Wytyczne 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO

Wersja 2.0

Przyjęta 7 lipca 2021 r.

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

Historia wersji

Wersja 2.0	7 lipca 2021 r.	Przyjęcie wytycznych po konsultacjach publicznych
Wersja 1.0	2 września 2020 r.	Przyjęcie wytycznych do konsultacji publicznych

STRESZCZENIE

Pojęcia administratora, współadministratora i podmiotu przetwarzającego odgrywają kluczową rolę w stosowaniu ogólnego rozporządzenia o ochronie danych 2016/679 (RODO), ponieważ określają, kto jest odpowiedzialny za przestrzeganie różnych zasad ochrony danych oraz w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa. Dokładne znaczenie tych pojęć oraz kryteria ich prawidłowej interpretacji muszą być wystarczająco jasne i spójne w całym Europejskim Obszarze Gospodarczym (EOG).

Pojęcia administratora, współadministratora i podmiotu przetwarzającego są pojęciami *funkcjonalnymi* w tym sensie, że ich celem jest podział obowiązków zgodnie z rzeczywistymi rolami stron oraz pojęciami *autonomicznymi* w tym sensie, że powinno się je interpretować głównie zgodnie z prawem Unii o ochronie danych.

Administrator

W zasadzie nie ma ograniczeń co do rodzaju podmiotu, który może przyjąć rolę administratora, jednak w praktyce zazwyczaj to organizacja jako taka, a nie osoba fizyczna w organizacji (np. dyrektor generalny, pracownik lub członek zarządu), pełni funkcję administratora.

Administrator to organ, który *decyduje* o pewnych kluczowych elementach przetwarzania. Definicja administrowania może wynikać z przepisów prawa lub analizy elementów stanu faktycznego lub okoliczności sprawy. Niektóre działania związane z przetwarzaniem można postrzegać jako naturalnie związane z rolą podmiotu (pracodawca wobec pracowników, wydawca wobec abonentów lub stowarzyszenie wobec swoich członków). W wielu przypadkach w identyfikacji administratora mogą pomóc postanowienia umowy, choć nie są one decydujące we wszystkich okolicznościach.

Administrator określa cele i sposoby przetwarzania, czyli *dlaczego* i *jak* przetwarzać dane. Administrator decyduje zarówno o celach jak i o sposobach przetwarzania. Jednakże niektóre bardziej praktyczne aspekty wdrażania („sposoby przetwarzania inne niż istotne") można pozostawić do decyzji podmiotowi przetwarzającemu. Aby administrator został uznany za administratora, nie musi on mieć faktycznego dostępu do przetwarzanych danych.

Współadministratorzy

Ze współadministratorami możemy mieć do czynienia w sytuacji, gdy w przetwarzaniu bierze udział więcej niż jeden podmiot. W RODO wprowadzono szczególne zasady dla współadministratorów i określono ramy regulujące ich relacje. Współadministracja ma miejsce przede wszystkim w sytuacji, gdy w określaniu celów i sposobów przetwarzania udział biorą co najmniej dwa podmioty. Wspólny udział może przybrać formę *wspólnej decyzji* podjętej przez co najmniej dwa podmioty lub wynikać ze *zbieżnych decyzji* co najmniej dwóch podmiotów, w przypadku gdy decyzje te wzajemnie się uzupełniają i są konieczne, aby przetwarzanie odbywało się w taki sposób, że mają one konkretny wpływ na określenie celów i sposobów przetwarzania. Ważnym kryterium jest to, że przetwarzanie danych nie byłoby możliwe bez udziału obu stron w tym sensie, że przetwarzanie danych przez każdą ze stron jest nierozłączne, tzn. ściśle związane. Wspólny udział musi obejmować z jednej strony określenie celów, a z drugiej – określenie sposobów przetwarzania.

Podmiot przetwarzający

Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Istnieją dwa podstawowe warunki

uznania za podmiot przetwarzający: jest on odrębnym podmiotem w stosunku do administratora oraz przetwarza dane osobowe w imieniu administratora.

Podmiot przetwarzający nie może przetwarzać danych inaczej niż zgodnie z instrukcjami administratora. Możliwe jest jednak pozostawienie w ramach tych instrukcji pewnej swobody co do tego, jak najlepiej służyć interesom administratora i umożliwienie podmiotowi przetwarzającemu wyboru najodpowiedniejszych środków technicznych i organizacyjnych. Jeśli jednak podmiot przetwarzający wykracza poza instrukcje administratora i zaczyna określać własne cele i środki przetwarzania, dopuszcza się naruszenia przepisów RODO. W takiej sytuacji podmiot przetwarzający zostaje uznany za administratora w odniesieniu do tego przetwarzania i może podlegać sankcjom z tytułu wykroczenia poza instrukcje administratora.

Relacja między administratorem a podmiotem przetwarzającym

Administrator korzysta wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z wymaganiami RODO. Elementami, które należy wziąć pod uwagę, mogą być: wiedza fachowa podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych); wiarygodność podmiotu przetwarzającego; zasoby podmiotu przetwarzającego oraz stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji.

Przetwarzanie danych osobowych przez podmiot przetwarzający musi być uregulowane umową lub innym aktem prawnym, który musi być sporządzony na piśmie, w tym w formie elektronicznej, i być wiążący. Administrator i podmiot przetwarzający mogą wynegocjować własną umowę zawierającą wszystkie obowiązkowe elementy lub oprzeć się, w całości lub w części, na standardowych klauzulach umownych.

W RODO wymieniono elementy, które należy uwzględnić w umowie o przetwarzaniu danych. Umowa o przetwarzaniu danych nie powinna jednak ograniczać się do powtórzenia przepisów RODO; powinna raczej zawierać bardziej szczegółowe, konkretne informacje na temat sposobu spełnienia wymogów i poziomu ochrony wymaganego do przetwarzania danych osobowych, które jest przedmiotem umowy o przetwarzaniu.

Relacje między współadministratorami

Współadministratorzy w przejrzysty sposób określają i uzgadniają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Określenie zakresu ich odpowiedzialności dotyczy w szczególności wykonywania przez osoby, których dane dotyczą, przysługujących im praw oraz obowiązków w odniesieniu do udzielania informacji. Oprócz tego podział odpowiedzialności powinien obejmować inne obowiązki administratora, takie jak obowiązki dotyczące ogólnych zasad ochrony danych, podstawy prawnej, środków bezpieczeństwa, obowiązku powiadamiania o naruszeniu ochrony danych, oceny skutków dla ochrony danych, korzystania z usług podmiotów przetwarzających, przekazywania danych do państw trzecich oraz kontaktów z osobami, których dane dotyczą, i organami nadzorczymi.

Każdy współadministrator ma obowiązek zapewnić, że posiada podstawę prawną do przetwarzania danych oraz że dane nie są dalej przetwarzane w sposób niezgodny z celami, dla których zostały pierwotnie zgromadzone przez administratora udostępniającego dane.

W RODO nie określono formy prawnej uzgodnień między współadministratorami. Z uwagi na pewność prawa oraz w celu zapewnienia przejrzystości i rozliczalności EROD zaleca, aby takie uzgodnienia były dokonywane w formie wiążącego dokumentu, takiego jak umowa lub inny wiążący akt prawny na mocy prawa Unii lub państwa członkowskiego, któremu podlegają administratorzy.

Uzgodnienia należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą, a zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

Niezależnie od uzgodnień osoby, których dane dotyczą, mogą wykonywać przysługujące im prawa wobec każdego ze współadministratorów. Organy nadzorcze nie są związane uzgodnieniami ani w kwestii kwalifikacji stron jako współadministratorów, ani w kwestii wskazanego punktu kontaktowego.

SPIS TREŚCI

Europejska Rada Ochrony Danych

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

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. 12 i 22 swojego regulaminu wewnętrznego,

mając na uwadze, że prace przygotowawcze nad niniejszymi wytycznymi obejmowały gromadzenie informacji od zainteresowanych stron, zarówno w formie pisemnej, jak i podczas spotkania z zainteresowanymi stronami, w celu określenia najpilniejszych wyzwań;

PRZYJMUJE NINIEJSZE WYTYCZNE:

WPROWADZENIE

1. Niniejszy dokument ma na celu przedstawienie wytycznych dotyczących pojęć administratora i podmiotu przetwarzającego w oparciu o przepisy RODO dotyczące definicji zawarte w art. 4 oraz przepisy dotyczące obowiązków zawarte w rozdziale IV. Głównym celem jest wyjaśnienie znaczenia pojęć oraz wyjaśnienie różnych ról i podziału odpowiedzialności między tymi podmiotami.

2. Pojęcie administratora i jego interakcja z pojęciem podmiotu przetwarzającego odgrywają kluczową rolę w stosowaniu RODO, ponieważ określają, kto jest odpowiedzialny za przestrzeganie różnych przepisów o ochronie danych oraz w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa. W RODO wyraźnie wprowadza się zasadę rozliczalności, tj. administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych określonych w art. 5 i jest w stanie wykazać ich przestrzeganie. Ponadto w RODO wprowadza się również bardziej szczegółowe przepisy dotyczące korzystania z usług podmiotu przetwarzającego (podmiotów przetwarzających), a niektóre przepisy dotyczące przetwarzania danych osobowych są skierowane nie tylko do administratorów, ale również do podmiotów przetwarzających.

3. Dlatego niezwykle ważne jest, aby dokładne znaczenie tych pojęć i kryteria ich prawidłowego stosowania były wystarczająco jasne i wspólne dla całej Unii Europejskiej i EOG.

4. Grupa Robocza Art. 29 wydała wytyczne dotyczące pojęć administratora/podmiotu przetwarzającego w opinii 1/2010 (WP169)[2] w celu przedstawienia wyjaśnień i konkretnych przykładów w odniesieniu do tych pojęć. Od czasu wejścia w życie RODO pojawiło się wiele pytań dotyczących tego, w jakim stopniu RODO wprowadziło zmiany w pojęciach administratora i podmiotu przetwarzającego oraz ich odnośnych ról. Pytania dotyczyły w szczególności istoty i skutków pojęcia współadministracji (np.

[1] Odniesienia do „państw członkowskich" w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Grupa Robocza art. 29, Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjęta w dniu 16 lutego 2010 r., 264/10/PL, WP 169.

zgodnie z art. 26 RODO) oraz szczególnych obowiązków podmiotów przetwarzających określonych w rozdziale IV (np. zgodnie z art. 28 RODO). W związku z tym, a także ponieważ EROD uznaje, że konkretne zastosowanie tych pojęć wymaga dalszych wyjaśnień, EROD uważa obecnie za konieczne przedstawienie szerzej opracowanych i bardziej szczegółowych wytycznych w celu zapewnienia spójnego i zharmonizowanego podejścia w całej UE i EOG. Niniejsze wytyczne zastępują poprzednią opinię Grupy Roboczej Art. 29 dotyczącą tych pojęć (WP169).

5. W części I niniejszych wytycznych omówiono definicje różnych pojęć administratora, współadministratorów, podmiotu przetwarzającego oraz strony trzeciej/odbiorcy. W części II przedstawiono dalsze wskazówki dotyczące konsekwencji związanych z różnymi rolami administratora, współadministratorów i podmiotu przetwarzającego.

CZĘŚĆ I – POJĘCIA

1 UWAGI OGÓLNE

6. W art. 5 ust. 2 RODO wyraźnie wprowadza się zasadę rozliczalności, co oznacza, że:

   - administrator *jest odpowiedzialny za przestrzeganie* zasad określonych w art. 5 ust. 1 RODO; oraz że
   - administrator musi być w stanie *wykazać przestrzeganie* zasad określonych w art. 5 ust. 1 RODO.

   Zasada ta została opisana w opinii Grupy Roboczej Art. 29[3] i nie będzie tutaj szczegółowo omawiana.

7. Celem włączenia zasady rozliczalności do RODO i uczynienia jej główną zasadą było podkreślenie, że administratorzy danych muszą wdrożyć odpowiednie i skuteczne środki oraz być w stanie wykazać zgodność z przepisami.[4]

8. Zasada rozliczalności została doprecyzowana w art. 24, który stanowi, że administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami RODO i aby móc to **wykazać**. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Zasada rozliczalności znajduje również odzwierciedlenie w art. 28, w którym określono obowiązki administratora podczas korzystania z usług podmiotu przetwarzającego.

9. Zasada rozliczalności jest skierowana bezpośrednio do administratora. Niektóre z bardziej szczegółowych przepisów dotyczą jednak zarówno administratorów, jak i podmiotów przetwarzających, np. przepisy dotyczące uprawnień organów nadzorczych zawarte w art. 58. Zarówno administratorzy, jak i podmioty przetwarzające mogą podlegać karze pieniężnej w przypadku naruszenia dotyczących ich obowiązków przewidzianych w RODO, oraz oba te podmioty ponoszą bezpośrednią odpowiedzialność względem organów nadzorczych z tytułu obowiązku przechowywania i dostarczania na żądanie odpowiedniej dokumentacji, współpracy w przypadku prowadzenia postępowania i wykonywania rozkazów administracyjnych. Jednocześnie należy przypomnieć, że podmioty przetwarzające muszą zawsze stosować się do instrukcji administratora i działać wyłącznie na ich podstawie.

[3] Grupa Robocza Art. 29, Opinia 3/2010 w sprawie zasady rozliczalności przyjęta w dniu13 lipca 2010 r., 00062/10/PL, WP 173.
[4] Motyw 74 RODO.

10. Zasada rozliczalności, wraz z pozostałymi, bardziej szczegółowymi przepisami dotyczącymi sposobu przestrzegania przepisów RODO i podziału odpowiedzialności sprawia zatem, że konieczne jest określenie poszczególnych ról kilku podmiotów zaangażowanych w przetwarzanie danych osobowych.

11. Ogólne spostrzeżenie dotyczące pojęć administratora i podmiotu przetwarzającego w RODO jest takie, że nie zmieniły się one w porównaniu z dyrektywą 95/46/WE i że ogólnie rzecz ujmując, kryteria dotyczące sposobu przypisywania poszczególnych ról pozostają takie same.

12. Pojęcia „administrator" i „podmiot przetwarzający" są pojęciami *funkcjonalnymi*: ich celem jest podział obowiązków stosownie do rzeczywistych ról stron.[5] Oznacza to, że status prawny podmiotu jako „administratora " lub „podmiotu przetwarzającego" należy zasadniczo określać w oparciu o jego rzeczywiste działania w konkretnej sytuacji, a nie w oparciu o formalne wyznaczenie podmiotu jako „administratora danych" lub „podmiotu przetwarzającego" (np. w umowie)[6]. Oznacza to, że podział ról powinien zazwyczaj wynikać z analizy elementów stanu faktycznego lub okoliczności sprawy i jako taki nie podlega uzgodnieniom.

13. Pojęcia administratora i podmiotu przetwarzającego są również pojęciami *autonomicznymi* w tym sensie, że chociaż zewnętrzne źródła prawne mogą być pomocne w ustaleniu, kto jest administratorem danych, interpretacji należy dokonywać przede wszystkim zgodnie z przepisami dotyczącymi ochrony danych. Pojęcia administratora nie powinny naruszać inne, często kolidujące lub pokrywające się, pojęcia z innych dziedzin prawa, takie jak twórca lub posiadacz praw w prawach własności intelektualnej lub prawie konkurencji.

14. Ponieważ podstawowym celem przypisania roli administratora jest zapewnienie rozliczalności oraz skutecznej i pełnej ochrony danych osobowych, pojęcie „administratora" powinno się interpretować w sposób odpowiednio szeroki, zapewniając w ten sposób w jak największym stopniu skuteczną i pełną ochronę osób, których dane dotyczą[7], tak aby zapewnić pełną skuteczność unijnych przepisów o ochronie danych, nie dopuścić do powstania luk i zapobiec ewentualnemu obchodzeniu przepisów, a jednocześnie nie osłabiać roli podmiotu przetwarzającego.

2 DEFINICJA ADMINISTRATORA

2.1 Definicja administratora

15. Zgodnie z definicją zawartą w art. 4 ust. 7 RODO administrator oznacza:

> „***osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot**, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego,*

[5] Opinia Grupy Roboczej Art. 29 nr 1/2010, WP 169, s. 9.

[6] Zobacz również opinię rzecznika generalnego P. Mengozziego, w wyroku w sprawie C-25/17, *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta*, ECLI:EU:C:2018:57, pkt 68 (*„Jestem skłonny uznać, [...] że przy określaniu „administratora danych" w rozumieniu dyrektywy 95/46 nadmierny formalizm pozwoliłby na łatwe obejście przepisów dyrektywy 95/46 oraz że w konsekwencji [...] należy opierać się raczej na analizie okoliczności faktycznych niż na analizie formalnej*.")

[7] TSUE, sprawa C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, wyrok z dnia 13 maja 2014 r., pkt 34; TSUE, sprawa C-210/16, Wirtschaftsakademie Schleswig-Holstein, wyrok z dnia 5 czerwca 2018 r., pkt 28; TSUE, sprawa C-40/17, Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV, wyrok z dnia 29 lipca 2019 r., pkt 66.

to również ***w prawie Unii lub w prawie państwa członkowskiego*** *może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania*".

16. Definicja administratora składa się z pięciu głównych modułów, które do celów niniejszych wytycznych zostaną poddane odrębnej analizie. Zalicza się do nich następujące procesy:

- „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot"
- „ustala"
- „samodzielnie lub wspólnie z innymi"
- „cele i sposoby"
- „przetwarzania danych osobowych".

2.1.1 „Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot"

17. Pierwszy moduł odnosi się do rodzaju podmiotu, który może być administratorem. Zgodnie z RODO, administratorem danych może być „*osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot*". Oznacza to, że w zasadzie nie ma ograniczeń co do rodzaju podmiotu, który może pełnić rolę administratora. Może to być organizacja, ale może to być również osoba fizyczna lub grupa osób[8]. W praktyce jednak to zwykle organizacja jako taka, a nie osoba fizyczna w organizacji (np. dyrektor generalny, pracownik lub członek zarządu), działa jako administrator w rozumieniu RODO. Jeśli chodzi o przetwarzanie danych w ramach grupy przedsiębiorstw, szczególną uwagę należy zwrócić na kwestię, czy przedsiębiorstwo może działać jako administrator lub podmiot przetwarzający, np. gdy przetwarza dane w imieniu spółki dominującej.

18. Czasami przedsiębiorstwa i organy publiczne wyznaczają konkretną osobę odpowiedzialną za realizację działań związanych z przetwarzaniem. Nawet jeżeli do zapewnienia zgodności z przepisami o ochronie danych wyznaczona zostanie konkretna osoba fizyczna, osoba ta nie będzie administratorem, lecz będzie działać w imieniu podmiotu prawnego (przedsiębiorstwa lub organu publicznego), który będzie ponosić ostateczną odpowiedzialność w przypadku naruszenia przepisów na skutek działania w charakterze administratora. Podobnie nawet jeśli określony dział lub jednostka organizacji ponosi odpowiedzialność operacyjną za zapewnienie zgodności w odniesieniu do niektórych czynności przetwarzania, nie oznacza to, że ten dział lub jednostka (a nie organizacja jako całość) staje się administratorem.

Przykład:

Dział marketingu przedsiębiorstwa ABC rozpoczyna kampanię reklamową promującą produkty ABC. Dział marketingowy decyduje o charakterze kampanii, środkach, jakie należy zastosować (e-mail, media społecznościowe itp.), o tym, do jakich klientów należy dotrzeć i jakie dane należy wykorzystać, aby kampania była jak najskuteczniejsza. Nawet jeżeli dział marketingu działał w sposób w znacznym stopniu niezależny, co do zasady to przedsiębiorstwo ABC będzie uważane za administratora, ponieważ kampania reklamowa jest inicjowana przez przedsiębiorstwo i odbywa się w ramach jej działalności gospodarczej i do jej celów.

[8] Na przykład w wyroku w sprawie C-25/17, *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551, pkt 75, TSUE uznał, że wspólnota świadków Jehowy działała jako administrator danych, wspólnie ze swoimi poszczególnymi członkami. Wyrok w sprawie C-25/17, *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551, pkt 75.

19. Zasadniczo można przyjąć, że każde przetwarzanie danych osobowych przez pracowników, które odbywa się w ramach działalności organizacji, odbywa się pod kontrolą tej organizacji[9]. W wyjątkowych okolicznościach może się jednak zdarzyć, że pracownik wykorzysta dane osobowe do własnych celów, tym samym bezprawnie przekraczając przyznane mu uprawnienia. (np. w celu założenia własnego przedsiębiorstwa lub w podobnym celu). Obowiązkiem organizacji jako administratora jest zatem upewnienie się, że istnieją odpowiednie środki techniczne i organizacyjne, w tym np. szkolenia i informowanie pracowników, mające na celu zapewnienie zgodności z RODO[10].

2.1.2 „ustala"

20. Drugi moduł koncepcji administratora odnosi się do *wpływu* administratora na przetwarzanie danych poprzez *wykonywanie uprawnień decyzyjnych*. Administrator to organ, który *decyduje* o pewnych kluczowych elementach przetwarzania. Definicja administrowania danymi może wynikać z przepisów prawa lub analizy elementów stanu faktycznego lub okoliczności sprawy. Należy przyjrzeć się konkretnym operacjom przetwarzania i zrozumieć, kto je ustala, biorąc pod uwagę w pierwszej kolejności następujące kwestie: *„dlaczego dane są przetwarzane*?" oraz *„kto zdecydował, że dane powinny być przetwarzane w określonym celu?"*.

Okoliczności powodujące powstanie administrowania

21. W związku z tym, że pojęcie administratora jest pojęciem funkcjonalnym, opiera się ono raczej na **analizie okoliczności faktycznych niż analizie formalnej**. W celu ułatwienia analizy można zastosować pewne zasady postępowania i praktyczne założenia, aby ukierunkować i uprościć proces. W większości sytuacji „organ ustalający" można łatwo i jasno identyfikować przez odniesienie do okoliczności prawnych lub faktycznych, z których normalnie może wynikać faktyczny „wpływ", o ile inne elementy nie wskazują inaczej. Można wyróżnić dwie kategorie sytuacji: (1) administrowanie wynikające z *przepisów prawnych*; oraz (2) administrowanie wynikające z *faktycznego wpływu*.

1) *Administrowanie wynikające z przepisów prawnych*

22. Istnieją przypadki, w których administrowanie można ustalić na podstawie wyraźnej kompetencji prawnej, np. gdy administrator lub szczegółowe kryteria potrzebne do jego wyznaczenia są określane przez przepisy prawa krajowego lub prawa Unii. Artykuł 4 ust. 7 stanowi bowiem, że *„jeżeli cele i sposoby takiego 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.*" Choć art. 4 ust. 7 odnosi się wyłącznie do „administratora" w liczbie pojedynczej, EROD uważa, że prawo Unii lub państwa członkowskiego może również przewidywać wyznaczenie więcej niż jednego administratora, być może nawet współadministratorów.

23. W przypadku gdy administrator został wyraźnie wyznaczony przez prawo, będzie to miało decydujące znaczenie dla ustalenia, kto działa jako administrator. Oznacza to, że ustawodawca wyznaczył jako administratora podmiot, który ma rzeczywistą zdolność do sprawowania kontroli. W niektórych państwach przepisy prawa krajowego przewidują, że organy publiczne odpowiadają za przetwarzanie danych osobowych w ramach swoich obowiązków.

[9] Pracowników, którzy mają dostęp do danych osobowych w organizacji, zasadniczo nie uważa się za „administratorów" ani „podmioty przetwarzające", lecz raczej za „osoby działające z upoważnienia administratora lub podmiotu przetwarzającego" w rozumieniu art. 29 RODO.
[10] Artykuł 24 ust. 1 RODO.

24. Częściej ma jednak miejsce sytuacja, w której przepisy prawa, zamiast bezpośrednio wyznaczyć administratora danych lub określić kryteria jego wyznaczania, ustalają zadanie lub nakładają na kogoś obowiązek gromadzenia i przetwarzania niektórych danych. W takim przypadku określenie, kto jest administratorem, wynika z prawa. Administratorem będzie zazwyczaj administrator wyznaczony przez prawo do realizacji tego celu, tego zadania publicznego. Tak może być na przykład w przypadku podmiotu, któremu powierzono pewne zadania publiczne (np. zabezpieczenie społeczne), których nie można wypełnić bez zgromadzenia przynajmniej niektórych danych osobowych, i który tworzy bazę danych lub rejestr w celu realizacji tych zadań publicznych. W takim przypadku określenie, kto jest administratorem – choć pośrednio – wynika z prawa. Ogólniej mówiąc, prawo może również nakładać na podmioty publiczne lub prywatne obowiązek zatrzymywania lub przekazywania określonych danych. Podmioty te byłyby wówczas zazwyczaj uznawane za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku.

Przykład: przepisy prawne

Prawo krajowe w kraju A nakłada na władze miejskie obowiązek zapewnienia obywatelom świadczeń z zakresu opieki społecznej, takich jak miesięczne wypłaty, w zależności od ich sytuacji finansowej. W celu realizacji tych płatności władze miejskie muszą gromadzić i przetwarzać dane dotyczące sytuacji finansowej wnioskodawców. Nawet jeśli ustawa nie stanowi wyraźnie, że władze miejskie są administratorami w zakresie tego przetwarzania, wynika to w sposób dorozumiany z przepisów prawnych.

2) *Administrowanie wynikające z faktycznego wpływu*

25. W przypadku braku administrowania wynikającego z przepisów prawnych kwalifikacja strony jako administratora musi zostać ustalona na podstawie oceny okoliczności faktycznych związanych z przetwarzaniem. Aby stwierdzić, czy dany podmiot ma decydujący wpływ na przetwarzanie danych osobowych, należy wziąć pod uwagę wszystkie istotne okoliczności faktyczne.

26. Potrzeba oceny faktów oznacza również, że rola administratora nie wynika z charakteru podmiotu przetwarzającego dane, ale z jego konkretnych działań w określonym kontekście. Innymi słowy, ten sam podmiot może działać jednocześnie jako administrator w przypadku niektórych operacji przetwarzania danych i jako przetwarzający w przypadku innych tego rodzaju operacji, a to czy kwalifikuje się jako administrator czy przetwarzający należy oceniać w odniesieniu do każdej konkretnej czynności przetwarzania danych.

27. W praktyce niektóre działania związane z przetwarzaniem można uznać za powiązane w sposób naturalny z rolą lub działalnością podmiotu, co ostatecznie pociąga za sobą odpowiedzialność z punktu widzenia ochrony danych. Może to wynikać z bardziej ogólnych przepisów prawnych lub z utrwalonej praktyki prawnej w różnych dziedzinach (prawo cywilne, prawo handlowe, prawo pracy itd.). W takim przypadku w zidentyfikowaniu administratora pomogą istniejące tradycyjne role i wiedza specjalistyczna, które zwykle wiążą się z pewną odpowiedzialnością: będzie nim na przykład pracodawca w odniesieniu do przetwarzania danych osobowych dotyczących jego pracowników, wydawca przetwarzający dane osobowe swoich abonentów lub stowarzyszenie przetwarzające dane osobowe swoich członków lub osób wspierających. Gdy podmiot angażuje się w przetwarzanie danych osobowych w ramach interakcji z własnymi pracownikami, klientami lub członkami, to zazwyczaj to ten podmiot określa cel i sposoby przetwarzania i w związku z tym działa jako administrator w rozumieniu RODO.

Przykład: kancelarie prawne

Przedsiębiorstwo ABC zatrudnia kancelarię prawną do reprezentowania jej w sporze. Aby wykonać to zadanie, kancelaria prawna musi przetwarzać dane osobowe związane ze sprawą. Podstawą przetwarzania danych osobowych jest upoważnienie kancelarii do reprezentowania klienta w sądzie. Mandat ten nie jest jednak ukierunkowany konkretnie na przetwarzanie danych osobowych. Kancelaria prawna działa w znacznym stopniu niezależnie, na przykład przy podejmowaniu decyzji o tym, z jakich informacji i w jak sposób będzie korzystać, a przedsiębiorstwo będące klientem nie wydało żadnych instrukcji dotyczących przetwarzania danych osobowych. Przetwarzanie, którego kancelaria dokonuje w celu wypełnienia zadania jako przedstawiciel prawny spółki, jest zatem związane z rolą funkcjonalną kancelarii, w związku z czym należy ją traktować jako administratora tego przetwarzania.

Przykład: operatorzy telekomunikacyjni[11]

Świadczenie usług łączności elektronicznej, takich jak usługi poczty elektronicznej, wiąże się z przetwarzaniem danych osobowych. Dostawca takich usług będzie zazwyczaj uważany za administratora w odniesieniu do przetwarzania danych osobowych, które jest niezbędne do świadczenia usługi jako takiej (np. danych dotyczących ruchu i rozliczeń). Jeżeli jedynym celem i rolą dostawcy jest umożliwienie przekazywania wiadomości e-mail, dostawca nie będzie uważany za administratora danych osobowych zawartych w samej wiadomości. Za administratora danych osobowych zawartych w wiadomości uznaje się zwykle osobę, od której pochodzi wiadomość, a nie dostawcę usług oferującego usługę transmisji.

28. W wielu przypadkach ocena warunków umowy między różnymi zaangażowanymi stronami może ułatwić ustalenie, która strona (lub strony) działa(ją) jako administrator(zy). Nawet jeżeli umowa nie określa, kto jest administratorem, może ona zawierać elementy wystarczające do stwierdzenia, kto pełni rolę decyzyjną w odniesieniu do celów i sposobów przetwarzania. Może się również zdarzyć, że umowa zawiera wyraźne stwierdzenie tożsamości administratora. Jeżeli nie ma powodu, aby wątpić, że dokładnie odzwierciedla to rzeczywistość, nic nie stoi na przeszkodzie stosowaniu się do warunków umowy. Jednak nie we wszystkich okolicznościach warunki umowy mają decydujące znaczenie, ponieważ umożliwiłoby to stronom podział odpowiedzialności według własnego uznania. Nie można zostać administratorem, ani uchylić się od obowiązków administratora poprzez zwykłe sformułowanie umowy w określony sposób, w przypadku gdy okoliczności faktyczne świadczą o czym innym.

29. Jeżeli jedna strona faktycznie decyduje o tym, dlaczego i w jaki sposób dane osobowe są przetwarzane, strona ta będzie administratorem, nawet jeżeli umowa mówi, że jest ona podmiotem przetwarzającym. Podobnie to nie dlatego, że w umowie handlowej użyto terminu „podwykonawca", dany podmiot należy uznać za podmiot przetwarzający z punktu widzenia prawa ochrony danych[12].

30. Zgodnie z podejściem faktycznym słowo „ustala" oznacza, że administratorem jest podmiot, który faktycznie wywiera decydujący wpływ na cele i sposoby przetwarzania. Zazwyczaj umowa dotycząca przetwarzania danych określa, kim są podmiot rozstrzygający (administrator) oraz strona poinstruowana (podmiot przetwarzający). Nawet jeśli podmiot przetwarzający oferuje usługę, która jest wstępnie zdefiniowana w dany sposób, administrator musi otrzymać szczegółowy opis usługi i musi

[11] EIOD uważa, że przykład ten, uprzednio zawarty w motywie 47 dyrektywy 95/46/WE, pozostaje istotny również w kontekście RODO.

[12] Zobacz np. Grupa Robocza Art. 29, opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT), 22 listopada 2006 r., WP128, s. 11.

podjąć ostateczną decyzję, czy zatwierdza sposób przetwarzania, i zażądać zmian, jeśli jest to konieczne. Ponadto podmiot przetwarzający nie może na późniejszym etapie zmieniać istotnych elementów przetwarzania bez zgody administratora.

Przykład: znormalizowana usługa przechowywania w chmurze

Duży dostawca usług przechowywania w chmurze oferuje swoim klientom możliwość przechowywania dużych ilości danych osobowych. Usługa jest całkowicie znormalizowana, a klienci mają niewielkie możliwości dostosowania jej do własnych potrzeb lub nie mają jej wcale. Warunki umowy są określane i sporządzane jednostronnie przez dostawcę usług w chmurze, a klient nie ma możliwości ich uzgodnienia. Przedsiębiorstwo X decyduje się na skorzystanie z usług dostawcy usług w chmurze w celu przechowywania danych osobowych swoich klientów. Przedsiębiorstwo X będzie nadal uznawane za administratora ze względu na podjętą decyzję o skorzystaniu z usług tego konkretnego dostawcy usług w chmurze w celu przetwarzania danych osobowych do swoich celów. W zakresie, w jakim dostawca usług w chmurze nie przetwarza danych osobowych do własnych celów i przechowuje dane wyłącznie w imieniu swoich klientów oraz zgodnie z instrukcjami, dostawca usług będzie uważany za podmiot przetwarzający.

2.1.3 „samodzielnie lub wspólnie z innymi”

31. Zgodnie z art. 4 ust. 7 „cele i sposoby” przetwarzania mogą być określone przez więcej niż jeden podmiot. Przepis ten stanowi, że administrator oznacza podmiot, który „samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych”. Oznacza to, że kilka różnych podmiotów może działać jako administratorzy w odniesieniu do tego samego przetwarzania, przy czym każdy z nich podlega obowiązującym przepisom o ochronie danych. W związku z tym organizacja może być administratorem, nawet jeśli nie podejmuje wszystkich decyzji dotyczących celów i sposobów przetwarzania. Kryteria współadministracji oraz zakres, w jakim dwa podmioty lub większa ich liczba wspólnie sprawują kontrolę, mogą przybierać różne formy, co zostało wyjaśnione w dalszej części[13].

2.1.4 „cele i sposoby”

32. Czwarty moduł definicji administratora odnosi się do przedmiotu, na który administrator ma wpływ, a mianowicie „celów i sposobów” przetwarzania. Moduł ten stanowi ważny element definicji administratora: co strona powinna określić, aby uznano ją za administratora.

33. Słowniki definiują „cel” jako „oczekiwany rezultat, który jest zamierzony lub który kieruje zaplanowanymi działaniami”, a „sposób” jako „określenie sposobu osiągnięcia rezultatu lub celu”.

34. Ogólne rozporządzenie o ochronie danych stanowi, że dane są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami. Dlatego szczególne znaczenie ma określenie „celów” przetwarzania i „sposobów” ich osiągnięcia.

35. Określanie celów i sposobów sprowadza się do określenia odpowiednio „dlaczego” i „jak” prowadzi się czynności przetwarzania danych[14]: biorąc pod uwagę konkretną operację przetwarzania, administrator jest podmiotem, który określił, *dlaczego* odbywa się przetwarzanie (tj. „w jakim celu”; lub „po co”) i *jak* ten cel zostanie osiągnięty (tj. jakie środki zostaną zastosowane, aby osiągnąć ten cel). Osoba fizyczna lub prawna, która ma taki wpływ na przetwarzanie danych osobowych, uczestniczy tym

[13] Zobacz część I, sekcja 3 („Definicja współadministratorów”).

[14] Zobacz również opinię rzecznika generalnego Yves’a Bota w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2017:796, pkt 46.

samym w określaniu celów i sposobów tego przetwarzania zgodnie z definicją zawartą w art. 4 ust. 7 RODO.[15]

36. Administrator musi zdecydować zarówno o celu, jak i sposobie przetwarzania, jak opisano poniżej. W związku z tym administrator nie może poprzestać na określeniu celu. Musi również podjąć decyzje co do sposobów przetwarzania. Natomiast strona działająca jako podmiot przetwarzający nigdy nie określa celu przetwarzania.

37. W praktyce, jeżeli administrator angażuje podmiot przetwarzający w przetwarzanie w jego imieniu, często oznacza to, że podmiot przetwarzający będzie miał możliwość samodzielnego podejmowania pewnych decyzji co do sposobu przetwarzania. Europejska Rada Ochrony Danych uznaje, że podmiot przetwarzający może mieć pewien margines swobody, aby mógł podejmować pewne decyzje w odniesieniu do przetwarzania. W tym kontekście istnieje potrzeba zapewnienia wytycznych wyjaśniających, jak duży wpływ na „dlaczego" i „jak" może mieć uznanie podmiotu za administratora i w jakim zakresie podmiot przetwarzający może samodzielnie podejmować decyzje.

38. W sytuacji, gdy jeden podmiot wyraźnie określa cele i sposoby przetwarzania, powierzając innemu podmiotowi czynności przetwarzania, które są równoznaczne z wykonaniem jego szczegółowych instrukcji, sytuacja jest prosta i nie ma wątpliwości, że ten drugi podmiot należy uznać za podmiot przetwarzający, podczas gdy pierwszy podmiot jest administratorem.

Istotne i inne niż istotne sposoby przetwarzania

39. Pytanie brzmi gdzie wytyczyć granicę między decyzjami zastrzeżonymi dla administratora a decyzjami, które może podejmować podmiot przetwarzający według własnego uznania. Decyzje dotyczące celu przetwarzania danych są oczywiście zawsze podejmowane przez administratora.

40. Jeśli chodzi o określenie sposobów przetwarzania, można dokonać rozróżnienia między istotnymi sposobami przetwarzania a sposobami innymi niż istotne. „Istotne sposoby przetwarzania" są z natury zastrzeżone dla administratora. Podczas gdy sposoby przetwarzania inne niż istotne mogą być również określane przez podmiot przetwarzający, istotne sposoby przetwarzania określa administrator. „Istotne sposoby przetwarzania" to sposoby przetwarzania, które są ściśle związane z celem i zakresem przetwarzania, takie jak rodzaj przetwarzanych danych osobowych („*jakie dane będą przetwarzane?*"), czas trwania przetwarzania („*jak długo będą przetwarzane?*"), kategorie odbiorców („*kto będzie miał do nich dostęp?*") oraz kategorie osób, których dane dotyczą („*czyje dane osobowe są przetwarzane*?"). Wraz z celem przetwarzania danych, podstawowe sposoby przetwarzania są również ściśle powiązane z kwestią, czy przetwarzanie danych jest zgodne z prawem, niezbędne i proporcjonalne. „Sposoby przetwarzania inne niż istotne" dotyczą bardziej praktycznych aspektów wdrażania, takich jak wybór konkretnego rodzaju sprzętu lub oprogramowania lub szczegółowych środków bezpieczeństwa, których wybór może pozostać w gestii podmiotu przetwarzającego.

Przykład: zarządzanie listą płac

Pracodawca A zatrudnia inne przedsiębiorstwo, które zarządza wypłatą wynagrodzeń jego pracownikom. Pracodawca A wydaje jasne instrukcje dotyczące tego, komu należy wypłacić wynagrodzenie, jakie kwoty, w jakim terminie, przez jaki bank, jak długo dane mają być przechowywane, jakie dane należy ujawnić organowi podatkowemu itd. W tym przypadku przetwarzanie danych odbywa się na potrzeby przedsiębiorstwa A w celu wypłaty wynagrodzeń jego pracownikom, a administrator listy płac nie może wykorzystywać danych do żadnych własnych celów.

[15] Wyrok w sprawie C-25/17, *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551, pkt 68.

Sposób, w jaki administrator listy płac powinien dokonywać przetwarzania danych, jest w zasadzie jasno i ściśle określony. Administrator listy płac może jednak decydować o pewnych szczegółowych kwestiach związanych z przetwarzaniem, takich jak oprogramowanie, którego ma używać, sposób rozpowszechniania dostępu w ramach własnej organizacji itd. Nie zmienia to jego roli jako podmiotu przetwarzającego, o ile administrator nie postępuje z naruszeniem instrukcji przedsiębiorstwa A ani nie wykracza poza te instrukcje.

Przykład: płatności bankowe

W ramach instrukcji od Pracodawcy A, administracja listy płac przekazuje informacje do Banku B, aby ten mógł dokonać faktycznej wypłaty pracownikom Pracodawcy A. Czynność ta obejmuje przetwarzanie danych osobowych przez Bank B, które odbywa się w celu prowadzenia działalności bankowej. W ramach tej działalności bank decyduje niezależnie od Pracodawcy A o tym, jakie dane muszą być przetwarzane w celu świadczenia usługi, jak długo dane muszą być przechowywane itd. Pracodawca A nie może mieć żadnego wpływu na cel i sposoby przetwarzania danych przez Bank B. Bank B należy zatem uznać za administratora w odniesieniu do tego przetwarzania, a przekazanie danych osobowych z administracji listą płac należy uznać za ujawnienie informacji między dwoma administratorami danych, od Pracodawcy A do Banku B.

Przykład: księgowi

Pracodawca A zatrudnia również Biuro rachunkowe C do przeprowadzania kontroli księgowości i w związku z tym przekazuje C dane dotyczące transakcji finansowych (w tym dane osobowe). Biuro rachunkowe C przetwarza te dane bez szczegółowych instrukcji ze strony A. Biuro rachunkowe C samo decyduje, zgodnie z przepisami prawnymi regulującymi zadania związane z działalnością audytową prowadzoną przez C, że gromadzone przez nie dane będą przetwarzane wyłącznie do celów audytu A i określa, jakie dane musi posiadać, jakie kategorie osób muszą być zarejestrowane, jak długo dane mają być przechowywane i jakie środki techniczne należy zastosować. W tych okolicznościach Biuro rachunkowe C należy uznać za samodzielnego administratora w odniesieniu do świadczenia usług audytorskich na rzecz A. Ocena ta może być jednak różna w zależności od instrukcji ze strony A. W sytuacji, w której prawo nie określa szczegółowych obowiązków biura rachunkowego, a przedsiębiorstwo będące klientem dostarcza bardzo szczegółowych instrukcji dotyczących przetwarzania, biuro rachunkowe rzeczywiście działałoby jako podmiot przetwarzający. Można dokonać rozróżnienia między sytuacją, w której przetwarzanie odbywa się – zgodnie z przepisami regulującymi ten zawód – w ramach podstawowej działalności biura rachunkowego, a sytuacją, w której przetwarzanie danych jest bardziej ograniczonym, pomocniczym zadaniem wykonywanym w ramach działalności przedsiębiorstwa będącego klientem.

Przykład: usługi hostingowe

Pracodawca A zatrudnia dostawcę usług hostingowych H do przechowywania zaszyfrowanych danych na serwerach H. Dostawca usług hostingowych H nie określa, czy przechowywane przez niego dane są danymi osobowymi, ani też nie przetwarza danych w jakikolwiek inny sposób niż przechowując je na swoich serwerach. Ponieważ przechowywanie jest jedną z czynności przetwarzania danych osobowych, dostawca usług hostingowych H przetwarza dane osobowe w imieniu pracodawcy A, a zatem jest podmiotem przetwarzającym. Pracodawca A musi przekazać H niezbędne instrukcje, a zgodnie z art. 28 należy zawrzeć umowę o przetwarzaniu danych, zobowiązującą H do wdrożenia

technicznych i organizacyjnych środków bezpieczeństwa. H musi wesprzeć A w zapewnieniu podjęcia niezbędnych środków bezpieczeństwa i powiadomić je o wszelkich przypadkach naruszenia ochrony danych osobowych.

41. Nawet jeśli decyzje dotyczące sposobów przetwarzania innych niż istotne można pozostawić podmiotowi przetwarzającemu, administrator nadal określa pewne elementy w umowie dotyczącej przetwarzania danych, takie jak te dotyczące wymogu bezpieczeństwa, np. polecenie podjęcia wszelkich środków wymaganych na mocy art. 32 RODO. Umowa musi również stanowić, że podmiot przetwarzający pomaga administratorowi w zapewnieniu zgodności, na przykład, z art. 32. W każdym przypadku administrator pozostaje odpowiedzialny za wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z przepisami RODO i aby móc to wykazać (art. 24). Administrator musi przy tym wziąć pod uwagę charakter, zakres, kontekst i cele przetwarzania, a także zagrożenia dla praw i wolności osób fizycznych. Z tego powodu administratora należy w pełni poinformować o stosowanych środkach, tak aby mógł podjąć świadomą decyzję w tym zakresie. Aby administrator mógł wykazać zgodność przetwarzania z prawem, zaleca się udokumentowanie co najmniej niezbędnych środków technicznych i organizacyjnych w umowie lub innym prawnie wiążącym dokumencie zawartym między administratorem a podmiotem przetwarzającym.

Przykład: call center

Przedsiębiorstwo X decyduje się na outsourcing części obsługi klienta do call center. Call center otrzymuje dane identyfikacyjne dotyczące zakupów dokonywanych przez klientów, jak również dane kontaktowe. Call center wykorzystuje własne oprogramowanie i infrastrukturę informatyczną do zarządzania danymi osobowymi klientów przedsiębiorstwa X. Przedsiębiorstwo X podpisuje umowę dotyczącą przetwarzania danych z dostawcą call center zgodnie z art. 28 RODO, po ustaleniu, że techniczne i organizacyjne środki bezpieczeństwa proponowane przez call center są odpowiednie dla danego ryzyka oraz że call center będzie przetwarzać dane osobowe wyłącznie do celów Przedsiębiorstwa X i zgodnie z jego instrukcjami. Przedsiębiorstwo X nie dostarcza call center żadnych dalszych instrukcji dotyczących konkretnego oprogramowania, którego należy używać, ani żadnych szczegółowych instrukcji dotyczących konkretnych środków bezpieczeństwa, które należy wdrożyć. W tym przykładzie Przedsiębiorstwo X pozostaje administratorem, mimo, że call center określiło pewne sposoby przetwarzania inne niż istotne.

2.1.5 „przetwarzania danych osobowych”

42. Cele i sposoby przetwarzania określone przez administratora muszą odnosić się do „przetwarzania danych osobowych”. Zgodnie z art. 4 ust. 2 RODO przetwarzanie danych osobowych oznacza „*operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych*”. W rezultacie pojęcie administratora może być związane albo z pojedynczą operacją przetwarzania, albo z zestawem operacji. W praktyce może to oznaczać, że kontrola sprawowana przez dany podmiot może obejmować całość danego przetwarzania, ale może być również ograniczona do określonego etapu przetwarzania[16].

[16] Wyrok w sprawie C-40/17, *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV.*, ECLI:EU:C:2019:629, pkt 74: *„[J]ak zauważył w istocie rzecznik generalny [...] – [...] wydaje się, iż osoba fizyczna lub prawna może jedynie być administratorem w rozumieniu art. 2 lit. d) dyrektywy 95/46 wspólnie z innymi podmiotami w odniesieniu do operacji przetwarzania danych osobowych, których cele i sposoby określa wspólnie. Natomiast [...] osoby fizycznej lub prawnej nie można uznać za administratora w rozumieniu tego przepisu w*

43. W praktyce przetwarzanie danych osobowych, w którym uczestniczy kilka podmiotów, można podzielić na kilka mniejszych operacji przetwarzania, w przypadku których można by uznać, że każdy podmiot indywidualnie określa cel i sposoby. Z drugiej strony sekwencja lub zestaw operacji przetwarzania z udziałem kilku podmiotów może również mieć miejsce w tym samym celu lub w tych samych celach, w którym to przypadku możliwe jest, że przetwarzanie obejmuje jednego współadministratora lub większą liczbę współadministratorów. Innymi słowy, możliwe jest, że w skali mikro poszczególne operacje przetwarzania danych w łańcuchu wydają się niepowiązane, ponieważ każda z nich może mieć inny cel. Należy jednak dwukrotnie sprawdzić, czy w skali makro nie należałoby operacji przetwarzania danych uznać za „zestaw operacji" służących jednemu celowi lub wykorzystujących wspólnie określone sposoby przetwarzania danych.

44. Każdy, kto decyduje się na przetwarzanie danych, musi rozważyć, czy obejmuje to dane osobowe, a jeśli tak, jakie są obowiązki wynikające z RODO. Podmiot uznaje się za „administratora", nawet jeżeli jego działania nie są celowo ukierunkowane na przetwarzanie danych osobowych jako takich lub gdy błędnie założył, że nie przetwarza danych osobowych.

45. Nie jest konieczne, aby administrator miał faktyczny dostęp do przetwarzanych danych[17]. Osobę, która zleca czynności przetwarzania i tym samym ma decydujący wpływ na cel i (istotny) sposób przetwarzania (np. poprzez dostosowanie parametrów usługi w taki sposób, że wpływa to na to, czyje dane osobowe będą przetwarzane), należy uznać za administratora, nawet jeśli nigdy nie będzie miała faktycznego dostępu do danych.

Przykład: badanie rynku 1

Przedsiębiorstwo ABC chce zrozumieć, jakie rodzaje konsumentów są najbardziej zainteresowane jego produktami i zleca dostawcy usług XYZ uzyskanie odpowiednich informacji.

Przedsiębiorstwo ABC instruuje XYZ, jakiego rodzaju informacje je interesują i przekazuje listę pytań, które należy zadać osobom biorącym udział w badaniu rynku.

Przedsiębiorstwo ABC otrzymuje od XYZ jedynie informacje statystyczne (np. identyfikujące trendy konsumenckie w danym regionie) i nie ma dostępu do samych danych osobowych. Przedsiębiorstwo ABC postanowiło jednak, że powinno odbywać się przetwarzanie danych; przetwarzanie odbywa się dla jego celu i na potrzeby jego działalności, przy czym ABC dostarczyło XYZ szczegółowych instrukcji co do tego, jakie informacje należy zgromadzić. Przedsiębiorstwo ABC nadal należy zatem uznawać za administratora przetwarzania danych osobowych, którego celem jest dostarczenie żądanych informacji. XYZ może przetwarzać dane wyłącznie do celów określonych przez przedsiębiorstwo ABC i zgodnie z jego szczegółowymi instrukcjami, w związku z czym należy go uznać za podmiot przetwarzający.

Przykład: badanie rynku 2

Przedsiębiorstwo ABC chce zrozumieć, jakie rodzaje konsumentów będą najbardziej zainteresowane jego produktami. Dostawca usług XYZ jest agencją zajmującą się badaniami rynku, która gromadziła informacje na temat upodobań konsumentów za pomocą różnych kwestionariuszy dotyczących

odniesieniu do wcześniejszych lub późniejszych operacji łańcucha przetwarzania, których celów ani środków ona nie określa."

[17] Wyrok w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, pkt 38.

szerokiej gamy produktów i usług. Dostawca usług XYZ zebrał i przeanalizował te dane niezależnie, zgodnie z własną metodologią, nie otrzymując żadnych instrukcji od przedsiębiorstwa ABC. Aby dostarczyć usługę, o którą zwróciło się przedsiębiorstwo ABC, dostawca usług XYZ wygeneruje informacje statystyczne, ale zrobi to bez otrzymania jakichkolwiek dalszych instrukcji dotyczących tego, które dane osobowe należy przetwarzać lub jak je przetwarzać w celu wygenerowania tych statystyk. W tym przypadku dostawca usług XYZ pełni funkcję jedynego administratora i przetwarza dane osobowe do celów badania rynku, samodzielnie określając sposoby osiągnięcia tego celu. Przedsiębiorstwo ABC nie odgrywa żadnej szczególnej roli ani nie ponosi odpowiedzialności za czynności przetwarzania na mocy prawa o ochronie danych, ponieważ przedsiębiorstwo ABC otrzymuje zanonimizowane dane statystyczne i nie uczestniczy w określaniu celów i sposobów przetwarzania.

3 DEFINICJA WSPÓŁADMINISTRATORÓW

3.1 Definicja współadministratorów

46. Ze współadministratorami możemy mieć do czynienia w sytuacji, gdy w przetwarzaniu bierze udział więcej niż jeden podmiot.

47. Chociaż pojęcie to nie jest nowe i wprowadzono jest już na mocy dyrektywy 95/46/WE, w art. 26 RODO wprowadza się szczegółowe przepisy dotyczące współadministratorów i ustanawia ramy regulujące ich stosunki. Ponadto Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w niedawnych orzeczeniach doprecyzował to pojęcie i jego skutki[18].

48. Jak wyjaśniono w sekcji 2 część II, przypisanie roli współadministratorów będzie miało wpływ głównie na podział obowiązków w zakresie zgodności z przepisami o ochronie danych, a w szczególności praw osób fizycznych.

49. W tym kontekście celem poniższej sekcji jest przedstawienie wytycznych dotyczących pojęcia współadministratorów zgodnie z RODO i orzecznictwem TSUE, aby pomóc podmiotom w ustaleniu, w jakich sytuacjach działają jako współadministratorzy i jak stosować to pojęcie w praktyce.

3.2 Współadministracja

3.2.1 Kwestie ogólne

50. Definicja administratora zawarta w art. 4 ust. 7 RODO stanowi punkt wyjścia do określenia współadministracji. Rozważania zawarte w tej sekcji są zatem bezpośrednio związane z rozważaniami zawartymi w części dotyczącej pojęcia administratora i stanowią ich uzupełnienie. W związku z tym ocena współadministracji powinna odzwierciedlać ocenę „pojedynczej" administracji, o której mowa powyżej.

[18] Zobacz w szczególności *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu przeciwko Jehovan todistajat - uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV* (C-40/17). Należy zauważyć, że chociaż wyroki te zostały wydane przez TSUE w sprawie wykładni pojęcia współadministratorów na podstawie dyrektywy 95/46/WE, pozostają one aktualne w kontekście RODO, biorąc pod uwagę, że elementy określające to pojęcie na podstawie RODO pozostają takie same jak w przypadku dyrektywy.

51. Art. 26 RODO, który obejmuje definicję zawartą w art. 4 ust. 7 RODO stanowi, że „[j]eżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami." W szerokim ujęciu, współadministracja istnieje w odniesieniu do konkretnej czynności przetwarzania, gdy różne strony *wspólnie* określają cel i sposoby tej czynności przetwarzania. Dlatego też, aby ocenić, czy istnieje współadministracja należy zbadać, czy o określeniu celów i sposobów – co wskazuje na cechy administratora – decyduje więcej niż jedna strona. „Wspólnie" należy interpretować jako „razem z" lub „nie samodzielnie" w różnych formach i kombinacjach, jak wyjaśniono poniżej.

52. Ocenę współadministracji należy przeprowadzać na podstawie faktycznej, a nie formalnej analizy rzeczywistego wpływu na cele i sposoby przetwarzania. Wszystkie istniejące lub planowane uzgodnienia należy sprawdzić w świetle faktycznych okoliczności dotyczących stosunków między stronami. Wyłącznie formalne kryterium nie byłoby wystarczające z co najmniej z dwóch powodów: w niektórych przypadkach brakować będzie formalnego wyznaczenia współadministratora, określonego na przykład na mocy prawa lub w umowie; w innych przypadkach może się zdarzyć, że formalne wyznaczenie nie odzwierciedla rzeczywistych ustaleń, gdy formalnie powierzono rolę administratora podmiotowi, który faktycznie nie „określa" celów i sposobów przetwarzania.

53. Nie wszystkie operacje przetwarzania, w których uczestniczy kilka podmiotów, stanowią przypadek współadministracji. Współadministracja ma miejsce przede wszystkim w sytuacji, gdy **w określaniu celów i sposobów przetwarzania udział biorą co najmniej dwa podmioty**. Wspólny udział musi obejmować z jednej strony określenie celów, a z drugiej określenie sposobów przetwarzania. Jeżeli każdy z tych elementów jest określony przez wszystkie zainteresowane podmioty, należy je uznać za współadministratorów przedmiotowego przetwarzania.

3.2.2 Ocena wspólnego udziału

54. Wspólny udział w określaniu celów i sposobów przetwarzania oznacza, że więcej niż jeden podmiot ma decydujący wpływ na to, czy i w jaki sposób odbywa się przetwarzanie. W praktyce wspólny udział może przybierać różne formy. Na przykład wspólny udział może mieć formę **wspólnej decyzji** podjętej przez co najmniej dwa podmioty lub wynikać ze **zbieżnych decyzji** co najmniej dwóch podmiotów, dotyczących celów i istotnych sposobów przetwarzania.

55. Wspólny udział w formie *wspólnej decyzji* oznacza wspólne podejmowanie decyzji i wiąże się ze wspólnym zamiarem zgodnie z najbardziej powszechnym rozumieniem terminu „*wspólnie*", o którym mowa w art. 26 RODO.

Wspólny udział w formie *zbieżnych decyzji* wynika w szczególności z orzecznictwa TSUE dotyczącego pojęcia współadministratorów. Decyzje można uznać za zbieżne co do celów i sposobów przetwarzania, **jeżeli wzajemnie się uzupełniają i są niezbędne, aby zaistniało przetwarzanie, w taki sposób, że mają one wymierny wpływ na określenie celów i sposobów przetwarzania**. Należy podkreślić, że pojęcie zbieżnych decyzji należy rozpatrywać w odniesieniu do celów i sposobów przetwarzania, a nie innych aspektów stosunków handlowych między stronami[19]. Ważnym kryterium stwierdzenia zbieżnych decyzji w tym kontekście jest zatem to, **czy przetwarzanie nie byłoby możliwe bez udziału obu stron w ustalaniu celów i sposobów przetwarzania w tym sensie, że przetwarzanie przez każdą ze stron jest nierozłączne, tzn. ściśle związane.** Współadministratorów działających na podstawie zbieżnych decyzji należy jednak odróżnić od podmiotu przetwarzającego, ponieważ ten

[19] Wszystkie porozumienia handlowe wiążą się z podejmowaniem zbieżnych decyzji w ramach procesu, w którym dochodzi do porozumienia.

ostatni – uczestnicząc w przetwarzaniu – nie przetwarza danych do własnych celów, lecz przetwarza je w imieniu administratora.

56. Fakt, że jedna ze stron nie ma dostępu do przetwarzanych danych osobowych, nie wystarcza, aby wykluczyć współadministrację[20]. Na przykład w sprawie *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta* TSUE uznał, że należy uznać wspólnotę religijną wspólnie z jej członkami głosicielami za administratora danych osobowych w odniesieniu do przetwarzania danych osobowych dokonywanego przez tych członków głosicieli w ramach działalności kaznodziejskiej realizowanej przez odwiedzanie kolejnych gospodarstw domowych[21]. Trybunał uznał, że nie jest konieczne, by wspomniana wspólnota miała dostęp do danych, ani nie musi zostać ustalone, że udzielała ona swoim członkom pisemnych wytycznych lub instrukcji dotyczących tego przetwarzania[22]. Wspólnota uczestniczyła w określaniu celów i sposobów przetwarzania, organizując i koordynując działania swoich członków, co przyczyniło się do osiągnięcia celu wspólnoty świadków Jehowy[23]. Ponadto wspólnota miała ogólną wiedzę na temat tego, że takie przetwarzanie odbywa się dla celów propagowania jej wiary[24].

57. Należy również podkreślić, zgodnie z wyjaśnieniami TSUE, że podmiot będzie uznawany za współadministratora z innym(i) tylko w odniesieniu do tych operacji, dla których określa on, wspólnie z innymi, sposoby i cele tego samego przetwarzania danych, w szczególności w przypadku zbieżnych decyzji. Jeżeli jeden z tych podmiotów samodzielnie decyduje o celach i sposobach prowadzenia operacji, które następują wcześniej albo później w łańcuchu przetwarzania, podmiot ten musi być uznany za jedynego administratora tej wcześniejszej lub późniejszej operacji[25].

58. Istnienie wspólnej odpowiedzialności nie musi oznaczać równej odpowiedzialności różnych podmiotów zaangażowanych w przetwarzanie danych osobowych. Wręcz przeciwnie, TSUE wyjaśnił, że podmioty te mogą być zaangażowane na różnych etapach tego przetwarzania i w różnym stopniu, tak że poziom odpowiedzialności każdego z nich należy oceniać w odniesieniu do wszystkich istotnych okoliczności danego przypadku.

3.2.2.1 Wspólnie ustalone cele

59. Współadministracja istnieje wtedy, gdy podmioty uczestniczące w tym samym przetwarzaniu dokonują przetwarzania we wspólnie określonych celach. Ma to miejsce w przypadku, gdy zaangażowane podmioty przetwarzają dane w tych samych lub wspólnych celach.

60. Ponadto jeżeli podmioty nie mają tego samego celu przetwarzania danych, w świetle orzecznictwa TSUE współadministracja może również mieć miejsce, gdy zaangażowane podmioty realizują cele, które są ściśle ze sobą powiązane lub wzajemnie się uzupełniają. Może to mieć miejsce na przykład w przypadku wzajemnych korzyści wynikających z tej samej operacji przetwarzania, pod warunkiem że każdy z zaangażowanych podmiotów uczestniczy w określaniu celów i sposobów danej operacji

[20] Wyrok w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, pkt 38.
[21] Wyrok w sprawie C-25/17, *Tietosuojavaltuutettu przeciwko Jehovan todistajat – uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551, pkt 75.
[22] Tamże.
[23] Tamże, pkt 71.
[24] Tamże.
[25] Wyrok w sprawie C-40/17, *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV*, ECLI:EU:2018:1039, pkt 74 „Natomiast, bez uszczerbku dla ewentualnej odpowiedzialności cywilnej przewidzianej w tym względzie przez prawo krajowe, osoby fizycznej lub prawnej nie można uznać za administratora w rozumieniu tego przepisu w odniesieniu do wcześniejszych lub późniejszych operacji łańcucha przetwarzania, których celów ani środków ona nie określa."

przetwarzania. Pojęcie wzajemnych korzyści nie jest jednak rozstrzygające i może być jedynie wskazówką. Na przykład w sprawie *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV* TSUE wyjaśnił, że operator witryny internetowej uczestniczy w określaniu celów (i sposobów) przetwarzania danych, umieszczając w witrynie internetowej wtyczkę społecznościową, aby zoptymalizować reklamy swoich towarów poprzez uczynienie ich bardziej widocznymi w sieci społecznościowej. Trybunał uznał, że przedmiotowe operacje przetwarzania zostały przeprowadzone w interesie gospodarczym zarówno operatora witryny internetowej, jak i dostawcy wtyczki społecznościowej.[26]

61. Podobnie, jak zauważył TSUE w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, przetwarzanie danych osobowych poprzez statystyki odwiedzających fanpage ma w szczególności pozwolić Facebookowi na poprawę jego systemu reklam, jakie emituje on za pośrednictwem swego portalu, a administratorowi fanpage'a na uzyskanie statystyk do celów zarządzania promocją jego działalności[27]. Każdy podmiot w tym przypadku realizuje swój własny interes, ale obie strony uczestniczą w określaniu celów (i sposobów) przetwarzania danych osobowych w odniesieniu do osób odwiedzających fanpage'a[28].

62. W tym względzie należy podkreślić, że samo istnienie wzajemnych korzyści (np. handlowych) wynikających z działalności związanej z przetwarzaniem nie daje podstaw do sprawowania współadministracji. Jeżeli podmiot zaangażowany w przetwarzanie nie realizuje własnych celów w związku przetwarzaniem, a jedynie otrzymuje wynagrodzenie za świadczone usługi, działa raczej jako podmiot przetwarzający niż jako współadministrator.

3.2.2.2 Wspólnie ustalone sposoby przetwarzania

63. Współadministracja wymaga również, aby co najmniej dwa podmioty wywierały wpływ na sposoby przetwarzania. Nie oznacza to, że aby współadministracja istniała, każdy zaangażowany podmiot musi we wszystkich przypadkach określić wszystkie sposoby przetwarzania. Jak wyjaśnił TSUE, różne podmioty mogą być zaangażowane na różnych etapach tego przetwarzania i w różnym stopniu. Różni współadministratorzy mogą zatem w różnym stopniu określić sposoby przetwarzania, w zależności od tego, kto jest do tego faktycznie uprawniony.

64. Może się również zdarzyć, że jeden z zaangażowanych podmiotów zapewnia sposoby przetwarzania i udostępnia je innym podmiotom na potrzeby przetwarzania danych osobowych. Podmiot, który decyduje się stosować te sposoby w celu przetwarzania danych w określonym celu, również uczestniczy w określaniu sposobów przetwarzania.

65. O takim scenariuszu możemy mówić w przypadku platform, standardowych narzędzi lub innej infrastruktury umożliwiającej stronom przetwarzanie tych samych danych osobowych, które zostały utworzone w określony sposób przez jedną ze stron, aby mogły być wykorzystywane przez inne strony, które również mogą decydować o sposobie ich utworzenia[29]. Wykorzystanie już istniejącego systemu

[26] Wyrok w sprawie C-40/17,*Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV*, ECLI:EU:C:2018:1039, pkt 80.

[27] Wyrok w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, pkt 34.

[28] Wyrok w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, pkt 39.

[29] Dostawca systemu może być współadministratorem, jeżeli spełnione są kryteria wymienione powyżej, tj. jeżeli dostawca uczestniczy w określaniu celów i sposobów przetwarzania. W przeciwnym razie dostawcę należy uznać za podmiot przetwarzający.

technicznego nie wyklucza współadministracji, jeżeli użytkownicy systemu mogą decydować, aby dane osobowe były przetwarzane w tym kontekście.

66. Przykładem tego jest wyrok TSUE w sprawie *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, zgodnie z którym należy uznać, że administrator fanpage'a prowadzonego na Facebooku, określając parametry na podstawie grupy docelowej oraz cele zarządzania i promowania jego działalności, uczestniczy w określaniu sposobów przetwarzania danych osobowych osób odwiedzających jego fanpage'a.

67. Ponadto dokonany przez podmiot wybór wykorzystania do własnych celów narzędzia lub innego systemu opracowanego przez inny podmiot, umożliwiający przetwarzanie danych osobowych prawdopodobnie będzie równoznaczny ze wspólną decyzją w sprawie sposobów przetwarzania danych przez te podmioty. Wynika to ze sprawy *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV*, w której TSUE stwierdził, poprzez umieszczenie w swojej witrynie internetowej przycisku „Lubię to" Facebooka Fashion ID wpłynęła w decydujący sposób na gromadzenie i przekazywanie danych osobowych osób odwiedzających wspomnianą witrynę na rzecz Facebooka, a tym samym wspólnie z Facebookiem określiła sposoby tego przetwarzania[30].

68. Należy podkreślić, że **korzystanie ze wspólnego systemu lub wspólnej infrastruktury przetwarzania danych nie we wszystkich przypadkach prowadzi do zakwalifikowania zaangażowanych stron jako współadministratorów**, w szczególności gdy przetwarzanie jest rozłączne i mogłoby być przeprowadzone przez jedną stronę bez interwencji drugiej lub gdy dostawca jest podmiotem przetwarzającym ze względu na brak jakiegokolwiek własnego celu (istnienie zwykłej korzyści handlowej dla zaangażowanych stron nie jest wystarczające, by uznać je za cel przetwarzania).

Przykład: biuro podróży

Biuro podróży przesyła dane osobowe swoich klientów do linii lotniczych i sieci hoteli w celu rezerwacji pakietów turystycznych. Linia lotnicza i hotel potwierdzają dostępność potrzebnych miejsc i pokoi. Biuro podróży wystawia dokumenty i potwierdzenia dla swoich klientów. Każdy z podmiotów przetwarza dane w celu prowadzenia własnych działań i przy zastosowaniu własnych sposobów. W tym przypadku biuro podróży, linia lotnicza i hotel są trzema odrębnymi administratorami przetwarzającymi dane dla własnych i odrębnych celów i nie ma tu mowy o współadministracji.

Biuro podróży, sieć hoteli i linia lotnicza decydują się następnie wspólnie uczestniczyć w tworzeniu wspólnej platformy internetowej służącej wspólnemu świadczeniu usług turystycznych. Uzgadniają istotne sposoby przetwarzania danych, które będą stosowane, na przykład jakie dane będą przechowywane, w jaki sposób rezerwacja będzie przypisywana i zatwierdzana oraz kto może mieć dostęp do przechowywanych informacji. Postanawiają ponadto wymieniać się danymi swoich klientów w celu prowadzenia zintegrowanych działań marketingowych. W takim przypadku biuro podróży, linia lotnicza i sieć hoteli wspólnie ustalają, dlaczego i w jaki sposób przetwarzane są dane osobowe ich klientów, a zatem będą współadministratorami operacji przetwarzania dotyczących wspólnej internetowej platformy rezerwacji i wspólnych działań marketingowych. Każdy z podmiotów będzie jednak nadal sprawował wyłączną kontrolę nad innymi czynnościami przetwarzania, poza wspólną platformą internetową.

[30] Wyrok w sprawie C-40/17, *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV*, ECLI:EU:C:2018:1039, pkt 77-79.

Przykład: projekt badawczy realizowany przez instytuty

Kilka instytutów badawczych decyduje się na udział w określonym wspólnym projekcie badawczym i wykorzystanie w tym celu istniejącej platformy jednego z instytutów uczestniczących w projekcie. Każdy instytut wprowadza do platformy dane osobowe, które już posiada, do celów wspólnych badań i wykorzystuje dane dostarczone przez innych za pośrednictwem platformy do badań. W tym przypadku wszystkie instytuty kwalifikują się jako współadministratorzy przetwarzania danych osobowych w formie przechowywania i ujawniania informacji z tej platformy, ponieważ wspólnie zdecydowały o celu przetwarzania i sposobach przetwarzania (istniejąca platforma). Każdy z instytutów jest jednak odrębnym administratorem danych w odniesieniu do wszelkich innych operacji przetwarzania, które mogą być dokonywane poza platformą do ich własnych celów.

Przykład: działanie marketingowe

Przedsiębiorstwa A i B wprowadziły na rynek produkt pod wspólną marką C i chcą zorganizować imprezę promującą ten produkt. W tym celu decydują się na udostępnienie danych ze swoich baz klientów i potencjalnych klientów i na tej podstawie ustalają listę osób zaproszonych na wydarzenie. Uzgadniają również zasady wysyłania zaproszeń na wydarzenie, sposób zbierania informacji zwrotnych podczas wydarzenia oraz dalsze działania marketingowe. Przedsiębiorstwa A i B można uznać za współadministratorów przetwarzania danych osobowych związanych z organizacją imprezy promocyjnej, ponieważ wspólnie decydują o wspólnie określonym celu i podstawowych sposobach przetwarzania danych w tym kontekście.

Przykład: badania kliniczne[31]

Świadczeniodawca opieki zdrowotnej (prowadzący badanie) i uniwersytet (sponsor) decydują się na wspólne rozpoczęcie badania klinicznego w tym samym celu. Współpracują ze sobą przy sporządzaniu protokołu badania (tj. cel, metodologia/projekt badania, dane, które należy zgromadzić, kryteria wykluczenia/włączenia, ponowne wykorzystanie bazy danych (w stosownych przypadkach) itd.). Można ich uznać za współadministratorów w odniesieniu do tego badania klinicznego, ponieważ wspólnie określają i uzgadniają ten sam cel i istotne sposoby przetwarzania danych. Gromadzenie danych osobowych z dokumentacji medycznej pacjenta do celów badawczych należy odróżnić od przechowywania i wykorzystywania tych samych danych do celów opieki nad pacjentem, w przypadku których świadczeniodawca opieki zdrowotnej pozostaje administratorem.

W przypadku gdy prowadzący badanie nie bierze udziału w sporządzaniu protokołu (akceptuje jedynie protokół już opracowany przez sponsora), a protokół jest opracowany wyłącznie przez sponsora, prowadzącego badanie należy uznać za podmiot przetwarzający, a sponsora za administratora tego badania klinicznego.

Przykład: rekruterzy

Przedsiębiorstwo X pomaga przedsiębiorstwu Y w rekrutacji nowych pracowników za pomocą swojej słynnej usługi dodanej „global matchz". Przedsiębiorstwo X poszukuje odpowiednich kandydatów zarówno wśród CV otrzymanych bezpośrednio od przedsiębiorstwa Y, jak i tych, które posiada już we własnej bazie danych. Tę bazę dany tworzy we własnym zakresie przedsiębiorstwo X i samo nią

[31] EROD planuje przedstawić dalsze wytyczne dotyczące badań klinicznych w kontekście przyszłych wytycznych w sprawie przetwarzania danych osobowych do celów badań medycznych i naukowych.

zarządza. Dzięki temu przedsiębiorstwo X zwiększa dopasowanie między ofertami pracy a osobami poszukującymi pracy, a tym samym zwiększa swoje obroty. Nawet jeśli formalnie nie podjęły one wspólnej decyzji, przedsiębiorstwa X i Y wspólnie uczestniczą w przetwarzaniu danych w celu znalezienia odpowiednich kandydatów w oparciu o zbieżne decyzje: decyzję o stworzeniu usługi „global matchz" i zarządzaniu nią dla przedsiębiorstwa X oraz decyzję przedsiębiorstwa Y o wzbogaceniu bazy danych o CV, które otrzymuje bezpośrednio. Decyzje te wzajemnie się uzupełniają, są nierozłączne i niezbędne do znalezienia odpowiednich kandydatów. Dlatego w tym konkretnym przypadku należy uznać te podmioty za współadministratorów takiego przetwarzania. Przedsiębiorstwo X jest jednak wyłącznym administratorem przetwarzania niezbędnego do zarządzania bazą danych, a firma Y jest wyłącznym administratorem późniejszego przetwarzania danych dotyczących zatrudniania dla własnych celów (organizacja rozmów kwalifikacyjnych, zawarcie umowy i zarządzanie danymi kadrowymi).

Przykład: analiza danych dotyczących zdrowia

Przedsiębiorstwo ABC, twórca aplikacji do monitorowania ciśnienia krwi, oraz Przedsiębiorstwo XYZ, dostawca aplikacji dla pracowników służby zdrowia, chcą zbadać, w jaki sposób zmiany ciśnienia krwi mogą pomóc w przewidywaniu niektórych chorób. Przedsiębiorstwa postanawiają stworzyć wspólny projekt i dotrzeć do Szpitala DEF, aby go również zaangażować.

Dane osobowe, które będą przetwarzane w tym projekcie, składają się z danych osobowych, które Przedsiębiorstwo ABC, Szpital DEF i Przedsiębiorstwo XYZ przetwarzają oddzielnie jako indywidualni administratorzy. Decyzję o przetwarzaniu tych danych w celu oceny zmian ciśnienia krwi podejmują wspólnie trzy podmioty. Przedsiębiorstwo ABC, Szpital DEF i Przedsiębiorstwo XYZ wspólnie określiły cele przetwarzania danych. Przedsiębiorstwo XYZ proponuje istotne sposoby przetwarzania. Zarówno Przedsiębiorstwo ABC jak i Szpital DEF akceptują te istotne sposoby przetwarzania po tym, jak zostali włączeni w opracowanie niektórych funkcji aplikacji, tak aby mogli w odpowiedni sposób wykorzystywać wyniki. Te trzy organizacje zgadzają się więc co do wspólnego celu przetwarzania danych, jakim jest ocena, w jaki sposób zmiany ciśnienia krwi mogą pomóc w przewidywaniu niektórych chorób. Po zakończeniu badań Przedsiębiorstwo ABC, Szpital DEF i Przedsiębiorstwo XYZ mogą skorzystać z oceny, wykorzystując jej wyniki we własnej działalności. Z tych powodów organizacje te są współadministratorami tego konkretnego wspólnego przetwarzania danych.

Gdyby Przedsiębiorstwo XYZ zostało po prostu poproszone przez pozostałe organizacje o dokonanie tej oceny bez żadnego własnego celu i jedynie przetwarzało dane w imieniu innych, Przedsiębiorstwo XYZ byłoby podmiotem przetwarzającym, nawet gdyby powierzono mu określenie sposobów przetwarzania innych niż istotne.

3.2.3 Sytuacje, w których nie występuje współadministracja

69. Fakt, że w to samo przetwarzanie zaangażowanych jest kilka podmiotów, nie oznacza, że muszą one działać jako współadministratorzy takiego przetwarzania. Nie wszystkie rodzaje partnerstw, współpracy lub współdziałania oznaczają zakwalifikowanie do kategorii współadministratorów, ponieważ taka kwalifikacja wymaga indywidualnej analizy każdego przedmiotowego przetwarzania oraz dokładnej roli każdego podmiotu w odniesieniu do każdego przetwarzania. Poniższe przypadki stanowią niewyczerpujące przykłady sytuacji, w których nie występuje współadministracja.

70. Na przykład wymianę tych samych danych lub zbioru danych między dwoma podmiotami bez wspólnie określonych celów lub wspólnie określonych sposobów przetwarzania należy uznać za przekazywanie danych między odrębnymi administratorami.

Przykład: przekazywanie danych o pracownikach organom podatkowym

Przedsiębiorstwo gromadzi i przetwarza dane osobowe swoich pracowników w celu zarządzania płacami, ubezpieczeniami zdrowotnymi itd. Prawo nakłada na przedsiębiorstwo obowiązek przesyłania organom podatkowym wszystkich danych dotyczących wynagrodzeń w celu wzmocnienia kontroli podatkowej.

W tym przypadku, chociaż zarówno przedsiębiorstwo, jak i organy podatkowe, przetwarzają te same dane dotyczące wynagrodzeń, brak wspólnego celu lub sposobów przetwarzania tych danych spowoduje zakwalifikowanie tych dwóch podmiotów jako dwóch odrębnych administratorów.

71. Współadministrację można również wykluczyć w sytuacji, gdy kilka podmiotów korzysta ze wspólnej bazy danych lub wspólnej infrastruktury, jeżeli każdy podmiot niezależnie określa swoje własne cele.

Przykład: działania marketingowe w grupie przedsiębiorstw korzystających ze wspólnej bazy danych

Grupa przedsiębiorstw korzysta z tej samej bazy danych do zarządzania klientami i potencjalnymi klientami. Taka baza danych jest umieszczona na serwerach spółki dominującej, która w związku z tym jest podmiotem przetwarzającym dane przedsiębiorstw w odniesieniu do przechowywania danych. Każdy podmiot grupy wprowadza dane swoich klientów i potencjalnych klientów oraz przetwarza je wyłącznie do własnych celów. Ponadto każdy podmiot samodzielnie decyduje o dostępie, okresach przechowywania, poprawianiu lub usuwaniu danych swoich klientów i potencjalnych klientów. Nie mają one dostępu do danych innych podmiotów ani nie mogą z nich korzystać. Sam fakt, że przedsiębiorstwa te korzystają ze wspólnej bazy danych grupy, nie oznacza jeszcze, że są one współadministratorami. W tych okolicznościach każde przedsiębiorstwo jest zatem odrębnym administratorem.

Przykład: niezależni administratorzy korzystający ze wspólnej infrastruktury

Przedsiębiorstwo XYZ prowadzi bazę danych i udostępnia ją innym przedsiębiorstwom w celu przetwarzania i przechowywania danych osobowych o ich pracownikach. Przedsiębiorstwo XYZ jest podmiotem przetwarzającym dane w odniesieniu do przetwarzania i przechowywania danych o pracownikach innych przedsiębiorstw, ponieważ operacje te są wykonywane w imieniu tych innych przedsiębiorstw i zgodnie z ich instrukcjami. Ponadto inne przedsiębiorstwa przetwarzają dane bez żadnego udziału Przedsiębiorstwa XYZ i w celach, które w żaden sposób nie są tożsame z celami Przedsiębiorstwa XYZ.

72. Mogą również zaistnieć sytuacje, w których różne podmioty przetwarzają kolejno te same dane osobowe w łańcuchu operacji, przy czym każdy z tych podmiotów ma niezależny cel i niezależne sposoby przetwarzania w swojej części łańcucha. W przypadku braku wspólnego udziału w określaniu celów i sposobów dla tej samej operacji lub zestawu operacji przetwarzania, należy wykluczyć współadministrację, a poszczególne podmioty należy uznać za kolejnych niezależnych administratorów.

Przykład: analiza statystyczna na potrzeby zadania realizowanego w interesie publicznym

Zadaniem organu publicznego (Organu A) jest sporządzanie odpowiednich analiz i statystyk dotyczących zmian wskaźnika zatrudnienia w danym kraju. Wiele innych podmiotów publicznych jest prawnie zobowiązanych do ujawnienia określonych danych Organowi A, aby mógł zrealizować to zadanie. Organ A decyduje się na wykorzystanie określonego systemu do przetwarzania danych, w tym ich gromadzenia. Oznacza to również, że pozostałe jednostki są zobowiązane do korzystania z tego

systemu do udostępniania swoich danych. W tym przypadku, bez uszczerbku dla jakiegokolwiek podziału ról wynikającego z prawa, Organ A będzie jedynym administratorem przetwarzania danych do celów analizy i statystyki wskaźnika zatrudnienia przetwarzanych w systemie, ponieważ to Organ A określa cel przetwarzania danych i zdecydował o sposobie przetwarzania. Oczywiście pozostałe podmioty publiczne, jako administratorzy ich własnych działań związanych z przetwarzaniem, są odpowiedzialne za zapewnienie dokładności danych, które wcześniej przetwarzały, a które następnie ujawniają Organowi A.

4 DEFINICJA PODMIOTU PRZETWARZAJĄCEGO

73. Podmiot przetwarzający, zgodnie z art. 4 ust. 8, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Podobnie jak definicja administratora, definicja podmiotu przetwarzającego przewiduje szeroki krąg podmiotów, podmiotem przetwarzającym może być „*osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot*". Oznacza to, że w zasadzie nie ma ograniczeń co do tego, który rodzaj podmiotu może pełnić rolę podmiotu przetwarzającego. Może to być organizacja, ale może to być również osoba fizyczna.

74. W RODO określono obowiązki mające bezpośrednie zastosowanie do podmiotów przetwarzających, które są szczegółowo opisane w sekcji 1 części II niniejszych wytycznych. Podmiot przetwarzający może zostać pociągnięty do odpowiedzialności lub ukarany grzywną w przypadku niedopełnienia takich obowiązków lub w przypadku działania poza zgodnymi z prawem instrukcjami administratora lub wbrew nim.

75. W przetwarzaniu danych osobowych może uczestniczyć wiele podmiotów przetwarzających. Na przykład, administrator może sam zdecydować się na bezpośrednie zaangażowanie wielu podmiotów przetwarzających, angażując różne podmioty przetwarzające na odrębnych etapach przetwarzania (wiele podmiotów przetwarzających). Administrator może również zdecydować się na zaangażowanie jednego podmiotu przetwarzającego, który z kolei – za zgodą administratora – angażuje jeden podmiot przetwarzający lub większą liczbę takich podmiotów („podwykonawcy przetwarzania"). Czynności przetwarzania powierzone podmiotowi przetwarzającemu mogą ograniczać się do ściśle określonego zadania lub kontekstu bądź mogą być określone w sposób bardziej ogólny i szeroki.

76. Dwa podstawowe warunki zakwalifikowania podmiotu jako podmiotu przetwarzającego to:

    a) pełnienie roli *odrębnego podmiotu* w stosunku do administratora; oraz

    b) przetwarzanie danych osobowych *w imieniu administratora*.

77. *Odrębny podmiot* oznacza, że administrator decyduje się na przekazanie całości lub części czynności przetwarzania organizacji zewnętrznej. W ramach grupy przedsiębiorstw jedno przedsiębiorstwo może być podmiotem przetwarzającym innego przedsiębiorstwa działającego jako administrator, ponieważ oba przedsiębiorstwa są odrębnymi podmiotami. Z drugiej strony, dział w przedsiębiorstwie nie może być podmiotem przetwarzającym dla innego działu tego samego podmiotu.

78. Jeżeli administrator postanawia przetwarzać dane samodzielnie, korzystając z własnych zasobów w ramach swojej organizacji, na przykład za pośrednictwem własnego personelu, nie jest to sytuacja, w której występuje podmiot przetwarzający. Pracowników i innych osób, które działają pod bezpośrednim zwierzchnictwem administratora, takich jak pracownicy zatrudnieni na czas określony,

nie należy uznawać za podmioty przetwarzające, ponieważ przetwarzają oni dane osobowe w ramach podmiotu administratora. Zgodnie z art. 29 są oni również związani instrukcjami administratora.

79. *Przetwarzanie danych osobowych w imieniu administratora* wymaga przede wszystkim, aby odrębny podmiot przetwarzał dane osobowe na rzecz administratora. W art. 4 ust. 2 przetwarzanie definiuje się jako pojęcie obejmujące szeroki zakres operacji, począwszy od gromadzenia, przechowywania i przeglądania, a skończywszy na wykorzystaniu, rozpowszechnianiu lub udostępnianiu w inny sposób i niszczeniu. Pojęcie „przetwarzania" opisano bardziej szczegółowo w pkt 2.1.5.

80. Po drugie, przetwarzanie musi odbywać się w imieniu administratora, ale poza jego bezpośrednim zwierzchnictwem lub kontrolą. Działanie „w czyimś imieniu" oznacza działanie w interesie innego podmiotu i przypomina pojęcie prawne „przekazania uprawnień". W przepisach dotyczących ochrony danych wzywa się podmiot przetwarzający dane do wykonania instrukcji wydanych przez administratora, przynajmniej w odniesieniu do celu przetwarzania oraz istotnych elementów sposobu przetwarzania. Legalność przetwarzania danych zgodnie z art. 6, a w stosownych przypadkach art. 9 rozporządzenia, wynika z działalności administratora danych, a podmiot przetwarzający nie może przetwarzać danych inaczej niż zgodnie z instrukcjami administratora. Mimo to, jak opisano powyżej, możliwe jest pozostawienie w ramach tych instrukcji pewnej swobody co do tego, jak najlepiej służyć interesom administratora i umożliwienie podmiotowi przetwarzającemu wybór najodpowiedniejszych środków technicznych i organizacyjnych[32].

81. Działanie „w czyimś imieniu" oznacza również, że podmiot przetwarzający nie może przetwarzać danych dla własnych celów. Zgodnie z art. 28 ust. 10, jeśli podmiot przetwarzający wykracza poza instrukcje administratora i zaczyna określać własne cele i środki przetwarzania, dopuszcza się naruszenia przepisów RODO. W takiej sytuacji podmiot przetwarzający zostaje uznany za administratora w odniesieniu do tego przetwarzania i może podlegać sankcjom z tytułu wykroczenia poza instrukcje administratora.

Przykład: przedsiębiorstwo nazywane podmiotem przetwarzającym, ale działające jak administrator

Dostawca usług MarketinZ świadczy usługi reklamowe i marketingu bezpośredniego na rzecz różnych przedsiębiorstw. Przedsiębiorstwo GoodProductZ zawiera umowę z MarketinZ, zgodnie z którą przedsiębiorstwo MarketinZ świadczy usługi reklamy handlowej dla klientów GoodProductZ i jest określane jako podmiot przetwarzający dane. MarketinZ postanawia jednak korzystać z bazy danych klientów GoodProducts również do celów innych niż reklama GoodProducts, takich jak rozwijanie własnej działalności gospodarczej. Decyzja o dodaniu dodatkowego celu do celu, w którym dane osobowe zostały przekazane, przekształca MarketinZ w administratora zestawu operacji przetwarzania, a ich przetwarzanie w tym celu stanowiłoby naruszenie RODO.

82. Europejska Rada Ochrony Danych przypomina, że nie każdy dostawca usług, który przetwarza dane osobowe w trakcie świadczenia usługi, jest „podmiotem przetwarzającym" w rozumieniu RODO. Rola podmiotu przetwarzającego nie wynika z charakteru podmiotu, który przetwarza dane, lecz z jego konkretnych działań w określonym kontekście. Innymi słowy, ten sam podmiot może działać jednocześnie jako administrator w przypadku niektórych operacji przetwarzania danych oraz jako przetwarzający w przypadku innych tego rodzaju operacji, a to, czy kwalifikuje się go jako administratora czy podmiot przetwarzający należy oceniać w odniesieniu do konkretnych zestawów danych lub operacji. Charakter usługi będzie decydował o tym, czy czynność przetwarzania jest równoznaczna z przetwarzaniem danych osobowych w imieniu administratora w rozumieniu RODO. W

[32] Zobacz część I, pkt 2.1.4 opisujący rozróżnienie między istotnymi sposobami przetwarzania a sposobami przetwarzania innymi niż istotne.

praktyce, jeżeli świadczona usługa nie jest konkretnie ukierunkowana na przetwarzanie danych osobowych lub jeżeli takie przetwarzanie nie stanowi kluczowego elementu usługi, dostawca usług może być w stanie niezależnie określić cele i sposoby takiego przetwarzania, które są wymagane do świadczenia tej usługi. W takiej sytuacji dostawca usług powinien być postrzegany jako odrębny administrator, a nie jako podmiot przetwarzający[33]. Aby ustalić stopień wpływu, jaki każdy podmiot faktycznie ma na określanie celów i sposobów przetwarzania, konieczna jest jednak analiza poszczególnych przypadków.

Przykład: usługi taxi

Korporacja taxi oferuje platformę internetową, która umożliwia przedsiębiorstwom zarezerwowanie taksówki do przewozu pracowników lub gości na lotnisko i z lotniska. Podczas rezerwacji taksówki przedsiębiorstwo ABC podaje imię i nazwisko pracownika, który powinien zostać odebrany z lotniska, tak aby kierowca mógł potwierdzić tożsamość pracownika w momencie odbioru. W tym przypadku korporacja taxi przetwarza dane osobowe pracownika w ramach obsługi Przedsiębiorstwa ABC, ale przetwarzanie jako takie nie jest celem usługi. Korporacja taxi zaprojektowała internetową platformę rezerwacji online w ramach rozwijania własnej działalności gospodarczej polegającej na świadczeniu usług przewozowych, bez żadnych instrukcji ze strony Przedsiębiorstwa ABC. Korporacja taxi również samodzielnie określa kategorie danych, które gromadzi i to, jak długo je przechowuje. Korporacja taxi działa zatem jako administrator we własnym imieniu, niezależnie od faktu, że przetwarzanie danych odbywa się na podstawie zapytania o usługę złożonego przez Przedsiębiorstwo ABC.

83. Europejska Rada Ochrony Danych zauważa, że dostawca usług może nadal działać jako podmiot przetwarzający, nawet jeśli przetwarzanie danych osobowych nie jest głównym lub podstawowym przedmiotem usługi, pod warunkiem że klient usługi nadal w praktyce określa cele i sposoby przetwarzania. Przy podejmowaniu decyzji o ewentualnym powierzeniu przetwarzania danych osobowych określonemu dostawcy usług administratorzy powinni dokładnie ocenić, czy dany dostawca usług umożliwia im sprawowanie wystarczającego stopnia kontroli, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania, a także potencjalne zagrożenia dla osób, których dane dotyczą.

Przykład: call center

Przedsiębiorstwo X zleca obsługę klienta Przedsiębiorstwu Y, które udostępnia call center, aby odpowiadać na pytania klientów Przedsiębiorstwa X. Aby świadczyć usługę wsparcia klienta, Przedsiębiorstwo Y musi mieć dostęp do baz danych klienta Przedsiębiorstwa X. Przedsiębiorstwo Y może uzyskać dostęp do danych wyłącznie w celu zapewnienia wsparcia, które zamówiło Przedsiębiorstwo X, i nie może przetwarzać danych w celach innych niż określone przez Przedsiębiorstwo X. Przedsiębiorstwo Y należy postrzegać jako podmiot przetwarzający dane osobowe, a pomiędzy Przedsiębiorstwem X i Y musi zostać zawarta umowa dotycząca przetwarzania danych.

Przykład: ogólne wsparcie IT

Przedsiębiorstwo Z zatrudnia dostawcę usług informatycznych, aby zapewnić ogólne wsparcie dla swoich systemów informatycznych, które zawierają ogromną ilość danych osobowych. Dostęp do danych osobowych nie jest głównym przedmiotem usługi wsparcia, ale jest nieuniknione, że dostawca

[33] Zobacz również motyw 81 RODO, w którym mowa o „powierzaniu podmiotowi przetwarzającemu czynności przetwarzania", co wskazuje, że czynność przetwarzania jako taka stanowi istotny element decyzji administratora o zwróceniu się do podmiotu przetwarzającego o przetwarzanie danych osobowych w jego imieniu.

usług IT ma systematyczny dostęp do danych osobowych podczas świadczenia usługi. Przedsiębiorstwo Z stwierdza zatem, że dostawcę usług IT – będącego odrębnym przedsiębiorstwem i nieuchronnie zobowiązanego do przetwarzania danych osobowych, nawet jeśli nie jest to głównym celem usługi – należy uznać za podmiot przetwarzający. W związku z tym z dostawcą usług IT zawarta zostaje umowa dotycząca przetwarzania danych.

Przykład: konsultant IT usuwający błąd w oprogramowaniu

Przedsiębiorstwo ABC zatrudnia informatyka z innego przedsiębiorstwa w celu usunięcia błędu w oprogramowaniu, które jest wykorzystywane przez to przedsiębiorstwo. Konsultant IT nie jest zatrudniony do przetwarzania danych osobowych, a Przedsiębiorstwo ABC stwierdza, że jakikolwiek dostęp do danych osobowych będzie czysto incydentalny, a więc w praktyce bardzo ograniczony. ABC stwierdza zatem, że specjalista IT nie jest podmiotem przetwarzającym (ani samodzielnym administratorem) i że przedsiębiorstwo ABC podejmie odpowiednie środki zgodnie z art. 32 RODO w celu uniemożliwienia konsultantowi IT przetwarzania danych osobowych w sposób nieuprawniony.

84. Jak stwierdzono powyżej, nic nie stoi na przeszkodzie, aby podmiot przetwarzający oferował wstępnie określoną usługę, ale administrator musi podjąć ostateczną decyzję o aktywnym zatwierdzeniu sposobu przetwarzania, przynajmniej w zakresie dotyczącym istotnych sposobów przetwarzania. Podmiot przetwarzający dysponuje marginesem swobody w odniesieniu do sposobów przetwarzaniach innych niż istotne, zob. pkt 2.1.4. powyżej.

Przykład: dostawca usług w chmurze

Gmina postanowiła skorzystać z usług dostawcy usług w chmurze w celu przetwarzania informacji w swoich szkołach i placówkach oświatowych. Usługa w chmurze zapewnia usługi przesyłania wiadomości, wideokonferencje, przechowywanie dokumentów, zarządzanie kalendarzem, przetwarzanie tekstów itd. i będzie obejmować przetwarzanie danych osobowych uczniów i nauczycieli. Dostawca usług w chmurze oferuje standardową usługę oferowaną na całym świecie. Gmina musi jednak upewnić się, że obowiązująca umowa jest zgodna z art. 28 ust. 3 RODO, aby dane osobowe, których jest administratorem, były przetwarzane wyłącznie do celów gminy. Musi również upewnić się, że dostawca usług w chmurze przestrzega szczegółowych instrukcji dotyczących okresów przechowywania, usuwania danych itd., niezależnie od tego, co zazwyczaj oferuje standardowa usługa.

5 DEFINICJA STRONY TRZECIEJ/ODBIORCY

85. W rozporządzeniu zdefiniowano nie tylko pojęcia administratora i podmiotu przetwarzającego, ale także odbiorcy i strony trzeciej. W przeciwieństwie do pojęć administratora i podmiotu przetwarzającego, rozporządzenie nie określa szczególnych obowiązków ani zakresu odpowiedzialności odbiorców i stron trzecich. Można je uznać za pojęcia względne w tym znaczeniu, że opisują one relacje między administratorem lub podmiotem przetwarzającym z określonej perspektywy, np. administrator lub podmiot przetwarzający ujawnia dane odbiorcy. Odbiorca danych osobowych i strona trzecia mogą być jednocześnie uznawani za administratora lub podmiot przetwarzający z innych perspektyw. Na przykład podmioty, które z jednej perspektywy należy postrzegać jako odbiorców lub strony trzecie, są administratorami przetwarzania, dla którego określają cel i sposoby przetwarzania.

Strona trzecia

86. Artykuł 4 ust. 10 definiuje „*stronę trzecią*" jako osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż

- osoba, której dane dotyczą,
- administrator,
- podmiot przetwarzający i
- osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

87. Definicja zasadniczo odpowiada poprzedniej definicji „*strony trzeciej*" zawartej w dyrektywie 95/46/WE.

88. Podczas gdy pojęcia „*dane osobowe*", „*osoba, której dane dotyczą*", „*administrator*" i „*podmiot przetwarzający*" zostały zdefiniowane w rozporządzeniu, pojęcie „*osób, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe*" nie zostało zdefiniowane. Jest ono jednak ogólnie rozumiane jako odnoszące się do osób, które należą do podmiotu prawnego administratora lub podmiotu przetwarzającego (pracownik lub funkcja w dużym stopniu porównywalna do roli pracownika, np. personel tymczasowy zapewniany przez agencję pracy tymczasowej), ale tylko w zakresie, w jakim są one upoważnione do przetwarzania danych osobowych. Pracownik itd., który uzyskuje dostęp do danych, do których nie jest upoważniony, oraz w celach innych niż cele pracodawcy, nie należy do tej kategorii. Pracownik ten powinien być traktowany jako strona trzecia w stosunku do przetwarzania przez pracodawcę. Jeżeli pracownik przetwarza dane osobowe dla własnych celów, innych niż cele swojego pracodawcy, będzie on uważany za administratora i przejmie wszystkie wynikające z tego konsekwencje i odpowiedzialność w zakresie przetwarzania danych osobowych[34].

89. Strona trzecia odnosi się zatem do kogoś, kto w danej sytuacji nie jest osobą, której dane dotyczą, administratorem, podmiotem przetwarzającym ani pracownikiem. Administrator może na przykład zatrudnić podmiot przetwarzający i polecić mu przekazanie danych osobowych stronie trzeciej. Ta strona trzecia będzie wówczas uznawana za samodzielnego administratora przetwarzania, które prowadzi dla własnych celów. Należy zauważyć, że w ramach grupy przedsiębiorstw stroną trzecią jest przedsiębiorstwo inne niż administrator lub podmiot przetwarzający, mimo że należy ono do tej samej grupy co przedsiębiorstwo, które działa jako administrator lub podmiot przetwarzający.

Przykład: Usługi sprzątania

Przedsiębiorstwo A zawiera umowę z przedsiębiorstwem świadczącym usługi sprzątania, aby sprzątało ich biura. Osoby sprzątające nie powinny mieć dostępu do danych osobowych ani w inny sposób przetwarzać tych danych. Nawet jeśli mogą oni sporadycznie natknąć się na takie dane podczas poruszania się po biurze, mogą wykonywać swoje zadania bez dostępu do danych i mają umowny zakaz dostępu do danych osobowych lub przetwarzania w inny sposób danych osobowych, które Przedsiębiorstwo A przechowuje jako administrator. Osoby sprzątające nie są zatrudnione przez Przedsiębiorstwo A ani nie są postrzegane jako podlegające bezpośrednio temu przedsiębiorstwu. Przedsiębiorstwo nie ma zamiaru angażować przedsiębiorstwa świadczącego usługi sprzątania ani jego pracowników w przetwarzanie danych osobowych w imieniu Przedsiębiorstwa A. Przedsiębiorstwo

[34] Pracodawca (jako pierwotny administrator) mógłby jednak ponosić pewną odpowiedzialność w przypadku, gdy nowe przetwarzanie danych miało miejsce na skutek braku odpowiednich środków bezpieczeństwa.

świadczące usługi sprzątania i jego pracownicy powinni być zatem postrzegani jako strona trzecia, a administrator musi upewnić się, że istnieją odpowiednie środki bezpieczeństwa uniemożliwiające im dostęp do danych i wprowadzić obowiązek zachowania poufności w przypadku przypadkowego ujawnienia danych osobowych.

Przykład: grupy przedsiębiorstw – spółka dominująca i jednostki zależne

Przedsiębiorstwa X i Y wchodzą w skład grupy Z. Przedsiębiorstwa X i Y przetwarzają dane dotyczące ich pracowników do celów zarządzania pracownikami. W pewnym momencie spółka dominująca ZZ decyduje się zażądać danych dotyczących pracowników od wszystkich jednostek zależnych w celu opracowania statystyk obejmujących całą grupę. Podczas przekazywania danych z przedsiębiorstw X i Y do ZZ, to ostatnie należy traktować jako stronę trzecią, niezależnie od faktu, że wszystkie przedsiębiorstwa są częścią tej samej grupy. Przedsiębiorstwo ZZ będzie administratorem danych przetwarzanych do celów statystycznych.

Odbiorca

90. Zgodnie z art. 4 ust. 9 „*odbiorca*" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Nie należy jednak uznawać organów publicznych za odbiorców w sytuacji, gdy otrzymują one dane osobowe w ramach konkretnego dochodzenia zgodnie z prawem Unii lub prawem państwa członkowskiego (np. organy podatkowe i celne, jednostki prowadzące dochodzenia finansowe itd.)[35].

91. Definicja zasadniczo odpowiada poprzedniej definicji „*odbiorcy*" zawartej w dyrektywie 95/46/WE.

92. Definicja ta obejmuje każdego, kto otrzymuje dane osobowe, niezależnie od tego, czy jest on stroną trzecią, czy nie. Na przykład, gdy administrator danych przesyła dane osobowe innemu podmiotowi – podmiotowi przetwarzającemu lub stronie trzeciej – podmiot ten jest odbiorcą. Odbiorcę będącego stroną trzecią uważa się za administratora każdego przetwarzania, którego dokonuje dla własnych celów po otrzymaniu danych.

Przykład: ujawnianie danych między przedsiębiorstwami

Biuro podróży ExploreMore organizuje podróże na życzenie swoich klientów indywidualnych. W ramach tej usługi przesyłają dane osobowe klientów liniom lotniczym, hotelom i organizatorom wycieczek, aby te mogły realizować swoje usługi. ExploreMore, hotele, linie lotnicze i organizatorzy wycieczek są postrzegani jako administratorzy przetwarzania, którego dokonują w ramach swoich odpowiednich usług. Nie istnieje relacja między administratorem a podmiotem przetwarzającym. Linie lotnicze, hotele i organizatorzy wycieczek powinni być jednak postrzegani jako odbiorcy w momencie otrzymywania danych osobowych od ExploreMore.

[35] Zobacz również motyw 31 RODO.

CZĘŚĆ II – KONSEKWENCJE PRZYPISANIA RÓŻNYCH RÓL

1 RELACJA MIĘDZY ADMINISTRATOREM A PODMIOTEM PRZETWARZAJĄCYM

93. Wyraźną nowością w RODO są przepisy, które nakładają obowiązki bezpośrednio na podmioty przetwarzające. Na przykład podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy (art. 28 ust. 3); podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania (art. 30 ust. 2) oraz wdraża odpowiednie środki techniczne i organizacyjne (art. 32). Podmiot przetwarzający musi również wyznaczyć inspektora ochrony danych w określonych warunkach (art. 37) i ma obowiązek zawiadomić administratora bez zbędnej zwłoki po uzyskaniu informacji o naruszeniu ochrony danych osobowych (art. 33 ust. 2). Ponadto przepisy dotyczące przekazywania danych do państw trzecich (rozdział V) mają zastosowanie zarówno do podmiotów przetwarzających, jak i do administratorów. W tym względzie EROD uważa, że art. 28 ust. 3 RODO, choć określa treść niezbędnej umowy między administratorem a podmiotem przetwarzającym, nakłada na podmioty przetwarzające bezpośrednie obowiązki, w tym obowiązek wspomagania administratora w zapewnianiu zgodności[36].

1.1 Wybór podmiotu przetwarzającego

94. Administrator **korzysta „wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych", by przetwarzanie spełniało wymogi RODO – w tym w zakresie bezpieczeństwa przetwarzania – i zapewniało ochronę praw osób, których dane dotyczą[37]. Administrator jest zatem odpowiedzialny za ocenę adekwatności gwarancji udzielonych przez podmiot przetwarzający i powinien być w stanie udowodnić, że poważnie wziął pod uwagę wszystkie elementy przewidziane w RODO.

95. Gwarancje „zapewniane" 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. Często będzie to wymagało wymiany odpowiedniej dokumentacji (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).

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.

[36] Na przykład w razie potrzeby i na żądanie podmiot przetwarzający powinien pomagać administratorowi w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków dla ochrony danych (motyw 95 RODO). Należy to zawrzeć w umowie między administratorem a podmiotem przetwarzającym zgodnie z art. 28 ust. 3 lit. f) RODO.

[37] Artykuł 28 ust. 1 i motyw 81 RODO.

97. Administrator powinien wziąć pod uwagę następujące elementy[38], aby ocenić, czy gwarancje są wystarczające: **wiedza fachowa** (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych); **wiarygodność** podmiotu przetwarzającego; **zasoby** podmiotu przetwarzającego. Reputacja podmiotu przetwarzającego na rynku może być również istotnym czynnikiem, który administratorzy powinni wziąć pod uwagę.

98. Ponadto jako element umożliwiający wykazanie wystarczających gwarancji można wykorzystać przestrzeganie zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji[39]. Podmioty przetwarzające dane powinny zatem informować administratora o tej okoliczności, jak również o wszelkich zmianach w tym zakresie.

99. Obowiązek korzystania wyłącznie z usług podmiotów przetwarzających „zapewniających wystarczające gwarancje" zawarty w art. 28 ust. 1 RODO jest obowiązkiem ciągłym. Nie kończy się w momencie zawarcia umowy lub innego aktu prawnego przez administratora i podmiot przetwarzający. Administrator powinien raczej w odpowiednich odstępach czasu weryfikować gwarancje podmiotu przetwarzającego, w tym w stosownych przypadkach przez audyty i inspekcje[40].

1.2 Forma umowy lub innego aktu prawnego

100. Wszelkie przetwarzanie danych osobowych przez podmiot przetwarzający musi być uregulowane umową lub innym aktem prawnym na mocy prawa Unii lub państwa członkowskiego zawartym między administratorem a podmiotem przetwarzającym, zgodnie z wymogami art. 28 ust. 3 RODO.

101. Taki akt prawny ma **formę pisemną, w tym formę elektroniczną**[41]. W związku z tym niepisanych umów (niezależnie od stopnia ich szczegółowości lub skuteczności) nie można uznać za wystarczające do spełnienia wymogów określonych w art. 28 RODO. Aby uniknąć jakichkolwiek trudności w wykazaniu, że umowa lub inny akt prawny faktycznie obowiązują, EROD zaleca dopilnowanie, aby w akcie prawnym znalazły się niezbędne podpisy, zgodnie z obowiązującym prawem (np. prawem zobowiązań).

102. Ponadto umowa lub inny akt prawny na mocy prawa Unii lub prawa państwa członkowskiego muszą być **wiążące dla podmiotu przetwarzającego** w stosunku do administratora danych, tj. muszą nakładać na podmiot przetwarzający obowiązki wiążące na mocy prawa Unii lub prawa państwa członkowskiego. Musi on również określać obowiązki administratora. W większości przypadków będzie to umowa, ale rozporządzenie odnosi się również do „innego aktu prawnego", takiego jak przepisy prawa krajowego (pierwotne lub wtórne) lub inny instrument prawny. Jeżeli akt prawny nie zawiera minimalnej wymaganej treści, należy go uzupełnić umową lub innym aktem prawnym zawierającym brakujące elementy.

103. Ponieważ rozporządzenie ustanawia wyraźny obowiązek zawarcia umowy na piśmie, w przypadku gdy nie obowiązuje żaden inny odpowiedni akt prawny, jej brak stanowi naruszenie RODO[42]. Zarówno

[38] Zobacz motyw 81 RODO.
[39] Artykuł 28 ust. 5 i motyw 81 RODO.
[40] Zobacz również art. 28 ust. 3 lit. h) RODO.
[41] Artykuł 28 ust. 9 RODO.
[42] To, czy istnieje (lub nie) pisemne porozumienie, nie determinuje jednak tego, czy istnieje relacja między administratorem a podmiotem przetwarzającym. Jeżeli istnieje powód, by sądzić, że umowa nie odpowiada rzeczywistości pod względem faktycznej kontroli, na podstawie analizy okoliczności faktycznych dotyczących relacji między stronami i przetwarzania danych osobowych, porozumienie może zostać unieważnione. I odwrotnie, można uznać, że relacja administrator-podmiot przetwarzający nadal istnieje w przypadku braku pisemnej umowy o przetwarzaniu danych. Oznaczałoby to jednak naruszenie art. 28 ust. 3 RODO. Ponadto w

administrator, jak i podmiot przetwarzający są odpowiedzialni za zapewnienie zawarcia umowy lub innego aktu prawnego regulującego przetwarzanie[43]. Z zastrzeżeniem przepisów art. 83 RODO właściwy organ nadzorczy będzie mógł nałożyć grzywnę administracyjną zarówno na administratora, jak i podmiot przetwarzający, biorąc pod uwagę okoliczności każdej indywidualnego przypadku. Umowy zawarte przed datą rozpoczęcia stosowania RODO należało zaktualizować w świetle art. 28 ust. 3. Brak takiej aktualizacji, mającej na celu dostosowanie uprzednio istniejącej umowy do wymogów RODO, stanowi naruszenie art. 28 ust. 3.

Pisemną umowę na podstawie art. 28 ust. 3 RODO można również zawrzeć w szerszej umowie, takiej jak umowa o gwarantowanym poziomie usług. Aby ułatwić wykazanie zgodności z RODO, EROD zaleca, aby elementy umowy, które mają na celu wprowadzenie w życie art. 28 RODO, były wyraźnie oznaczone jako takie w jednym miejscu (np. w załączniku).

104. Aby spełnić obowiązek zawarcia umowy, **administrator i podmiot przetwarzający mogą wynegocjować własną umowę** zawierającą wszystkie obowiązkowe elementy **lub oprzeć się, w całości lub w części, na standardowych klauzulach umownych w odniesieniu do obowiązków wynikających z art. 28**[44].

105. Zestaw standardowych klauzul umownych może być ewentualnie przyjęty przez Komisję[45] albo przez organ nadzorczy zgodnie z mechanizmem spójności[46]. Klauzule te mogą stanowić część certyfikacji przyznanej administratorowi lub podmiotowi przetwarzającemu na mocy art. 42 lub 43[47].

106. Europejska Rada Ochrony Danych pragnie wyjaśnić, że administratorzy i podmioty przetwarzające nie mają obowiązku zawierania umowy opartej na standardowych klauzulach umownych (SKU), ani forma ta nie jest koniecznie preferowana w stosunku do negocjowania umowy indywidualnej. Oba warianty są odpowiednie do celów zapewnienia zgodności z przepisami o ochronie danych, w zależności od konkretnych okoliczności, o ile spełniają wymogi określone w art. 28 ust. 3.

107. Jeżeli strony chcą skorzystać ze standardowych klauzul umownych, klauzule dotyczące ochrony danych w ich umowie muszą być takie same jak klauzule zawarte w SKU. Standardowe klauzule umowne często zawierają puste miejsca do wypełnienia lub opcje do wyboru przez strony. Ponadto, jak również

---

pewnych okolicznościach brak jasnej definicji relacji między administratorem a podmiotem przetwarzającym może rodzić problem braku podstawy prawnej, na której powinno opierać się każde przetwarzanie, np. w odniesieniu do przekazywania danych między administratorem a domniemanym podmiotem przetwarzającym.

[43] Artykuł 28 ust. 3 ma zastosowanie nie tylko do administratorów. W sytuacji, gdy jedynie podmiot przetwarzający podlega terytorialnemu zakresowi RODO, obowiązek ten ma bezpośrednie zastosowanie wyłącznie do podmiotu przetwarzającego, zob. również wytyczne EROD 3/2018 w sprawie terytorialnego zakresu RODO, s. 12.

[44] Artykuł 28 ust. 6 RODO. EROD przypomina, że standardowe klauzule umowne do celów zapewnienia zgodności z art. 28 RODO nie są tożsame ze standardowymi klauzulami umownymi, o których mowa w art. 46 ust. 2. Podczas gdy pierwszy z nich określa i wyjaśnia, w jaki sposób będą przestrzegane przepisy art. 28 ust. 3 i 4, drugi zapewnia odpowiednie zabezpieczenia w przypadku przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 45 ust. 3.

[45] Artykuł 28 ust. 7 RODO. Artykuł 28 ust. 7 RODO. Artykuł 28 ust. 7 RODO. Artykuł 28 ust. 7 RODO. Zob. wspólna opinia EROD i EIOD 1/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_pl

[46] Artykuł 28 ust. 8 RODO. Rejestr decyzji podejmowanych przez organy nadzorcze i sądy w sprawach rozpatrywanych w ramach mechanizmu spójności, w tym standardowe klauzule umowne do celów zgodności z art. 28 RODO, jest dostępny pod adresem: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_pl

[47] Artykuł 28 ust. 6 RODO.

wspomniano powyżej, SKU będą zasadniczo włączone do większej umowy opisującej przedmiot umowy, jej warunki finansowe i inne uzgodnione klauzule: strony będą mogły dodawać dodatkowe klauzule (np. dotyczące prawa właściwego i jurysdykcji), o ile nie będą one sprzeczne, bezpośrednio lub pośrednio, z SKU[48] i nie będą podważać ochrony zapewnianej przez RODO oraz przepisy Unii lub państw członkowskich dotyczące ochrony danych.

108. Umowy między administratorami a podmiotami przetwarzającymi mogą niekiedy być sporządzane jednostronnie przez jedną ze stron. Wybór strony lub stron sporządzających umowę może zależeć od kilku czynników, w tym: pozycji stron na rynku i siły kontraktowej, ich wiedzy technicznej, a także dostępu do usług prawnych. Na przykład niektórzy dostawcy usług zazwyczaj ustanawiają standardowe warunki, które obejmują umowy o przetwarzaniu danych.

109. 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 przetwarzającymi, pozostawia on swobodę negocjacji między takimi stronami umów. W niektórych sytuacjach administrator lub podmiot przetwarzający mogą mieć słabszą pozycję negocjacyjną, by dostosować umowę o ochronie danych do swoich potrzeb. Poleganie na standardowych klauzulach umownych przyjętych zgodnie z art. 28 (akapity 7 i 8) może przyczynić się do zrównoważenia pozycji negocjacyjnych i zapewnienia, by umowy były zgodne z RODO.

110. Fakt, że umowa i jej szczegółowe warunki handlowe zostały przygotowane przez dostawcę usług, a nie przez administratora danych, nie jest sam w sobie problematyczny i nie stanowi wystarczającej podstawy do stwierdzenia, że dostawca usług powinien być uważany za administratora. Ponadto nie należy uznawać braku równowagi w uprawnieniach umownych małego administratora w odniesieniu do dużych dostawców usług za uzasadnienie dla akceptowania przez administratora klauzul i warunków umów, które nie są zgodne z przepisami o ochronie danych, ani nie może zwalniać administratora z obowiązków w zakresie ochrony danych. Administrator musi ocenić te warunki i o ile dobrowolnie je akceptuje i korzysta z usługi, przyjmuje również pełną odpowiedzialność za zgodność z RODO. Wszelkie proponowane przez podmiot przetwarzający zmiany w umowach o przetwarzaniu danych zawartych w standardowych warunkach powinny być bezpośrednio zgłaszane administratorowi i przez niego zatwierdzane, z uwzględnieniem stopnia swobody, jaką dysponuje podmiot przetwarzający w odniesieniu do elementów przetwarzania innych niż istotne (zob. pkt 40–41 powyżej). Samo opublikowanie tych zmian na stronie internetowej podmiotu przetwarzającego nie jest zgodne z art. 28.

[48] EROD przypomina, że ten sam stopień elastyczności jest dozwolony, gdy strony decydują się na wykorzystanie SKU jako odpowiedniego zabezpieczenia w przypadku przekazywania danych do państw trzecich zgodnie z art. 46 ust. 2 lit. c) lub art. 46 ust. 2 lit. d) RODO. Zgodnie z motywem 109 RODO „[m]ożliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony”.

1.3 Treść umowy lub innego aktu prawnego

111. Zanim skupimy się na każdym ze szczegółowych wymogów określonych w RODO dotyczących treści umowy lub innego aktu prawnego, konieczne jest przedstawienie pewnych uwag ogólnych.

112. Chociaż elementy określone w art. 28 rozporządzenia stanowią jego podstawową treść, umowa powinna być dla administratora i podmiotu przetwarzającego sposobem na dalsze wyjaśnienie sposobu wdrożenia tych zasadniczych elementów za pomocą szczegółowych instrukcji. Zatem **umowa o przetwarzaniu danych nie powinna ograniczać się do powtórzenia przepisów RODO**: powinna raczej zawierać bardziej szczegółowe, konkretne informacje na temat sposobu spełnienia wymogów i poziomu ochrony wymaganego do przetwarzania danych osobowych, które jest przedmiotem umowy o przetwarzaniu. Negocjowanie i zapisy umowy nie są działaniem *pro forma*, lecz okazją na sprecyzowanie szczegółów dotyczących przetwarzania[49]. W istocie „ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających [...] wymagają dokonania [...] jasnego podziału obowiązków" w ramach RODO[50].

113. Jednocześnie umowa powinna „***uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą***"[51]. Ogólnie rzecz biorąc, umowa między stronami powinna być sporządzona w świetle konkretnych działań związanych z przetwarzaniem danych. Na przykład nie ma potrzeby nakładania szczególnie rygorystycznych zabezpieczeń i procedur na podmiot przetwarzający, któremu powierzono czynność przetwarzania, z której wynikają jedynie niewielkie zagrożenia: chociaż każdy podmiot przetwarzający musi spełniać wymogi określone w rozporządzeniu, środki i procedury powinny być dostosowane do konkretnej sytuacji. W każdym razie umowa musi obejmować wszystkie elementy art. 28 ust. 3. Jednocześnie umowa powinna zawierać pewne elementy, które mogą pomóc podmiotowi przetwarzającemu w zrozumieniu zagrożeń dla praw i wolności osób, których dane dotyczą, wynikających z przetwarzania: ponieważ działalność jest wykonywana w imieniu administratora, często administrator ma większe zrozumienie zagrożeń, jakie niesie ze sobą przetwarzanie, ponieważ jest świadomy okoliczności, w których odbywa się przetwarzanie.

114. Przechodząc do **wymaganej treści** umowy lub innego aktu prawnego, zgodnie z interpretacją EROD art. 28 ust. 3, umowa musi określać:

- **przedmiot** przetwarzania (np. nagrania z monitoringu wizyjnego osób wchodzących do obiektu o wysokim poziomie bezpieczeństwa i wychodzących z niego). Chociaż przedmiot przetwarzania jest pojęciem szerokim, należy go sformułować w sposób wystarczająco szczegółowy, aby było jasne, jaki jest główny cel przetwarzania;
- **czas trwania**[52] przetwarzania: należy określić dokładny okres lub kryteria stosowane do jego ustalenia; na przykład można odnieść się do okresu obowiązywania umowy o przetwarzaniu danych;
- **charakter** przetwarzania: rodzaj operacji wykonywanych w ramach przetwarzania (na przykład: „filmowanie", „nagrywanie", „archiwizacja obrazów", ...) **i cel** przetwarzania (na przykład: wykrywanie nielegalnego wejścia). Opis ten powinien być możliwie jak najbardziej wyczerpujący,

[49] Zobacz również opinię 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO), s. 5.
[50] Zobacz motyw 79 RODO.
[51] Zobacz motyw 81 RODO.
[52] Czas trwania przetwarzania niekoniecznie odpowiada okresowi obowiązywania umowy (może istnieć prawny obowiązek przechowywania danych dłużej lub krócej).

w zależności od konkretnej czynności przetwarzania, aby umożliwić stronom zewnętrznym (np. organom nadzorczym) zrozumienie treści i ryzyka przetwarzania powierzonego podmiotowi przetwarzającemu;

- **rodzaj danych osobowych**: powinien on być określony w sposób jak najbardziej szczegółowy (na przykład: obrazy wideo osób wchodzących do obiektu i wychodzących z niego). Samo określenie, że chodzi o „dane osobowe zgodnie z art. 4 ust. 1 RODO" lub „szczególne kategorie danych osobowych zgodnie z art. 9" nie byłoby wystarczające. W przypadku szczególnych kategorii danych umowa lub akt prawny powinny przynajmniej określać, o jakie rodzaje danych chodzi, na przykład „informacje dotyczące dokumentacji medycznej" lub „informacje o tym, czy osoba, której dane dotyczą, jest członkiem związku zawodowego";
- **kategorie osób, których dane dotyczą**: również powinny być wskazane w dość szczególny sposób (na przykład: „osoby odwiedzające", „pracownicy", „kurier" itp.);
- **obowiązki i prawa administratora**: prawa administratora są szerzej omówione w kolejnych sekcjach (np. w odniesieniu do prawa administratora do przeprowadzania kontroli i audytów). Jeżeli chodzi o obowiązki administratora, do przykładów należy obowiązek przekazania podmiotowi przetwarzającemu danych wymienionych w umowie, dostarczenia i udokumentowania wszelkich instrukcji dotyczących przetwarzania danych przez podmiot przetwarzający, zapewnienia, przed przetwarzaniem i w trakcie całego procesu przetwarzania, spełniania przez podmiot przetwarzający obowiązków określonych w RODO w zakresie nadzorowania przetwarzania, w tym przez przeprowadzanie kontroli i audytów u podmiotu przetwarzającego.

115. Chociaż w RODO wymienia się elementy, które zawsze muszą być zawarte w umowie, może zaistnieć potrzeba uwzględnienia innych istotnych informacji, w zależności od kontekstu i ryzyka związanego z przetwarzaniem, a także wszelkich dodatkowych obowiązujących wymogów.

1.3.1 Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a) RODO)

116. Konieczność określenia tego obowiązku wynika z faktu, że podmiot przetwarzający przetwarza dane w imieniu administratora. Administratorzy muszą przekazywać podmiotom przetwarzającym instrukcje dotyczące każdej czynności przetwarzania. Takie instrukcje mogą obejmować dopuszczalne i niedopuszczalne sposoby przetwarzania danych osobowych, bardziej szczegółowe procedury, sposoby zabezpieczania danych itd. Podmiot przetwarzający nie może wykraczać poza instrukcje przekazane przez administratora. Podmiot przetwarzający może jednak sugerować elementy, które – jeśli zostaną zaakceptowane przez administratora – staną się częścią wydanych instrukcji.

117. Jeżeli podmiot przetwarzający przetwarza dane w sposób wykraczający poza instrukcje administratora i działanie takie jest równoznaczne z podjęciem decyzji określającej cele i sposoby przetwarzania, podmiot przetwarzający narusza swoje obowiązki, a nawet jest uznawany za administratora w odniesieniu do tego przetwarzania zgodnie z art. 28 ust. 10 (zob. pkt 1.5 poniżej[53]).

118. Instrukcje wydane przez administratora muszą być **udokumentowane**. W tym celu zaleca się włączenie procedury i wzoru udzielania dalszych instrukcji w załączniku do umowy lub innego aktu prawnego. Ewentualnie instrukcje można przekazywać w dowolnej formie pisemnej (np. e-mail), a także w każdej innej udokumentowanej formie, o ile możliwe jest prowadzenie ewidencji takich instrukcji. W każdym

[53] Zob. część II, pkt 1.5 („Podmiot przetwarzający określający cele i sposoby przetwarzania").

przypadku, aby uniknąć trudności w wykazaniu, że instrukcje administratora zostały należycie udokumentowane, EROD zaleca przechowywanie takich instrukcji wraz z umową lub innym aktem prawnym.

119. Spoczywający na podmiocie przetwarzającym obowiązek powstrzymania się od wszelkich czynności przetwarzania, które nie opierają się na instrukcjach administratora, dotyczy również **przekazywania** danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Umowa powinna określać wymogi dotyczące przekazywania danych do państw trzecich lub organizacji międzynarodowych, z uwzględnieniem przepisów rozdziału V RODO.

120. Europejska Rada Ochrony Danych zaleca, aby administrator zwracał należytą uwagę na tę konkretną kwestię, zwłaszcza gdy podmiot przetwarzający zamierza powierzyć niektóre czynności przetwarzania innym podmiotom przetwarzającym oraz gdy podmiot przetwarzający posiada oddziały lub jednostki zlokalizowane w państwach trzecich. Jeżeli instrukcje administratora nie pozwalają na przekazywanie lub ujawnianie danych do państw trzecich, podmiot przetwarzający nie będzie mógł powierzyć przetwarzania danych podwykonawcy w państwie trzecim, ani zlecić przetwarzania danych w jednym ze swoich oddziałów poza UE.

121. Podmiot przetwarzający może przetwarzać dane w sposób inny niż na udokumentowane polecenie administratora, **jeżeli podmiot przetwarzający jest zobowiązany do przetwarzania lub przekazywania danych osobowych na podstawie prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający**. Przepis ten dodatkowo wskazuje, jak ważne jest staranne negocjowanie i sporządzanie umów o przetwarzaniu danych, ponieważ, na przykład, może zaistnieć potrzeba zasięgnięcia porady prawnej przez każdą ze stron co do istnienia takiego wymogu prawnego. Należy to zrobić w odpowiednim czasie, ponieważ podmiot przetwarzający ma obowiązek poinformować administratora o takim wymogu przed rozpoczęciem przetwarzania. Obowiązek informacyjny nie istnieje jedynie w przypadku, gdy to samo prawo (Unii lub państwa członkowskiego) zabrania podmiotowi przetwarzającemu informować administratora z „ważnych względów interesu publicznego". W każdym przypadku wszelkie przekazywanie lub ujawnianie może mieć miejsce wyłącznie, gdy zezwala na to prawo Unii, w tym zgodnie z art. 48 RODO.

1.3.2 Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (art. 28 ust. 3 lit. B) RODO)

122. W umowie należy zaznaczyć, że podmiot przetwarzający musi dopilnować, aby każdy, kto zezwala na przetwarzanie danych osobowych, był zobowiązany do zachowania poufności. Może to nastąpić albo na podstawie konkretnego porozumienia umownego lub na mocy już istniejących zobowiązań ustawowych.

123. Szerokie pojęcie „osób upoważnionych do przetwarzania danych osobowych" obejmuje pracowników i pracowników tymczasowych. Ogólnie rzecz biorąc, podmiot przetwarzający powinien udostępniać dane osobowe tylko tym pracownikom, którzy rzeczywiście potrzebują ich do wykonywania zadań, do których podmiot przetwarzający został zatrudniony przez administratora.

124. Zobowiązanie do lub obowiązek zachowania poufności muszą być „odpowiednie", tj. muszą skutecznie zabraniać upoważnionej osobie ujawniania jakichkolwiek informacji poufnych bez upoważnienia, oraz muszą być wystarczająco szerokie, aby obejmować wszystkie dane osobowe przetwarzane w imieniu administratora, jak również warunki przetwarzania danych osobowych.

1.3.3 Podmiot przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32 (art. 28 ust. 3 lit. c) RODO).

125. Artykuł 32 nakłada na administratora i podmiot przetwarzający obowiązek wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa. Chociaż obowiązek ten jest już bezpośrednio nałożony na podmiot przetwarzający, którego operacje przetwarzania wchodzą w zakres RODO, obowiązek podjęcia wszelkich środków wymaganych na mocy art. 32 musi znaleźć odzwierciedlenie w umowie dotyczącej czynności przetwarzania powierzonych przez administratora.

126. Jak wskazano wcześniej, umowa o przetwarzaniu danych nie powinna być jedynie powtórzeniem przepisów RODO. Umowa musi zawierać informacje lub odniesienia do informacji dotyczących środków bezpieczeństwa, które mają zostać przyjęte, **obowiązek podmiotu przetwarzającego uzyskania zgody administratora przed wprowadzeniem zmian** oraz regularny przegląd środków bezpieczeństwa w celu zapewnienia ich adekwatności w odniesieniu do ryzyka, które może zmieniać się w czasie. Stopień szczegółowości informacji na temat środków bezpieczeństwa, które mają być zawarte w umowie, musi umożliwiać administratorowi ocenę stosowności środków zgodnie z art. 32 ust. 1 RODO. Ponadto opis ten jest również niezbędny, aby umożliwić administratorowi wywiązanie się z obowiązku rozliczalności na mocy art. 5 ust. 2 i art. 24 RODO w odniesieniu do środków bezpieczeństwa nałożonych na podmiot przetwarzający. Z art. 28 ust. 3 lit. f) i h) RODO można wywnioskować odpowiedni obowiązek podmiotu przetwarzającego dotyczący wsparcia administratora i udostępnienia wszelkich informacji niezbędnych do wykazania zgodności.

127. Poziom instrukcji przekazywanych podmiotowi przetwarzającemu przez administratora dotyczących środków, które należy wdrożyć, będzie zależał od konkretnych okoliczności. W niektórych przypadkach administrator może przedstawić jasny i szczegółowy opis środków bezpieczeństwa, które mają zostać wdrożone. W innych przypadkach administrator może opisać minimalne cele w zakresie bezpieczeństwa, które należy osiągnąć, zwracając się do podmiotu przetwarzającego o zaproponowanie wdrożenia konkretnych środków bezpieczeństwa. W każdym przypadku administrator musi dostarczyć podmiotowi przetwarzającemu opis czynności przetwarzania i celów bezpieczeństwa (w oparciu o ocenę ryzyka dokonaną przez administratora), a także zatwierdzić środki zaproponowane przez podmiot przetwarzający. Opis można zawrzeć w załączniku do umowy. Administrator wykonuje swoje uprawnienia decyzyjne w odniesieniu do głównych cech środków bezpieczeństwa, czy to przez wyraźne wymienienie środków, czy też przez zatwierdzenie tych zaproponowanych przez podmiot przetwarzający.

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).

128. Umowa musi określać, że podmiot przetwarzający nie może zatrudnić innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora oraz czy taka zgoda będzie miała charakter szczegółowy czy ogólny. W przypadku ogólnej zgody podmiot przetwarzający informuje administratora o każdej zmianie podwykonawców przetwarzania danych na podstawie pisemnej zgody i umożliwia administratorowi zgłoszenie sprzeciwu. Zaleca się, aby w umowie określono proces postępowania w tym zakresie. Należy zauważyć, że obowiązek podmiotu przetwarzającego polegający na informowaniu administratora o każdej zmianie podwykonawcy przetwarzania oznacza, że podmiot przetwarzający aktywnie wskazuje lub sygnalizuje takie zmiany administratorowi[54]. Ponadto w

[54] W tym przypadku nie wystarczy, aby podmiot przetwarzający jedynie zapewnił administratorowi ogólny dostęp do wykazu podwykonawców przetwarzania, który może być okresowo aktualizowany, bez wskazywania każdego

przypadku gdy wymagana jest szczegółowa zgoda, w umowie należy określić procedurę uzyskiwania takiej zgody.

129. Jeżeli podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, muszą oni zawrzeć umowę nakładającą takie same obowiązki w zakresie ochrony danych, jak te nałożone na pierwotny podmiot przetwarzający, lub należy te obowiązki nałożyć na podstawie innego aktu prawnego na mocy prawa Unii lub prawa państwa członkowskiego (zob. również pkt 160 poniżej). Obejmuje to również obowiązek wynikający z art. 28 ust. 3 lit. h), aby umożliwić audyty przeprowadzane przez administratora lub innego audytora upoważnionego przez administratora[55]. Podmiot przetwarzający odpowiada wobec administratora za przestrzeganie przez pozostałe podmioty przetwarzające obowiązków w zakresie ochrony danych (więcej szczegółów na temat zalecanej treści umowy znajduje się w pkt 1.6 poniżej[56]).

1.3.5 Podmiot przetwarzający pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw (art. 28 ust. 3 lit. E) RODO).

130. O ile zapewnienie, że żądania osób, których dane dotyczą, są rozpatrywane leży w gestii administratora, umowa musi przewidywać, że podmiot przetwarzający ma obowiązek udzielenia pomocy „w miarę możliwości poprzez odpowiednie środki techniczne i organizacyjne". Charakter tej pomocy może być bardzo różny „biorąc pod uwagę charakter przetwarzania" i w zależności od rodzaju działalności powierzonej podmiotowi przetwarzającemu. Szczegóły dotyczące pomocy udzielanej przez podmiot przetwarzający powinny zostać zawarte w umowie lub w załączniku do niej.

131. O ile pomoc może polegać po prostu na niezwłocznym przekazaniu każdego otrzymanego żądania lub umożliwieniu administratorowi bezpośredniego pozyskiwania odpowiednich danych osobowych i zarządzania nimi, w niektórych okolicznościach podmiot przetwarzający otrzyma bardziej szczegółowe, techniczne obowiązki, zwłaszcza gdy jest w stanie pozyskiwać dane osobowe i zarządzać nimi.

132. Należy pamiętać, że choć można zlecić podmiotowi przetwarzającemu praktyczne zarządzanie indywidualnymi żądaniami, to administrator ponosi odpowiedzialność za ich realizację. W związku z tym administrator ocenia czy żądania osób, których dane dotyczą, są dopuszczalne lub czy spełnione są wymogi określone w RODO, na zasadzie indywidualnej lub na podstawie jasnych instrukcji przekazanych podmiotowi przetwarzającemu w umowie przed rozpoczęciem przetwarzania. Ponadto administrator nie może przedłużyć terminów określonych w rozdziale III ze względu na fakt, że podmiot przetwarzający musi dostarczyć niezbędne informacje.

1.3.6 Podmiot przetwarzający pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 (art. 28 ust. 3 lit. F RODO).

133. Umowa nie może ograniczać się jedynie do powtórzenia tych obowiązków pomocy: **umowa powinna zawierać szczegółowe informacje na temat tego, w jaki sposób podmiot przetwarzający ma pomóc administratorowi w wypełnieniu wymienionych obowiązków**. Na przykład w załącznikach do umowy można dodać procedury i wzory formularzy, co umożliwi podmiotowi przetwarzającemu przekazanie administratorowi wszelkich niezbędnych informacji.

---

nowego podwykonawcy. Innymi słowy, podmiot przetwarzający musi aktywnie informować administratora o wszelkich zmianach w wykazie (tj. o każdym nowym planowanym podwykonawcy przetwarzania).

[55] Zobacz również opinię EROD 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO), przyjętą 9 lipca 2019 r., pkt 44.

[56] Zobacz część II, pkt 1.6 („Podwykonawcy przetwarzania danych").

134. Rodzaj i stopień pomocy udzielanej przez podmiot przetwarzający może się znacznie różnić, „uwzględniając charakter przetwarzania oraz dostępne mu informacje". Administrator musi odpowiednio poinformować podmiot przetwarzający o ryzyku związanym z przetwarzaniem oraz o wszelkich innych okolicznościach, które mogą pomóc podmiotowi przetwarzającemu w wypełnianiu jego obowiązków.

135. Przechodząc do konkretnych obowiązków, podmiot przetwarzający ma po pierwsze obowiązek pomagać administratorowi w spełnieniu obowiązku przyjęcia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania[57]. Chociaż obowiązek ten może się do pewnego stopnia pokrywać z wymogiem, aby podmiot przetwarzający sam przyjął odpowiednie środki bezpieczeństwa, w przypadku gdy operacje przetwarzania prowadzone przez podmiot przetwarzający wchodzą w zakres RODO, pozostają one dwoma odrębnymi obowiązkami, ponieważ jeden odnosi się do środków własnych podmiotu przetwarzającego, a drugi do środków administratora.

136. Po drugie, podmiot przetwarzający musi pomagać administratorowi w wypełnianiu obowiązku powiadamiania organu nadzorczego i osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. Podmiot przetwarzający musi powiadomić administratora o każdym przypadku wykrycia naruszenia ochrony danych osobowych mającego wpływ na urządzenia/systemy informatyczne podmiotu przetwarzającego lub podwykonawcy przetwarzania oraz pomóc administratorowi w uzyskaniu informacji, które należy zawrzeć w sprawozdaniu dla organu nadzorczego[58]. W RODO wymaga się, aby administrator zgłaszał naruszenie bez zbędnej zwłoki, aby zminimalizować szkodę poniesioną przez osoby fizyczne i zmaksymalizować możliwość zaradzenia naruszeniu w odpowiedni sposób. W związku z tym podmiot przetwarzający powinien powiadomić administratora danych bez zbędnej zwłoki[59]. W zależności od szczególnych cech przetwarzania powierzonego podmiotowi przetwarzającemu właściwe może być, aby strony uwzględniły w umowie konkretny termin (np. liczbę godzin), w którym podmiot przetwarzający powinien zgłosić naruszenie administratorowi, a także punkt kontaktowy dla takich zgłoszeń, sposób zgłoszenia i minimalny zakres jego treści oczekiwane przez administratora[60]. Ustalenia umowne między administratorem a podmiotem przetwarzającym mogą również obejmować upoważnienie i zobowiązanie podmiotu przetwarzającego do bezpośredniego zgłaszania naruszenia ochrony danych zgodnie z art. 33 i 34, przy czym odpowiedzialność prawna za zgłoszenie spoczywa na administratorze[61]. Jeżeli podmiot przetwarzający zgłosi naruszenie ochrony danych bezpośrednio organowi nadzorczemu i poinformuje osoby, których dane dotyczą, zgodnie z art. 33 i 34, podmiot przetwarzający musi również poinformować administratora i przekazać administratorowi kopie zgłoszenia i informacje przekazane osobom, których dane dotyczą.

137. Ponadto podmiot przetwarzający musi również pomagać administratorowi w przeprowadzaniu, w razie potrzeby, ocen skutków dla ochrony danych oraz w konsultowaniu się z organem nadzorczym, gdy wynik oceny wykaże, że istnieje wysokie ryzyko, którego nie można zminimalizować.

[57] Artykuł 32 RODO.
[58] Artykuł 33 ust. 3 RODO.
[59] Więcej informacji można znaleźć w Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 WP250rev.01, 6 lutego 2018 r., s. 13–14.
[60] Zobacz również opinię EROD 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO), przyjętą 9 lipca 2019 r., pkt 40.
[61] Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 WP250rev.01, 6 lutego 2018 r., s. 14.

138. Obowiązek udzielenia pomocy nie polega na przeniesieniu odpowiedzialności, ponieważ obowiązki te spoczywają na administratorze. Na przykład, chociaż ocenę skutków dla ochrony danych może przeprowadzić podmiot przetwarzający, administrator pozostaje odpowiedzialny za obowiązek przeprowadzenia takiej oceny[62], a podmiot przetwarzający jest zobowiązany jedynie do udzielenia administratorowi pomocy „w razie potrzeby i na żądanie”[63]. W związku z tym to administrator, a nie podmiot przetwarzający, musi podjąć inicjatywę przeprowadzenia oceny skutków dla ochrony danych.

1.3.7 Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora podmiot przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie (art. 28 ust. 3 lit. g) RODO).

139. Warunki umowy mają zagwarantować, aby dane osobowe podlegały odpowiedniej ochronie po zakończeniu „świadczenia usług związanych z przetwarzaniem”: do administratora należy zatem decyzja, co podmiot przetwarzający powinien zrobić z danymi osobowymi.

140. Administrator może zdecydować czy dane osobowe mają zostać usunięte czy zwrócone już na początku i określić to w umowie, w drodze pisemnego powiadomienia, które należy terminowo przesłać podmiotowi przetwarzającemu. Umowa lub inny akt prawny powinny odzwierciedlać możliwość zmiany przez administratora wyboru dokonanego przed zakończeniem świadczenia usług związanych z przetwarzaniem. W umowie należy określić procedurę udzielania takich instrukcji.

141. Jeżeli administrator zdecyduje się na usunięcie danych osobowych, podmiot przetwarzający powinien zapewnić bezpieczne usunięcie danych, również w celu zapewnienia zgodności z art. 32 RODO. Podmiot przetwarzający powinien potwierdzić administratorowi, że usunięcie zostało zakończone w uzgodnionym terminie i w uzgodniony sposób.

142. Podmiot przetwarzający musi usunąć wszystkie istniejące kopie danych, chyba że prawo Unii lub prawo państwa członkowskiego wymagają ich dalszego przechowywania. Jeżeli podmiot przetwarzający lub administrator wie o takim wymogu prawnym, powinien poinformować o tym drugą stronę tak szybko, jak to możliwe.

1.3.8 Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich (art. 28 ust. 3 lit. h) RODO).

143. Umowa zawiera szczegółowe informacje na temat częstotliwości i sposobu przepływu informacji między podmiotem przetwarzającym a administratorem, tak aby administrator był w pełni poinformowany o szczegółach przetwarzania, które są istotne dla wykazania zgodności z obowiązkami określonymi w art. 28 RODO. 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

[62] Grupa Robocza Art. 29, Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679, WP248 rev.01, s 14.
[63] Zobacz motyw 95 RODO.

wymogów zatrzymywania danych, lokalizacji danych, przekazywania danych, tego, kto ma dostęp do danych i kto jest ich odbiorcą, podwykonawców przetwarzania danych itd.

144. W umowie określa się również dalsze szczegóły dotyczące umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie inspekcji i audytów i do udziału w nich.

W RODO określono, że inspekcje i audyty przeprowadza administrator lub strona trzecia upoważniona przez administratora. Celem takiego audytu jest zapewnienie, aby administrator posiadał wszystkie informacje dotyczące czynności przetwarzania prowadzonej w jego imieniu oraz gwarancje udzielone przez podmiot przetwarzający. Podmiot przetwarzający może zaproponować wybór konkretnego audytora, ale ostateczna decyzja należy do administratora zgodnie z art. 28 ust. 3 lit. h) RODO[64]. Ponadto nawet jeżeli inspekcję przeprowadza audytor zaproponowany przez podmiot przetwarzający, administrator zachowuje prawo do zakwestionowania zakresu, metodyki i wyników inspekcji[65].

Strony powinny współpracować w dobrej wierze i ocenić, czy i kiedy istnieje potrzeba przeprowadzenia audytu w siedzibie podmiotu przetwarzającego, a także jaki rodzaj audytu lub inspekcji (zdalny/na miejscu/inny sposób zgromadzenia niezbędnych informacji) byłby potrzebny i odpowiedni w danym przypadku, biorąc również pod uwagę względy bezpieczeństwa; ostateczny wybór w tym zakresie należy do administratora. Po uzyskaniu wyników inspekcji administrator powinien mieć możliwość zwrócenia się do podmiotu przetwarzającego o podjęcie dalszych działań, np. w celu usunięcia stwierdzonych niedociągnięć i braków[66]. Podobnie należy ustanowić szczególne procedury dotyczące inspekcji podwykonawców przetwarzania przez podmiot przetwarzający i administratora (zob. pkt 1.6 poniżej[67]).

145. Kwestia podziału kosztów audytów między administratorem a podmiotem przetwarzającym nie jest objęta RODO i odbywa się na podstawie względów komercyjnych. Artykuł 28 ust. 3 lit. h) wymaga jednak, by umowa zawierała zobowiązanie podmiotu przetwarzającego do udostępnienia administratorowi wszelkich niezbędnych informacji oraz zobowiązanie do umożliwienia przeprowadzania audytów, w tym inspekcji, prowadzonych przez administratora lub innego audytora wyznaczonego przez administratora, oraz do udziału w nich. W praktyce oznacza to, że strony nie powinny wprowadzać do umowy klauzul przewidujących zapłatę kosztów lub opłat, które byłyby wyraźnie nieproporcjonalne lub nadmierne, a tym samym miałyby efekt odstraszający dla jednej ze stron. Takie klauzule faktycznie oznaczałyby, że prawa i obowiązki określone w art. 28 ust. 3 lit. h) nigdy nie byłyby wykonywane w praktyce i stałyby się czysto teoretyczne, podczas gdy stanowią one integralną część gwarancji ochrony danych przewidzianych w art. 28 RODO.

1.4 Instrukcje naruszające przepisy o ochronie danych

146. Artykuł 28 ust. 3 stanowi, że podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

[64] Zobacz wspólną opinię EROD i EIOD 1/2021 w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi, pkt 43.
[65] Zobacz opinię 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO), pkt 43.
[66] Zobacz opinię 14/2019 w sprawie projektu standardowych klauzul umownych przedłożonego przez duński organ nadzorczy (art. 28 ust. 8 RODO), pkt 43.
[67] Zobacz część II, pkt 1.6 („Podwykonawcy przetwarzania danych").

147. Podmiot przetwarzający ma bowiem obowiązek stosowania się do poleceń administratora danych, ale ma również ogólny obowiązek przestrzegania prawa. Polecenie, które narusza przepisy o ochronie danych prowadzi do konfliktu między wyżej wymienionymi dwoma obowiązkami.

148. Po otrzymaniu informacji, że jedna z jego instrukcji może naruszać przepisy o ochronie danych, administrator będzie musiał ocenić sytuację i ustalić, czy instrukcja rzeczywiście narusza przepisy o ochronie danych.

149. EROD zaleca, aby strony wynegocjowały i uzgodniły w umowie skutki zgłoszenia przez podmiot przetwarzający instrukcji naruszającej prawo oraz skutki niepodejmowania przez administratora działań w tym kontekście. Jednym z przykładów może być wprowadzenie klauzuli o rozwiązaniu umowy, jeżeli administrator nadal będzie wydawał niezgodne z prawem instrukcje. Innym przykładem może być klauzula dotycząca możliwości zawieszenia przez podmiot przetwarzający wykonania danej instrukcji do czasu potwierdzenia, zmiany lub wycofania instrukcji przez administratora[68].

1.5 Podmiot przetwarzający określający cele i sposoby przetwarzania

150. Jeżeli podmiot przetwarzający naruszy rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (art. 28 ust. 10 RODO).

1.6 Podwykonawcy przetwarzania

151. 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 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 (zob. pkt 83 powyżej).

152. Chociaż łańcuch może być dość długi, administrator zachowuje swoją kluczową rolę w określaniu celu i sposobów przetwarzania. Zgodnie z art. 28 ust. 2 RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. W obu przypadkach podmiot przetwarzający musi uzyskać pisemną zgodę administratora przed powierzeniem podwykonawcy przetwarzania danych osobowych. 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)[69].

153. Uprzednia pisemna zgoda może mieć charakter szczegółowy, tj. odnosić się do konkretnego podwykonawcy w odniesieniu do konkretnej czynności przetwarzania i w określonym czasie, lub może

[68] Zobacz wspólną opinię EROD i EIOD 1/2021 w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi pkt 39.
[69] Informacje te są potrzebne, aby administrator mógł przestrzegać zasady rozliczalności określonej w art. 24 oraz przepisów art. 28 ust. 1, art. 32 i rozdziału V RODO.

mieć charakter ogólny. Należy to określić w umowie lub innym akcie prawnym regulującym przetwarzanie.

154. 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.

155. Jeżeli administrator zdecyduje się udzielić **szczegółowej zgody**, powinien określić na piśmie, do którego podwykonawcy przetwarzania i jakiej czynności przetwarzania się ona odnosi. Każda późniejsza zmiana będzie wymagała dodatkowej zgody administratora przed jej wprowadzeniem. Jeżeli administrator nie udzieli odpowiedzi na wniosek podmiotu przetwarzającego o udzielenie szczegółowej zgody w ustalonym terminie, należy go uznać za odrzucony. Administrator udziela zgody lub wstrzymuje jej udzielenie, uwzględniając spoczywający na nim obowiązek korzystania wyłącznie z usług podmiotów przetwarzających zapewniających „wystarczające gwarancje" (zob. pkt 1.1 powyżej[70]).

156. Administrator może również udzielić **ogólnej zgody** na korzystanie z usług podwykonawców (w umowie, w tym w załączniku do umowy, zawierającym wykaz takich podwykonawców), którą należy uzupełnić o kryteria wyboru podmiotu przetwarzającego (np. gwarancje dotyczące środków technicznych i organizacyjnych, wiedzy fachowej, wiarygodności i zasobów)[71]. W takim przypadku podmiot przetwarzający w odpowiednim czasie informuje administratora o każdym planowanym dodaniu lub zastąpieniu podwykonawcy(ów), aby zapewnić administratorowi możliwość zgłoszenia sprzeciwu.

157. W związku z tym główna różnica między szczegółową a ogólną zgodą polega na znaczeniu braku odpowiedzi administratora: w przypadku ogólnej zgody brak sprzeciwu administratora w określonym terminie można interpretować jako udzielenie zgody.

158. W obu przypadkach umowa powinna zawierać szczegółowe informacje na temat terminu zatwierdzenia lub sprzeciwu administratora oraz sposobu, w jaki strony zamierzają komunikować się na ten temat (np. wzory). Takie ramy czasowe muszą być rozsądne w świetle rodzaju przetwarzania, złożoności czynności powierzonych podmiotowi przetwarzającemu (i podwykonawcom przetwarzania) oraz relacji między stronami. Ponadto umowa powinna zawierać szczegółowe informacje na temat praktycznych kroków podjętych w następstwie sprzeciwu administratora (np. poprzez określenie ram czasowych, w których administrator i podmiot przetwarzający powinni zdecydować o zakończeniu przetwarzania).

159. Niezależnie od zaproponowanych przez administratora kryteriów wyboru dostawców, podmiot przetwarzający ponosi wobec administratora danych pełną odpowiedzialność za wykonanie obowiązków podwykonawcy przetwarzania (art. 28 ust. 4 RODO). W związku z tym podmiot przetwarzający powinien dopilnować, aby proponowani przez niego podwykonawcy udzielali wystarczających gwarancji.

160. Ponadto, jeżeli podmiot przetwarzający zamierza zatrudnić (zatwierdzonego) podwykonawcę, musi zawrzeć z nim umowę nakładającą takie same obowiązki, jakie administrator nałożył na pierwszy podmiot przetwarzający, lub obowiązki te muszą wynikać z innego aktu prawnego na mocy prawa Unii lub prawa państwa członkowskiego. Cały łańcuch działań związanych z przetwarzaniem danych musi

[70] Zobacz część II pkt 1.1 („Wybór podmiotu przetwarzającego").

[71] Ten obowiązek administratora wynika z zasady rozliczalności określonej w art. 24 oraz z obowiązku przestrzegania przepisów art. 28 ust. 1, art. 32 i rozdziału V RODO.

być uregulowany pisemnymi umowami. 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. Oznacza to również, że jeżeli podmiot przetwarzający powierza podwykonawcy określoną część przetwarzania, do której niektóre z obowiązków nie mogą mieć zastosowania, obowiązki te nie powinny być włączane „domyślnie" do umowy z podwykonawcą, ponieważ spowodowałoby to jedynie niepewność. Na przykład, jeżeli chodzi o pomoc w wypełnianiu obowiązków związanych z naruszeniem ochrony danych, podwykonawca przetwarzania może zgłosić naruszenie ochrony danych bezpośrednio administratorowi, jeżeli wszystkie trzy podmioty wyrażą na to zgodę. W przypadku takiego bezpośredniego zgłoszenia należy powiadomić podmiot przetwarzający i przesłać mu kopię zgłoszenia.

2 SKUTKI WSPÓŁADMINISTRACJI

2.1 Określenie w przejrzysty sposób odpowiedzialności współadministratorów dotyczącej wypełniania obowiązków wynikających z RODO

161. Zgodnie z art. 26 ust. 1 RODO współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z rozporządzenia.

162. Współadministratorzy muszą zatem określić, „kto co robi", decydując między sobą, kto będzie musiał wykonywać jakie zadania, aby upewnić się, że przetwarzanie jest zgodne z mającymi zastosowanie obowiązkami wynikającymi z RODO w odniesieniu do danego wspólnego przetwarzania. Innymi słowy, należy dokonać podziału odpowiedzialności za zgodność, co wynika z użycia terminu „*odpowiednie*" w art. 26 ust. 1. Nie wyklucza to faktu, że prawo Unii lub prawo państwa członkowskiego może już określać pewne obowiązki każdego współadministratora. W takim przypadku uzgodnienia dotyczące współadministratorów powinny również obejmować wszelkie dodatkowe obowiązki niezbędne do zapewnienia zgodności z RODO, które nie zostały uwzględnione w przepisach prawnych[72].

163. Celem tych przepisów jest zapewnienie, aby w przypadku zaangażowania wielu podmiotów, zwłaszcza w złożonych środowiskach przetwarzania danych, odpowiedzialność za zgodność z przepisami o ochronie danych została wyraźnie przypisana, aby uniknąć sytuacji, w której ochrona danych osobowych jest ograniczona lub w której spór kompetencyjny negatywny prowadzi do luk prawnych, w wyniku których niektóre obowiązki nie są wypełniane przez żadną ze stron zaangażowanych w przetwarzanie danych. W tym miejscu należy wyjaśnić, że w celu osiągnięcia porozumienia operacyjnego wszystkie obowiązki muszą być przydzielone zgodnie z okolicznościami faktycznymi. Europejska Rada Ochrony Danych zauważa, że zdarzają się sytuacje, w których wpływ jednego współadministratora i jego faktyczny wpływ utrudniają osiągnięcie porozumienia. Okoliczności te nie podważają jednak współadministracji i nie mogą służyć zwolnieniu którejkolwiek ze stron z obowiązków wynikających z RODO.

164. W szczególności art. 26 ust. 1 stanowi, że współadministratorzy określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, „w szczególności" w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich

[72] „W każdym przypadku uzgodnienia dotyczące współadministratorów powinny obejmować wszystkie obowiązki współadministratorów, w tym te, które mogły już zostać określone przez prawo Unii lub prawo państwa członkowskiego, bez uszczerbku dla spoczywającego na współadministratorach obowiązku udostępnienia zasadniczej treści uzgodnień współadministratorów zgodnie z art. 26 ust. 2 RODO."

obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają.

165. Z przepisu tego jasno wynika, że współadministratorzy muszą określić, kto będzie odpowiadał odpowiednio za odpowiadanie na żądania w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw na mocy RODO, oraz za podawanie informacji, o których mowa w art. 13 i 14 RODO. Sprowadza się to jedynie określenia w ich wewnętrznych stosunkach, która ze stron jest zobowiązana do odpowiadania na żądania osób, których dane dotyczą. . Niezależnie od takich ustaleń osoba, której dane dotyczą, może skontaktować się ze współadministratorami zgodnie z art. 26 ust. 3 RODO. Użycie sformułowania „w szczególności" wskazuje jednak, że obowiązki objęte podziałem odpowiedzialności za przestrzeganie przepisów przez każdą zainteresowaną stronę, o których mowa w tym przepisie, nie są wyczerpujące. Wynika z tego, że podział odpowiedzialności za przestrzeganie przepisów między współadministratorów nie ogranicza się do kwestii, o których mowa w art. 26 ust. 1, lecz obejmuje inne obowiązki administratorów wynikające z RODO. Współadministratorzy muszą zapewnić, aby cały proces wspólnego przetwarzania był w pełni zgodny z RODO.

166. W tym kontekście przy określaniu swoich obowiązków, oprócz tych, o których mowa w art. 26 ust. 1, współadministratorzy powinni wziąć pod uwagę środki zgodności i związane z nimi obowiązki, w tym między innymi:

- wdrożenie ogólnych zasad ochrony danych (art. 5);
- podstawę prawną przetwarzania[73] (art. 6);
- środki bezpieczeństwa (art. 32);
- zgłoszenie do organu nadzorczego i osoby, której dane dotyczą, naruszenia ochrony danych osobowych[74] (art. 33 i 34);
- oceny skutków dla ochrony danych (art. 35 i 36)[75];
- korzystanie z usług podmiotu przetwarzającego (art. 28);
- przekazywanie danych do państw trzecich (rozdział V);

[73] Chociaż RODO nie wyklucza stosowania przez współadministratorów innej podstawy prawnej w odniesieniu do różnych operacji przetwarzania, które przeprowadzają, zaleca się stosowanie, w miarę możliwości, tej samej podstawy prawnej w konkretnym celu.

[74] Zobacz również wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 WP250rev.01, zgodnie z którymi współadministracja obejmuje „*ustalenia, która strona będzie odpowiedzialna za wywiązywanie się z zobowiązań ustanowionych w art. 33 i 34. Grupa Robocza art. 29 zaleca, aby uzgodnienia umowne między współadministratorami uwzględniały postanowienia wskazujące administratora, który będzie zajmował się dbaniem o wypełnianie ustanowionych w RODO obowiązków w zakresie zgłaszania naruszeń"* (s. 13).

[75] Zobacz również wytyczne EROD dotyczące ocen skutków dla ochrony danych, WP 248.rev01, które stanowią: „*Jeżeli operacja przetwarzania obejmuje współadministratorów, muszą oni dokładnie określić swoje obowiązki. W swojej ocenie skutków dla ochrony danych administratorzy powinni określić, która strona ponosi odpowiedzialność za poszczególne środki mające na celu wyeliminowanie ryzyka oraz za ochronę praw i wolności osób, których dane dotyczą. Każdy administrator danych powinien wyrazić swoje potrzeby i dzielić się przydatnymi informacjami bez ujawniania tajemnic (np.: ochrona tajemnicy przedsiębiorstwa, własności intelektualnej, poufnych informacji handlowych) albo słabych stron.*" (s. 7).

- organizację kontaktów z osobami, których dane dotyczą, i organami nadzorczymi.

167. Inne zagadnienia, które można rozważyć w zależności od danego przetwarzania i intencji stron, to na przykład ograniczenia wykorzystania danych osobowych w innym celu przez jednego ze współadministratorów. W związku z tym obaj administratorzy są zawsze zobowiązani do zapewnienia, by obaj mieli podstawę prawną przetwarzania. Czasami, w kontekście współadministracji, dane osobowe są udostępniane przez jednego administratora innemu administratorowi. W ramach odpowiedzialności każdy administrator ma obowiązek dopilnować, by dane nie były dalej przetwarzane w sposób niezgodny z celami, dla których zostały pierwotnie zgromadzone przez administratora udostępniającego dane[76].

168. Współadministratorom przysługuje pewien stopień elastyczności w podziale obowiązków między sobą, o ile zapewnią pełną zgodność z RODO w odniesieniu do danego przetwarzania. Przy przydzielaniu należy wziąć pod uwagę takie czynniki, jak to, kto jest kompetentny i jest w stanie skutecznie zagwarantować prawa osoby, której dane dotyczą, a także wywiązać się ze stosownych obowiązków wynikających z RODO. EROD zaleca udokumentowanie istotnych czynników i wewnętrznej analizy przeprowadzonej w celu przydzielenia różnych obowiązków. Analiza ta stanowi część dokumentacji zgodnie z zasadą rozliczalności.

169. Obowiązki nie muszą być równo rozłożone między współadministratorów. W tym zakresie TSUE stwierdził niedawno, że *„istnienie wspólnej odpowiedzialności nie musi oznaczać równej odpowiedzialności różnych podmiotów zaangażowanych w przetwarzanie danych osobowych*."[77] Mogą jednak wystąpić przypadki, w których nie wszystkie obowiązki można rozdzielić, a wszyscy współadministratorzy mogą być zmuszeni do przestrzegania tych samych wymogów wynikających z RODO, biorąc pod uwagę charakter i kontekst wspólnego przetwarzania. Na przykład współadministratorzy korzystający ze wspólnych narzędzi lub systemów przetwarzania danych muszą zapewnić zgodność zwłaszcza z zasadą celowości oraz wdrożyć odpowiednie środki bezpieczeństwa danych osobowych przetwarzanych w ramach wspólnych narzędzi.

170. Innym przykładem jest wymóg, aby każdy współadministrator prowadził rejestr czynności przetwarzania lub wyznaczył inspektora ochrony danych, jeżeli spełnione są warunki określone w art. 37 ust. 1. Takie wymogi nie są związane ze wspólnym przetwarzaniem, ale mają zastosowanie do nich jako do administratorów.

2.2 Podział obowiązków musi być dokonany w drodze uzgodnień

2.2.1 Forma dokumentu

171. Artykuł 26 ust. 1 RODO przewiduje jako nowy obowiązek współadministratorów, że powinni oni określić swoje obowiązki *„w drodze wspólnych uzgodnień*". W RODO nie określono formy prawnej takich uzgodnień. Współadministratorzy mogą zatem swobodnie ustalić formę uzgodnień.

172. Ponadto uzgodnienia dotyczące podziału obowiązków są wiążące dla każdego ze współadministratorów. Współadministratorzy zobowiązują się wobec siebie, że będą ponosić

[76] Każde ujawnienie przez administratora wymaga zgodnej z prawem podstawy i oceny zgodności, niezależnie od tego, czy odbiorca jest odrębnym administratorem, czy współadministratorem. Innymi słowy, współadministracja nie oznacza automatycznie, że współadministrator otrzymujący dane może również zgodnie z prawem przetwarzać je do dodatkowych celów, które wykraczają poza zakres wspólnej administracji.
[77] Wyrok w sprawie C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388, pkt 43.

odpowiedzialność za wywiązanie się z odpowiednich obowiązków określonych w uzgodnieniach wchodzących w zakres ich odpowiedzialności.

173. W związku z tym, z uwagi na pewność prawa, nawet jeśli RODO nie zawiera wymogu prawnego dotyczącego umowy lub innego aktu prawnego, EROD zaleca, aby takie uzgodnienia były dokonywane w formie wiążącego dokumentu, takiego jak umowa lub inny wiążący akt prawny na mocy prawa Unii lub państwa członkowskiego, któremu podlegają administratorzy. Zapewni to pewność i będzie stanowić dowód przejrzystości i odpowiedzialności. W przypadku nieprzestrzegania uzgodnionego podziału, wiążący charakter uzgodnień pozwala jednemu administratorowi na dochodzenie odpowiedzialności drugiego administratora za to, co zostało określone w umowie jako wchodzące w zakres jego odpowiedzialności. Ponadto, zgodnie z zasadą rozliczalności, wykorzystanie umowy lub innego aktu prawnego umożliwi współadministratorom wykazanie, że spełniają oni obowiązki nałożone na nich na mocy RODO.

174. W uzgodnieniu należy w jasny i prosty sposób wyrazić, jaki jest podział obowiązków, tj. zadań, między współadministratorami[78]. Wymóg ten jest ważny, ponieważ zapewnia pewność prawa i pozwala uniknąć ewentualnych konfliktów nie tylko w stosunkach między współadministratorami, ale również z osobami, których dane dotyczą i organami ochrony danych.

175. Aby lepiej określić podział odpowiedzialności między stronami, EROD zaleca, aby uzgodnienia zawierały również ogólne informacje na temat wspólnego przetwarzania, w szczególności poprzez określenie przedmiotu i celu przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą.

2.2.2 Obowiązki wobec osób, których dane dotyczą

176. W RODO przewidziano szereg obowiązków współadministratorów wobec osób, których dane dotyczą:

Uzgodnienia należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą

177. W uzupełnieniu do tego, co wyjaśniono powyżej w pkt 2.1 niniejszych wytycznych, ważne jest, aby współadministratorzy wyjaśnili w porozumieniu swoją rolę, „w szczególności" w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14. W art. 26 RODO podkreśla się znaczenie tych szczególnych obowiązków. Współadministratorzy muszą zatem zorganizować i uzgodnić, w jaki sposób i przez kogo informacje zostaną dostarczone oraz w jaki sposób i przez kogo zostaną udzielone odpowiedzi na żądania osoby, której dane dotyczą. Niezależnie od treści uzgodnień dotyczących tej konkretnej kwestii osoba, której dane dotyczą, może skontaktować się ze współadministratorami w celu wykonania swoich praw zgodnie z art. 26 ust. 3, jak wyjaśniono poniżej.

178. Sposób, w jaki zobowiązania te są zorganizowane w ramach uzgodnienia, powinien „należycie", tj. dokładnie odzwierciedlać rzeczywistość wspólnego przetwarzania. Na przykład, jeżeli tylko jeden ze współadministratorów komunikuje się z osobami, których dane dotyczą, do celów wspólnego

[78] Jak stwierdzono w motywie 79 RODO, *„(...) obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami*".

przetwarzania, taki administrator może być w stanie lepiej informować osoby, których dane dotyczą, i ewentualnie odpowiadać na ich żądania.

Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.

179. Przepis ten ma na celu zapewnienie, że osoba, której dane dotyczą, jest świadoma „zasadniczej treści uzgodnień". Na przykład dla osoby, której dane dotyczą, musi być całkowicie jasne, który administrator danych służy jako punkt kontaktowy do wykonywania praw osoby, której dane dotyczą (niezależnie od tego, czy osoba ta może wykonywać swoje prawa wobec każdego współadministratora). Obowiązek udostępnienia zasadniczej treści uzgodnień osobom, których dane dotyczą, jest istotny w przypadku współadministracji, tak aby osoba, której dane dotyczą, wiedziała, który z administratorów za co odpowiada.

180. Zakres pojęcia „zasadniczej treści uzgodnień" nie jest określony w RODO. Europejska Rada Ochrony Danych zaleca, aby zasadnicza treść obejmowała co najmniej wszystkie elementy informacji, o których mowa w art. 13 i 14, które powinny być już dostępne dla osoby, której dane dotyczą, przy czym w odniesieniu do każdego z tych elementów w uzgodnieniu należy określić, który współadministrator jest odpowiedzialny za zapewnienie zgodności z tymi elementami. Zasadnicza treść uzgodnień musi również wskazywać punkt kontaktowy, jeżeli został wyznaczony.

181. Nie określono sposobu udostępniania takich informacji osobie, której dane dotyczą. W przeciwieństwie do innych przepisów RODO (takich jak art. 30 ust. 4 dotyczący rejestru przetwarzania lub art. 40 ust. 11 dotyczący rejestru zatwierdzonych kodeksów postępowania) art. 26 nie wskazuje, że zasadnicza treść uzgodnień powinna być dostępna „na żądanie" lub "udostępniona opinii publicznej za pomocą odpowiednich środków". W związku z tym współadministratorzy decydują o najskuteczniejszym sposobie udostępnienia zasadniczej treści uzgodnień osobom, których dane dotyczą (np. wraz z informacjami, o których mowa w art. 13 lub 14, w polityce ochrony prywatności lub na żądanie inspektora ochrony danych, jeżeli taki istnieje, lub wyznaczonemu punktowi kontaktowemu). Współadministratorzy powinni odpowiednio zapewnić, aby informacje były przekazywane w spójny sposób.

W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

182. Artykuł 26 ust. 1 przewiduje możliwość wyznaczenia przez współadministratorów w porozumieniu punktu kontaktowego dla osób, których dane dotyczą. Nie ma obowiązku wyznaczenia punktu kontaktowego.

183. Dzięki wyznaczeniu jednego sposobu kontaktowania się z wieloma współadministratorami osoby, których dane dotyczą, wiedzą, z kim mogą się kontaktować we wszystkich kwestiach związanych z przetwarzaniem ich danych osobowych. Ponadto umożliwia to wielu współadministratorom skuteczniejsze koordynowanie swoich stosunków i komunikacji z osobami, których dane dotyczą.

184. Z tych powodów, aby ułatwić osobom, których dane dotyczą, wykonywanie ich z praw wynikających z RODO, EROD zaleca współadministratorom wyznaczenie takiego punktu kontaktowego.

185. Punktem kontaktowym może być inspektor ochrony danych, jeżeli taki istnieje, przedstawiciel w Unii (w przypadku współadministratorów niemających siedziby w Unii) lub jakikolwiek inny punkt kontaktowy, w którym można uzyskać informacje.

Niezależnie od uzgodnień osoby, których dane dotyczą, mogą wykonywać przysługujące im prawa wobec każdego ze współadministratorów

186. Zgodnie z art. 26 ust. 3 osoba, której dane dotyczą, nie jest związana warunkami uzgodnień i może wykonywać swoje prawa wynikające z RODO wobec każdego ze współadministratorów.

187. Na przykład w przypadku współadministratorów mających siedzibę w różnych państwach członkowskich lub gdy tylko jeden ze współadministratorów ma siedzibę w Unii, osoba, której dane dotyczą, może, według własnego wyboru, skontaktować się z administratorem mającym siedzibę w państwie członkowskim jej zwykłego pobytu lub miejsca pracy albo z administratorem mającym siedzibę w Unii lub w EOG.

188. Nawet jeżeli uzgodnienia i dostępna ich zasadnicza treść wskazują punkt kontaktowy do przyjmowania i rozpatrywania wszystkich wniosków osób, których dane dotyczą, same osoby, których dane dotyczą, mogą zdecydować inaczej.

189. W związku z tym ważne jest, aby współadministratorzy z wyprzedzeniem ustalili sposób zarządzania odpowiedziami na żądania, które mogą otrzymywać od osób, których dane dotyczą. Dlatego zaleca się, aby współadministratorzy informowali innych odpowiedzialnych administratorów lub wyznaczony punkt kontaktowy o otrzymywanych żądaniach, aby można było je skutecznie rozpatrywać. Zobowiązanie osób, których dane dotyczą, do kontaktowania się z wyznaczonym punktem kontaktowym lub odpowiedzialnym administratorem stanowiłoby nadmierne obciążenie dla osoby, której dane dotyczą, co jest sprzeczne z celem, jakim jest ułatwienie im korzystania z praw przysługujących im na mocy RODO.

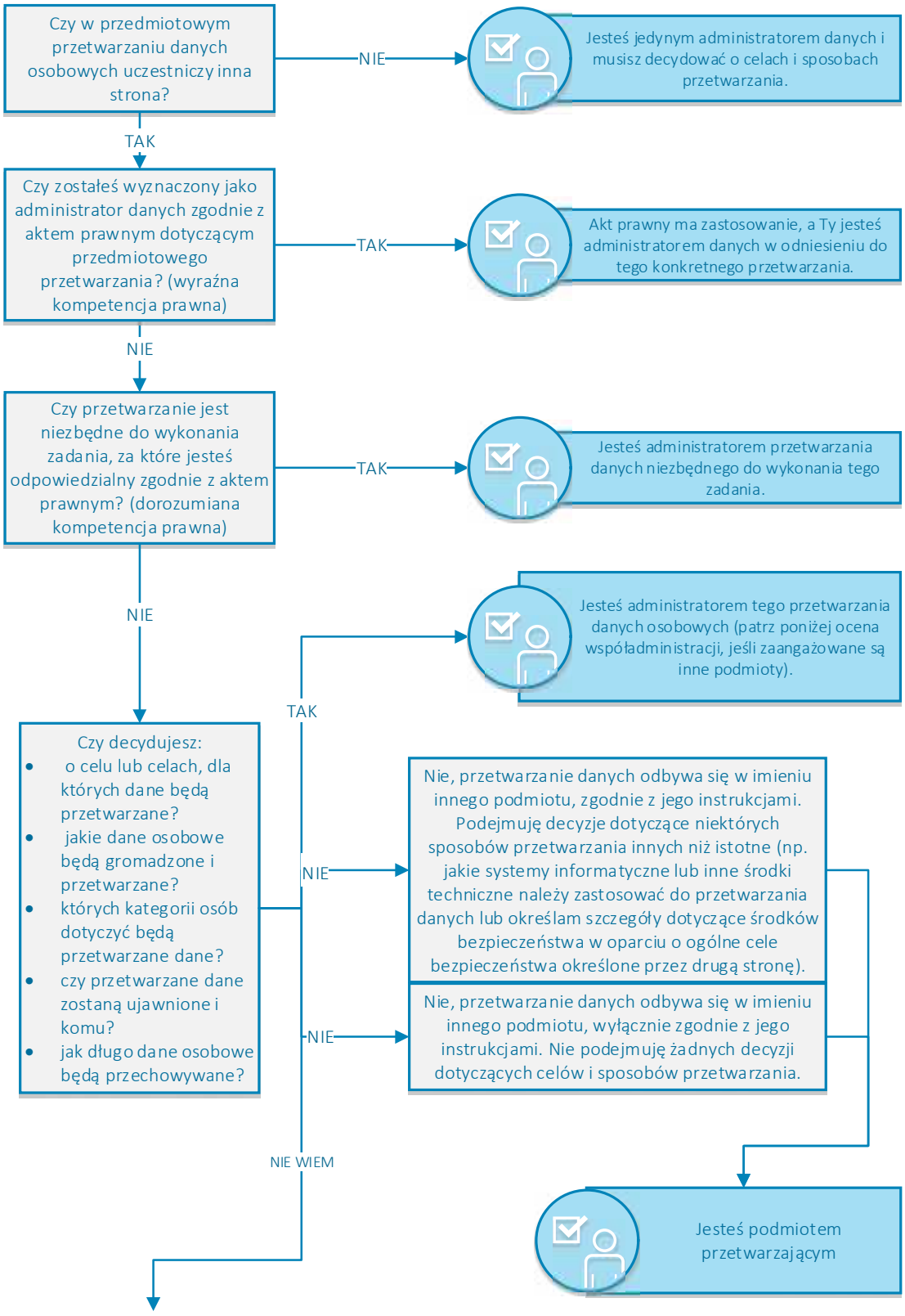
2.3 Obowiązki wobec organów ochrony danych

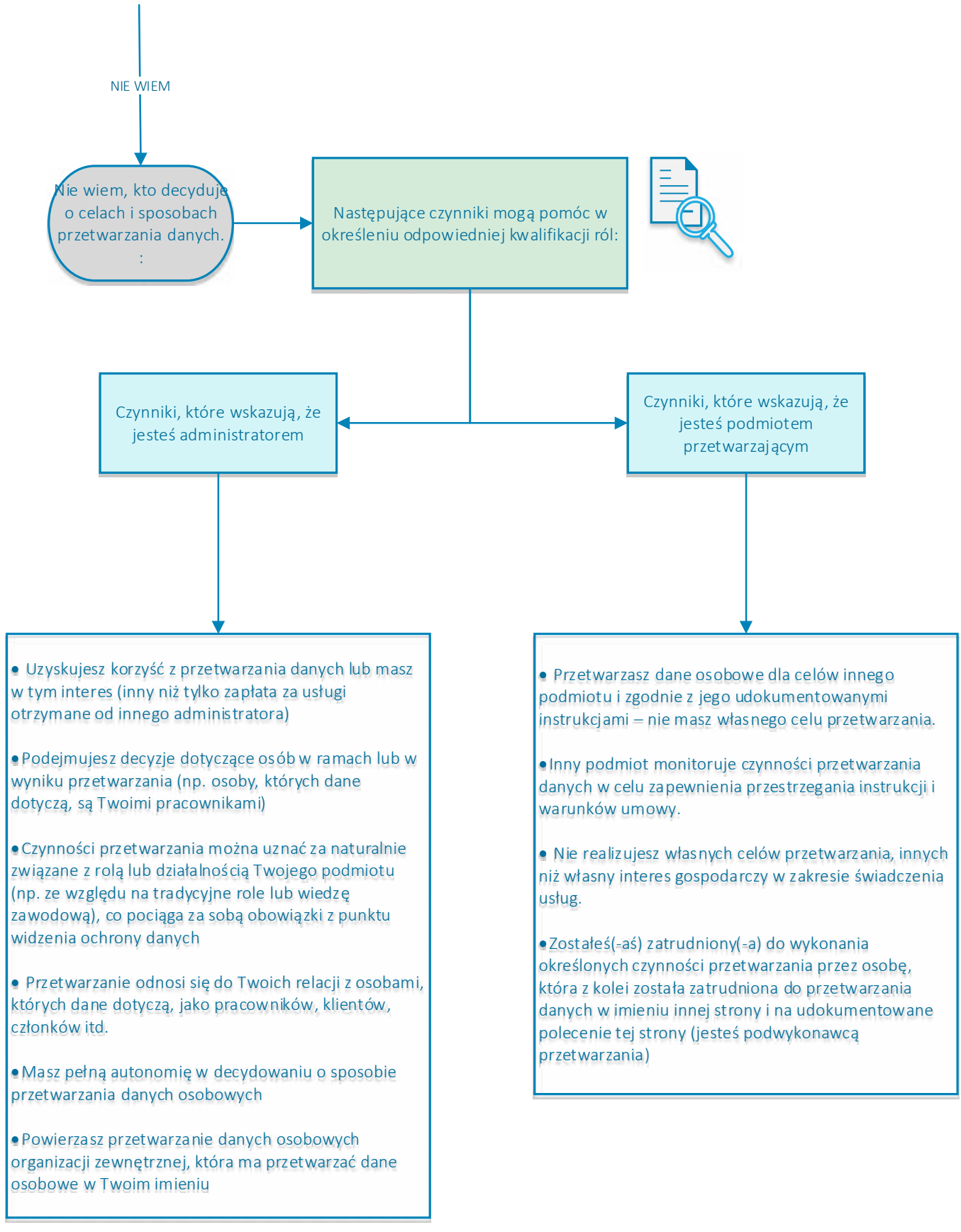
190. Współadministratorzy powinni określić w uzgodnieniach sposób komunikowania się z właściwymi nadzorczymi organami ochrony danych. Taka komunikacja mogłaby obejmować ewentualne konsultacje na mocy art. 36 RODO, zgłoszenie naruszenia ochrony danych osobowych, wyznaczenie inspektora ochrony danych.

191. Należy przypomnieć, że organy ochrony danych nie są związane uzgodnieniami ani w kwestii kwalifikacji stron jako współadministratorów, ani w kwestii wskazanego punktu kontaktowego. W związku z tym organy mogą kontaktować się ze współadministratorami w celu wykonania ich uprawnień na mocy art. 58 w odniesieniu do wspólnego przetwarzania.

Załącznik I – Schemat stosowania w praktyce pojęć administratora, podmiotu przetwarzającego i współadministratorów

Uwaga: aby właściwie ocenić rolę każdego zaangażowanego podmiotu, należy najpierw zidentyfikować konkretne przetwarzanie danych osobowych, o którym mowa, oraz jego dokładny cel. Jeżeli zaangażowanych jest wiele podmiotów, należy ocenić, czy cele i sposoby przetwarzania są określane wspólnie, co prowadzi do współadministracji.




NIE WIEM
Nie wiem, kto decyduje o celach i sposobach przetwarzania danych. :
Następujące czynniki mogą pomóc w określeniu odpowiedniej kwalifikacji ról:
Czynniki, które wskazują, że jesteś administratorem
Czynniki, które wskazują, że jesteś podmiotem przetwarzającym
• Uzyskujesz korzyść z przetwarzania danych lub masz w tym interes (inny niż tylko zapłata za usługi otrzymane od innego administratora)
• Podejmujesz decyzje dotyczące osób w ramach lub w wyniku przetwarzania (np. osoby, których dane dotyczą, są Twoimi pracownikami)
• Czynności przetwarzania można uznać za naturalnie związane z rolą lub działalnością Twojego podmiotu (np. ze względu na tradycyjne role lub wiedzę zawodową), co pociąga za sobą obowiązki z punktu widzenia ochrony danych
• Przetwarzanie odnosi się do Twoich relacji z osobami, których dane dotyczą, jako pracowników, klientów, członków itd.
• Masz pełną autonomię w decydowaniu o sposobie przetwarzania danych osobowych
• Powierzasz przetwarzanie danych osobowych organizacji zewnętrznej, która ma przetwarzać dane osobowe w Twoim imieniu
• Przetwarzasz dane osobowe dla celów innego podmiotu i zgodnie z jego udokumentowanymi instrukcjami – nie masz własnego celu przetwarzania.
• Inny podmiot monitoruje czynności przetwarzania danych w celu zapewnienia przestrzegania instrukcji i warunków umowy.
• Nie realizujesz własnych celów przetwarzania, innych niż własny interes gospodarczy w zakresie świadczenia usług.
• Zostałeś(-aś) zatrudniony(-a) do wykonania określonych czynności przetwarzania przez osobę, która z kolei została zatrudniona do przetwarzania danych w imieniu innej strony i na udokumentowane polecenie tej strony (jesteś podwykonawcą przetwarzania)

Współadministracja – jeśli jesteś administratorem danych, a w przetwarzanie danych osobowych zaangażowane są inne strony: