach można dopuścić udostępnienie danych za uprzednią wyraźną zgodą przekazującego podmiotu publicznego albo pod warunkiem, że otrzymująca strona trzecia w sposób wiążący zobowiązała się do przestrzegania zasad i gwarancji zawartych w danej umowie międzynarodowej.

45. Ponadto w umowie międzynarodowej można określić wyjątkowe okoliczności, w których dalsze udostępnianie jest możliwe bez uprzedniej zgody lub wyżej wspomnianych zobowiązań zgodnie z wyjątkami wymienionymi w art. 49 RODO, na przykład jeżeli takie szczególne udostępnienie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, lub też niezbędne do ustalenia, dochodzenia lub ochrony roszczeń. Tego rodzaju wyjątkowe okoliczności mogą występować również wówczas, gdy dalsze udostępnianie jest konieczne na mocy prawa strony otrzymującej na potrzeby bezpośrednio powiązanych postępowań przygotowawczych/sądowych.

46. W przypadkach wymienionych w powyższym punkcie w umowie międzynarodowej należy wyraźnie określić szczególne i wyjątkowe okoliczności, w których dopuszcza się tego rodzaju udostępnianie danych. Przed udostępnieniem danych otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa powinny być również zobowiązane do powiadomienia o tym fakcie przekazującego podmiotu publicznego i przedstawienia mu informacji na temat udostępnianych danych, otrzymującej strony trzeciej i podstawy prawnej udostępniania. Z kolei przekazujący podmiot publiczny powinien

[20] Zob. powyżej w sekcji 2.3.1.

prowadzić rejestr takich powiadomień od otrzymującego podmiotu publicznego lub otrzymującej organizacji międzynarodowej i przekazywać te informacje na żądanie swojemu organowi nadzorczemu. Jeżeli takie powiadomienie poprzedzające udostępnienie będzie stanowiło naruszenie obowiązków zachowania poufności przewidzianych w prawie, np. obowiązku zachowania poufności postępowania przygotowawczego, konkretne informacje należy przekazać najszybciej jak to możliwe po udostępnieniu. W takim przypadku przekazujący podmiot powinien regularnie otrzymywać ogólne informacje na temat rodzaju wniosków, jakie wpłynęły w określonym okresie, w tym informacje na temat kategorii danych, których dotyczyły wnioski, podmiotu składającego wniosek oraz podstawy prawnej ujawnienia danych.

47. We wszystkich powyższych scenariuszach umowa międzynarodowa powinna dopuszczać ujawnienie danych osobowych innym organom publicznym w państwie trzecim otrzymującego podmiotu publicznego wyłącznie w stopniu, który jest niezbędny i proporcjonalny w demokratycznym społeczeństwie do ochrony ważnych celów leżących w ogólnym interesie publicznym zgodnych z celami wymienionymi w art. 23 ust. 1 RODO oraz zgodnie z orzecznictwem TSUE. Aby przeprowadzić ocenę ewentualnego dostępu organów publicznych państwa trzeciego do celów nadzoru, przekazujący organ publiczny powinien uwzględnić elementy przypomniane w czterech niezbędnych gwarancjach europejskich[21]. Elementy te obejmują między innymi dostęp osób, których dane dotyczą, do skutecznych środków ochrony w państwie trzecim otrzymującego podmiotu publicznego w sytuacji, w której dostęp do ich danych osobowych mają organy publiczne[22]. Jeżeli dane przekazuje się organizacjom międzynarodowym, w każdym przypadku taki dostęp musi być zgodny z prawem międzynarodowym publicznym i bez uszczerbku w szczególności dla przywilejów i immunitetów danej organizacji międzynarodowej.

48. W zależności od konkretnego przypadku warto stosować wymóg dołączenia do umowy międzynarodowej załącznika zawierającego wykaz przepisów regulujących dalsze udostępnianie innym podmiotom publicznym, w tym do celów nadzoru w państwie przeznaczenia. O wszelkich zmianach tego załącznika należy powiadomić stronę przekazującą w określonym terminie.

2.6 Dane wrażliwe

49. Jeżeli w umowie międzynarodowej przewidziano przekazywanie danych wrażliwych w rozumieniu art. 9 ust. 1 RODO, należy uwzględnić dodatkowe zabezpieczenia dotyczące szczególnych rodzajów ryzyka, jakie otrzymujący podmiot publiczny lub otrzymująca organizacja międzynarodowa powinny wdrożyć. Takie zabezpieczenia mogą na przykład obejmować ograniczenia, takie jak ograniczenia dostępu, ograniczenia celów, do których informacje można przetwarzać, ograniczenia dalszego przekazywania itp. lub szczególne zabezpieczenia, np. dodatkowe środki bezpieczeństwa wymagające specjalistycznego przeszkolenia pracowników, którzy mogą uzyskać dostęp do informacji.

2.7 Mechanizmy zaskarżenia

50. Aby zagwarantować egzekwowalne i skuteczne prawa osób, których dane dotyczą, w umowie międzynarodowej należy zapewnić system, dzięki któremu osoby, których dane dotyczą, nadal mogą korzystać z mechanizmów zaskarżenia po przekazaniu dotyczących ich danych do państwa spoza EOG lub do organizacji międzynarodowej. Takie mechanizmy zaskarżenia muszą zapewnić możliwość dochodzenia roszczeń osobom fizycznym, które wskutek nieprzestrzegania przepisów wybranego instrumentu zostały poszkodowane, co oznacza, że w ramach tych mechanizmów należy zapewnić

[21] Zob. Zalecenia 02/2020 EROD dotyczące niezbędnych gwarancji europejskich dla środków nadzoru.
[22] Zob. Zalecenia 02/2020 EROD, gwarancja D, s. 13 i nast.

osobom, których dane osobowe zostały przekazane z EOG, możliwość składania skarg dotyczących tego rodzaju nieprzestrzegania przepisów oraz należy zagwarantować rozpatrzenie tych skarg. W szczególności osobie, której dane dotyczą, należy zapewnić skuteczny tryb składania skarg do podmiotów publicznych, które są stronami danej umowy międzynarodowej, i (bezpośrednio albo za pośrednictwem odpowiedniej strony) do niezależnego mechanizmu nadzoru. Ponadto zasadniczo powinien być dostępny środek ochrony prawnej przed sądem.

51. Po pierwsze, otrzymujący podmiot publiczny powinien zobowiązać się do wdrożenia mechanizmu skutecznego i terminowego rozpatrywania składanych przez osoby, których dane dotyczą, skarg w przedmiocie przestrzegania uzgodnionych zabezpieczeń w zakresie ochrony danych. Ponadto osoby, których dane dotyczą, muszą mieć możliwość uzyskania skutecznych administracyjnych środków zaskarżenia przed niezależnym organem nadzoru, w tym w miarę dostępności, niezależnym organem ochrony danych[23].

52. Po drugie, w umowie należy przewidzieć środek ochrony prawnej przed sądem, w tym możliwość uzyskania odszkodowania za szkody zarówno materialne, jak i niematerialne poniesione na skutek niezgodnego z prawem przetwarzania danych osobowych. Jeżeli nie można zapewnić skutecznych sądowych środków zaskarżenia, na przykład ze względu na ograniczenia w prawie krajowym lub szczególny status otrzymującego podmiotu publicznego, np. organizacji międzynarodowych, w umowie międzynarodowej należy określić alternatywne zabezpieczenia. W ramach takich alternatywnych zabezpieczeń osobom, których dane dotyczą, należy zapewnić gwarancje, które są merytorycznie równoważne gwarancjom wymaganym w art. 47 Karty Praw Podstawowych Unii Europejskiej („Karta UE")[24].

53. W tym przypadku w umowie międzynarodowej można ustanowić strukturę umożliwiającą osobie, której dane dotyczą, dochodzenie swoich praw na drodze pozasądowej, na przykład za pomocą quasi-sądowych, wiążących mechanizmów takich jak arbitraż lub alternatywnych metod rozwiązywania sporów takich jak mediacja, co zagwarantowałoby niezależną kontrolę i byłoby wiążące dla otrzymującego podmiotu publicznego[25]. Ponadto podmiot publiczny przekazujący dane osobowe może zobowiązać się do wypłaty odszkodowania za szkody wynikające z niezgodnego z prawem przetwarzania danych osobowych potwierdzonego w drodze niezależnej kontroli.
W wyjątkowych sytuacjach w umowie można wprowadzić inne, równie niezależne i skuteczne mechanizmy zaskarżenia, na przykład skuteczne mechanizmy zaskarżenia wdrażane przez organizacje międzynarodowe.

54. W odniesieniu do wszystkich wyżej wymienionych mechanizmów zaskarżenia w umowie międzynarodowej należy zobowiązać strony do wzajemnego informowania się o wyniku postępowania, w szczególności w przypadku odrzucenia lub braku rozstrzygnięcia skargi wniesionej przez osobę fizyczną.

55. Mechanizmowi zaskarżenia musi towarzyszyć możliwość zawieszenia lub zakończenia przekazywania danych osobowych na podstawie danej umowy międzynarodowej przez przekazujący podmiot publiczny, jeżeli stronom nie uda się rozstrzygnąć sporu na drodze polubownej, do czasu w którym podmiot ten uzna, że dana sprawa została w sposób zadowalający rozwiązana przez otrzymujący

[23] Zob. również sekcja 2.8 dotycząca mechanizmów nadzoru.

[24] Wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 96, 186 i nast.

[25] Wyrok TSUE z 6 października 2015 r. w sprawie C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), pkt 41 i 95; wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 186, 187, 189, 195 i nast.

podmiot publiczny. Jeżeli takie zawieszenie lub zakończenie przekazywania danych rzeczywiście ma miejsce, otrzymujący podmiot publiczny musi jednocześnie zobowiązać się do zwrotu lub usunięcia otrzymanych danych osobowych. O zawieszeniu lub zakończeniu przekazywania danych przekazujący podmiot publiczny musi powiadomić właściwy krajowy organ nadzorczy.

2.8 Mechanizmy nadzoru

56. W celu zapewnienia, aby wszystkie obowiązki ustanowione na mocy umowy międzynarodowej były przestrzegane, w umowie tej należy określić niezależny mechanizm nadzoru umożliwiający monitorowanie prawidłowego stosowania umowy oraz przypadków kolidowania z prawami przewidzianymi w tej umowie.

57. Po pierwsze, w umowie należy przewidzieć wewnętrzny mechanizm nadzoru zapewniający przestrzeganie jej postanowień. Każda strona umowy powinna przeprowadzać okresowe wewnętrzne kontrole obowiązujących procedur i skutecznego stosowania zabezpieczeń przewidzianych w umowie. W toku takich okresowych wewnętrznych kontroli należy również weryfikować wszelkie zmiany przepisów, które uniemożliwiłyby przestrzeganie przez strony zasad i zabezpieczeń w zakresie ochrony danych określonych w umowie międzynarodowej. Ponadto można określić, że strona umowy może zwrócić się do innej strony umowy z wnioskiem o przeprowadzenie takiego przeglądu. Umowa międzynarodowa musi zawierać nakaz udzielania odpowiedzi na zapytania drugiej strony dotyczące skutecznego wykonania zabezpieczeń przewidzianych w umowie. Każda strona przeprowadzająca przegląd powinna przedstawić wyniki kontroli drugiej stronie lub pozostałym stronom umowy. Najlepiej byłoby, gdyby informacje te były przekazywane również do niezależnego mechanizmu nadzoru, którym objęta jest dana umowa.

58. Ponadto umowa międzynarodowa musi stanowić, że strona ma obowiązek niezwłocznie poinformować drugą stronę, jeżeli z jakiegokolwiek powodu nie jest w stanie skutecznie wdrożyć zabezpieczeń przewidzianych w umowie. W takim przypadku umowa międzynarodowa musi przewidywać możliwość zawieszenia lub zakończenia przekazywania danych osobowych na podstawie tej umowy otrzymującemu podmiotowi publicznemu przez przekazujący podmiot publiczny do czasu, w którym otrzymujący podmiot publiczny poinformuje przekazujący podmiot publiczny, że ponownie jest w stanie działać z poszanowaniem przewidzianych zabezpieczeń. O zmianie sytuacji, a także o zawieszeniu przekazywania danych lub rozwiązaniu umowy podmiot przekazujący musi powiadomić właściwy krajowy organ nadzorczy.

59. Po drugie, w umowie należy przewidzieć niezależny mechanizm nadzoru odpowiadający za zapewnienie, aby strony przestrzegały postanowień umowy. Wymóg ten wynika bezpośrednio z Karty Praw Podstawowych UE[26] i Europejskiej Konwencji Praw Człowieka (EKPC)[27] zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka i na warunkach określonych w prawie pierwotnym[28], a także powiązanym orzecznictwie.

---

[26] Art. 7, 8 i 47 Karty Praw Podstawowych UE.

[27] Art. 8 EKPC.

[28] Art. 6 Traktatu z Lizbony.

1. Unia uznaje prawa, wolności i zasady określone w Karcie praw podstawowych Unii Europejskiej z 7 grudnia 2000 roku, w brzmieniu dostosowanym 12 grudnia 2007 roku w Strasburgu, która ma taką samą moc prawną jak Traktaty.

Postanowienia Karty w żaden sposób nie rozszerzają kompetencji Unii określonych w Traktatach.

Prawa, wolności i zasady zawarte w Karcie są interpretowane zgodnie z postanowieniami ogólnymi określonymi w tytule VII Karty regulującymi jej interpretację i stosowanie oraz z należytym uwzględnieniem wyjaśnień, o których mowa w Karcie, które określają źródła tych postanowień.

2. Unia przystępuje do europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Przystąpienie do Konwencji nie ma wpływu na kompetencje Unii określone w Traktatach.

3. Prawa podstawowe, zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz wynikające z tradycji konstytucyjnych wspólnych Państwom Członkowskim, stanowią część prawa Unii jako zasady ogólne prawa.

60. Od 2015 r.[29] Trybunał Sprawiedliwości Unii Europejskiej kilkukrotnie potwierdził konieczność obowiązywania niezależnego mechanizmu zaskarżenia i nadzoru[30]. Podobnie Europejski Trybunał Praw Człowieka wielokrotnie podkreślał w swoich wyrokach, że każdy przypadek kolidowania z prawem do poszanowania życia prywatnego określonym w art. 8 EKPC musi podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru[31].

61. W umowie można na przykład określić, że nadzór sprawuje właściwy organ nadzorczy, jeżeli taki organ funkcjonuje w państwie podmiotu publicznego otrzymującego dane osobowe z EOG, nawet jeżeli w RODO nie wskazano, że właściwy organ nadzorczy musi pełnić rolę zewnętrznego organu nadzoru. Ponadto umowa może obejmować dobrowolne zobowiązanie strony otrzymującej do współpracy z organami nadzorczymi w EOG.

62. W przypadku braku organu nadzorczego odpowiedzialnego w szczególności za nadzór nad przepisami prawa w dziedzinie ochrony danych w państwie trzecim lub w organizacji międzynarodowej potrzebę zapewnienia niezależnych, skutecznych i bezstronnych mechanizmów nadzoru należy zaspokoić w inny sposób. Rodzaj stosowanego niezależnego mechanizmu nadzoru może zależeć od konkretnej sytuacji.

63. Umowa mogłaby na przykład dotyczyć istniejących w państwie trzecim organów nadzoru innych niż organ nadzorczy ds. ochrony danych. Ponadto, jeżeli ze strukturalnego lub instytucjonalnego punktu widzenia nie można zapewnić niezależnego nadzoru zewnętrznego, np. ze względu na przywileje i immunitety niektórych organizacji międzynarodowych, nadzór można zagwarantować za pomocą funkcjonalnie autonomicznych mechanizmów. Mechanizm taki musi obejmować organ, który choć sam nie jest organem zewnętrznym, wypełnia swoje zadania w sposób niezależny, tj. nie wykonuje poleceń, dysponuje wystarczającymi zasobami ludzkimi, technicznymi i finansowymi itp. Decyzje organu nadzoru są wiążące dla strony otrzymującej.

2.9 Klauzula regulująca rozwiązanie umowy

64. W umowie międzynarodowej należy przewidzieć, że wszelkie dane osobowe przekazane z EOG na podstawie umowy międzynarodowej przed jej faktycznym rozwiązaniem będą nadal przetwarzane zgodnie z postanowieniami umowy międzynarodowej.

[29] Wyrok TSUE z 6 października 2015 r. w sprawie C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), pkt 41 i 95.
[30] Opinia 1/15 TSUE z 27 lipca 2017 r. dotycząca umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera, 26 lipca 2017 r., pkt 228 i nast.; TSUE, 30 kwietnia 2019 r., opinia 1/17 dotycząca Kompleksowej umowy gospodarczo-handlowej między Kanadą a Unią Europejską, pkt 190 i nast.
[31] Orzeczenie Europejskiego Trybunału Praw Człowieka z 6 września 1978 r., Klass/Niemcy, pkt 55 i 56. Wymóg wynikający z orzeczenia Europejskiego Trybunału Praw Człowieka dotyczy również każdego przypadku kolidowania z art. 7 i 8 Karty UE, gdyż – zgodnie z art. 52 ust. 3 Karty UE – znaczenie i zakres tych praw podstawowych są takie same jak praw przyznanych w art. 8 EKPC.

3 SZCZEGÓŁOWE INFORMACJE NA TEMAT ART. 46 RODO

3.1 Szczegółowe informacje na temat prawnie wiążących i egzekwowalnych instrumentów – art. 46 ust. 2 lit. a) RODO

65. Zgodnie z art. 46 ust. 2 lit. a) RODO podmioty publiczne z EOG mogą przekazywać dane osobowe do państwa trzeciego lub organizacji międzynarodowej w oparciu o zawarte instrumenty, bez konieczności uzyskania uprzedniego zezwolenia ze strony organu nadzorczego. Takie instrumenty muszą być prawnie wiążące i egzekwowalne. Zgodnie z tym przepisem można zatem stosować traktaty międzynarodowe, traktaty publicznoprawne lub administracyjne umowy samowykonalne.

66. Zgodnie z wymogami RODO każdy prawnie wiążący i egzekwowalny instrument powinien obejmować podstawowy zbiór zasad ochrony danych i praw osób, których dane dotyczą.

67. Strony mają obowiązek stosowania wystarczających zabezpieczeń w zakresie ochrony danych przy przekazywaniu danych osobowych. W umowie należy zatem również określić sposób, w jaki otrzymujący podmiot publiczny będzie stosował zbiór podstawowych zasad ochrony danych i praw osób, których dane dotyczą, do wszystkich przekazywanych danych osobowych, aby zgodnie z RODO zagwarantować odpowiedni stopień ochrony osób fizycznych.

68. Jeżeli nie ma możliwości zapewnienia skutecznych sądowych środków zaskarżenia za pomocą prawnie wiążących i egzekwowalnych instrumentów, w związku z czym konieczne jest uzgodnienie alternatywnych mechanizmów zaskarżenia, podmioty publiczne z EOG powinny zasięgnąć opinii właściwego organu nadzorczego przed zawarciem takich instrumentów.

69. Nawet jeśli forma instrumentu nie jest rozstrzygająca, ale jest on prawnie wiążący i egzekwowalny, według EROD najlepszym rozwiązaniem byłoby włączenie szczegółowych klauzul ochrony danych bezpośrednio do instrumentu. Jeżeli jednak ze względu na szczególne okoliczności rozwiązania tego nie można zastosować, EROD zdecydowanie zaleca uwzględnienie co najmniej ogólnej klauzuli określającej zasady ochrony danych bezpośrednio w treści instrumentu oraz umieszczenie bardziej szczegółowych przepisów i zabezpieczeń w załączniku do tego instrumentu.

3.2 Szczegółowe informacje na temat uzgodnień administracyjnych – art. 46 ust. 3 lit. b) RODO

70. W art. 46 ust. 3 lit. b) RODO przewidziano alternatywne instrumenty w postaci uzgodnień administracyjnych, np. protokołu ustaleń, które służą zapewnieniu ochrony poprzez zobowiązania podjęte przez obie strony w celu realizacji ich wspólnych uzgodnień.

71. W tym kontekście w art. 46 ust. 1 i motywie 108 RODO określono, że uzgodnienia te muszą uwzględniać zapewnienie egzekwowalnych praw osób, których dane dotyczą, i skutecznych środków ochrony prawnej. W przypadku gdy w uzgodnieniach administracyjnych, które nie są prawnie wiążące, przewidziano zabezpieczenia, należy uzyskać zezwolenie właściwego organu nadzorczego.

72. Należy dokładnie ocenić, czy powinno się skorzystać z niewiążących prawnie uzgodnień administracyjnych w celu zapewnienia zabezpieczeń w sektorze publicznym, biorąc pod uwagę cel przetwarzania i charakter danych. Jeżeli prawo krajowe państwa trzeciego lub przepisy wewnętrzne/ramy regulacyjne organizacji międzynarodowej nie przewidują praw ochrony danych osobowych i środków zaskarżenia dla osób fizycznych z EOG, należy w pierwszej kolejności zawrzeć

prawnie wiążącą umowę. Niezależnie od przyjętego instrumentu obowiązujące środki muszą być skuteczne, aby zapewnić odpowiednie wdrożenie, egzekwowanie i nadzór.

73. W ramach uzgodnień administracyjnych należy przedsięwziąć kroki w celu zapewnienia skutecznych praw indywidualnych, środków zaskarżenia i nadzoru. W szczególności, aby zapewnić skuteczne i egzekwowalne prawa, niewiążący instrument powinien obejmować zapewnienia ze strony podmiotu publicznego otrzymującego dane osobowe z EOG, że w jego prawie krajowym w pełni uwzględniono prawa indywidualne, z których osoby fizyczne z EOG mogą korzystać na tych samych warunkach co obywatele i rezydenci danego państwa trzeciego. To samo dotyczy sytuacji, w której osoby z EOG mają dostęp do administracyjnych i sądowych środków zaskarżenia w granicach krajowych ram prawnych otrzymującego podmiotu publicznego. Podobnie, organizacje międzynarodowe powinny przedstawić zapewnienia dotyczące praw indywidualnych wynikających z ich przepisów wewnętrznych, jak również dotyczące dostępnych mechanizmów zaskarżenia.

74. Jeżeli tak nie jest, prawa indywidualne należy zagwarantować w drodze konkretnych zobowiązań stron w połączeniu z mechanizmami proceduralnymi, aby zapewnić ich skuteczność i możliwość zaskarżenia po stronie osób fizycznych. Te konkretne zobowiązania i mechanizmy proceduralne muszą umożliwiać w praktyce zapewnienie zgodności ze stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE na podstawie RODO.
Takie mechanizmy proceduralne mogą na przykład obejmować zobowiązania stron do wzajemnego informowania się o żądaniach osób fizycznych z EOG oraz do terminowego rozstrzygania sporów lub roszczeń.

75. Ponadto w przypadku gdy strony samodzielnie nie mogą rozwiązać takich sporów lub roszczeń w sposób polubowny, osobie fizycznej należy – za pomocą alternatywnych mechanizmów – zapewnić możliwość uzyskania niezależnych i skutecznych środków zaskarżenia, np. poprzez umożliwienie jej skorzystania z alternatywnego mechanizmu rozstrzygania sporów, takiego jak arbitraż lub mediacja. Taki alternatywny mechanizm rozstrzygania sporów musi mieć charakter wiążący[32].

76. W zależności od konkretnego przypadku w umowie administracyjnej należy przewidzieć połączenie wszystkich lub niektórych ze wspomnianych środków w celu zapewnienia skutecznych środków zaskarżenia. Dopuszczalne jest także zastosowanie innych środków nieuwzględnionych w tych wytycznych, o ile służą one zapewnieniu niezależnych i skutecznych środków zaskarżenia.

77. Każde uzgodnienie administracyjne opracowane zgodnie z art. 46 ust. 3 lit. b) RODO zostanie indywidualnie sprawdzone przez właściwy organ nadzorczy, a następnie, w stosownych przypadkach, zostanie poddane odpowiedniej procedurze EROD. Właściwy organ nadzorczy sprawdzi te uzgodnienia w oparciu o ogólne zalecenia określone w niniejszych wytycznych, ale w poszczególnych przypadkach może także wnieść o zapewnienie większych gwarancji.

[32] Wyrok TSUE z 16 lipca 2020 r., w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd i Maximillian Schrems („Schrems II"), pkt 189, 196 i nast.

4 PYTANIA DOTYCZĄCE KWESTII PROCEDURALNYCH

78. Uzgodnienia administracyjne na podstawie art. 46 ust. 3 lit. b) RODO będą sprawdzane indywidualnie ze względu na wymogi dotyczące uzyskania zezwolenia od właściwego organu nadzorczego, który zgodnie z art. 46 ust. 4 RODO stosuje mechanizm spójności opisany w art. 64 ust. 2 RODO. EROD zaleca również, aby przy włączaniu alternatywnych mechanizmów zaskarżenia do wiążących i egzekwowalnych instrumentów zgodnie z art. 46 ust. 2 lit. a) RODO zasięgnąć porady właściwego organu nadzorczego. EROD zdecydowanie radzi, aby konsultować się z właściwym organem nadzorczym na wczesnym etapie.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)