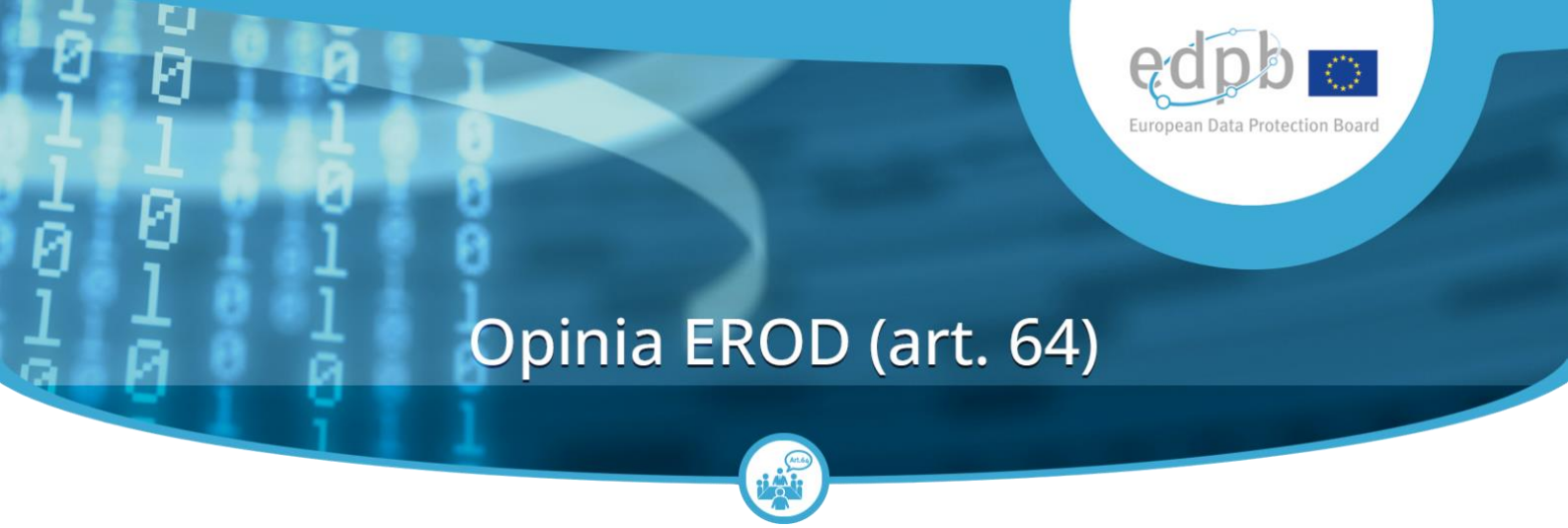

Opinia 22/2024 w sprawie niektórych obowiązków wynikających z polegania na podmiocie przetwarzającym (podmiotach przetwarzających) i podwykonawcy (podwykonawcach) przetwarzania danych

Przyjęta 7 października 2024 r.

Streszczenie

Duński organ nadzorczy zwrócił się do EROD o wydanie opinii w sprawach mających charakter ogólny, zgodnie z art. 64 ust. 2 RODO. Opinia ta stanowi uzupełnienie zharmonizowanej interpretacji przez krajowe organy nadzorcze niektórych aspektów art. 28 RODO, w stosownych przypadkach w związku z rozdziałem V RODO. W szczególności w opinii poruszono pytania dotyczące interpretacji niektórych obowiązków administratorów polegających na podmiotach przetwarzających i podwykonawcach przetwarzania, wynikających w szczególności z art. 28 RODO, a także brzmienia umów między administratorem a podmiotem przetwarzającym. Pytania dotyczą przetwarzania danych osobowych w EOG, jak również przetwarzania po przekazaniu danych do państwa trzeciego.

W niniejszej opinii EROD stwierdza, że administratorzy powinni mieć w każdej chwili łatwo dostępne informacje na temat tożsamości (tj. nazwa, adres, osoba wyznaczona do kontaktów) wszystkich podmiotów przetwarzających dane, podwykonawców przetwarzania itp., tak aby mogli oni jak najlepiej wypełniać swoje obowiązki wynikające z art. 28 RODO, niezależnie od ryzyka związanego z czynnością przetwarzania. W tym celu podmiot przetwarzający powinien przez cały czas proaktywnie przekazywać administratorowi wszystkie takie informacje i je aktualizować.

Art. 28 ust. 1 RODO stanowi, że administratorzy mają obowiązek korzystać z usług podmiotów przetwarzających, którzy zapewnią „wystarczające gwarancje" wdrożenia „odpowiednich" środków, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. EROD uważa w swojej opinii, że oceniając przestrzeganie przez administratorów tego obowiązku i zasady rozliczalności (art. 24 ust. 1 RODO), organy nadzorcze powinny wziąć pod uwagę, że korzystanie z usług podmiotów przetwarzających nie powinno obniżać stopnia ochrony praw osób, których dane dotyczą. *Obowiązek* administratora polegający na weryfikacji, czy podmioty przetwarzające (lub podwykonawcy przetwarzania) posiadają „wystarczające gwarancje" w celu wdrożenia odpowiednich środków określonych przez administratora, powinien mieć zastosowanie niezależnie od ryzyka naruszenia praw i wolności osób, których dane dotyczą. Jednak *zakres* takiej weryfikacji będzie w praktyce różny, w zależności od charakteru tych środków technicznych i organizacyjnych, które mogą być bardziej rygorystyczne lub bardziej rozbudowane, w zależności od poziomu takiego ryzyka.

EROD precyzuje ponadto w tej opinii, że chociaż pierwotny podmiot przetwarzający powinien dopilnować, że zaproponowani podwykonawcy przetwarzania dają wystarczające gwarancje, ostateczna decyzja o tym, czy skorzystać z usług konkretnego podwykonawcy przetwarzania, oraz związana z tym odpowiedzialność, w tym w odniesieniu do weryfikacji gwarancji, pozostają w gestii administratora. Organy nadzorcze powinny ocenić, czy administrator jest w stanie wykazać, że weryfikacja wystarczalności gwarancji zapewnionych przez jego podmioty przetwarzające (lub podwykonawców przetwarzania) została przeprowadzona w sposób zadowalający dla administratora. Administrator może opierać się na informacjach otrzymanych od swojego podmiotu przetwarzającego i w razie potrzeby je uzupełnić (na przykład, gdy wydają się one niekompletne, nieprawidłowe lub budzą wątpliwości). W szczególności, w przypadku przetwarzania stwarzającego wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, administrator powinien zwiększyć stopień weryfikacji, jeżeli chodzi o sprawdzanie dostarczonych informacji. W tym względzie EROD uważa, że zgodnie z RODO administrator nie ma obowiązku systematycznego zwracania się o umowy dotyczące podwykonawstwa przetwarzania, w celu sprawdzenia, czy obowiązki ochrony danych przewidziane w

pierwotnej umowie zostały przeniesione na kolejne ogniwa łańcucha przetwarzania. Administrator powinien ocenić, indywidualnie dla każdego przypadku, czy żądanie kopii takich umów lub ich sprawdzanie w dowolnym momencie jest konieczne, aby wykazać zgodność w świetle zasady rozliczalności.

Jeżeli przekazywanie danych osobowych poza EOG odbywa się między dwoma podmiotami przetwarzającymi (lub podwykonawcami przetwarzania), zgodnie z poleceniem administratora, administrator nadal podlega obowiązkom wynikającym z art. 28 ust. 1 RODO dotyczącym „wystarczających gwarancji", oprócz tych określonych w art. 44, w celu zapewnienia, że stopień ochrony zagwarantowany w RODO nie został naruszony przez przekazanie danych osobowych. Zgodnie z orzecznictwem i jak wyjaśniono w zaleceniach EROD 01/2020 podmiot przetwarzający/przekazujący powinien przygotować odpowiednią dokumentację. Administrator powinien ocenić taką dokumentację i być w stanie przedstawić ją właściwemu organowi nadzorczemu. Administrator może opierać się na dokumentacji lub informacjach otrzymanych od podmiotu przetwarzającego/przekazującego i w razie potrzeby je uzupełnić. Zakres i charakter obowiązku dokonania przez administratora oceny tej dokumentacji może zależeć od podstawy, na jakiej przekazano dane, oraz od tego, czy jest to przekazanie pierwotne czy dalsze.

EROD odniosła się również w tej opinii do kwestii brzmienia umów między administratorem a podmiotem przetwarzającym. W tym względzie podstawowym elementem jest zobowiązanie podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, chyba że na podmiot przetwarzający *„obowiązek [przetwarzania] nakłada prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający"* (art. 28 ust. 3 lit. a) RODO) – przypominając ogólną zasadę, zgodnie z którą umowy nie mogą być nadrzędne wobec prawa. W świetle swobody zawierania umów przyznanej stronom w celu dostosowania umowy między administratorem a podmiotem przetwarzającym do ich okoliczności, w granicach art. 28 ust. 3 RODO, EROD jest zdania, że włączenie słów „*chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający*" (dosłownie lub w bardzo podobnych słowach) jest wysoce zalecane, ale nie obowiązkowe.

Jeśli chodzi o warianty podobne do *„chyba, że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego"*, EROD jest zdania, że należy to do swobody zawierania umów przysługującej stronom i nie narusza art. 28 ust. 3 lit. a) RODO jako takiego. Jednocześnie EROD wskazuje w swojej opinii szereg kwestii, ponieważ taka klauzula nie zwalnia podmiotu przetwarzającego z przestrzegania obowiązków wynikających z RODO.

W przypadku danych osobowych przekazywanych poza EOG, EROD uważa za mało prawdopodobne, aby sformułowanie *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego"* samo w sobie wystarczyło do osiągnięcia zgodności z art. 28 ust. 3 lit. a) RODO w związku z rozdziałem V. Jak wskazują zalecenia Komisji Europejskiej dotyczące standardowych klauzul umownych (ang. *standard contractual clauses,* (SCC) w sprawie międzynarodowego przekazywania danych i wiążących reguł korporacyjnych dla administratorów (ang. *binding corporate rules for controllers*, BCR-C), art. 28 ust. 3 lit. a) RODO nie uniemożliwia – co do zasady – włączenia do umowy przepisów, które dotyczą wymogów prawa państwa trzeciego w zakresie przetwarzania przekazanych danych osobowych. Jednakże, podobnie jak w przypadku tych dokumentów, należy dokonać rozróżnienia między prawem (prawami) kraju trzeciego, który naruszyłby stopień ochrony

gwarantowany przez RODO, a tymi, które by tego nie zrobiły. EROD przypomina również, że możliwość, w której prawo państwa trzeciego utrudniania przestrzeganie RODO, powinna być czynnikiem branym pod uwagę przez strony przed zawarciem umowy (między administratorem a podmiotem przetwarzającym lub między podmiotem przetwarzającym a podwykonawcą przetwarzania).

Jeżeli podmiot przetwarzający przetwarza dane osobowe w obrębie EOG, w pewnych okolicznościach może nadal mieć do czynienia z prawem państwa trzeciego. EROD podkreśla, że dodanie w umowie sformułowania podobnego do *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”* nie zwalnia podmiotu przetwarzającego z jego obowiązków wynikających z RODO.

EROD jest również zdania, że następujące po zobowiązaniu podmiotu przetwarzającego do przetwarzania danych wyłącznie na udokumentowane polecenie sformułowanie *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”* (dosłownie lub w bardzo podobnych słowach) nie może być interpretowane jako udokumentowane polecenie administratora.

Spis treści

uwzględniając art. 63 i art. 64 ust. 2 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, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 10 i 22 swojego regulaminu wewnętrznego,

a także mając na uwadze, co następuje:

(1) głównym zadaniem Europejskiej Rady Ochrony Danych (zwanej dalej „EROD”) jest zapewnienie spójnego stosowania RODO w całym Europejskim Obszarze Gospodarczym („EOG”). Artykuł 64 ust. 2 RODO stanowi, że każdy organ nadzorczy („ON”), przewodniczący EROD lub Komisja mogą wystąpić o zbadanie przez EROD sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim EOG w celu wydania opinii. Celem niniejszej opinii jest zbadanie sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim EOG;

(2) opinię EROD należy przyjąć zgodnie z art. 64 ust. 3 RODO w związku z art. 10 ust. 2 regulaminu wewnętrznego EROD w terminie ośmiu tygodni od dnia, w którym przewodniczący i właściwe organy nadzorcze zadecydują o kompletności akt. Ze względu na złożony charakter sprawy termin ten można przedłużyć o dalsze sześć tygodni na podstawie decyzji przewodniczącego.

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1 WPROWADZENIE

1.1 Streszczenie faktów

1. 5 lipca 2024 r. duński organ nadzorczy (zwany dalej „DK ON”) zwrócił się do Europejskiej Rady Ochrony Danych (zwanej dalej „EROD”) z wnioskiem o wydanie opinii w sprawie obowiązków administratorów w zakresie rozliczalności w odniesieniu do łańcucha przetwarzania danych oraz relacji między administratorami a podmiotami przetwarzającymi (lub podwykonawcami przetwarzania) (zwany dalej „wnioskiem”).

2. 8 lipca 2024 r. DK ON oświadczył, że akta są kompletne. W dniu 9 lipca 2024 r. przewodnicząca EROD uznała akta za kompletne. W tym samym dniu akta zostały rozpowszechnione przez Sekretariat EROD. Przewodnicząca, biorąc pod uwagę złożoność sprawy, postanowiła wydłużyć przewidziany prawem termin zgodnie z art. 64 ust. 3 RODO i art. 10 ust. 4 regulaminu wewnętrznego.

[1] Odniesienia do „państw członkowskich” w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG”. Odniesienia do „Unii” w niniejszej opinii należy rozumieć jako odniesienia do „EOG”.

3. W swoim wniosku DK ON odnosi się również do sprawozdania przyjętego przez EROD w styczniu 2023 r. w sprawie ustaleń z pierwszego skoordynowanego działania w zakresie egzekwowania przepisów[2] w ramach skoordynowanego egzekwowania prawa[3]. Ww. skoordynowane działanie skupiało się na korzystaniu przez sektor publiczny z usług opartych na chmurze. W sprawozdaniu EROD, organy nadzorcze biorące udział w skoordynowanym działaniu zidentyfikowały osiem trudności, w szczególności w odniesieniu do korzystania z usług w chmurze przez organy publiczne, i przedstawiły listę punktów, na które zainteresowane strony powinny zwrócić uwagę przy ocenie usług w chmurze i korzystaniu z dostawców usług przetwarzania w chmurze[4]. O ile w przypadku większości tych punktów zakres obowiązków nałożonych na mocy RODO jest jasny zarówno dla administratorów, jak i podmiotów przetwarzających, to według DK ON dokładny zakres niektórych obowiązków wynikających z RODO pozostaje niejasny[5].

   DK ON zadał następujące pytania:

4. Pytanie 1.1: Biorąc pod uwagę art. 5 ust. 2 i art. 24 ust. 1 RODO, w przypadku korzystania z usług podmiotu przetwarzającego do przetwarzania danych w imieniu administratora, w celu udokumentowania zgodności z m.in. art. 28 ust. 1 i art. 28 ust. 2 (w tym podczas okazywania dokumentacji organowi nadzorczemu podczas kontroli):

   a. Czy administrator musi wskazać wszystkich podwykonawców podmiotu przetwarzającego, podwykonawców podwykonawców itd. w całym łańcuchu przetwarzania, czy też wskazać tylko pierwszą linię podwykonawców przetwarzania, z których usług korzysta podmiot przetwarzający?

   b. W jakim zakresie i na jakim poziomie szczegółowości administrator musi zweryfikować i udokumentować:

      i. odpowiedniość zabezpieczeń zapewnionych przez podmioty przetwarzające, ich podwykonawców przetwarzania itd.,
      ii. treść umów między pierwotnym podmiotem przetwarzającym a dodatkowymi podmiotami przetwarzającymi w celu ustalenia, czy na dodatkowe podmioty przetwarzające nałożono takie same obowiązki zgodnie z art. 28 ust. 4 RODO; oraz
      iii. Czy podmioty przetwarzające, ich podwykonawcy przetwarzania itd. spełniają wymogi administratora określone w art. 28 ust. 1?

5. Pytanie 1.2: W przypadku przekazywania danych lub dalszego przekazywania danych od podmiotu przetwarzającego (lub podwykonawcy przetwarzania) do innego podmiotu przetwarzającego (lub podwykonawcy przetwarzania) zgodnie z poleceniem administratora: W jakim zakresie administrator, w ramach swojego obowiązku wynikającego z art. 28 ust. 1 RODO w związku z art. 44 RODO, musi ocenić i być w stanie przedstawić dokumentację podmiotów przetwarzających (lub podwykonawców przetwarzania), zapewniającą, że (dalsze) przekazywanie danych nie narusza stopnia ochrony danych osobowych?

---

[2] Sprawozdanie w sprawie skoordynowanego działania w zakresie egzekwowania przepisów z 2022 r. – korzystanie przez sektor publiczny z usług opartych na chmurze, 17 stycznia 2023 r. (zwane dalej „sprawozdaniem CEF w sprawie usług przetwarzania w chmurze").

[3] Ramy skoordynowanego egzekwowania prawa zostały ustanowione przez EROD w październiku 2020 r. w celu usprawnienia egzekwowania przepisów i współpracy między organami nadzorczymi. Zob. dokument EROD w sprawie ram skoordynowanego egzekwowania prawa na podstawie rozporządzenia 2016/679, przyjęty w dniu 20 października 2020 r., wersja 1.1.

[4] CEF Report on Cloud Services (*„Sprawozdanie CEF w sprawie usług przetwarzania w chmurze"*), str. 10-20.

[5] Wniosek, str. 1.

6. Pytanie 1.3: Czy zakres obowiązków wynikających z art. 28 ust. 1 i art. 28 ust. 2 RODO w związku z art. 5 ust. 2 i art. 24 RODO, jak wskazano w odpowiedzi do pytania 1.1 i pytania 1.2, różni się w zależności od ryzyka związanego z czynnością przetwarzania? Jeżeli tak, jaki jest zakres takich obowiązków w odniesieniu do czynności przetwarzania niskiego ryzyka, a jaki w odniesieniu do czynności przetwarzania wysokiego ryzyka?

7. Pytanie 2: Czy umowa lub inny instrument prawny na mocy prawa Unii lub prawa państwa członkowskiego zgodnie z art. 28 ust. 3 RODO muszą zawierać wyjątek przewidziany w art. 28 ust. 3 lit. a) *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający*" (dosłownie lub w bardzo podobnych słowach), aby była zgodna z RODO?

8. Pytanie 2a: jeżeli odpowiedź na pytanie 2 jest przecząca, czy w przypadku, gdy umowa lub inny instrument prawny na mocy prawa Unii lub państwa członkowskiego, który rozszerza zakres wyjątku z art. 28 ust. 3 lit. a) RODO, aby objąć również ogólnie prawo państwa trzeciego (np. „chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego"), samo w sobie stanowi to naruszenie art. 28 ust. 3 lit. a) RODO?

9. Pytanie 2b: Jeżeli odpowiedź na pytanie 2a jest przecząca, czy taki rozszerzony zakres wyjątku należy zamiast tego interpretować jako udokumentowane polecenie administratora w rozumieniu art. 28 ust. 3 lit. a) RODO?

1.2 Dopuszczalność wniosku o wydanie opinii w trybie art. 64 ust. 2 RODO

10. Artykuł 64 ust. 2 RODO stanowi, że w szczególności każdy organ nadzorczy może wystąpić o przeanalizowanie przez EROD sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim w celu wydania opinii.

11. Pierwsze pytania zadane przez DK ON dotyczą obowiązków administratorów w zakresie rozliczalności wynikających z art. 28 RODO (pytania 1.1, 1.2 i 1.3), natomiast ostatnie odnosi się do konkretnej treści umowy lub instrumentu prawnego między administratorem a podmiotem przetwarzającym na podstawie art. 28 ust. 3 lit. a) RODO (pytanie 2).

12. EROD uważa, że pytania te są związane z interpretacją RODO, w szczególności w odniesieniu do relacji między administratorami a ich podmiotami przetwarzającymi (lub podwykonawcami przetwarzania) oraz do interpretacji art. 5 ust. 2, art. 24 i art. 28 RODO. Wniosek jest powiązany, z jednej strony, z obowiązkami administratorów w zakresie rozliczalności oraz z poziomem dokumentacji, jakiego organy nadzorcze powinny oczekiwać od wszystkich administratorów korzystających z usług podmiotów przetwarzających (lub podwykonawców przetwarzania) do wykonywania czynności przetwarzania w ich imieniu, a z drugiej strony z treścią umów lub instrumentów prawnych między administratorem a podmiotem przetwarzającym. W związku z tym niniejszy wniosek dotyczy *„sprawy mającej charakter ogólny*" w rozumieniu art. 64 ust. 2 RODO.

13. Ponadto EROD uważa, że wniosek DK ON jest uzasadniony zgodnie z art. 10 ust. 3 regulaminu wewnętrznego EROD, ponieważ DK ON przedstawił argumenty na rzecz potrzeby spójnej interpretacji pytań, do których odnosi się wniosek.

14. Zgodnie z art. 64 ust. 3 RODO EROD nie wydaje opinii, jeżeli wcześniej już wydała w tej sprawie opinię[6]. EROD nie udzieliła jeszcze odpowiedzi na pytania wynikające z wniosku DK ON. Ponadto dostępne wytyczne EROD, w tym w szczególności wytyczne EROD 07/2020 dotyczące pojęć administratora

[6] Artykuł 64 ust. 3 RODO i art. 10 ust. 4 regulaminu wewnętrznego EROD.

i podmiotu przetwarzającego[7] (zwane dalej „wytycznymi EROD 07/2020"), zawierają pewne wskazówki dotyczące obowiązków administratora w zakresie rozliczalności, wynikających z art. 28 RODO, ale istniejące wytyczne nie odpowiadają w pełni na wszystkie pytania zawarte we wniosku[8]. W szczególności, na przykład, dostępne wytyczne dotyczące art. 28 ust. 3 lit. a) RODO nie odpowiadają konkretnie na pytanie zawarte we wniosku DK ON w kwestii tego, czy słowa *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający*" powinny zostać uwzględnione w umowach lub instrumentach prawnych między administratorem a podmiotem przetwarzającym.

15. Z tych powodów EROD uważa, że wniosek DK ON jest dopuszczalny, a pytania wynikające z wniosku DK ON powinny zostać przeanalizowane w opinii przyjętej zgodnie z art. 64 ust. 2 RODO.

2 W SPRAWIE ZASADNOŚCI WNIOSKUERROR! BOOKMARK NOT DEFINED.

2.1 W sprawie interpretacji art. 28 ust. 1, art. 28 ust. 2 i art. 28 ust. 4 RODO w związku z art. 5 ust. 2 i art. 24 ust. 1 (pytania 1.1 i 1.3)

16. W niniejszej sekcji omówiono pytania 1.1 i 1.3 skierowane do EROD, przedstawione w sekcji „dopuszczalność" powyżej.

17. Artykuł 28 RODO określa relacje między administratorem a podmiotem przetwarzającym i nakłada bezpośrednie obowiązki na administratorów i podmioty przetwarzające. Na wstępie należy zauważyć, że w art. 4 ust. 8 RODO „podmiot przetwarzający" jest zdefiniowany w sposób ogólny, który obejmuje zarówno pierwotny podmiot przetwarzający, z którego usług korzysta bezpośrednio administrator, jak i podmiot przetwarzający podmiotu przetwarzającego, itd. w całym łańcuchu przetwarzania.

18. EROD podkreśla, że ocena roli stron (oraz tego, czy działają one jako wyłączni administratorzy lub współadministratorzy czy też jako podmioty przetwarzające) wykracza poza zakres wniosku. EROD przypomina, że to przede wszystkim do stron należy ocena ich rzeczywistej roli w zależności od elementów stanu faktycznego lub okoliczności sprawy[9], nie naruszając przy tym kompetencji ON do sprawdzenia, czy ich ocena jest prawdziwa.

19. W świetle powyższych pytań w niniejszej opinii skupiono się wyłącznie na zakresie i zasięgu obowiązków administratora wynikających z art. 28 ust. 1 RODO w celu sprawdzenia, czy podmioty przetwarzające (lub podwykonawcy przetwarzania) zapewniają „wystarczające gwarancje", zgodnie z art. 28 ust. 2, oraz związanych z nimi obowiązków administratora w zakresie rozliczalności, o których mowa w art. 5 ust. 2 i art. 24 ust. 1 RODO[10].

---

[7] Wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO, wersja 2.1, przyjęte 7 lipca 2021 r.

[8] Zob. w szczególności wytyczne EROD 07/2020, sekcja 1.1 „Wybór podmiotu przetwarzającego" na stronie 34, sekcja 1.3.4 *„Podmiot przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4 (art. 28 ust. 3 lit. d) RODO)"* na stronie 41, sekcja 1.6 „Podwykonawcy przetwarzania" na stronie 46.

[9] Wytyczne EROD 07/2020, pkt 12.

[10] Kwestia ta jest odrębna i niezależna od wszelkich innych obowiązków administratora (lub podmiotów przetwarzających bądź podwykonawców przetwarzania) w zakresie zapewnienia zgodności z RODO, np. z zasadą zgodności z prawem, z art. 32 lub obowiązkami wynikającymi z rozdziału V RODO. Administrator może nadal

20. Ponadto EROD zauważa, że powyższe pytania nie dotyczą odpowiedzialności administratora wobec osób, których dane dotyczą, za czynności przetwarzania prowadzone w jego imieniu, na przykład w odniesieniu do prawa osób, których dane dotyczą, do odszkodowania na podstawie art. 82 RODO. Niniejsza sekcja skupi się zatem na udzieleniu ON wyjaśnień dotyczących interpretacji art. 28 ust. 1 i art. 28 ust. 2 RODO w związku z art. 5 ust. 2 i art. 24 RODO w odniesieniu do niektórych obowiązków wynikających z polegania na podmiotach przetwarzających i podwykonawcach przetwarzania. W celu udzielenia odpowiedzi na te pytania EROD przeprowadzi analizę, skupiając się na sytuacjach, w których nie dochodzi do przekazania danych osobowych poza EOG. Z kolei poniższa sekcja dotycząca pytania 1.2 ocenia sytuacje, w których dochodzi do przekazania danych w całym łańcuchu przetwarzania.

2.1.1 Identyfikacja podmiotów w łańcuchu przetwarzania

21. Odnosząc się do kwestii, czy administrator powinien zasadniczo zidentyfikować wszystkich podwykonawców podmiotu przetwarzającego, ich podwykonawców przetwarzania itd. w całym łańcuchu przetwarzania, czy też zidentyfikować tylko pierwszą linię podwykonawców przetwarzania, z których usług korzysta podmiot przetwarzający, EROD przypomina przede wszystkim, że *„Chociaż łańcuch [przetwarzania] może być dość długi, administrator zachowuje swoją kluczową rolę w określaniu celu i sposobów przetwarzania”*[11].

22. EROD odczytuje terminy „zidentyfikować” i „informacje o tożsamości” do celów odpowiedzi na pytanie jako odnoszące się do nazwy, adresu, osoby wyznaczonej do kontaktu (imię i nazwisko, stanowisko, dane kontaktowe) podmiotu przetwarzającego oraz opisu przetwarzania (w tym wyraźne rozgraniczenie obowiązków, jeżeli upoważnionych jest kilku podwykonawców przetwarzania)[12].

23. Jeżeli chodzi o wybór podmiotów przetwarzających, administratorzy powinni być w stanie skutecznie określić cele i sposoby przetwarzania zgodnie z art. 4 ust. 7 RODO. W związku z tym określenie odbiorców (w tym podmiotów przetwarzających) uważa się za „istotne sposoby” przetwarzania, o których decyduje administrator[13].

24. W tym celu, w odniesieniu do korzystania przez pierwotny podmiot przetwarzający z usług **dodatkowych podmiotów przetwarzających**, zgodnie z art. 28 ust. 2 RODO konieczna jest uprzednia szczegółowa lub ogólna pisemna zgoda administratora. W wytycznych EROD 07/2020 wyjaśniono, że obowiązki przewidziane w art. 28 ust. 2 są *„uruchamiane w przypadku, gdy podmiot przetwarzający (podwykonawca) zamierza zaangażować innego uczestnika, a tym samym dodać kolejne ogniwo do łańcucha i powierzyć mu czynności wymagające przetwarzania danych osobowych*”[14].

---

ponosić odpowiedzialność za przetwarzanie danych w ramach swojego administrowania, które nie jest zgodne z takimi przepisami RODO, nawet jeżeli spełnił obowiązki weryfikacji swoich podmiotów przetwarzających (lub podwykonawców przetwarzania) zgodnie z art. 28 ust. 1 RODO szczegółowo opisanym w niniejszej opinii, a niniejsza opinia nie dotyczy odpowiedzialności administratora za przestrzeganie przepisów RODO innych niż art. 24 ust. 1, art. 28 ust. 1 i art. 28 ust. 2 RODO.

[11] Wytyczne EROD 07/2020, pkt 152.

[12] Odzwierciedla to informacje wymagane do identyfikacji podmiotów przetwarzających w załączniku IV do wydanych przez Komisję Europejską standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi (decyzja wykonawcza Komisji 2021/915 z dnia 4 czerwca 2021 r.) i załączniku III do wydanych przez Komisję Europejską standardowych klauzul umownych dotyczących międzynarodowego przekazywania danych (decyzja wykonawcza Komisji 2021/914 z dnia 4 czerwca 2021 r.).

[13] Wytyczne EROD 07/2020, pkt 40.

[14] Wytyczne EROD 07/2020, pkt 151 brzmi następująco: *„Działalność związana z przetwarzaniem danych jest często prowadzona przez wiele podmiotów, a łańcuchy podwykonawstwa stają się coraz bardziej złożone. Ogólne rozporządzenie o ochronie danych wprowadza szczególne obowiązki, które są uruchamiane w przypadku, gdy*

25. Jeżeli administrator postanawia zaakceptować niektórych podwykonawców przetwarzania w momencie podpisywania umowy, w umowie lub załączniku do niej należy umieścić wykaz zatwierdzonych podwykonawców przetwarzania. Wykaz ten należy następnie aktualizować zgodnie z ogólną lub szczegółową zgodą administratora danych[15].

26. Jeżeli chodzi o korzystanie z usług podwykonawców przetwarzania, w RODO przewidziano możliwość uzyskania ogólnej lub szczegółowej zgody. **W przypadku szczegółowej zgody** administrator powinien określić na piśmie, który podwykonawca przetwarzania jest upoważniony i do jakiej konkretnej czynności przetwarzania, a także na jaki czas[16]. Jeżeli administrator nie udzieli odpowiedzi na wniosek podmiotu przetwarzającego o udzielenie szczegółowej zgody w ustalonym terminie, należy go uznać za odrzucony[17].

27. **W przypadku ogólnej zgody** podmiot przetwarzający powinien zapewnić administratorowi możliwość zatwierdzenia wykazu podwykonawców przetwarzania w momencie podpisania ogólnej zgody oraz możliwość – w tym w wystarczających ramach czasowych – wyrażenia sprzeciwu wobec wszelkich późniejszych zmian dotyczących podwykonawców przetwarzania[18]. EROD przypomina, że do pierwotnego **podmiotu przetwarzającego powinno należeć proaktywne przekazywanie określonych informacji** administratorowi, a „*obowiązek podmiotu przetwarzającego polegający na informowaniu administratora o każdej zmianie podwykonawcy przetwarzania oznacza, że podmiot przetwarzający **aktywnie** wskazuje lub sygnalizuje takie zmiany administratorowi*”[19].

28. Oznacza to, że informacje dotyczące identyfikacji wszystkich podwykonawców podmiotu przetwarzającego powinny być łatwo dostępne dla administratora danych. Identyfikacja tych podmiotów ma szczególne znaczenie dla administratora, aby mógł on mieć kontrolę nad swoimi czynnościami przetwarzania, za które jest odpowiedzialny i może zostać pociągnięty do odpowiedzialności w przypadku naruszenia RODO.

29. Podmiot przetwarzający powinien zatem przedstawić wszystkie informacje na temat sposobu prowadzenia czynności przetwarzania w imieniu administratora, w tym informacje na temat

---

podmiot przetwarzający (podwykonawca) zamierza zaangażować innego uczestnika, a tym samym dodać kolejne ogniwo do łańcucha i powierzyć mu czynności wymagające przetwarzania danych osobowych. Analizę tego, czy dostawca usług działa jako podwykonawca przetwarzania, przeprowadza się zgodnie z tym, co opisano powyżej w odniesieniu do pojęcia podmiotu przetwarzającego”.

[15] Wytyczne EROD 07/2020, pkt 154.

[16] Wytyczne EROD 07/2020, pkt 153 i 155. Zgodnie z klauzulą 7.7 opcją 1 standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi, wykaz podwykonawców przetwarzania mających szczegółową zgodę administratora danych powinien być zawarty w załączniku IV, który należy aktualizować.

[17] Wytyczne EROD 07/2020, pkt 155.

[18] Zob. również wytyczne EROD 07/2020, pkt 156: „*Administrator może również udzielić ogólnej zgody na korzystanie z usług podwykonawców (w umowie, w tym w załączniku do umowy, zawierającym wykaz takich podwykonawców) (...)*”. W tym kontekście istotna jest również opinia EROD 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez DK ON (art. 28 ust. 8 RODO). Zgodnie z klauzulą 7.7 opcją 2 wydanych przez Komisję Europejską standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi, podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podwykonawców przetwarzania widniejących w uzgodnionym wykazie oraz wyraźnie informuje administratora na piśmie o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podwykonawców przetwarzania z wyprzedzeniem.

[19] Wytyczne EROD 07/2020, pkt 128 (wytłuszczenie dodano). Zob. również przypis 14.

podwykonawcy przetwarzania, z którego usług korzysta[20] oraz opis przetwarzania powierzonego podwykonawcy przetwarzania[21].

30. Inne powody prawne uzasadniają potrzebę zidentyfikowania przez administratora wszystkich podmiotów przetwarzających i podwykonawców przetwarzania. Podmioty przetwarzające, którym dane są ujawniane lub przekazywane, uważa się za „odbiorców"[22].

- Aby spełnić wymogi przejrzystości określone w art. 13 ust. 1 lit. e) i art. 14 ust. 1 lit. e) RODO, administratorzy powinni poinformować osoby, których dane dotyczą, o odbiorcach danych lub kategoriach odbiorców danych, określając je w sposób jak najbardziej szczegółowy i konkretny[23]. Informacje na temat „kategorii odbiorców" muszą być również zawarte w rejestrach czynności przetwarzania [art. 30 ust. 1 lit. d)].

- W art. 15 RODO przewidziano prawo dostępu do między innymi informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione[24]. Trybunał Sprawiedliwości wyjaśnił, że przepis ten pociąga za sobą obowiązek przekazania przez administratora osobie, której dane dotyczą, faktycznej tożsamości odbiorców[25]. Poza rodzajem przypadków, w których administrator może

[20] Wytyczne EROD 7/2020, pkt 143.

[21] Zob. np. załącznik IV do standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi oraz załącznik II do standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych.

[22]Art. 4 ust. 9 RODO; wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, przyjęte dnia 29 listopada 2017 r., ostatnio zmienione i przyjęte w dniu 11 kwietnia 2018 r., WP260 rev.01, zatwierdzone przez EROD (zwane dalej „wytycznymi Grupy Roboczej Art. 29 w sprawie przejrzystości"), str. 37.

[23] Wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości, str. 37 (*„Zgodnie z zasadą rzetelności administratorzy muszą przedstawić informacje na temat odbiorców, którzy mają największe znaczenie dla osoby, której dane dotyczą*. *W praktyce zazwyczaj będzie to odbiorca wymieniony z nazwiska lub nazwy, tak aby osoby, których dane dotyczą, wiedziały dokładnie, kto jest w posiadaniu ich danych osobowych. Jeśli administrator zamierza przedstawić kategorie odbiorców, informacje powinny być w jak największym stopniu szczegółowe, tzn. należy wskazać rodzaj odbiorcy (np. poprzez odniesienie do działalności, którą prowadzi), branżę, sektor, podsektor oraz lokalizację odbiorcy"); wytyczne EROD 01/2022 dotyczące praw osób, których dane dotyczą – Prawo dostępu, wersja 2.1, przyjęte 28 marca 2023 r. [zwane dalej *„wytycznymi EROD 01/2022 (prawo dostępu)")]*, pkt 117 *(„już na podstawie art. 13 i 14 RODO informacje na temat odbiorców lub kategorii odbiorców powinny być możliwie najbardziej konkretne, aby uczynić zadość zasadom przejrzystości i rzetelności*); zob. TSUE, wyrok z dnia 12 stycznia 2023 r., *RW przeciwko Österreichische Post AG*, C-154/21, pkt 25; opinia rzecznika generalnego w sprawie TSUE C-154/21, pkt 36 (*„art. 13 i 14 RODO [...] ustanawiają ciążący na administratorze danych obowiązek przekazania osobie, której dane dotyczą, informacji dotyczących kategorii odbiorców lub konkretnych odbiorców dotyczących jej danych osobowych, gdy dane te pozyskano od osoby, której dane dotyczą, względnie nie od tej osoby*").

[24] Artykuł 15 ust. 1 lit. c) RODO. Wytyczne EROD 01/2022 (prawo dostępu), pkt 116-117.

[25] Wyrok TSUE z dnia 12 stycznia 2023 r., *RW przeciwko Österreichische Post AG*, C-154/21, pkt 51: *„art. 15 ust. 1 lit. c) RODO należy interpretować w ten sposób, że przewidziane w tym przepisie prawo dostępu osoby, której dane dotyczą, do dotyczących jej danych osobowych oznacza, w przypadku gdy dane te zostały lub zostaną ujawnione odbiorcom, że na administratorze danych ciąży obowiązek podania tej osobie dokładnej tożsamości tych odbiorców, chyba że nie jest możliwe zidentyfikowanie tych odbiorców lub tenże administrator danych wykaże, że wnioski o uzyskanie dostępu złożone przez osobę, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne w rozumieniu art. 12 ust. 5 RODO, w których to przypadkach administrator może wskazać tej osobie wyłącznie kategorie odnośnych odbiorców*".
Trybunał przyznał, że osoba, której dane dotyczą, może również *„zdecydować się na ograniczenie się do zażądania informacji dotyczących kategorii odbiorców*". Wyrok TSUE z dnia 12 stycznia 2023 r., *RW przeciwko Österreichische Post AG*, C-154/21, pkt 43.
Wytyczne EROD 01/2022 (prawo dostępu), pkt 117.

wskazać osobie, której dane dotyczą, wyłącznie kategorie odbiorców, co do zasady administrator powinien zawsze mieć możliwość uzyskania imienia, nazwiska lub nazwy odbiorców i przekazania bez zbędnej zwłoki niezbędnych informacji osobom, których dane dotyczą.

- Artykuł 19 RODO stanowi, że administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. TSUE wyjaśnił, że artykuł 19 zdanie drugie RODO wyraźnie przyznaje osobie, której dane dotyczą, prawo do bycia informowaną o konkretnych odbiorcach[26].

31. Chociaż nie jest to wyraźnie określone w tych przepisach, EROD uważa, że do celów art. 28 ust. 1 i art. 28 ust. 2 RODO administratorzy powinni posiadać informacje na temat tożsamości wszystkich podmiotów przetwarzających, podwykonawców przetwarzania itp., które są łatwo dostępne w każdej chwili,[27] tak aby mogli oni jak najlepiej wypełniać swoje obowiązki wynikające z wyżej wymienionych przepisów. Taki dostęp jest również niezbędny, aby administratorzy mogli gromadzić i oceniać wszystkie informacje niezbędne do spełnienia wymogów określonych w RODO, w tym aby mogli bez zbędnej zwłoki odpowiadać na żądania o udzielenie dostępu na podstawie art. 15 RODO i szybko reagować na naruszenia ochrony danych, które mogą mieć miejsce w całym łańcuchu przetwarzania. Miałoby to zastosowanie niezależnie od ryzyka związanego z czynnością przetwarzania.

32. W tym celu podmiot przetwarzający powinien przez cały czas proaktywnie przekazywać administratorowi[28] wszystkie informacje na temat tożsamości wszystkich podmiotów przetwarzających, podwykonawców przetwarzania itp. przetwarzających dane w imieniu administratora oraz powinien stale aktualizować te informacje dotyczące wszystkich podwykonawców przetwarzania, z których usług korzysta. Administrator i podmiot przetwarzający mogą zawrzeć w umowie dalsze szczegóły dotyczące tego, w jaki sposób i w jakim formacie podmiot przetwarzający ma dostarczać te informacje, ponieważ administrator może zażądać określonego formatu, aby łatwiej było mu je pobrać i nimi zarządzać.

2.1.2 Weryfikacja i udokumentowanie przez administratora wystarczalności gwarancji zapewnionych przez wszystkie podmioty przetwarzające biorące udział w łańcuchu przetwarzania.

33. Pytania 1.1.b.i, 1.1.b.iii i 1.3 mają na celu wyjaśnienie, w jakim zakresie i na jakim poziomie szczegółowości administrator powinien weryfikować i dokumentować wystarczalność zabezpieczeń zapewnianych przez wszystkie podmioty przetwarzające w łańcuchu przetwarzania oraz w jakim stopniu obowiązki wynikające z art. 28 ust. 1 i art. 28 ust. 2 RODO w związku z art. 5 ust. 2 i art. 24 RODO różnią się w zależności od ryzyka związanego z czynnością przetwarzania. W odniesieniu do tych pytań EROD podkreśla następujące elementy.

[26] Wyrok TSUE z dnia 12 stycznia 2023 r., *RW przeciwko Österreichische Post AG*,C-154/21, pkt 41.

[27] Informacje te są niezbędne, aby administrator mógł wypełnić swoje obowiązki również w przypadku przerwania łańcucha przetwarzania danych, ponieważ jeden podmiot przetwarzający (lub podwykonawca przetwarzania) jest niedostępny, niechętny lub niewypłacalny i należy skontaktować się z innym podmiotem przetwarzającym (lub podwykonawcą przetwarzania).

[28] Aby zapewnić zgodność z art. 28 ust. 2 RODO, w celu umożliwienia administratorowi podjęcia decyzji o dodaniu podwykonawców przetwarzania, a także aby zapewnić zgodność z art. 28 ust. 1 RODO, w celu umożliwienia administratorowi sprawdzenia, czy podmioty przetwarzające (lub podwykonawcy przetwarzania) przedstawiają wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych.

34. W art. 5 ust. 2 RODO zapisano zasadę rozliczalności, czyniąc administratora danych odpowiedzialnym za zgodność z zasadami ochrony danych określonymi w art. 5 ust. 1 RODO i za możliwość wykazania tej zgodności. Art. 5 ust. 2 RODO ma zastosowanie do wszystkich ogólnych zasad wymienionych w art. 5 ust. 1 RODO.

35. Art. 24 ust. 1 RODO zawiera obowiązek wykazania przez administratora, że przetwarzanie odbywa się zgodnie z RODO, ale dalej rozwija jeden z obowiązków, do których ma zastosowanie zasada rozliczalności: wdrożenie „odpowiednich środków technicznych i organizacyjnych"[29]. Art. 24 ust. 1 RODO odnosi się do pojęcia „ryzyka"[30], mającego znaczenie dla jego stosowania, jako jednego z kryteriów, które administrator musi wziąć pod uwagę przy ocenie odpowiedniości takich środków[31]. Art. 24 ust. 1 RODO dodaje również, że środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

36. Jak stwierdził TSUE, *„w art. 5 ust. 2 i art. 24 RODO nałożono na administratorów danych osobowych ogólne wymogi dotyczące rozliczalności i przestrzegania przepisów. W szczególności przepisy te wymagają od administratorów wprowadzenia odpowiednich środków mających na celu zapobieżenie ewentualnym naruszeniom uregulowań przewidzianych w RODO w celu zapewnienia prawa do ochrony danych"* [32].

[29] Wyrok z dnia 25 stycznia 2024 r., *BL przeciwko MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, pkt 36: *„Artykuł 24 RODO przewiduje, że na administratorze danych osobowych ciąży ogólny obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić, by przetwarzanie to odbywało się zgodnie z tym rozporządzeniem, i być w stanie to wykazać*".

[30] W motywie 75 RODO wymieniono kilka przykładów ryzyka: *„przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną*"; w motywie 76 sprecyzowano: *„Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko"*. Jak podsumował TSUE *„zgodnie z motywem 76 tego rozporządzenia prawdopodobieństwo i powaga ryzyka zależą od specyfiki danego przetwarzania, a ryzyko to powinno podlegać obiektywnej ocenie*". (TSUE, wyrok z dnia 14 grudnia 2023 r., *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, pkt 36).

[31] Jak stwierdził TSUE, *„art. 24 wymienia w ust. 1 pewną liczbę kryteriów, które należy uwzględnić przy ocenie, czy takie środki mają odpowiedni charakter, a mianowicie charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i powadze zagrożenia"*, wyrok z dnia 14 grudnia 2023 r., *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, pkt 25. W tym samym orzeczeniu TSUE sprecyzował, że *„Okoliczność, czy takie środki mają odpowiedni charakter, należy oceniać w sposób konkretny, badając, czy środki te zostały wdrożone przez tego administratora z uwzględnieniem różnych kryteriów wskazanych (...) oraz potrzeb ochrony danych konkretnie związanych z danym przetwarzaniem, a także ryzyka wynikającego z tego przetwarzania"*, pkt 30; przypomniano również w wyroku z dnia 25 stycznia 2024 r., *BL przeciwko MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, pkt 38*: *„Z brzmienia art. 24 i 32 RODO wynika zatem, że odpowiedni charakter środków wdrożonych przez administratora należy oceniać w sposób konkretny, biorąc pod uwagę różne kryteria, o których mowa w tych artykułach, oraz potrzeby ochrony danych specyficznie związane z danym przetwarzaniem, a także wynikające z niego ryzyko, tym bardziej że wspomniany administrator musi być w stanie wykazać zgodność tych środków z RODO, której to możliwości zostałby pozbawiony, gdyby dopuścić domniemanie niewzruszalne".* Należy zauważyć, że analiza TSUE odnosi się również do art. 32 RODO.

[32] Wyrok z dnia 27 października 2022 r. w sprawie *Proximus NV przeciwko Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, pkt 81. Zob. również wytyczne EROD 07/2020, pkt 9.

37. Zasada rozliczalności jest skierowana do administratora, w tym w przypadku, gdy administrator powierzył podmiotom przetwarzającym lub podwykonawcom przetwarzania przetwarzanie danych osobowych w jego imieniu.

38. Zgodnie z art. 28 ust. 1 RODO, w przypadku gdy administrator zleca podmiotowi przetwarzającemu przetwarzanie danych osobowych w jego imieniu, administrator musi korzystać wyłącznie z usług takiego podmiotu przetwarzającego, który zapewnia *„wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi”* RODO *„i chroniło prawa osób, których dane dotyczą”*[33]. Jak wskazano w wytycznych EROD 07/2020, zasada rozliczalności znajduje również odzwierciedlenie w art. 28 RODO[34].

39. W tym względzie EROD podkreśla, że do celów oceny zgodności z art. 24 ust. 1 i art. 28 ust. 1 RODO organy nadzorcze powinny wziąć pod uwagę, że **korzystanie z usług podmiotów przetwarzających nie powinno obniżać stopnia ochrony praw osób, których dane dotyczą,** porównując z sytuacją, w której przetwarzanie jest przeprowadzane bezpośrednio przez administratora. Odnosi się to do korzystania z usług pierwotnego podmiotu przetwarzającego, ale także korzystania z usług dodatkowych podmiotów przetwarzających w całym łańcuchu przetwarzania, np. podwykonawców przetwarzania i podwykonawców podwykonawców przetwarzania. Art. 24 ust. 1 i art. 28 ust. 1 RODO należy interpretować w ten sposób, że zobowiązują one administratora do zapewnienia, aby łańcuch przetwarzania składał się wyłącznie z podmiotów przetwarzających, podwykonawców przetwarzania, podwykonawców podwykonawców przetwarzania (itd.), którzy zapewniają „wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych”. Ponadto administrator powinien być w stanie udowodnić, że poważnie wziął pod uwagę wszystkie elementy przewidziane w RODO[35]. Ma to zastosowanie nawet wtedy, gdy łańcuch przetwarzania jest długi i złożony, a poszczególne podmioty przetwarzające, podwykonawcy przetwarzania itd. uczestniczą na różnych etapach czynności przetwarzania. Administrator powinien dochować należytej staranności przy wyborze swoich podmiotów przetwarzających i nadzorze nad nimi.

40. Jeżeli chodzi o wybór **pierwotnego podmiotu przetwarzającego** administrator powinien indywidualnie dla każdego przypadku zweryfikować, czy udzielone gwarancje są wystarczające, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, a także zagrożeń dla praw i wolności osób fizycznych, na podstawie rodzaju przetwarzania powierzonego podmiotowi przetwarzającemu[36]. Zgodnie z art. 28 ust. 5 RODO podmiot przetwarzający może wykazać wystarczające gwarancje między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania na podstawie art. 40 lub zatwierdzonego mechanizmu certyfikacji na podstawie art. 42.

41. Jak wcześniej wspomniała EROD, przy weryfikacji gwarancji zapewnianych przez podmioty przetwarzające administrator powinien wziąć pod uwagę kilka elementów[37], a często będzie to wymagało wymiany odpowiedniej dokumentacji[38]. W każdym przypadku *„[g]warancje «zapewniane»*

[33] Wytyczne EROD 07/2020, pkt 94.
[34] Wytyczne EROD 07/2020, pkt 8.
[35] Wytyczne EROD 07/2020, pkt 94.
[36] Wytyczne EROD 07/2020, pkt 96.
[37] Wytyczne EROD 07/2020, pkt 97–98 (dotyczące wiedzy fachowej podmiotu przetwarzającego, jego wiarygodności i zasobów, a także reputacji podmiotu przetwarzającego na rynku oraz przestrzegania zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji).
[38] Wytyczne EROD 07/2020, pkt 95 (gdzie wymieniono kilka przykładów: np. polityki prywatności, warunków świadczenia usług, rejestru czynności przetwarzania, polityki zarządzania dokumentacją, polityki bezpieczeństwa informacji, sprawozdań z zewnętrznych audytów ochrony danych, uznanych międzynarodowych certyfikatów, takich jak normy ISO 27000).

przez podmiot przetwarzający to te, które podmiot przetwarzający jest w stanie wykazać w sposób zadowalający administratora, ponieważ są to jedyne gwarancje, które administrator może skutecznie uwzględnić przy ocenie wypełniania swoich obowiązków"[39]. Ani sam art. 28 ust. 1 RODO, ani poprzednie dokumenty EROD nie zawierają wyczerpującej listy dokumentów lub działań, które podmiot przetwarzający musi wykazać lub udowodnić, ponieważ w dużej mierze zależy to od konkretnych okoliczności przetwarzania[40]. Administrator może na przykład zdecydować się na sporządzenie kwestionariusza, aby zebrać informacje od podmiotu przetwarzającego w celu zweryfikowania odpowiednich gwarancji, poprosić o odpowiednią dokumentację, oprzeć się na publicznie dostępnych informacjach bądź certyfikatach lub sprawozdaniach z audytów wiarygodnych stron trzecich bądź przeprowadzić audyty na miejscu.

42. EROD określiła już, że obowiązek korzystania wyłącznie z usług podmiotów przetwarzających „zapewniających wystarczające gwarancje" zawarty w art. 28 ust. 1 RODO jest obowiązkiem ciągłym, a administrator powinien w odpowiednich odstępach czasu weryfikować gwarancje podmiotu przetwarzającego[41].

43. W świetle pytania 1.3, na które DK ON zwrócił uwagę w swoim wniosku dotyczącym ryzyka związanego z przetwarzaniem, EROD podkreśla, że pojęcie ryzyka odgrywa ważną rolę w szeregu przepisów RODO, w szczególności w odniesieniu do przepisów związanych z rozdziałem IV RODO[42].

44. Należy podkreślić, że odniesienia do „ryzyka" w art. 24 ust. 1 i motywie 74 RODO nie należy interpretować jako oznaczającego, że administrator może zaniedbać swoje obowiązki wynikające z RODO lub odstąpić od swoich obowiązków wynikających z RODO, jedynie na podstawie faktu, że uważa ryzyko naruszenia praw i wolności osób, których dane dotyczą, za „niskie". Obowiązek wdrożenia „odpowiednich środków technicznych i organizacyjnych" w celu zapewnienia zgodności z RODO, zgodnie z art. 24 ust. 1 RODO, zawsze ma zastosowanie, ale środki potrzebne do osiągnięcia tego rezultatu mogą się różnić w zależności od ryzyka[43].

45. O ile art. 28 ust. 1 RODO nie zawiera konkretnych odniesień do „ryzyka", wymaga on rozważenia stopnia ryzyka naruszenia praw i wolności osób, których dane dotyczą. Zawarty w art. 28 ust. 1 wymóg korzystania wyłącznie z usług podmiotów przetwarzających zapewniających „wystarczające gwarancje" wdrożenia „odpowiednich środków technicznych i organizacyjnych" należy interpretować jako oznaczający konieczność rozważenia zapewnienia przez podmioty przetwarzające wystarczających gwarancji wdrożenia takich środków w świetle ryzyka związanego z przetwarzaniem, ponieważ na przykład poziom środków bezpieczeństwa, które mają zostać wdrożone, zależy również od ryzyka.

---

[39] Wytyczne EROD 07/2020, pkt 95.

[40] Wytyczne EROD 07/2020, pkt 96 („*Ocena administratora, czy gwarancje są wystarczające, jest formą oceny ryzyka, która w znacznym stopniu zależy od rodzaju przetwarzania powierzonego podmiotowi przetwarzającemu i musi być dokonywana indywidualnie dla każdego przypadku, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, a także zagrożeń dla praw i wolności osób fizycznych. W związku z tym EROD nie może przedstawić wyczerpującej listy dokumentów lub działań, które podmiot przetwarzający musi wykazać lub udowodnić w danym scenariuszu, ponieważ w dużej mierze zależy to od konkretnych okoliczności przetwarzania."*

[41] Wytyczne EROD 07/2020, pkt 99: „*w tym w stosownych przypadkach poprzez audyty i inspekcje*".

[42] Termin „ryzyko" jest przywołany w art. 24, 25, 27, 30, 32, 33, 34, 35, 36 i 39 RODO.

[43] TSUE, wyrok z dnia 14 grudnia 2023 r., *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, pkt 35: „*w motywie 74 RODO podkreślono, że ważne jest, aby administrator był zobowiązany do wdrożenia odpowiednich i skutecznych środków oraz był w stanie wykazać zgodność czynności przetwarzania z tym rozporządzeniem, w tym skuteczność środków, które powinny uwzględniać kryteria związane z cechami danego przetwarzania i wynikającym z niego ryzykiem, które są również określone w art. 24 i 32 tego rozporządzenia*".

46. Ryzyko związane z czynnością przetwarzania odgrywa ważną rolę w określaniu odpowiedniości środków technicznych i organizacyjnych, a także innych kryteriów wymienionych w art. 24 ust. 1 RODO[44]. W zależności od poziomu ryzyka związanego z czynnością przetwarzania (na przykład w przypadku przetwarzania szczególnych kategorii danych osobowych) administrator może określić bardziej rygorystyczne lub szersze środki techniczne i organizacyjne. Każdy podmiot przetwarzający powinien zatem zapewnić wystarczające gwarancje skutecznego wdrożenia „odpowiednich" środków określonych przez administratora.

47. EROD uważa, że ***obowiązek*** **administratora polegający na weryfikacji, czy podmioty przetwarzające (lub podwykonawcy przetwarzania) przedstawiają wystarczające gwarancje w celu wdrożenia środków określonych przez administratora, powinien mieć zastosowanie niezależnie od ryzyka naruszenia praw i wolności osób, których dane dotyczą**.

48. **W praktyce *zakres* takiej weryfikacji będzie jednak różny, w zależności od charakteru środków organizacyjnych i technicznych określonych przez administratora, na podstawie między innymi ryzyka związanego z przetwarzaniem.** Na przykład, jeżeli czynności przetwarzania stwarzają mniejsze ryzyko naruszenia praw i wolności osób, których dane dotyczą, „odpowiednie środki" będą mniej rygorystyczne. W związku z tym w praktyce zakres weryfikacji prowadzonej przez administratora może być węższy. I odwrotnie, w przypadku wyższego ryzyka wynikającego z danego przetwarzania, stopień weryfikacji dokonywanej przez administratora może być większy pod kątem sprawdzenia wystarczających gwarancji przedstawionych przez cały łańcuch przetwarzania, biorąc pod uwagę, że „odpowiednie środki", które należy wdrożyć, mają szerszy zakres i są solidniejsze, tak aby przeciwdziałać ryzyku dla osób, których dane dotyczą.

49. W tym względzie, w zależności od poziomu ryzyka związanego z czynnością przetwarzania, administrator może zwiększyć stopień weryfikacji, weryfikując umowy dotyczące podwykonawstwa przetwarzania samodzielnie i (lub) nałożyć również na pierwotny podmiot przetwarzający obowiązek rozszerzenia weryfikacji i dokumentacji.

50. Zgodnie z zasadą rozliczalności wszelkie środki uznane za niezbędne do zapewnienia zgodności z RODO, również na podstawie ryzyka związanego z przetwarzaniem, powinny być odpowiednio udokumentowane przez administratora[45]. Realizację tego obowiązku ułatwiają z jednej strony **obowiązki w zakresie pomocy i audytu** nałożone na podmioty przetwarzające oraz, z drugiej strony, **informacje przekazane administratorowi przez pierwotny podmiot przetwarzający** przed skorzystaniem z usług dodatkowych podmiotów przetwarzających.

---

[44] Artykuł 24 ust. 1 odnosi się do „*charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia*".

[45] W odniesieniu do ciężaru dowodu spoczywającego na administratorze danych, zob. wyrok TSUE z dnia 14 grudnia 2023 r., *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, pkt 52: *„Z brzmienia art. 5 ust. 2, art. 24 ust. 1 i art. 32 ust. 1 RODO jednoznacznie wynika, że ciężar udowodnienia, iż dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tych danych w rozumieniu art. 5 ust. 1 lit. f) i art. 32 tego rozporządzenia, spoczywa na danym administratorze"*; zob. również wyrok TSUE z dnia 25 stycznia 2024 r., BL przeciwko MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, pkt 42 *„w tym względzie należy podkreślić, że z łącznej lektury art. 5, 24 i 32 RODO w świetle jego motywu 74 wynika, iż w ramach powództwa o odszkodowanie opartego na art. 82 tego rozporządzenia ciężar udowodnienia, że dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tych danych w rozumieniu art. 5 ust. 1 lit. f) i art. 32 tego rozporządzenia, spoczywa na danym administratorze. Taki rozkład ciężaru dowodu może nie tylko zachęcać administratorów danych do przyjęcia środków bezpieczeństwa wymaganych przez RODO, lecz również zapewniać skuteczność prawa do odszkodowania przewidzianego w art. 82 tego rozporządzenia i być zgodny z zamiarami prawodawcy Unii, o których mowa w motywie 11 tego rozporządzenia"*.

51. Po pierwsze, EROD zauważa, że podmioty przetwarzające mają obowiązek pomagać administratorowi w zapewnieniu zgodności z niektórymi wymogami RODO [na podstawie art. 28 ust. 3 lit. e) i f)][46]. Ogólniej mówiąc, podmiot przetwarzający ma obowiązek przekazać administratorowi wszelkie informacje niezbędne do wykazania zgodności z art. 28 [art. 28 ust. 3 lit. h)][47]. Administrator powinien być w pełni poinformowany o szczegółach przetwarzania, które są istotne dla wykazania zgodności z obowiązkami określonymi w art. 28 RODO, a podmiot przetwarzający powinien przekazać wszystkie informacje na temat sposobu wykonywania czynności przetwarzania w imieniu administratora danych[48]. Umowa powinna zawierać informacje na temat częstotliwości i sposobu przepływu informacji[49].

52. W związku z tym administrator może oprzeć się na informacjach przekazanych przez podmiot przetwarzający, zgodnie z art. 28 ust. 3 lit. h) RODO, przy wypełnianiu obowiązku dokumentowania przyjętych środków, pod warunkiem, że informacje przekazane przez podmiot przetwarzający faktycznie wykazują ich przestrzeganie. Ponieważ podmiot przetwarzający może zapoznać się ze szczegółami przetwarzania, którego dokonuje, oraz przetwarzania prowadzonego przez podwykonawców przetwarzania, powinien on proaktywnie przekazywać administratorowi wszystkie istotne informacje[50].

53. Powyższe ma zastosowanie również do podwykonawców przetwarzania. Podmioty przetwarzające są faktycznie zobowiązane do przekazywania obowiązków w zakresie pomocy kolejnym ogniwom łańcucha przetwarzania (art. 28 ust. 4 RODO).

54. Po drugie, **korzystanie z usług podwykonawców przetwarzania,** o czym jest mowa powyżej, jest możliwe wyłącznie na podstawie uprzedniej pisemnej zgody administratora, która może mieć charakter szczegółowy lub ogólny. Jeżeli administrator decyduje się udzielić ogólnej zgody, *„powinien ją uzupełnić o kryteria wyboru podmiotu przetwarzającego (np. gwarancje dotyczące środków technicznych i organizacyjnych, wiedzy fachowej, wiarygodności i zasobów)*[51].

55. Jak wyjaśniła EROD, *„[w] celu oceny i podjęcia decyzji, czy zezwolić na podwykonawstwo, podmiot przetwarzający będzie musiał dostarczyć administratorowi wykaz podwykonawców przetwarzania (obejmujący dla każdego z nich: ich lokalizację, czynności, które będą wykonywać, oraz dowód wdrożenia zabezpieczeń)*"[52]. Informacje te są potrzebne, aby administrator mógł przestrzegać zasady rozliczalności określonej w art. 5 ust. 2 i art. 24 oraz przepisów art. 28 ust. 1, art. 32 i rozdziału V

[46] Zob. wytyczne EROD 07/2020, pkt 130-138.
[47] Zob. wytyczne EROD 07/2020, pkt 143-145.
[48] Wytyczne EROD 07/2020, pkt 143.
[49] Wytyczne EROD 07/2020, pkt 143.
[50] Wytyczne EROD 07/2020, pkt 143, odnoszący się do art. 28 ust. 3 lit. h): *Na przykład administratorowi mogą zostać udostępnione odpowiednie fragmenty rejestrów podmiotu przetwarzającego dotyczące czynności przetwarzania. Podmiot przetwarzający powinien przekazać wszelkie informacje na temat sposobu, w jaki będzie przetwarzać dane w imieniu administratora. Informacje takie powinny obejmować informacje na temat funkcjonowania wykorzystywanych systemów, środków bezpieczeństwa, sposobu spełniania wymogów zatrzymywania danych, lokalizacji danych, przekazywania danych, tego, kto ma dostęp do danych i kto jest ich odbiorcą, podwykonawców przetwarzania danych itd.".* Możliwość przeprowadzenia audytu przez administratora określono również w pkt 144: *„Celem takiego audytu jest zapewnienie, aby administrator posiadał wszystkie informacje dotyczące czynności przetwarzania prowadzonej w jego imieniu oraz gwarancje udzielone przez podmiot przetwarzający."*
[51] Wytyczne EROD 07/2020, pkt 156.
[52] Wytyczne EROD 07/2020, pkt 152.

RODO[53]. W odniesieniu do przekazywania danych osobowych poza EOG EROD odnosi się do odpowiedzi przedstawionej poniżej na pytanie 1.2 zadane przez DK ON.

56. Jak przypomniała EROD, pierwotny podmiot przetwarzający powinien dopilnować, aby proponowani przez niego podwykonawcy przetwarzania zapewniali wystarczające gwarancje[54]. Konieczność dostarczenia przez pierwotny podmiot przetwarzający powyższych informacji wskazuje, że **podmiot przetwarzający ma pewną rolę do odegrania w wyborze podwykonawców przetwarzania i weryfikacji zapewnianych przez nich gwarancji oraz powinien przekazać administratorowi wystarczające informacje**. Jest to również spójne z faktem, że niezależnie od wskazanych przez administratora kryteriów wyboru dodatkowych podmiotów przetwarzających, pierwotny podmiot przetwarzający ponosi wobec administratora danych pełną odpowiedzialność za wykonanie obowiązków przez podwykonawców przetwarzania (art. 28 ust. 4 RODO).

57. W tym względzie, nawet jeśli zgodnie z art. 28 ust. 4 RODO, na podmiocie przetwarzającym, który korzysta z usług podwykonawcy przetwarzania, spoczywa bezpośrednia odpowiedzialność za zapewnienie nałożenia na takiego innego przetwarzającego takich samych obowiązków ochrony danych, jak określono w pierwotnej umowie między administratorem a podmiotem przetwarzającym, nie znosi to odpowiedzialności administratora za zapewnienie zgodności z wymogami art. 28 ust. 1 i art. 24 ust. 1 RODO oraz za możliwość wykazania tej zgodności.

58. **Ostateczna decyzja w sprawie skorzystania z usług konkretnego podwykonawcy (podwykonawcy) przetwarzania i związanej z tym odpowiedzialności, w tym w odniesieniu do weryfikacji wystarczalności gwarancji zapewnianych przez podmiot przetwarzający (lub podwykonawcę przetwarzania), pozostaje w gestii administratora.** Jak już wspomniano, w przypadku ogólnej lub szczegółowej zgody do administratora należy zawsze decyzja, czy zatwierdzić korzystanie z usług tego podwykonawcy przetwarzania, czy nie.

59. Oceniając zgodność z art. 24 ust. 1 i art. 28 ust. 1 RODO, organy nadzorcze powinny ocenić, czy administrator jest w stanie wykazać, że weryfikacja wystarczalności gwarancji zapewnionych przez jego podwykonawców przetwarzania została przeprowadzona w sposób zadowalający dla administratora. Oznacza to, że administrator może opierać się na informacjach otrzymanych od swojego podmiotu przetwarzającego i w razie potrzeby je uzupełniać. Na przykład w przypadku, gdy informacje przekazane administratorowi wydają się niekompletne, nieprawidłowe lub budzą wątpliwości, lub w stosownych przypadkach oparte są na okolicznościach sprawy zawierającej ryzyko związane z przetwarzaniem, administrator powinien poprosić o dodatkowe informacje lub zweryfikować otrzymane informacje i w razie potrzeby je uzupełnić lub poprawić.

60. W szczególności, w przypadku przetwarzania stwarzającego wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, administrator powinien zwiększyć stopień weryfikacji, jeżeli chodzi o sprawdzanie dostarczonych informacji dotyczących gwarancji przedstawionych przez różne podmioty przetwarzające w łańcuchu przetwarzania.

[53] Wytyczne EROD 07/2020, przypis 69.
[54] Wytyczne EROD 07/2020, pkt 159.

2.1.3 Weryfikacja umowy między pierwotnym podmiotem przetwarzającym a dodatkowymi podmiotami przetwarzającymiError! Bookmark not defined.

61. DK ON pyta zasadniczo, czy i w jakim zakresie administrator ma obowiązek sprawdzić i udokumentować, że umowy dotyczące podwykonawstwa przetwarzania nakładają na dodatkowe podmioty przetwarzające takie same obowiązki.

62. Artykuł 28 ust. 4[55] nakłada w tym względzie bezpośredni obowiązek na podmioty przetwarzające. Ponadto art. 28 ust. 3 lit. d) zobowiązuje administratora i podmiot przetwarzający do „ustanowienia" w umowie obowiązku przestrzegania przez podmiot przetwarzający warunków, o których mowa w art. 28 ust. 4, co czyni ten wymóg obowiązkiem umownym nałożonym na podmiot przetwarzający. Innymi słowy, **pierwotny podmiot przetwarzający jest prawnie i umownie zobowiązany do przeniesienia na inne podmioty tych samych obowiązków ochrony danych w umowach dotyczących podwykonawstwa przetwarzania, które zawiera z dodatkowymi podmiotami przetwarzającymi.**

[55] Art. 28 ust. 4 RODO: *„Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia."*

63. Podobnie dodatkowe podmioty przetwarzające będą umownie zobowiązane (przez pierwotny podmiot przetwarzający) do nałożenia takich samych obowiązków ochrony danych na własne podmioty przetwarzające, i na kolejne podmioty w łańcuchu przetwarzania[56]. Nie jest wymagane, aby umowa dotycząca podwykonawstwa przetwarzania miała identyczne brzmienie, jak umowa o przetwarzaniu danych zawarta z pierwotnym podmiotem przetwarzającym[57].

64. EROD przypomina, że jeżeli podwykonawca przetwarzania nie wywiązuje się ze swoich obowiązków, ostateczna odpowiedzialność za wykonanie zobowiązań przez tego innego podwykonawcę przetwarzania spoczywa na administratorze. Pierwotny podmiot przetwarzający pozostanie jednak odpowiedzialny wobec administratora, tak aby administrator miał możliwość wystąpienia z roszczeniem umownym wobec swojego pierwotnego podmiotu przetwarzającego, jeżeli taki podmiot przetwarzający nie nałoży na kolejne podmioty tych samych obowiązków ochrony danych w umowach dotyczących podwykonawstwa przetwarzania.

65. Podmioty przetwarzające mają obowiązek przekazać administratorowi wszelkie informacje niezbędne do wykazania zgodności z art. 28 ust. 3 lit. h RODO. W związku z tym, na wniosek administratora pierwotny podmiot przetwarzający będzie musiał przedstawić umowy dotyczące podwykonawstwa przetwarzania zawarte między pierwotnym podmiotem przetwarzającym a dodatkowymi podmiotami przetwarzającymi.

66. W tym względzie wydane przez KE standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi [58] i międzynarodowe klauzule umowne dotyczące międzynarodowego przekazywania danych[59] zapewniają administratorowi możliwość zażądania kopii umowy dotyczącej

[56]We Wspólnej opinii EROD i EIOD 2/2021 dotyczącej decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich podkreślono, że wymóg określony w art. 28 ust. 4 RODO musi być brany pod uwagę przez strony w relacji między podmiotami przetwarzającymi (pkt 66).

[57] Wytyczne EROD 07/2020, pkt 160: *„Nakładanie «tych samych» obowiązków należy interpretować w sposób funkcjonalny, a nie formalny: nie jest konieczne, aby umowa zawierała dokładnie takie same słowa, jak te użyte w umowie między administratorem a podmiotem przetwarzającym, lecz powinna zapewnić, aby obowiązki co do istoty były takie same".* EROD zauważa również, że w przypadku gdy dwa podmioty przetwarzające opierają się na module trzecim (relacja między podmiotami przetwarzającymi) standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych, pierwotny podmiot przetwarzający zapewnia dodatkowego gwaranta. Zgodnie z klauzulą 8.1.d standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych, podmiot przekazujący dane (pierwotny podmiot przetwarzający) gwarantuje, że na podmiot odbierający dane (podwykonawcę przetwarzania) nałożył takie same obowiązki ochrony danych – na mocy prawa Unii lub prawa państwa członkowskiego – jak w umowie lub innym instrumencie prawnym między administratorem a podmiotem przekazującym dane.

[58] Zgodnie z sekcją 7 dotyczącą korzystania z usług podwykonawców, art. 7 ust. 7 lit. c) standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi stanowi: *„Na wniosek administratora podmiot przetwarzający przekazuje administratorowi kopię umowy, jaką zawarł z podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem".* Decyzja wykonawcza Komisji 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia (UE) 2018/1725 („wydane przez KE standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi").

[59] Moduł drugi (przekazywanie danych przez administratora podmiotowi przetwarzającemu), klauzula 9 lit. c) standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych stanowi: *„Na żądanie podmiotu przekazującego dane podmiot odbierający dane przekazuje podmiotowi przekazującemu dane kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie*

podwykonawstwa przetwarzania zawartej między pierwotnym podmiotem przetwarzającym a dodatkowymi podmiotami przetwarzającymi. Taką możliwość przewidują również trzy standardowe klauzule umowne między administratorami a podmiotami przetwarzającymi przyjęte przez organy nadzorcze[60]. Możliwość ta wyraża prawo administratora do audytu, o którym mowa w art. 28 ust. 3 lit. h) RODO. Na żądanie administratora podmiot przetwarzający powinien dostarczyć taką kopię.

67. EROD zauważa jednak, że standardowe klauzule umowne nie regulują, czy administrator *musi* zażądać takiej kopii w celu zapewnienia zgodności z art. 28 ust. 1 RODO.

68. W związku z tym to, czy administrator zdecyduje się zażądać takiej kopii, czy też nie, nie może stanowić o odpowiedzialności administratora. Podmiot przetwarzający ponosi również, w każdym przypadku, zobowiązania prawne i umowne zobowiązujące go do nałożenia takich samych obowiązków ochrony danych, jak w pierwotnej umowie.

69. Niemniej **administrator nie ma obowiązku systematycznego zwracania się o umowy dotyczące podwykonawstwa przetwarzania, w celu sprawdzenia, czy obowiązki ochrony danych przewidziane w pierwotnej umowie zostały przeniesione na kolejne ogniwa łańcucha przetwarzania**. Administrator powinien ocenić, indywidualnie dla każdego przypadku, czy żądanie kopii takich umów lub ich sprawdzanie w dowolnym momencie jest konieczne, aby wykazać zgodność w świetle zasady rozliczalności. Jeżeli chodzi o korzystanie z prawa do przeprowadzenia audytu na mocy art. 28 ust. 3 lit. h) administrator powinien mieć zaplanowany proces przeprowadzenia kampanii audytowych, w celu sprawdzenia w drodze kontroli wyrywkowej, czy umowy z podwykonawcami przetwarzania zawierają niezbędne obowiązki ochrony danych.

70. Konieczność zażądania kopii umowy dotyczącej podwykonawstwa przetwarzania zależy zatem od okoliczności danej sprawy. Przykładowo, w razie wątpliwości co do spełniania przez podmiot przetwarzający lub podwykonawcę przetwarzania wymogów art. 28 ust. 1 i art. 28 ust. 4 lub na wniosek organu nadzorczego, administrator powinien zwrócić się o udostępnienie umowy w celu jej weryfikacji (np. w przypadku, gdy ochrona danych dodatkowego podmiotu przetwarzającego została naruszona lub w przypadku istnienia innych publicznie dostępnych informacji lub innych informacji dostępnych administratorowi), np. mogą istnieć wzory umowy dotyczące przetwarzania danych przez podwykonawcę przetwarzania, które nie spełniają wymogów art. 28 ust. 3 RODO.

71. Aby zapewnić zgodność z art. 28 ust. 1 w świetle zasady rozliczalności, kopia umów dotyczących podwykonawstwa przetwarzania może pomóc administratorowi wykazać, że jego podmioty przetwarzające i podwykonawcy przetwarzania zapewniają wystarczające gwarancje, w tym że podmiot przetwarzający przestrzega art. 28 ust. 4 RODO. EROD zauważa, że administrator może nie być w stanie ocenić, czy zapewnione gwarancje w odniesieniu do podwykonawcy przetwarzania są

koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii". Ponadto moduł trzeci (przekazywanie między podmiotami przetwarzającymi) stanowi, że *„Na żądanie podmiotu przekazującego dane lub administratora podmiot odbierający dane przekazuje kopię umowy dotyczącej podwykonawstwa przetwarzania oraz wszelkich późniejszych zmian. W zakresie koniecznym do zapewnienia ochrony tajemnic handlowych lub innych informacji poufnych, w tym danych osobowych, podmiot odbierający dane może zredagować tekst umowy przed udostępnieniem jej kopii".* Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych")

[60] Standardowe klauzule umowne DK ON do celów zgodności z art. 28 RODO, w szczególności klauzula 7.5; standardowe klauzule umowne LT ON do celów zgodności z art. 28 RODO, w szczególności klauzula 18; standardowe klauzule umowne SI ON do celów zgodności z art. 28 RODO, w szczególności klauzula 6.5.

wystarczające, czy nie, bez uzyskania dostępu do treści umowy dotyczącej podwykonawstwa przetwarzania i jej oceny. O ile gwarancje mogą być przewidziane na piśmie w umowie, klauzule umowne nie mogą – same w sobie – wykazać, że wystarczające gwarancje są skutecznie wdrażane przez strony umowy.

2.2 W sprawie interpretacji art. 28 ust. 1 RODO w związku z art. 44 RODO (przekazywanie w łańcuchu przetwarzania – pytania 1.2 i 1.3)

72. Pytanie 1.2 zawarte we wniosku ma na celu wyjaśnienie, w przypadkach przekazywania danych lub dalszego przekazywania danych od podmiotu przetwarzającego (lub podwykonawcy przetwarzania) do innego podmiotu przetwarzającego (lub podwykonawcy przetwarzania), w jakim stopniu administrator powinien – w ramach swojego obowiązku wynikającego z art. 28 ust. 1 RODO w związku z art. 44 RODO – ocenić dokumentację otrzymaną od podmiotu przetwarzającego (lub podwykonawcy przetwarzania), iż stopień ochrony danych osobowych nie został naruszony w wyniku pierwotnego lub dalszego przekazywania danych.

73. Pytanie 1.3 ma na celu wyjaśnienie, czy zakres obowiązków wynikających z art. 28 ust. 1 RODO w związku z art. 5 ust. 2 i art. 24 RODO, jak wskazano w odpowiedzi do pytania 1.2, różni się w zależności od ryzyka związanego z czynnością przetwarzania. Jeżeli tak, DK ON chciałby wiedzieć, jaki jest zakres takich obowiązków w odniesieniu do czynności przetwarzania „niskiego ryzyka” i „wysokiego ryzyka”.

Wyjaśnienia wprowadzające

74. W celu zapewnienia jasności przedstawiono pewne wyjaśnienia wprowadzające dotyczące powyższych pytań w kontekście niniejszej opinii.

75. Po pierwsze, EROD rozumie termin „przekazanie" w znaczeniu określonym w wytycznych EROD 05/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a rozdziału V RODO[61] [zwanych dalej „wytycznymi EROD 05/2021 (wzajemne zależności)"], które odnoszą się również do wytycznych EROD 3/2018 w sprawie terytorialnego zakresu stosowania RODO[62]. Jak już wcześniej podkreśliła EROD, zdalny dostęp z państwa trzeciego stanowi przekazanie, jeśli spełnia kryteria określone w wytycznych EROD 05/2021 (wzajemne zależności)[63]. W każdym przypadku występowanie przekazania powoduje zastosowanie rozdziału V RODO.

76. Po drugie, ponieważ pytanie 1.2 odnosi się do sytuacji, w której podmiot przetwarzający (lub podwykonawca przetwarzania) dokonuje pierwotnego lub dalszego przekazywania danych innemu podmiotowi przetwarzającemu (lub podwykonawcy przetwarzania), administrator danych nie jest podmiotem przekazującym dane; podmiotem przekazującym dane jest raczej podmiot przetwarzający, który przekazuje dane osobowe innemu podmiotowi przetwarzającemu w łańcuchu w imieniu administratora danych, a nie odrębnemu administratorowi danych. Nie obejmuje to zatem danych osobowych przekazywanych odrębnym administratorom, w tym trybunałom państw trzecich, sądom lub organom administracyjnym. W związku z tym interpretacja art. 48 RODO nie wchodzi w zakres tych pytań.

77. Po trzecie, EROD zauważa, że pytanie 1.2 odnosi się do przekazywania odbywającego się w całym łańcuchu przetwarzania zgodnie z udokumentowanym poleceniem administratora, na podstawie art. 28 ust. 3 lit. a) RODO. Warto podkreślić, że to administrator decyduje, czy przekazanie danych osobowych poza EOG jest możliwe w ramach czynności przetwarzania powierzonych podmiotom przetwarzającym (lub podwykonawcom przetwarzania). Podmiot przetwarzający nie powinien dokonywać żadnego pierwotnego lub dalszego przekazania, które nie jest na polecenie administratora[64]. Udokumentowane polecenie administratora dotyczące pierwotnego lub dalszego przekazywania danych osobowych muszą być przekazywane kolejnym ogniwom łańcucha przetwarzania[65].

78. Po czwarte, EROD wyjaśnia, że pojęcie ryzyka, o którym mowa w pytaniu 1.3, należy rozumieć jako ryzyko naruszenia praw i wolności osób, których dane dotyczą i których dane osobowe są przetwarzane, w rozumieniu motywów 75 i 76 RODO (jak wspomniano w pkt 35 powyżej).

---

[61] Wytyczne EROD 05/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO, wersja 2.0, przyjęte 14 lutego 2023 r., w których w pkt 9 określono trzy kryteria łączne kwalifikowania operacji przetwarzania jako przekazywanie, a w sekcji 2 wyszczególniono te kryteria bardziej ogólnie.

[62] Wytyczne EROD 05/2021 (wzajemne zależności), pkt 12 odnoszący się do wytycznych EROD nr 3/2018 w sprawie terytorialnego zakresu stosowania RODO, wersja 2.1, przyjęte 12 listopada 2019 r. (ze sprostowaniem z dnia 7 stycznia 2020 r.), str. 5 i sekcje 1–3. Zob. w szczególności „d) Podmiot przetwarzający niemający jednostki organizacyjnej w Unii" w sekcji 2.

[63] Wytyczne EROD 05/2021 (wzajemne zależności), pkt 16.

[64] Art. 29 RODO. Jak przypomniała EROD, *„Umowa powinna określać wymogi dotyczące przekazywania danych do państw trzecich lub organizacji międzynarodowych, z uwzględnieniem przepisów rozdziału V RODO*" (wytyczne EROD 07/2020, pkt 119). Administrator może na przykład zakazać przekazywania danych lub zezwolić na ich przekazywanie wyłącznie do określonych państw.

[65] Art. 28 ust. 4 RODO.

Odpowiedzialność administratora istnieje nawet wtedy, gdy podmioty przetwarzające (lub podwykonawcy przetwarzania) dokonują pierwotnego lub dalszego przekazywania

79. Jeśli chodzi o treść wniosku, EROD wskazała już, że *„(...) w sytuacji, gdy podmiot przetwarzający (zgodnie z art. 3 ust. 1 lub albo zgodnie z art. 3 ust. 2 w odniesieniu do konkretnej operacji przetwarzania (...)) przesyła dane innemu podmiotowi przetwarzającemu lub nawet administratorowi w państwie trzecim na polecenie administratora, przekazanie będzie miało miejsce. W takich przypadkach podmiot przetwarzający działa jako podmiot przekazujący dane w imieniu administratora i musi zapewnić przestrzeganie przepisów rozdziału V w odniesieniu do tego przekazywania zgodnie z poleceniami administratora, w tym zapewnić wykorzystanie odpowiedniego narzędzia przekazywania. Biorąc pod uwagę, że przekazywanie danych jest czynnością przetwarzania prowadzoną w imieniu administratora,* ***administrator również jest odpowiedzialny w tym względzie i może ponosić odpowiedzialność na podstawie rozdziału V, a także musi zadbać o to, by podmiot przetwarzający zapewniał wystarczające gwarancje zgodnie z art. 28”***[66].

80. Innymi słowy w przypadku przekazania, nawet jeżeli nie jest ono dokonywane bezpośrednio przez administratora, lecz przez podmiot przetwarzający w imieniu administratora, administrator nadal podlega obowiązkom wynikającym zarówno z art. 44 RODO, jak i z art. 28 ust. 1 RODO[67][68].

Odpowiedzialność wynikająca z art. 44 RODO

81. Obowiązki określone w art. 44 RODO[69] są nałożone zarówno na podmioty przetwarzające dane (w kontekście tej opinii działających jako podmioty przekazujące dane), jak i na administratorów[70]. W związku z tym zarówno podmioty przetwarzające, jak i administratorzy powinni zapewnić, aby stopień ochrony danych osobowych nie został naruszony w wyniku pierwotnego lub dalszego przekazywania, niezależnie od podstawy przekazywania danych[71]. Na przykład zarówno administrator, jak i podmiot przetwarzający pozostają, co do zasady, odpowiedzialni na podstawie rozdziału V RODO za niezgodne z prawem pierwotne lub wtórne przekazanie,[72] w związku z czym w przypadku naruszenia mogą zostać pociągnięci do odpowiedzialności zarówno wspólnie, jak i indywidualnie.

[66] Wytyczne EROD 05/2021 (wzajemne zależności), pkt 19, wytłuszczenie dodano.

[67] Istotne jest również wskazanie, że art. 28 ust. 1 RODO odnosi się do spełnienia wymogów RODO, a zatem należy go interpretować jako obejmujący przepisy rozdziału V dotyczące pierwotnego lub dalszego przekazywania danych osobowych do państw trzecich. Dotyczy to zarówno pierwotnego, jak i dalszego przekazywania, zob. art. 44 RODO.

[68] Do celów tej sekcji niniejszej opinii uwzględniono obowiązki wynikające z art. 44 i art. 28 ust. 1 RODO, przy czym określono, że administrator nadal podlega wszystkim obowiązkom mającym zastosowanie do administratorów danych na mocy RODO.

[69] Art. 44 RODO odnosi się do postanowień rozdziału V RODO.

[70] Art. 44 RODO odnosi się zarówno do „administratora, jak i podmiotu przetwarzającego” w celu zapewnienia zgodności z rozdziałem V; zob. również motyw 101. Z tego powodu zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0, przyjęte 18 czerwca 2021 r. (zwane dalej „zaleceniami EROD 01/2020”) mają zastosowanie do „podmiotów przekazujących” (niezależnie od tego, czy to administratorzy czy podmioty przetwarzające (lub podwykonawcy przetwarzania) przetwarzają dane osobowe).

[71] Wyrok TSUE z dnia 16 lipca 2020 r., *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi* (zwany dalej „wyrokiem TSUE Schrems II”), sprawa C-311/18, ECLI:EU:C:2020:559 pkt 92.

[72] Administrator może zwrócić się do swojego podmiotu przetwarzającego o odszkodowanie odpowiadające jego części odpowiedzialności, o ile spełnione są warunki określone w art. 82 ust. 5 RODO.

Odpowiedzialność wynikająca z art. 28 ust. 1 RODO

82. Zgodnie z zasadą rozliczalności administratorzy są zobowiązani do wprowadzenia „odpowiednich środków" mających na celu zapobieżenie ewentualnym naruszeniom uregulowań przewidzianych w RODO w celu zapewnienia prawa do ochrony danych,[73] co obejmuje zapobieganie naruszeniom rozdziału V RODO. Odpowiedzialność ta ma zastosowanie przed rozpoczęciem przekazywania danych i tak długo, jak przekazywane dane osobowe są przetwarzane w państwie trzecim.

83. Jak wyjaśniono w pkt 47–48 powyżej, *obowiązek administratora* polegający na weryfikacji, czy podmioty przetwarzające (lub podwykonawcy przetwarzania) przedstawiają wystarczające gwarancje w celu wdrożenia środków określonych przez administratora na podstawie art. 28 ust. 1 RODO[74], powinien mieć zastosowanie niezależnie od ryzyka naruszenia praw i wolności osób, których dane dotyczą. W praktyce *zakres* takiej weryfikacji będzie jednak różny, w zależności od charakteru środków organizacyjnych i technicznych określonych przez administratora, na podstawie między innymi ryzyka związanego z przetwarzaniem[75]. W tym względzie istnienie pierwotnego lub dalszego przekazania do państw trzecich w całym łańcuchu przetwarzania może zwiększać ryzyko wynikające z przetwarzania i w związku z tym mieć wpływ na „odpowiednie" środki określone przez administratora[76].

84. Na żądanie administrator – z pomocą podmiotu przetwarzającego i podwykonawców przetwarzania – powinien być w stanie wykazać właściwemu organowi nadzorczemu, że spełnia wymogi art. 28 ust. 1 RODO. Odpowiednia dokumentacja może opierać się – między innymi – na informacjach otrzymanych od podmiotów przetwarzających w kontekście korzystania z usług podmiotów przetwarzających (lub podwykonawców przetwarzania)[77] (zob. pkt 54-56), ale także z pomocą podmiotów przetwarzających, zgodnie z art. 28 ust. 3 lit. h) RODO (zob. pkt 51-52).

[73] Zob. sekcja powyżej dotycząca art. 5 ust. 2 i art. 24 ust. 1 w połączeniu z art. 28 ust. 1 RODO.

[74] W celu uniknięcia wątpliwości należy wyjaśnić, że „odpowiednich środków technicznych i organizacyjnych", o których mowa w art. 24 ust. 1 i art. 28 ust. 1 RODO, nie należy mylić ze „środkami uzupełniającymi", o których mowa w zaleceniach EROD 01/2020 (pkt 50: „«*Środki uzupełniające» są z definicji uzupełnieniem zabezpieczeń, które już zapewnia narzędzie przekazywania z art. 46 RODO, oraz wszelkich innych mających zastosowanie wymogów bezpieczeństwa (np. technicznych środków bezpieczeństwa) ustanowionych w RODO*", odwołując się do motywu 109 RODO i wyroku TSUE Schrems II, pkt 133).

[75] Zob. definicję ryzyka, jak wyjaśniono w pkt 35 i 78.

[76] Motyw 116 RODO stanowi: *„Transgraniczne przekazywanie danych osobowych poza Unię może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji."*

[77] Zobacz również klauzulę 9 lit. a) modułu trzeciego (przekazywanie między podmiotami przetwarzającymi) standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych oraz załącznik III do nich; zob. również klauzulę 9 lit. a) modułu drugiego (przekazywanie przez administratora podmiotowi przetwarzającemu); oraz klauzulę 7.7 lit. a) standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi i załącznik IV do nich „Wykaz podwykonawców przetwarzania". Zarówno załącznik II do standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych, jak i załącznik IV do standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi należy uzupełnić o następujące informacje na temat podwykonawców przetwarzania w przypadku szczególnego upoważnienia ze strony administratora: nazwa, adres, imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów, stanowisko i dane kontaktowe oraz opis przetwarzania. Ponadto załącznik I do standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych, sekcja B „Opis przekazywania danych" stanowi, że „W przypadku przekazywania podwykonawcom przetwarzania należy również określić przedmiot, charakter i czas trwania przetwarzania". Podobnie załącznik II do standardowych klauzul umownych między administratorem a podmiotem przetwarzającym zawiera sformułowanie „W przypadku przetwarzania przez podwykonawców przetwarzania należy również określić przedmiot, charakter i czas trwania przetwarzania".

85. Administrator potrzebuje również wszystkich istotnych informacji, aby wydać wymagane polecenie, aby przekazać dane osobowe do odpowiednich państw trzecich oraz aby móc przestrzegać zasady rozliczalności określonej w art. 5 ust. 2 i art. 24 RODO, a także przepisów art. 28 ust. 1, art. 32 i rozdziału V RODO[78]. Administrator może zgłosić sprzeciw lub nie zezwolić na korzystanie z usług dodatkowego podmiotu przetwarzającego, jeżeli wiązałoby się to z przekazaniem danych osobowych od pierwotnego podmiotu przetwarzającego (jako przekazującego) do planowanego dodatkowego podmiotu przetwarzającego (jako odbierającego) na podstawie otrzymanych informacji.

86. Zgodnie z pkt 58 powyżej administrator jest ostatecznie odpowiedzialny za wszelkie naruszenie art. 28 ust. 1 RODO, jeżeli chodzi o korzystanie z usług podmiotów przetwarzających (lub podwykonawców przetwarzania) i może zostać za nie pociągnięty do odpowiedzialności. EROD podkreśla, że praktyczne trudności, na które powołują się administratorzy, dotyczące kontroli korzystania przez ich podmiot przetwarzający z usług podwykonawców przetwarzania – co może utrudniać im weryfikację „wystarczających gwarancji", zwłaszcza w odniesieniu do przekazywania danych do państw trzecich – nie zwalniają administratora z odpowiedzialności za przetwarzanie[79].

87. Poniżej przytoczono niektóre przykłady dokumentacji, którą administrator powinien ocenić i być w stanie przedstawić właściwemu organowi nadzorczemu – zidentyfikowanie przekazania, podstawa, na jakiej przekazano dane oraz, w stosownych przypadkach, „ocena skutków przekazania danych" i środki uzupełniające.

Zidentyfikowanie przekazania:

88. W pierwszej kolejności, w przypadku gdy dane osobowe zostaną przekazane do państw trzecich w związku z korzystaniem z usług podmiotów przetwarzających (lub podwykonawców przetwarzania), administrator powinien ocenić dokumentację dotyczącą zidentyfikowania przekazania i być w stanie ją przedstawić[80]. Administrator powinien dopilnować, aby podmiot przekazujący (który przetwarza dane osobowe w jego imieniu) sporządził zidentyfikowanie przekazania i określił w nim, jakie dane osobowe są przekazywane (w tym zdalny dostęp), gdzie i w jakich celach[81]. Administrator może oprzeć się na takim zidentyfikowaniu przekazania i w razie potrzeby go uzupełnić. Na przykład w przypadku gdy zidentyfikowanie przekazania otrzymane przez administratora wydaje się niekompletne[82], nieprawidłowe lub budzi wątpliwości, administrator powinien zwrócić się o dodatkowe informacje, sprawdzić istniejące informacje i w razie potrzeby uzupełnić je lub skorygować.

89. Administrator powinien otrzymać te informacje[83] przed skorzystaniem z usług dodatkowego podmiotu przetwarzającego. Należy również przypomnieć, że administrator podlega szczególnym wymogom w zakresie przejrzystości w odniesieniu do przekazywania danych do państw trzecich na podstawie art. 13 ust. 1 lit. f), art. 14 ust. 1 lit. f), art. 15 ust. 1 lit. c) i art. 15 ust. 2 RODO oraz wymogowi prowadzenia rejestrów czynności przetwarzania na podstawie art. 30 ust. 1 lit. d) i e) RODO. Aby

[78] Wytyczne EROD 07/2020, pkt 152, przypis 69.
[79] CEF Report on Cloud Services (*„Sprawozdanie CEF w sprawie usług przetwarzania w chmurze"*), str. 16.
[80] „Zidentyfikowanie przekazania" odnosi się do pierwszego kroku (tzw. „Rozpoznanie przeprowadzanych operacji przekazywania") zaleceń EROD 01/2020, sekcja 2.1 „Krok 1: Rozpoznanie przeprowadzanych operacji przekazywania". Ten pierwszy krok ma zastosowanie niezależnie od podstawy, na jakiej przekazano dane.
[81] Należy uściślić, że cele, podobnie jak „istotne sposoby przetwarzania" są określane przez administratora (zob. wytyczne EROD 07/2020, pkt 40).
[82] Np. jeżeli w zidentyfikowaniu przekazania nie określono lokalizacji podwykonawców przetwarzania lub jeżeli w zidentyfikowaniu przekazania nie uwzględniono przekazania danych w formie zdalnego dostępu, gdy te mają miejsce.
[83] Jak wyjaśniono powyżej w pkt 54–56.

spełnić te wymogi, administrator powinien wiedzieć, gdzie znajdują się podwykonawcy przetwarzania i gdzie odbywa się przekazanie danych – w tym zdalny dostęp[84].

Podstawa, na jakiej przekazano dane, oraz w stosownych przypadkach „ocena skutków przekazywania danych" i środki uzupełniające:

90. Administrator powinien ocenić i być w stanie przedstawić dokumentację dotyczącą podstawy przekazania danych,[85] na której opiera się podmiot przekazujący, zgodnie z poleceniem administratora[86]. Oznacza to, że administrator powinien otrzymać te informacje od podmiotów przetwarzających (lub podwykonawców przetwarzania)/podmiotów przekazujących przed dokonaniem przekazania danych. EROD przypomniała w tym kontekście, że administrator podlega szczególnym wymogom w zakresie przejrzystości w odniesieniu do „stwierdzenia lub braku stwierdzenia odpowiedniego stopnia ochrony" na podstawie art. 45 RODO lub „odpowiednich zabezpieczeń" zapewnionych zgodnie z art. 46 RODO (art. 13 ust. 1 lit. f), art. 14 ust. 1 lit. f) i art. 15 ust. 2 RODO[87]).

91. Jeśli chodzi o zakres obowiązku dokonania przez administratora oceny tej dokumentacji, zależy on od rodzaju podstawy wykorzystanej do pierwotnego lub dalszego przekazania danych przez podmioty przetwarzające lub podwykonawców przetwarzania (jako podmiotów przekazujących dane)[88]:

92. Przekazania danych można dokonać na podstawie **decyzji stwierdzającej odpowiedni stopień ochrony**, jeżeli zgodnie z art. 45 RODO Komisja zdecydowała, że państwo trzecie, terytorium lub co najmniej jeden określony sektor w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Aby ocenić, czy stopień ochrony jest odpowiedni, Komisja bierze pod uwagę – oprócz innych kryteriów – zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz praw osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia[89].

93. W związku z powyższym, w przypadku gdy przekazania danych dokonuje podmiot przetwarzający lub podwykonawca przetwarzania (w imieniu administratora) na podstawie decyzji stwierdzającej

[84] Takie zidentyfikowanie przekazania jest również konieczne, gdy strony uzupełniają odpowiednie załączniki do standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych oraz standardowych klauzul umownych KE między administratorami a podmiotami przetwarzającymi (zob. przypis 80 powyżej).

[85] Zalecenia EROD 01/2020, sekcja 2.2. „Krok 2: Określenie wykorzystywanych narzędzi przekazywania".

[86] Art. 28 ust. 3 lit. a) RODO.

[87] Wytyczne EROD 01/2022 (prawo dostępu), pkt 122.

[88] Zgodnie z udokumentowanym poleceniem administratora dotyczącym przekazywania danych osobowych w całym łańcuchu przetwarzania.

[89] Zob. art. 45 RODO i dokument „Odpowiedni stopień ochrony przekazywanych danych osobowych" Grupy Roboczej Art. 29, przyjęty 28 listopada 2017 r., WP 254, zatwierdzony przez EROD w dniu 25 maja 2018 r., str. 7: *„Dalsze przekazywanie danych osobowych przez pierwotnego odbiorcę pierwotnego przekazania danych powinno być dozwolone tylko wtedy, gdy dalszy odbiorca (tj. odbiorca dalszego przekazywania danych) również podlega przepisom (w tym przepisom umownym) zapewniającym odpowiedni stopień ochrony i przestrzega odpowiednich instrukcji podczas przetwarzania danych w imieniu administratora. Dalsze przekazywanie danych nie może podważać stopnia ochrony osób fizycznych, których dane są przekazywane. Pierwotny odbiorca danych przekazywanych z UE jest odpowiedzialny za zapewnienie odpowiednich zabezpieczeń dla dalszego przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony. Takie dalsze przekazywanie danych powinno odbywać się wyłącznie w ograniczonych i określonych celach oraz tak długo, jak długo istnieje podstawa prawna takiego przetwarzania*".

odpowiedni stopień ochrony zgodnie z art. 45 RODO, stopień weryfikacji wymagany od administratora na podstawie art. 28 ust. 1 RODO, w którym jest mowa o tym, że jego podmiot przetwarzający (lub podwykonawca przetwarzania) przedstawia wystarczające gwarancje w odniesieniu do zgodności z rozdziałem V RODO, powinien zawierać następujące elementy:

- czy decyzja stwierdzająca odpowiedni poziom ochrony jest w mocy[90];

- oraz czy przekazywanie danych dokonywane w imieniu administratora wchodzi w zakres takiej decyzji (np. kategorie danych osobowych lub sektory objęte zakresem stosowania)[91].

94. Jeżeli dane osobowe przekazane przez podmiot przetwarzający lub podwykonawcę przetwarzania (w imieniu administratora) na podstawie decyzji stwierdzającej odpowiedni stopień ochrony podlegają **dalszemu przekazaniu** z tego państwa trzeciego, nie powinno się obniżać stopnia ochrony osób fizycznych, który gwarantuje RODO w odniesieniu do takiego dalszego przekazywania danych[92]. W tym względzie, zgodnie z art. 45 ust. 2 lit. a) RODO, każda decyzja stwierdzająca odpowiedni stopień ochrony wydana przez Komisję Europejską obejmuje między innymi przepisy państw trzecich regulujące dalsze przekazywanie danych. W związku z tym, zgodnie z art. 44 RODO administrator nie musi samodzielnie sprawdzać tych wymogów.

95. Jeżeli chodzi o obowiązek administratora wynikający z art. 28 ust. 1 RODO, oznacza to, że administrator powinien zapewnić, aby podmiot przetwarzający (lub podwykonawca przetwarzania) przedstawił „wystarczające gwarancje" również w odniesieniu do dalszego przekazywania danych przez podmiot przetwarzający (lub podwykonawcę przetwarzania) z odpowiedniego państwa.

96. W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony przekazywanie danych może być uzależnione od zapewnienia „**odpowiednich zabezpieczeń**" zgodnie z **art. 46 RODO**. W takim przypadku administrator powinien ocenić wprowadzone odpowiednie zabezpieczenia i zwracać uwagę na wszelkie problematyczne przepisy, które mogłyby uniemożliwić podwykonawcy przetwarzania wywiązanie się z obowiązków określonych w jego umowie zawartej z pierwotnym podmiotem przetwarzającym[93]. W szczególności administrator powinien zapewnić przeprowadzenie takiej „oceny skutków przekazania danych"[94], zgodnie z orzecznictwem[95] i jak wyjaśniono w zaleceniach EROD 01/2020. Dokumentacja dotycząca wdrożonych odpowiednich zabezpieczeń, „oceny skutków przekazania danych" i ewentualnych środków uzupełniających powinna zostać sporządzona przez podmiot przetwarzający/przekazujący dane[96] (w stosownych przypadkach we współpracy z

[90] Zalecenia EROD 01/2020, pkt 19: *„Jeśli przekazują Państwo [podmiot przekazujący dane] dane osobowe do państw trzecich, regionów lub sektorów, których dotyczy decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony (w stosownym zakresie), nie ma potrzeby podejmowania jakichkolwiek dalszych kroków wskazanych w niniejszych zaleceniach. Konieczne będzie jednak nadal monitorowanie, czy decyzje stwierdzające odpowiedni stopień ochrony nie zostały uchylone lub unieważnione."*

[91] Zalecenia EROD 01/2020, pkt 19.

[92] Zob. art. 44 RODO: *„(…) spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej".*

[93] W tym względzie zob. wyrok TSUE Schrems II, pkt 132 i 133, w których TSUE podkreśla umowny charakter standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych.

[94] Ocenę tę wyjaśniono bardziej szczegółowo w zaleceniach EROD 01/2020, krok 3 „Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania".

[95] Wyrok TSUE Schrems II, pkt 134.

[96] Zalecenia EROD 1/2022 w sprawie wniosku o zatwierdzenie oraz w sprawie elementów i zasad, które można znaleźć w wiążących regułach korporacyjnych dla administratorów danych (art. 47 RODO), przyjęte 20 czerwca 2023 r., wersja 2.1, pkt 10: „(...) *każdy podmiot przekazujący dane jest na przykład odpowiedzialny za ocenę, w*

podmiotem przetwarzającym/odbierającym dane[97]). Administrator może opierać się na ocenie przygotowanej przez podmiot przetwarzający (lub podwykonawcę przetwarzania) i w razie potrzeby ją uzupełnić. Na przykład, jeżeli ocena otrzymana przez administratora wydaje się niekompletna, nieprawidłowa lub budzi wątpliwości, administrator powinien poprosić o dodatkowe informacje, zweryfikować je i w razie potrzeby uzupełnić/poprawić, pamiętając, że ocena powinna być zgodna z zaleceniami EROD 01/2020 i określonymi w nich krokami[98]. Obejmuje to identyfikację przepisów i praktyk istotnych w świetle wszystkich okoliczności związanych z przekazaniem danych[99] oraz, w razie potrzeby, określenie odpowiednich środków uzupełniających[100]. W tym względzie administrator powinien zwrócić szczególną uwagę, czy podmiot przekazujący dane, tj. podmiot przetwarzający lub podwykonawca podmiotu przetwarzającego, ocenił, czy w przepisach lub praktykach państwa trzeciego istnieje jakikolwiek element, który może wpłynąć na skuteczność odpowiednich zabezpieczeń podstawy przekazywania danych, na której opiera się podmiot przekazujący dane[101], w szczególności ze względu na przepisy i praktyki regulujące dostęp organów publicznych państwa trzeciego do przekazywanych danych osobowych[102].

97. Ponadto, podobnie jak w przypadku przekazywania danych na podstawie decyzji stwierdzającej odpowiedni stopień ochrony (art. 45 RODO, zob. pkt 94 i 95 powyżej), jeżeli dane osobowe są przekazywane przez podmiot przetwarzający (lub podwykonawcę przetwarzania) na podstawie odpowiednich zabezpieczeń zgodnie z art. 46 RODO, obowiązek administratora wynikający z art. 28 ust. 1 RODO obejmuje również upewnienie się, że podmiot przetwarzający (lub podwykonawca przetwarzania) przedstawia wystarczające gwarancje w odniesieniu do **dalszego przekazywania** danych. Odpowiednie zabezpieczenia, o których mowa w art. 46 RODO, zazwyczaj obejmują przepisy określające zasady regulujące dalsze przekazywanie danych[103]. Oznacza to, że administratorzy nie muszą sprawdzać, czy te zasady jako takie są zgodne z wymogami rozdziału V RODO. Administratorzy powinni jednak być w stanie przedstawić dokumentację dotyczącą takiego dalszego przekazywania. Oznacza to, że administrator powinien otrzymać te informacje od podmiotów przetwarzających (lub podwykonawców przetwarzania)/podmiotów przekazujących, z których wynika, że podmioty

odniesieniu do każdego przekazania, osobno dla każdego przypadku, czy istnieje potrzeba wdrożenia środków uzupełniających, w celu zapewnienia stopnia ochrony zasadniczo równoważnego stopniowi ochrony zapewnianemu przez RODO."

[97] W wyroku TSUE Schrems II, pkt 134, TSUE zauważył, że w stosownych przypadkach taką weryfikację można przeprowadzić we współpracy z podmiotem odbierającym dane. Zob. również zalecenia EROD 01/2020, sekcja 4.

[98] Zob. w szczególności „Krok 3: Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania", „Krok 4: Przyjęcie środków uzupełniających" oraz „Krok 6: Ponowna ocena w odpowiednich odstępach czasu", jak wyjaśniono w zaleceniach EROD 01/2020.

[99] Wyrok TSUE Schrems II, pkt 126. Zob. również zalecenia EROD 01/2020, sekcja 2.3. „Krok 3: Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania", a w szczególności pkt 33. W wyroku TSUE Schrems II, pkt 134, TSUE zauważył, że w stosownych przypadkach taką weryfikację można przeprowadzić we współpracy z podmiotem odbierającym dane (zob. również zalecenia EROD 01/2020, pkt 30).

[100] Zgodnie z orzecznictwem do administratora lub podmiotu przetwarzającego należy sprawdzenie w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z odbiorcą danych, czy prawo państwa trzeciego przeznaczenia zapewnia odpowiedni, w świetle prawa Unii, stopień ochrony danych osobowych przekazywanych na podstawie standardowych klauzul ochrony danych, udzielając w razie potrzeby dodatkowych zabezpieczeń w stosunku do tych zapewnianych w niniejszych klauzulach (wyrok TSUE Schrems II, pkt 134). Zob. również zalecenia EROD 01/2020, sekcja 2.4, „Krok 4: Przyjęcie środków uzupełniających".

[101] Zob. zalecenia EROD 01/2020, sekcja 2.3 („Krok 3").

[102] Zob. zalecenia EROD 01/2020, pkt 41 i nast.

[103] Zob. np. klauzula 8.7 (moduł pierwszy), odpowiednio 8.8 (moduł drugi i trzeci) standardowych klauzul umownych KE dotyczących przekazywania danych (decyzja wykonawcza Komisji 2021/914) z dnia 4 czerwca 2021 r.

odbierające dane rzeczywiście spełniają wymogi dotyczące dalszego przekazywania danych określone w instrumencie odpowiednich zabezpieczeń.

2.3 W sprawie interpretacji art. 28 ust. 3 lit. a) RODO (pytanie 2)

98. Aby zapewnić przejrzysty podział obowiązków i odpowiedzialności zarówno wewnętrznie (między administratorami a podmiotami przetwarzającymi), jak i zewnętrznie wobec osób, których dane dotyczą, i organów regulacyjnych, zgodnie z art. 28 ust. 3 RODO, wszelkie przetwarzanie danych osobowych przez podmiot przetwarzający musi być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego[104] zawartym między administratorem a podmiotem przetwarzającym. Zgodnie z art. 28 ust. 3 lit. a) RODO umowa stanowi w szczególności, że podmiot przetwarzający *„przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający”*. Przepis ten stanowi również, że *„w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny”*.

99. Wniosek odnosi się do istnienia umów, które zawierają zobowiązanie do przetwarzania danych osobowych wyłącznie na polecenie administratora *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”* (pomijając odniesienie do prawa Unii lub prawa państwa członkowskiego). W tym względzie do EROD skierowano kilka pytań, które omówiono łącznie w poniższej sekcji:

> 2 Czy umowa lub inny instrument prawny na mocy prawa Unii lub prawa państwa członkowskiego zgodnie z art. 28 ust. 3 RODO muszą zawierać wyjątek przewidziany w art. 28 ust. 3 lit. a) *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający*” (dosłownie lub w bardzo podobnych słowach), aby była zgodna z RODO?
>
> 2a Jeżeli odpowiedź na pytanie 2 jest przecząca, czy w przypadku, gdy umowa lub inny instrument prawny na mocy prawa Unii lub państwa członkowskiego rozszerza zakres wyjątku z art. 28 ust. 3 lit. a) RODO, aby objąć również prawo państwa trzeciego (np. „chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”), czy samo w sobie stanowi to naruszenie art. 28 ust. 3 lit. a) RODO?

100. Wytyczne EROD 07/2020 przypominają *„jak ważne jest staranne negocjowanie i sporządzanie umów o przetwarzaniu danych”* w odniesieniu do wszelkich obowiązków prawnych UE lub państwa członkowskiego, którym podlega podmiot przetwarzający[105]. Jeżeli chodzi o ich treść, w wytycznych EROD 07/2020 zauważono, że *„aby zapewnić przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z RODO, umowa między administratorem a podmiotem przetwarzającym musi spełniać wymogi art. 28 RODO. Każda taka umowa powinna uwzględniać szczególne obowiązki administratorów i podmiotów przetwarzających. Chociaż art. 28 zawiera wykaz punktów, które należy uwzględnić w każdej umowie regulującej stosunki między administratorami danych a podmiotami*

[104] W dalszej części termin „**umowa**” będzie stosowany w odniesieniu do „umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego”.
[105] Wytyczne EROD 07/2020, pkt 121.

przetwarzającymi, pozostawia on swobodę negocjacji między takimi stronami umów"[106]*.* Pole do negocjacji jest ograniczone wymogami określonymi w art. 28 ust. 3 RODO.

101. Przede wszystkim podstawowym elementem umowy jest zobowiązanie podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora.

102. Jak jednak stwierdzono w art. 28 ust. 3 lit. a) RODO, podmioty przetwarzające dane osobowe mogą zgodnie z prawem przetwarzać dane osobowe – inaczej niż na udokumentowane polecenie administratora – w celu wypełnienia obowiązków prawnych wynikających z prawa Unii lub prawa państw członkowskich (zwanych dalej „**obowiązkiem prawnym Unii/państwa członkowskiego**"). Ten sam przepis wymaga również od podmiotu przetwarzającego zobowiązania do informowania administratora – z wyprzedzeniem – o przypadkach, w których zastosowanie ma obowiązek prawny Unii/państwa członkowskiego dotyczący przetwarzania/przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny". Zobowiązanie to jest wyraźnie zawarte, z brzmieniem bardzo podobnym do art. 28 ust. 3 lit. a) RODO, w standardowych klauzulach umownych KE między administratorami a podmiotami przetwarzającymi[107] oraz w kilku standardowych klauzulach umownych, w szczególności standardowych klauzulach umownych przyjętych przez duńskie[108], słoweńskie[109] i litewskie[110] ON do celów zapewnienia zgodności z art. 28 RODO.

[106] Wytyczne EROD 07/2020, pkt 109.

[107] Zob. w szczególności klauzule 7.1 lit. a) i 7.8 lit. a):
– Klauzula 7.1.a: *„Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane."* (wyróżnienie dodane). We wspólnej opinii w sprawie projektu standardowych klauzul umownych KE, EROD i EIOD zaleciły uwzględnienie pełnego brzmienia art. 28 ust. 3 lit. a) (a tym samym dodanie odniesienia do obowiązku podmiotu przetwarzającego w zakresie informowania administratora o obowiązku prawnym) w celu zwiększenia spójności. Wspólna opinia EROD i EIOD 1/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi dotyczących kwestii, o których mowa w art. 28 ust. 7 rozporządzenia (UE) 2016/679 i art. 29 ust. 7 rozporządzenia (UE) 2018/1725, pkt 38. Sformułowanie *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający"* było już obecne w projekcie standardowych klauzul umownych.
– Klauzula 7.8.a: *„Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725."* W odniesieniu do klauzuli 7.8 lit. a) EROD i EIOD zalecili włączenie odniesienia do możliwości dokonywania przez podmiot przetwarzający przekazania danych w oparciu o szczególny wymóg wynikający z prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający, co początkowo nie zostało określone w projekcie standardowych klauzul umownych. Załącznik 2 do wspólnej opinii EROD i EIOD nr 1/2021, Uwagi do klauzuli 7.7 lit. a).

[108] Standardowe klauzule umowne duńskiego ON do celów zgodności z art. 28 RODO, w szczególności klauzule 4.1 i 8.2. W opinii EROD nr 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonej przez DK ON (art. 28 ust. 8 RODO) EROD zaleciła włączenie brzmienia art. 28 ust. 3 lit. a) w celu zapewnienia pewności prawa.

[109] Standardowe klauzule umowne słoweńskiego ON do celów zgodności z art. 28 RODO, w szczególności klauzule 3.1 i 7.2.

[110] Standardowe klauzule umowne litewskiego ON do celów zgodności z art. 28 RODO, w szczególności klauzule 4.1, 22 i 23.

103. Oprócz zobowiązania do przetwarzania danych wyłącznie na podstawie udokumentowanego polecenia administratora, art. 28 ust. 3 lit. a) RODO zawiera zatem trzy główne elementy: (a) przepis regulujący sytuacje, w których obowiązek prawny zobowiązuje podmiot przetwarzający do przetwarzania danych osobowych, które nie opiera się na poleceniu administratora, a zatem nie odbywa się w imieniu administratora, (b) konieczność poinformowania administratora przez podmiot przetwarzający[111] oraz (c) odniesienie do takiego obowiązku prawnego wynikającego z prawa Unii lub prawa państwa członkowskiego.

104. W tym kontekście EROD przypomina, że zgodnie z ogólną zasadą umowy nie mogą być nadrzędne wobec prawa. Oznacza to, że bez względu na to, czy klauzula przewidziana w art. 28 ust. 3 lit. a) RODO (*„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający”*) jest zawarta w umowie, nie może ona uniemożliwiać realizacji obowiązków prawnych w uzupełnieniu lub, w niektórych przypadkach, w sprzeczności z wymogami umownymi. Ponadto zgodnie z ogólną zasadą, że umowa nie tworzy zobowiązań wobec osób trzecich, umowa nie może wiązać, na przykład, organów publicznych państwa członkowskiego lub państwa trzeciego[112].

105. Wszystkie umowy między administratorem a podmiotem przetwarzającym muszą uwzględniać sytuacje, w których podmiot przetwarzający może być na mocy przepisów zobowiązany do przetwarzania danych osobowych w sposób inny, niż na podstawie polecenia administratora. Ponadto spoczywający na podmiocie przetwarzającym obowiązek poinformowania administratora przed przeprowadzeniem przetwarzania, które nie opiera się na jego poleceniach, również jest kluczowym elementem umowy, który także należy uwzględnić[113].

106. W przypadku danych osobowych przetwarzanych poza EOG odniesienie do prawa Unii lub prawa państwa członkowskiego może nie mieć istotnego znaczenia, biorąc pod uwagę fakt, że podmiot przetwarzający spoza EOG tylko w wyjątkowych przypadkach będzie podlegał obowiązkom prawnym Unii lub państwa członkowskiego. W tym względzie EROD zauważa, że standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych, które mają spełniać, oprócz wymogów określonych w art. 46 ust. 1 i art. 46 ust. 2 lit. d) RODO, wymogi art. 28 ust. 3 i 4 RODO[114], nie zawierają

[111] Art. 28 ust. 3 lit. a) RODO stanowi, że w przypadku gdy prawo Unii lub prawo państwa członkowskiego zobowiązuje podmiot przetwarzający do przetwarzania danych osobowych, *wówczas „przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;”*.

[112] Dlatego też standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych zawierają szereg zabezpieczeń zobowiązujących podmiot przekazujący i podmiot odbierający dane do oceny obowiązkowych wymogów ustawodawstwa państwa trzeciego przed przekazaniem danych, w celu zapewnienia, aby nie wykraczały one poza to, co jest konieczne w społeczeństwie demokratycznym [klauzula 14 lit. a)–d)], zobowiązujących podmiot odbierający dane do powiadomienia podmiotu przekazującego w przypadku zmian, a podmiot przekazujący do podjęcia odpowiednich działań [klauzula 14 lit. e) i f)] oraz nakładających na odbierającego dane obowiązki w przypadku dostępu organów publicznych (klauzula 15). Zob. wyrok TSUE Schrems II, pkt 125 i 141.

[113]W opinii EROD 18/2021 w sprawie projektu standardowych klauzul umownych przedłożonej przez litewski ON (art. 28 ust. 8 RODO) EROD zaleciła włączenie ostatniego elementu art. 28 ust. 3 lit. a) do standardowych klauzul umownych (tj. obowiązku poinformowania administratora przez podmiot przetwarzający o mającym zastosowanie obowiązku prawnym), opinia EROD 18/2021, pkt 19.

[114] Zob. motyw 9 standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych *„Jeżeli przetwarzanie wiąże się z przekazywaniem danych przez administratorów podlegających rozporządzeniu (UE) 2016/679 podmiotom przetwarzającym nieobjętym terytorialnym zakresem stosowania rozporządzenia lub przez podmioty przetwarzające podlegające rozporządzeniu (UE) 2016/679 podwykonawcom przetwarzania nieobjętym terytorialnym zakresem stosowania rozporządzenia, standardowe klauzule umowne określone*

sformułowania podobnego do sformułowania „chyba że" w art. 28 ust. 3 lit. a) RODO. Jednak wymóg przetwarzania danych osobowych wyłącznie zgodnie z udokumentowanym poleceniem administratora, chyba że wymaga tego prawo UE lub prawo państwa członkowskiego, został już pośrednio uwzględniony w klauzuli 8.1 standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych.[115] Ponadto nie oznacza to, że obowiązek poinformowania określony w art. 28 ust. 3 lit. a) RODO nie został uwzględniony, ponieważ standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych wyraźnie zawierają konieczność poinformowania podmiotu przekazującego o tym, że podmiot odbierający nie jest w stanie zastosować się do polecenia administratora[116]. W związku z tym zobowiązanie podmiotu przetwarzającego do poinformowania administratora w przypadku, gdy ma zastosowanie prawny obowiązek przetwarzania (wynikający z prawa UE lub prawa państwa członkowskiego lub prawa państwa trzeciego), wynika ze standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych bez użycia dokładnego sformułowania *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający"* w art. 28 ust. 3 lit. a) RODO (element c), o którym mowa powyżej).

107. Jest to zgodne z celem art. 28 ust. 3 lit. a) RODO, jakim jest zapewnienie, aby administrator został poinformowany, gdy prawo wymaga od podmiotu przetwarzającego przetwarzania danych osobowych w sposób inny niż na polecenie administratora.

w załączniku do niniejszej decyzji również powinny umożliwiać spełnienie wymogów określonych w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679."

[115] Klauzula 8 dotycząca zabezpieczeń w zakresie ochrony danych (moduł drugi: Przekazywanie danych od administratora danych do podmiotu przetwarzającego) stanowi w sekcji 8.1 – polecenie:
„(a) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie podmiotu przekazującego dane. Podmiot przekazujący dane może wydawać takie polecenia w całym okresie obowiązywania umowy.
(b) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia."
Podobnie w module trzecim (przekazywanie danych między podmiotami przetwarzającymi) klauzula 8 dotycząca zabezpieczeń w zakresie ochrony danych stanowi w sekcji 8.1 – polecenie:
„(a) Podmiot przekazujący dane poinformował podmiot odbierający dane, że działa jako podmiot przetwarzający na polecenie administratora/administratorów danych, które to polecenie podmiot przekazujący dane udostępnia podmiotowi odbierającemu dane przed ich przetwarzaniem.
(b) Podmiot odbierający dane przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, zakomunikowane podmiotowi odbierającemu dane przez podmiot przekazujący dane, oraz na każde dodatkowe udokumentowane polecenia podmiotu przekazującego dane. Takie dodatkowe polecenia nie mogą być sprzeczne z poleceniami administratora. Administrator lub podmiot przekazujący dane może wydawać dalsze udokumentowane polecenia dotyczące przetwarzania danych w okresie obowiązywania umowy.
(c) Podmiot odbierający dane niezwłocznie informuje podmiot przekazujący dane, jeżeli nie może wykonać tego polecenia. Jeżeli podmiot odbierający dane nie może wykonać polecenia administratora, podmiot przekazujący dane niezwłocznie zgłasza ten fakt administratorowi."

[116] Oprócz klauzuli 8.1 (zob. poprzedni przypis) klauzula 14 stanowi w sekcji 14 lit. e), że: *„Podmiot odbierający dane zobowiązuje się do niezwłocznego powiadomienia podmiotu przekazującego dane, jeśli po uzgodnieniu niniejszych klauzul i w okresie obowiązywania umowy ma powody, aby sądzić, że podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymogami określonymi w lit. a), w tym w wyniku zmiany przepisów państwa trzeciego lub środka (takiego jak żądanie ujawnienia danych) wskazującego na stosowanie takich przepisów w praktyce, które nie jest zgodne z wymogami określonymi w lit. a). [W odniesieniu do modułu trzeciego: Podmiot przekazujący dane przekazuje to powiadomienie administratorowi.]"*

108. W świetle powyższej analizy EROD jest zdania, że włączenie do umowy zawartej między administratorem a podmiotem przetwarzającym[117] wyjątku przewidzianego w art. 28 ust. 3 lit. a) RODO *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający”* (dosłownie lub w bardzo podobnych słowach) jest wysoce zalecane, ale nie jest bezwzględnie wymagane w celu zapewnienia zgodności z art. 28 ust. 3 lit. a) RODO. Stanowisko to pozostaje bez uszczerbku dla konieczności umownego obowiązku poinformowania administratora, gdy prawo wymaga od podmiotu przetwarzającego przetwarzania danych osobowych w sposób inny niż na polecenie administratora, jak przewidziano w art. 28 ust. 3 lit. a) RODO. W przypadku gdy jest oczywiste, że obowiązki prawne Unii lub państwa członkowskiego mają znaczenie dla przetwarzania, zastosowanie brzmienia art. 28 ust. 3 lit. a) RODO pomogłoby wykazać zgodność.

109. EROD przechodzi teraz do rozważenia, czy umowa zawierająca szerszy wyjątek obejmujący również prawo państwa trzeciego, taki jak na przykład wyjątek od zobowiązania do przetwarzania danych osobowych wyłącznie na podstawie udokumentowanego polecenia administratora *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”*, sama w sobie stanowi naruszenie art. 28 ust. 3 lit. a) RODO.

110. Sformułowanie to, jeżeli nie jest uzupełnione dalszym uszczegółowieniem, może obejmować dwie różne sytuacje, które wymagają oddzielnych analiz w świetle kontekstu prawnego:

- przewidywany obowiązek prawny lub wiążące postanowienie wynika z prawa Unii lub prawa państwa członkowskiego (EOG);
- przewidywany obowiązek prawny lub wiążące postanowienie wynika z prawa innego, niż prawo Unii lub praw państwa członkowskiego (EOG).

[117] W szczególności, w przypadku gdy administrator i podmiot przetwarzający opierają się na własnej umowie o przetwarzaniu, a nie na standardowych klauzulach umownych KE między administratorami a podmiotami przetwarzającymi, na standardowych klauzulach umownych przyjętych przez organy nadzorcze w celu zapewnienia zgodności z art. 28 RODO lub standardowych klauzulach umownych KE dotyczących międzynarodowego przekazywania danych. Zob. również motyw 109 i art. 28 ust. 6 rozporządzenia (UE) 2016/679.

111. Pierwsza sytuacja podlega wyraźnym przepisom art. 28 ust. 3 lit. a) RODO, określającym umowne zobowiązanie podmiotu przetwarzającego do przetwarzania wyłącznie zgodnie z udokumentowanym poleceniem administratora *„chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający”*. Dzieje się tak niezależnie od tego, czy przetwarzanie danych osobowych odbywa się na terytorium EOG, czy poza nim.

112. Prawo Unii, w tym RODO i obowiązki prawne państw członkowskich, stanowią część tej samej tradycji konstytucyjnej co RODO, które ustanawia ochronę osób fizycznych w związku z przetwarzaniem danych osobowych jako prawo podstawowe na podstawie art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (zwanego dalej „**TFUE**”) i art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „**Kartą**”)[118].

113. W przypadku gdy strony mogą wykazać, w oparciu o inne elementy ich umowy lub umów, że tylko ta pierwsza sytuacja mieści się w słowach*, „chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”*, wówczas sformułowanie to nie ma wpływu na gwarancje przewidziane w art. 28 ust. 3 lit. a) RODO.

114. W niektórych przypadkach umowa lub umowy stron wykraczają poza tę pierwszą sytuację, co oznacza, że odniesienie do „*prawa lub wiążącego postanowienia organu rządowego*” obejmuje obowiązki prawne/wiążące postanowienia wynikające z przepisów innych, niż prawo Unii lub prawo państwa członkowskiego (EOG) (druga sytuacja).

115. EROD zauważa, że obowiązki dotyczące przetwarzania danych oparte na przepisach innych, niż prawo Unii lub prawo państwa członkowskiego (EOG), nie podzielają tradycji konstytucyjnej jako takiej i nie mogą być automatycznie uznawane za takie same, jak te istniejące w ramach porządku prawnego UE (w świetle art. 44 RODO). W tym względzie EROD przypomina, że zgodnie z art. 6 RODO terminy „obowiązek prawny”, „interes publiczny” i „władza publiczna” odnoszą się do prawa Unii lub prawa państwa członkowskiego[119]. Analogicznie EROD zauważa, że art. 29 RODO dotyczący przetwarzania z upoważnienia administratora lub podmiotu przetwarzającego stanowi, że *„[p]odmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego”*. (wyróżnienie dodane)

116. W kontekście przekazywania danych można przewidzieć, że obowiązki prawne mogą wynikać również z przepisów innych niż prawo Unii lub prawo państwa członkowskiego. W przypadku gdy dochodzi do przekazywania danych, EROD przypomina, że oprócz art. 28 RODO zastosowanie ma rozdział V RODO.

---

[118] Motyw 1 RODO odnosi się do art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”) i art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej („Karta”). Art. 52 ust. 1 Karty stanowi, że *„Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób”.*

[119] Art. 6 ust. 3 RODO stanowi, że jeżeli podstawą prawną przetwarzania jest „obowiązek prawny” (art. 6 ust. 1 lit. c) RODO) lub „zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi” (art. 6 ust. 1 lit. e) RODO), odnosi się to do przepisów prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator. W odniesieniu do art. 6 RODO, motyw 40 RODO wyjaśnia, że w przypadku, gdy podstawa prawna przetwarzania jest przewidziana prawem, oznacza to *„albo w niniejszym rozporządzeniu, albo w innym akcie prawnym Unii lub w prawie państwa członkowskiego, o których mowa w niniejszym rozporządzeniu”*. Art. 49 ust. 4 RODO stanowi, że jedynie interes publiczny uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator danych, może prowadzić do zastosowania tego wyjątku.

EROD uważa, że w odniesieniu do danych osobowych przetwarzanych poza EOG art. 28 ust. 3 lit. a) RODO nie uniemożliwia – co do zasady – włączenia do umowy przepisów, które dotyczą wymogów prawa państwa trzeciego w zakresie przetwarzania przekazywanych danych osobowych. Takie przepisy mogą być zawarte w szczególności w celu zapewnienia zgodności z rozdziałem V RODO, jednak samo dodanie słów *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego"* najprawdopodobniej nie wystarczy.

117. W tym kontekście EROD zauważa, że standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych odnoszą się w szczególności do „Praw i praktyk lokalnych wpływających na przestrzeganie klauzul" w klauzuli 14 oraz „Obowiązków podmiotu odbierającego dane w przypadku dostępu organów publicznych" w klauzuli 15. Przed podpisaniem standardowych klauzul umownych strony muszą ocenić, czy istnieją prawa i praktyki lokalne wpływające na przestrzeganie klauzul (klauzula 14 standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych). Klauzula 14 zobowiązuje strony do zagwarantowania, że nie wiedzą o istnieniu prawa i praktyk w państwie trzecim, w którym podmiot odbierający dane ma siedzibę, które uniemożliwiałyby mu wypełnienie jego obowiązków wynikających ze standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych, po dokonaniu przez podmiot odbierający dane oceny takiego prawa i praktyk, oraz zobowiązuje podmiot odbierający dane do niezwłocznego powiadomienia podmiotu przekazującego dane o wszelkich zmianach, w którym to przypadku podmiot przekazujący dane określa odpowiednie środki w celu zaradzenia zaistniałej sytuacji, bądź klauzula 14 umożliwia mu wstrzymanie przekazywania danych, a nawet rozwiązanie umowy. Klauzula 15 nakłada na podmiot odbierający dane pewne obowiązki w przypadku dostępu organów publicznych państwa trzeciego. Określono w nim szereg kroków, jakie podmiot odbierający dane musi podjąć w związku z dostępem rządu państwa trzeciego (na żądanie lub bezpośrednio), mających na celu zapewnienie (ostatecznie), że administrator został poinformowany. Oprócz obowiązku powiadomienia podmiotu przekazującego odbierającego dane, podmiot odbierający dane ma między innymi obowiązek kontroli legalności żądania dostępu i udokumentowania takiej oceny prawnej, a także w określonych przypadkach obowiązek zakwestionowania ważności żądania. Podmiot przekazujący dane – w porozumieniu z administratorem, jeżeli podmiot przekazujący dane nie jest administratorem – będzie wówczas w stanie podjąć niezbędne środki, w tym ewentualne wstrzymanie przekazywania danych lub zakończenie stosowania standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych. To, czy jakiekolwiek (dalsze) przekazanie danych do rządu państwa trzeciego jest zgodne z RODO, będzie zależeć od indywidualnej analizy każdego przypadku (między innymi od podstawy prawnej, kontroli i zgodności z rozdziałem V RODO). W ramach modułu 3 standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych (relacja między podmiotami przetwarzającymi) podmiot odbierający/przetwarzający dane ma obowiązek udostępnić podmiotowi przekazującemu dane ocenę prawną. W tym względzie EROD odnosi się również do pkt 88-89 i 106 powyżej.

118. Ponadto, zgodnie ze standardowymi klauzulami umownymi KE dotyczącymi międzynarodowego przekazywania danych zarówno podmiot przekazujący, jak i odbierający dane są zobowiązani do upewnienia się, że ustawodawstwo kraju trzeciego umożliwia podmiotowi odbierającemu dane przestrzeganie standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych przed przekazaniem danych osobowych do tego kraju trzeciego[120]. W przypadku gdy podmiot przetwarzający przekazuje dane osobowe w imieniu administratora, taki obowiązek spoczywa również na administratorze (zob. również pkt 79 i następne powyżej).

[120] Wyrok TSUE *Schrems II*, pkt 141. Zob. również standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych, klauzula 14 lit. a)–d).

119. Podobnie zalecenia w sprawie wiążących reguł korporacyjnych (BCR) dla administratorów i dokumenty referencyjne dotyczące wiążących reguł korporacyjnych dla podmiotów przetwarzających również określają zestaw obowiązków na wypadek, gdyby członek objęty BCR stał w konflikcie między swoim prawem lokalnym a wiążącymi regułami korporacyjnymi[121] lub gdyby otrzymał od organu ścigania lub organu bezpieczeństwa państwa żądanie ujawnienia danych[122]. W szczególności w zaleceniach EROD nr[123] 1/2022 wskazano, że wiążące reguły korporacyjne dla administratorów (BCR-C) powinny zawierać klauzule dotyczące lokalnych przepisów i praktyk mających wpływ na przestrzeganie BCR-C (sekcja 5.4.1), a także obowiązków podmiotu odbierającego dane w przypadku wniosków o udzielenie dostępu składanych przez rząd (sekcja 5.4.2). BCR-C może służyć jako mechanizm przekazywania danych w przypadku przekazywania danych do podmiotów przetwarzających w ramach grupy.

120. W przypadkach, w których przekazywanie danych jest objęte decyzjami stwierdzającymi odpowiedni stopień ochrony, przepisy dotyczące *„dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa”* są jednym z elementów, które Komisja Europejska musi wziąć pod uwagę przy ocenie odpowiedniego stopnia ochrony, zgodnie z art. 45 ust. 2 lit. a) RODO[124].

121. To, co łączy decyzje stwierdzające odpowiedni stopień ochrony[125], standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych[126] oraz zalecenia i dokumenty referencyjne

[121] Sekcja 5.4.1 „Lokalne przepisy i praktyki wpływające na przestrzeganie BCR-C”, zalecenia 1/2022 w sprawie wniosku o zatwierdzenie oraz w sprawie elementów i zasad, które można znaleźć w wiążących regułach korporacyjnych dla administratorów danych (art. 47 RODO). Sekcja 6.3 „Potrzeba zachowania przejrzystości w przypadku, gdy przepisy krajowe uniemożliwiają grupie przestrzeganie wiążących reguł korporacyjnych” dokumentu roboczego Grupy Roboczej Art. 29 ustanawiającego tabelę z elementami i zasadami, które można znaleźć w wiążących regułach korporacyjnych dla podmiotów przetwarzających, WP 257 rev.01, zatwierdzonego przez EROD w dniu 25 maja 2018 r.

[122] Sekcja 5.4.2 „Obowiązki podmiotu odbierającego dane w przypadku wniosków o udzielenie dostępu składanych przez rząd”, zalecenia EROD 1/2022 w sprawie wniosku o zatwierdzenie oraz w sprawie elementów i zasad, które można znaleźć w wiążących regułach korporacyjnych dla administratorów danych (art. 47 RODO); zob. również sekcja 6.3 „Potrzeba zachowania przejrzystości w przypadku, gdy przepisy krajowe uniemożliwiają grupie przestrzeganie wiążących reguł korporacyjnych”, dokument roboczy ustanawiający tabelę z elementami i zasadami, które można znaleźć w wiążących regułach korporacyjnych dla podmiotów przetwarzających, WP 257 rev.01.

[123] Zalecenia EROD 1/2022 w sprawie wniosku o zatwierdzenie oraz w sprawie elementów i zasad, które można znaleźć w wiążących regułach korporacyjnych dla administratorów danych (art. 47 RODO).

[124] TSUE odniósł się do tego elementu w swoich rozstrzygnięciach w sprawach Schrems I i Schrems II. Wyrok TSUE z dnia 6 października 2015 r., *Maximillian Schrems przeciwko Data Protection Commissioner* (zwany dalej „wyrokiem TSUE Schrems I”), sprawa C-362/14, ECLI:EU:C:2015:650, pkt 91 i nast. Wyrok TSUE Schrems II, pkt 141, 174–177, 187–189.

[125] Zobacz art. 45 ust. 2 lit. a) RODO, który stanowi, że Komisja Europejska bierze pod uwagę „*praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;*”. Zob. również dokument referencyjny w sprawie odpowiedniego stopnia ochrony Grupy Roboczej Art. 29, WP 254 rev.01, przyjęty w dniu 6 lutego 2018 r., zatwierdzony przez EROD w dniu 25 maja 2018 r. Pojęcie „odpowiedniego stopnia ochrony” zostało rozwinięte przez TSUE w wyrokach Schrems I (pkt 73 i 74) i Schrems II (pkt 94).

[126] Klauzula 14 lit. a) standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych.

dotyczące BCR[127], to zrozumienie, że przepisy i praktyki państwa trzeciego, które szanują istotę podstawowych praw i wolności zapisanych w TFUE, Karcie i RODO i nie wykraczają poza to, co jest konieczne i proporcjonalne w społeczeństwie demokratycznym do ochrony jednego z celów wymienionych w art. 23 ust. 1 RODO, nie naruszą stopnia ochrony gwarantowanego przez RODO[128]. Z tego względu standardowe klauzule umowne KE dotyczące międzynarodowego przekazywania danych[129] oraz zalecenia i dokumenty referencyjne dotyczące BCR[130] zawierają przepisy, które wiążą różne konsekwencje z przepisami i praktykami, w zależności od tego, czy naruszają one stopień ochrony gwarantowany przez RODO. Umowy ad hoc oparte na art. 46 ust. 3 lit. a) RODO powinny również zawierać podobne postanowienia[131].

122. Z powyższego jasno wynika, że gdy przepisy państwa trzeciego wymagają od podmiotu przetwarzającego przetwarzania danych osobowych w sposób inny niż na polecenie administratora, stopień ochrony określony w RODO będzie przestrzegany tylko wtedy, gdy przepisy te spełniają wyżej wymienione warunki. W każdym przypadku podmiot przetwarzający powinien wdrożyć środki uzupełniające w przypadku niespełnienia wspomnianych warunków, a umowa powinna zapewnić spełnienie tych warunków.

123. Jeżeli podmiot przetwarzający przetwarza dane osobowe w obrębie EOG, w pewnych okolicznościach może nadal mieć do czynienia z prawem państwa trzeciego. EROD podkreśla, że dodanie w umowie odniesienia do prawa państwa trzeciego nie zwalnia podmiotu przetwarzającego z obowiązków wynikających z RODO.

124. W świetle powyższej analizy EROD stoi na stanowisku, że włączenie sformułowania podobnego do *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”*, należy do swobody zawierania umów przysługującej stronom i nie narusza art. 28 ust. 3 lit. a) RODO jako takiego. Pozostaje to bez uszczerbku dla obowiązku przestrzegania przepisów RODO w każdym przypadku przetwarzania danych osobowych. Ponadto taka klauzula nie zwalnia administratora ani podmiotu przetwarzającego z obowiązku przestrzegania zobowiązań wynikających z RODO, w szczególności w odniesieniu do informacji, które należy przekazać administratorowi oraz – w stosownych przypadkach – warunków międzynarodowego przekazywania danych osobowych przetwarzanych w imieniu administratora.[132]

125. Na koniec we wniosku zadano pytanie uzupełniające:

[127] Jest to wyraźnie określone w zaleceniach EROD 1/2022 (zalecenia BCR-C), wersja 2.1, pkt 5.4.1 i 5.4.2. To samo rozumienie pośrednio leży u podstaw sekcji 6.3 „Potrzeba zachowania przejrzystości w przypadku, gdy przepisy krajowe uniemożliwiają grupie przestrzeganie wiążących reguł korporacyjnych” dokumentu roboczego Grupy Roboczej Art. 29 ustanawiającego tabelę z elementami i zasadami, które można znaleźć w wiążących regułach korporacyjnych dla podmiotów przetwarzających, WP 257 rev.01, zatwierdzonego przez EROD w dniu 25 maja 2018 r.

[128] Zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, wersja 2.0, pkt. 38 oraz Zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, pkt 22 i 24.

[129] Klauzula 14 standardowych klauzul umownych KE dotyczących międzynarodowego przekazywania danych.

[130] Zob. przypis 127.

[131] Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych, v. 2.0, pkt 66.

[132] Obowiązkiem administratora jest w szczególności zapewnienie, że w odniesieniu do przetwarzania poza EOG, tylko prawo państwa trzeciego, które zapewnia zasadniczo równoważny stopień ochrony, może wymagać przetwarzania od podmiotu przetwarzającego. Zob. także pkt 116–122 powyżej.

Jeżeli odpowiedź na pytanie 2a jest przecząca, czy taki rozszerzony zakres wyjątku należy zamiast tego interpretować jako udokumentowane polecenie administratora w rozumieniu art. 28 ust. 3 lit. a) RODO?

126. W świetle odpowiedzi udzielonej powyżej EROD rozumie, że pozostałe pytanie dotyczy tego, czy strony mogą twierdzić, że sformułowanie *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”* (dosłownie lub w bardzo podobnych słowach) w ich umowie należy interpretować jako udokumentowane polecenie administratora w rozumieniu art. 28 ust. 3 lit. a) RODO.

127. EROD najpierw rozważa, czy argument ten jest możliwy do przyjęcia, jeżeli obowiązek prawny lub wiążące postanowienie wynikają z prawa Unii lub prawa państwa członkowskiego (EOG).

128. EROD zauważa, że pojęcie „polecenia” użyte w art. 28 ust. 3 lit. a) RODO odnosi się w szczególności do administratora danych określającego, jakiego przetwarzania danych oczekuje się od podmiotu przetwarzającego w jego imieniu i w jaki sposób[133]. Wszelkie postanowienia zawarte przez administratora w umowie z usługodawcą/podmiotem przetwarzającym, które nie polegają na żądaniu przetwarzania danych osobowych w imieniu administratora, również nie kwalifikują się jako polecenie w rozumieniu art. 28 ust. 3 lit. a) RODO. Ponadto polecenie administratora danych musiałoby być wystarczająco szczegółowe, aby objęło konkretne przetwarzanie danych osobowych, co nie ma miejsca w przypadku tego sformułowania. Ponadto administrator danych zawsze miałby (musiałby mieć) możliwość – i byłby prawnie zobowiązany w zakresie, w jakim polecenie przetwarzania danych osobowych w imieniu administratora stanowiłoby naruszenie RODO – do wycofania takiego polecenia. Podmiot przetwarzający powinien wówczas zastosować się do wycofania przez administratora polecenia i zaprzestać przetwarzania danych.

129. Wydając polecenie podmiotowi przetwarzającemu, administrator wprowadza w życie określenie celów i sposobów przetwarzania danych, w szczególności poprzez wpływanie na kluczowe elementy przetwarzania[134]. Co do zasady wpływ administratora na przetwarzanie danych osobowych ustaje, gdy prawo UE lub prawo państwa członkowskiego określa obowiązki podmiotu przetwarzającego dotyczące przetwarzania danych osobowych, którego administrator nie jest w stanie prowadzić lub wstrzymać[135]. O ile administrator może przypomnieć podmiotowi przetwarzającemu o obowiązku przestrzeganiu prawa UE lub prawa państwa członkowskiego, nie można tego rozumieć jako polecenia w rozumieniu art. 28 ust. 3 lit. a) RODO[136]. Samo RODO uznaje ten stan rzeczy, wskazując, że podmiot przetwarzający może przetwarzać dane wyłącznie na udokumentowane polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający (art. 28 ust. 3 lit. a) RODO) i musi niezwłocznie poinformować administratora, jeśli polecenie stanowi naruszenie RODO (art. 28 ust. 3 RODO akapit ostatni).

[133] Wytyczne EROD 07/2020, pkt 116.

[134] Wytyczne EROD 07/2020, pkt 20.

[135] W tym kontekście może to być sytuacja przewidziana w art. 4 ust. 7 RODO, który stanowi, że jeżeli cele i sposoby przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Zob. wyrok TSUE z dnia 11 stycznia 2024 r., *Belgian State (Données traitées par un journal officiel),* sprawa C-231/22, ECLI:EU:C:2024:7, pkt 28-30, 35 i 39; wytyczne EROD 07/2020, pkt 22–24.

[136] Takie przypomnienie będzie raczej uważane za wprowadzenie przez administratora zabezpieczeń umownych w celu zapewnienia, że przetwarzanie w imieniu administratora będzie zgodne ze wszystkimi wymogami RODO i zapewni ochronę praw osoby, której dane dotyczą.

130. EROD uważa, że powyższe uzasadnienie ma zastosowanie również w przypadku, gdy obowiązek prawny lub wiążące postanowienie wynikają z prawa państwa trzeciego. W takiej sytuacji prawo to ogranicza wpływ, jaki administrator danych może wywierać na przetwarzanie danych.

131. Oprócz powyższego, klauzula, zgodnie z którą podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”*, sama w sobie wskazuje, że przetwarzanie danych na polecenie administratora jest regułą, podczas gdy wyjątek istnieje właśnie w przypadku przetwarzania nie na polecenie administratora (na co wskazuje wyrażenie „chyba że”). Co więcej, to od decyzji podmiotu przetwarzającego nadal zależy, czy zastosuje się on do żądania prawnego lub wiążącego postanowienia, któremu podlega, czy też poniesie konsekwencje prawne niezastosowania się do niego.

132. Na tej podstawie EROD stwierdza, że *„chyba że obowiązek taki nakłada na niego prawo lub wiążące postanowienie organu rządowego”* (dosłownie lub w bardzo podobnych słowach) nie może być interpretowane jako udokumentowane polecenie administratora. Administrator pozostaje odpowiedzialny, jeśli nie zapewnił, że podmiot przetwarzający (lub podwykonawca przetwarzania) przetwarza dane osobowe wyłącznie na jego udokumentowane polecenie. Nie ma to jednak zastosowania w przypadku, gdy przetwarzanie danych jest wymagane na mocy prawa UE lub prawa państwa członkowskiego lub w przypadku przetwarzania poza EOG wymaganego na mocy prawa państwa trzeciego, któremu podlega podmiot przetwarzający (lub podwykonawca przetwarzania), a prawo to zapewnia zasadniczo równoważny stopień ochrony.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)