Nowoczesne Systemy Zarządzania
Zeszyt 19 (2024), nr 2 (kwiecień-czerwiec)
ISSN 1896-9380, s. 73-86
DOI: 10.37055/nsz/200428

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 19 (2024), No. 2 (April-June)
ISSN 1896-9380, pp. 73-86
DOI: 10.37055/nsz/200428

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Ryzyko błędnego określenia roli administratora danych osobowych oraz podmiotu przetwarzającego i jego konsekwencje dla organizacji

Risk of misidentifying the role of the controller and processor and its consequences for the organization

Radosław Mieszała
Politechnika Wrocławska, Polska
radoslaw.mieszala@pwr.edu.pl; ORCID: 0000-0002-3281-7475

Abstrakt. Artykuł ten jest interdyscyplinarną pracą skupiającą się na dziedzinie prawa oraz zarządzania, konkretnie zarządzania w ustaleniu roli danego podmiotu, który przetwarza dane osobowe za administratora danych osobowych czy podmiot przetwarzający. Autor podjął próbę przedstawienia czynników, które decydują o wpływie na to, jaką rolę dany podmiot powinien przyjąć i jaka jest różnica w ryzyku ponoszonym przez administratora danych osobowych, oraz udowodnienia, że ryzyko błędnego określenia roli administratora danych osobowych albo podmiotu przetwarzającego występuje mimo wielu wytycznych oraz samej regulacji RODO. Na wstępie opracowania zostają przedstawione pojęcia administratora danych osobowych oraz podmiotu przetwarzającego, a także różnice między tymi podmiotami. Następnie poruszona zostanie kwestia pomyłek związanych z błędnym określeniem roli administratora danych osobowych albo podmiotu przetwarzającego na wybranych przykładach.
Słowa kluczowe: ryzyko błędnego określenia roli administratora danych osobowych, administrator danych osobowych a podmiot przetwarzający, ryzyko związane z rolą administratora danych osobowych, ryzyko związane z rolą podmiotu przetwarzającego, RODO, uznanie podmiotu przetwarzającego za administratora danych osobowych, uznanie administratora danych osobowych za podmiot przetwarzający

Abstract. This article is an interdisciplinary work focusing on the field of law and management, specifically management in determining the role of a given entity that processes personal data for the controller or processor, in which the author has attempted to present the factors that determine the impact on what role a given entity should assume, moreover, what is the difference in the risk borne by the controller, and to prove that the risk of misdetermining the role of the controller or processor exists and takes place despite many guidelines and the GDPR regulation itself. At the outset, the paper introduces the concept

of controller and processor and the differences between these entities. Then the issue of confusion related to the misidentification of the role of controller or processor is addressed using selected examples.
Keywords: risk of mischaracterizing the role of the controller, controller versus processor, risks associated with the role of the controller, risks associated with the role of the processor, GDPR, recognition of the processor as the controller, recognition of the controller as the processor

Wprowadzenie

Artykuł jest interdyscyplinarną pracą skupiającą się na dziedzinie prawa oraz zarządzania, konkretnie zarządzania kontraktami. Autor podjął w nim próbę przedstawienia ryzyk związanych z błędnym określeniem ról oraz wskazówek, jakich to zastosowanie może stanowić ograniczenie ryzyka w kontekście nałożenia administracyjnych kar pieniężnych w rozumieniu art. 83 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, znanym również jako ogólne rozporządzenie o ochronie danych (dalej jako: RODO). Celem niniejszego opracowania było udowodnienie na wybranych przykładach, jak odpowiednie określenie roli administratora danych osobowych oraz podmiotu przetwarzającego pozwala ograniczyć ryzyko podmiotów biorących udział w przetwarzaniu danych osobowych. Na wstępie pracy przedstawiono pojęcie administratora danych osobowych oraz podmiotu przetwarzającego, a także różnice między tymi podmiotami. Ponadto pokazano, jaka jest różnica w ryzyku ponoszonym przez administratora danych osobowych oraz jak udowodnić, że ryzyko błędnego określenia roli administratora danych osobowych oraz podmiotu przetwarzającego występuje mimo wielu wytycznych oraz samej regulacji RODO. W ostatniej części artykułu przedstawiono kilka przypadków tzw. *case study* oraz wnioski, z jakich powodów zostały nałożone kary pieniężne w rozumieniu art. 83 RODO.

Różnica między administratorem danych osobowych a podmiotem przetwarzającym dane osobowe

Różnica między administratorem danych osobowych a podmiotem przetwarzającym dane osobowe oraz interakcje między tymi podmiotami mają kluczowe znaczenie w kontekście kwestii stosowania oraz ograniczania ryzyka zgodnie z RODO. Tego rodzaju rozróżnienie pozwala ustalić:

- kto jest przede wszystkim odpowiedzialny za zgodność przetwarzania danych osobowych z przepisami;
- w jaki sposób osoby, których dane są przetwarzane, mogą skutecznie egzekwować swoje prawa.

Jak więc widać, w relacji dotyczącej przetwarzania danych osobowych kluczowym w kontekście ryzyka jest ustalenie, który podmiot występuje jako administrator danych osobowych, a który jako podmiot przetwarzający.

Zgodnie z literaturą przedmiotu pojęcie administratora trzeba wykładać funkcjonalnie, tak aby przypisanie roli administratora nie polegało jedynie na określeniu formalnego wpływu na ustalenie celów i sposobów przetwarzania (Bielak-Jomaa, Lubasz, 2018). Zgodnie z wytycznymi Europejskiej Rady Ochrony Danych koncepcja administratora powinna być oceniana na zasadzie raczej faktycznej aniżeli formalnej analizy. Takie ustalenie – jaki podmiot jest administratorem danych osobowych – będzie przede wszystkim wynikać z okoliczności faktycznych, w zakresie których podmiot podjął decyzję o przetwarzaniu danych osobowych dla własnych celów (Grupa, 2010, s. 10; EDPB, 2020, s. 10). Również w jakże słusznej opinii rzecznika generalnego Paolo Mengozziego w sprawie Świadków Jehowy (Wyrok, 2018a, paragraf 68) zostało podkreślone, że nadmierne kładzenie nacisku na „formalne" podejście do decydowania o tym, która strona jest podmiotem przetwarzającym, a która administratorem danych osobowych, powodowałoby ułatwienie „obchodzenia" przepisów o ochronie danych osobowych. Jak wskazał rzecznik, konieczne jest bazowanie na analizie raczej faktycznej aniżeli formalnej: „W każdym razie pytanie prejudycjalne jest oparte na założeniu braku pisemnych instrukcji. Jestem skłonny uznać, podobnie jak rządy fiński, czeski i włoski, że przy określaniu «administratora danych» w rozumieniu dyrektywy 95/46 nadmierny formalizm pozwoliłby na łatwe obejście jej przepisów oraz że w konsekwencji, aby ocenić, czy wspólnota odgrywa rzeczywistą rolę w określaniu celów i sposobów przetwarzania danych, należy opierać się raczej na analizie okoliczności faktycznych niż na analizie formalnej" (Wyrok, 2018a, paragraf 68). Kluczowe znaczenie ma zatem efektywne zidentyfikowanie sprawowania kontroli – nawet w sytuacji, w której samo wyznaczenie czy też przetwarzanie danych osobowych odbywa się w sposób niezgodny z prawem (Wyrok, 2018a). Marlena Sakowska-Baryła również wskazuje, że decydowanie o celach i środkach przetwarzania powinno się rozumieć jako faktyczne podejmowanie decyzji w tym zakresie we własnym imieniu i jako to, w jakim celu oraz jak (jakim sposobem) przetwarzane mają być lub już są dane osobowe (Sakowska-Baryła, 2015).

Nie można jednak zapominać o art. 28 pkt 10 RODO: „Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania" (Rozporządzenie, 2016). Należy więc stwierdzić, że przetwarzający nie jest uprawniony do określania celów i środków przetwarzania. Kluczowe jest zatem to, aby w umowie o przetwarzaniu danych osobowych dokładnie określić, jakie są cele oraz środki przetwarzania, oraz to, aby podmiot przetwarzający działał zgodnie z instrukcjami administratora danych osobowych.

W innym przypadku podmiot przetwarzający może przekroczyć swoje uprawnienia (w szczególności gdy brak jest dokładnego ustalenia granic w tym zakresie w umowie o przetwarzaniu danych osobowych). W razie przekroczenia swoich uprawnień przez podmiot przetwarzający traci on swój uprzywilejowany status w odniesieniu do odpowiedzialności i podlega wszystkim obowiązkom administratora danych osobowych określonym w RODO (Wolff, Brink, 2021), co diametralnie zmienia postać rzeczy dla tego podmiotu przetwarzającego. Konsekwencje przekroczenia tych granic mogą być więc bardzo dotkliwe dla podmiotów przetwarzających, co dokładniej zostało opisane w rozdziale drugim, w którym dokonano również analizy przypadków. Jak więc widać, kwestia formalna w kontekście samej treści umowy o przetwarzaniu danych osobowych i jej przestrzegania ma, oprócz faktycznych ustaleń, niebagatelne znaczenie w kontekście chyba najważniejszym dla stron umowy, czyli ich odpowiedzialności.

Według wytycznych Grupy Roboczej ds. Ochrony Danych powołanej na mocy art. 29 RODO należy przeanalizować przetwarzanie danych osobowych (konkretne operacje przetwarzania danych osobowych) w ten sposób, ażeby odpowiedzieć sobie na pytania (Grupa, 2010, s. 10; EDPB, 2020, s. 10):

- Dlaczego ma miejsce dane przetwarzanie danych osobowych?
- Który podmiot rozpoczął określone przetwarzanie danych osobowych?
- Który podmiot zadecydował o tym, że określone przetwarzanie danych osobowych powinno mieć miejsce dla określonego celu?

Jak już wcześniej wspomniano, zasadniczo nie ma ograniczeń co do typu podmiotu, któremu można by było przypisać rolę administratora. Należy pamiętać, że w praktyce administratorem jest najczęściej organizacja, a nie indywiduum w danej organizacji, np. dyrektor, prezes, pracownik czy członek zarządu danej spółki (EDPB, 2020, s. 10). Zdarzało się jednak, że nawet osoby fizyczne były już uznawane za podmiot przetwarzający – tak na przykład było w słynnym orzeczeniu dotyczącym Świadków Jehowy (Wyrok, 2018a, pkt 75), w którym to Trybunał Sprawiedliwości Unii Europejskiej (TSUE) uznał, że religijne ugrupowanie Świadków Jehowy działało wspólnie z indywidualnymi członkami ugrupowania jako administratorzy danych osobowych. Trybunał Sprawiedliwości Unii Europejskiej wziął pod uwagę chociażby następującą kwestię dotyczącą tego, że członkowie wspólnoty Świadków Jehowy sporządzają podczas odwiedzania osób notatki, które mogą zawierać nazwiska i adresy nieznanych im osób bez ich wiedzy lub zgody. W niniejszej sprawie TSUE odpowiedział na następujące pytania (Wyrok, 2018a, pkt 24):

„1) Czy przewidziane w art. 3 ust. 2 tiret pierwsze i drugie dyrektywy 95/46 wyjątki dotyczące zakresu stosowania tej dyrektywy powinny być interpretowane w ten sposób, że dokonywane przez członków wspólnoty religijnej zbieranie i inne przetwarzanie danych osobowych mające miejsce w związku z działalnością kaznodziejską realizowaną poprzez odwiedzanie kolejnych gospodarstw domowych nie jest objęte zakresem stosowania tej dyrektywy?

Jakie znaczenie dla oceny możliwości stosowania dyrektywy 95/46 ma z jednej strony okoliczność, że działalność kaznodziejska, w ramach której zbierane są te dane, jest organizowana przez wspólnotę religijną i jej zbory, a z drugiej strony, że stanowi ona jednocześnie indywidualną praktykę religijną członków wspólnoty religijnej?

2) Czy definicja pojęcia «zbioru danych» zawarta w art. 2 lit. c dyrektywy 95/46 powinna być, uwzględniając motywy 26 i 27 tej dyrektywy, interpretowana w ten sposób, że całość danych osobowych, które nie są zbierane w sposób zautomatyzowany w związku z opisaną powyżej działalnością kaznodziejską realizowaną poprzez odwiedzanie kolejnych gospodarstw domowych (nazwisko i adres oraz inne możliwe dane i charakterystyki dotyczące osoby):
   a) nie stanowi takiego zbioru danych z tego powodu, że kartoteki lub rejestry, lub też inne systemy porządkujące służące wyszukiwaniu nie są wyraźnie objęte definicją zawartą w ustawie nr 523/1999, lub
   b) stanowi taki zbiór danych z tego powodu, że z danych tych, uwzględniając ich przeznaczenie, w rzeczywistości łatwo i bez nadmiernych kosztów mogą zostać uzyskane informacje potrzebne do dalszego wykorzystania, tak jak jest to przewidziane w ustawie nr 523/1999?
3) Czy zwrot «który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych» zawarty w art. 2 lit. d dyrektywy 95/46 należy interpretować w ten sposób, że wspólnota religijna, która organizuje działania, w ramach których zbierane są dane osobowe (między innymi przez podział obszarów aktywności osób prowadzących działalność kaznodziejską, przez obserwację działalności kaznodziejskiej oraz utrzymywanie rejestrów z osobami nieżyczącymi sobie wizyt głosicieli) w odniesieniu do tej działalności jej członków może być uznana za administratora danych, chociaż wspólnota religijna wskazuje, że jedynie poszczególni głosiciele mają dostęp do zgromadzonych informacji?
4) Czy wskazany art. 2 lit. d dyrektywy 95/46 powinien być interpretowany w ten sposób, że wspólnota religijna może być jedynie wówczas uznana za administratora danych, gdy stosuje inne szczególne środki, jak pisemne wytyczne lub instrukcje, za pomocą których kieruje zbieraniem danych, czy też wystarczy, że wspólnota religijna odgrywa faktyczną rolę w kierowaniu informacji działaniami swoich członków?".

Chyba jednymi z najważniejszych odpowiedzi i wniosków TSUE było to, że w niniejszej czynności działalność kaznodziejska obejmująca odwiedzanie kolejnych gospodarstw domowych praktykowana przez członków wspólnoty religijnej, takiej jak wspólnota Świadków Jehowy, nie należy do działań wyłączonych z zakresu stosowania dyrektywy 95/46 na podstawie art. 3 ust. 2 tiret pierwsze tej dyrektywy (Wyrok, 2018a, pkt 24, pkt 34-55).

Trybunał Sprawiedliwości Unii Europejskiej zauważył, że w niniejszej sprawie działalność prowadzona przez wspólnotę Świadków Jehowy nie mieści się w dwóch wyjątkach działalności prowadzonej przez organ państwowy oraz zwykłej działalności osobistej lub domowej. Czysta działalność domowa została zdefiniowana w sprawie Františka Ryneša (Wyrok, 2014) w paragrafach 31 i 33 jako działalność osoby przetwarzającej dane osobowe, a nie do osoby, której dane są przetwarzane. Sąd podkreślił, że aby ten wyjątek miał zastosowanie, musi to być działalność prowadzona w kontekście życia prywatnego lub rodzinnego osób fizycznych (Wyrok, 2014, pkt 31 i 33). Taka sytuacja nie miała miejsca w niniejszej sprawie, stąd nie podpada ona pod ten wyjątek.

Drugie pytanie, jakim zajął się TSUE, dotyczyło tego, że pojęcie zbioru danych w rozumieniu art. 2 ust. 1 lit. c dyrektywy 95/46 oznacza każdy uporządkowany zestaw danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego, czy są scentralizowane, zdecentralizowane lub rozproszone pod względem funkcjonalnym lub geograficznym. Ponadto zawartość zbioru, zgodnie z motywami 15 i 27 tej dyrektywy, musi mieć strukturę umożliwiającą łatwy dostęp do danych osobowych. W świetle tego TSUE zauważył, że dane osobowe zebrane podczas odwiedzania osób przez Świadków Jehowy, zebrane jako pomoc w zapamiętywaniu, przydzielone według sektora geograficznego w celu zorganizowania kolejnych wizyt, wchodzą w zakres stosowania art. 2 ust. 1 lit. c omawianej dyrektywy, a pytanie o konkretne kryterium lub formę, w jakiej są one ustrukturyzowane, jest bez znaczenia (Wyrok, 2018a, pkt 52-62).

W przypadku trzeciego i czwartego pytania TSUE przyjrzał się definicji administratora danych, wynikającej z art. 2 ust. 1 lit. d dyrektywy 95/46. Administrator danych został zdefiniowany jako osoba fizyczna lub prawna, która samodzielnie lub wspólnie z innymi określa cele i środki przetwarzania danych osobowych. Trybunał zauważył, że zasięg tej definicji jest obszerny, aby zagwarantować efektywną i pełną ochronę osób, których dotyczy. Oprócz tego stopień odpowiedzialności współadministratorów musi być oceniany w odniesieniu do wszystkich istotnych okoliczności danej sprawy, jak stwierdzono w sprawie Wirtschaftsakademie Schleswig-Holstein (Wyrok, 2018c, pkt 28, 43, 44.). Co więcej, w tej samej sprawie stwierdzono, że wspólna odpowiedzialność kilku podmiotów za to samo przetwarzanie nie zakłada, że każdy z nich ma dostęp do danych osobowych, których dotyczy to przetwarzanie.

W sprawie wspólnoty Świadków Jehowy nie ulegało wątpliwości, że angażuje się ona w działalność kaznodziejską, określa konkretne gromadzone dane i sposób ich późniejszego przetwarzania. Gromadzenie danych osobowych przyczyniło się do realizacji celu wspólnoty Świadków Jehowy, jakim było szerzenie jej wiary. Ponadto sąd uznał, że w związku z działalnością wspólnoty Świadków Jehowy społeczność ta zachęca swoich członków, którzy zajmują się działalnością kaznodziejską, do wykonywania czynności związanych z przetwarzaniem danych w kontekście ich aktywności.

W związku z tym sąd uznał, że organizując, koordynując i zachęcając swoich członków do działalności głoszenia w celu szerzenia swojej wiary, wspólnota Świadków Jehowy uczestniczyła wraz ze swoimi członkami w określaniu celów i sposobów przetwarzania danych osobowych. Sąd zauważył, że ustalenie to może być podważone przez zasadę autonomii organizacyjnej wspólnot religijnych na mocy art. 17 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), ale stwierdził, że każda osoba fizyczna ma obowiązek przestrzegania unijnych przepisów o ochronie danych.

Stanowisko to zostało także ujęte w sprawie Very Egenberger (Wyrok, 2018b, pkt 58), w aktach której zaznaczono, iż mimo że państwa członkowskie regulują swoje stosunki z kościołami, organizacjami i wspólnotami religijnymi, same działania kościołów, organizacji i wspólnot religijnych nie powinny być sprzeczne z prawem Unii Europejskiej: „Należy też stwierdzić, że art. 17 TFUE stanowi wyraz neutralności Unii względem sposobu, w jaki państwa członkowskie regulują swoje stosunki z kościołami, organizacjami i wspólnotami religijnymi. Artykuł ten nie wyłącza natomiast spod skutecznej kontroli sądowej przestrzegania kryteriów określonych w art. 4 ust. 2 dyrektywy 2000/78" (Wyrok, 2018b, pkt 58).

Uznanie za administratora danych osobowych lub podmiot przetwarzający, odpowiedzialność związana z daną rolą oraz konsekwencje błędnego określenia tych ról

Administrator ustala cele i sposoby przetwarzania, a więc kwestie dotyczące tego, jak dane przetwarzanie danych osobowych ma wyglądać, ale również dlaczego przetwarzanie danych osobowych ma w ogóle mieć miejsce. Kolejną bardzo ważną kwestią dotyczącą celów i sposobów przetwarzania jest to, że ich ustalenie musi nawiązywać do „przetwarzania danych osobowych, które zgodnie z RODO jest definiowane jako każda operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach osobowych" (Rozporządzenie, 2016). Należy pamiętać, że koncepcja administratora danych osobowych może być powiązana bądź to z pojedynczą operacją przetwarzania danych osobowych, bądź z zestawem takich operacji. W praktyce oznacza to, że „kontrolowanie" danych osobowych wykonywane przez daną organizację (administrują danymi osobowymi) może w swoim zakresie rozszerzać się na wszystkie „całościowe" przetwarzanie danych osobowych (tj. dotyczące wszystkich czynności przetwarzania danych osobowych w danej sprawie), ale może być również ograniczone do poszczególnych etapów (poszczególnego etapu) przetwarzania danych osobowych, co zostało ujęte w wyroku w sprawie Fashion ID (Wyrok, 2019, pkt 74), który dotyczył umieszczenia na stronie internetowej sprzedawcy tzw. „wtyczki internetowej" czy raczej wtyczki społecznościowej, czyli facebookowego przycisku „Lubię to" (Opinia, 2018).

W związku z takim umieszczeniem „wtyczki internetowej" następowało automatyczne przesłanie danych osobowych użytkownika przeglądającego tę stronę do szeroko znanego portalu Facebook (adres IP oraz identyfikator przeglądarki użytkownika), w tym przypadku dokładniej do spółki Facebook Ireland Limited. Spór odnosił się do tego, czy administratorem danych osobowych jest operator witryny internetowej instalujący opisaną wyżej „wtyczkę internetową", a konkretnie w tej sprawie firmy Fashion ID GmbH & Co. KG, czy też jednak spółka Facebook Ireland Limited.

Konkludując, w przypadku tej sprawy jednym z głównych wniosków w wyroku Trybunału Sprawiedliwości Unii Europejskiej było, co następuje: „operatora witryny internetowej, takiego jak Fashion ID GmbH & Co. KG, który umieszcza we wspomnianej witrynie wtyczkę społecznościową umożliwiającą przeglądarce osoby odwiedzającej tę witrynę pobieranie treści od dostawcy wspomnianej wtyczki i przekazywanie w tym celu temu dostawcy danych osobowych osoby odwiedzającej, można uznać za administratora danych w rozumieniu art. 2 lit. d dyrektywy 95/46. Jego odpowiedzialność jest jednak ograniczona do operacji lub do zestawu operacji przetwarzania danych osobowych, której lub których cele i sposoby rzeczywiście on określa, mianowicie gromadzenia rozpatrywanych danych i ich ujawniania poprzez transmisję" (Wyrok, 2019, pkt 107 ust. 2). Wyrok ten zatem podkreśla możliwość odpowiedzialności (ryzyka) danej strony przetwarzającej – administratora danych osobowych – co do samego przetwarzania danych osobowych, bo jest ona uzależniona od stopnia, w którym ten faktycznie jest administratorem danych osobowych, a więc odpowiedzialność tego podmiotu jest ograniczona do zakresu, w jakim ten „rzeczywiście określa cele i sposoby" przetwarzania danych osobowych.

Kolejną kwestią wartą podkreślenia i wydawać by się mogło paradoksalną jest to, że nie jest konieczne, aby sam administrator danych miał dostęp do danych osobowych, które są przetwarzane (EDPB, 2020, s. 16). Fakt ten z kolei potwierdza wyrok TSUE w sprawie Wirtschaftsakademie (Wyrok, 2018c). Sprawa ta polegała na tym, że owa firma prowadziła usługi edukacyjne za pomocą tzw. fanpage'a przez portal Facebook. Firma ta jako administrator fanpage'a grupy pozyskiwała dane statystyczne dotyczące osób odwiedzających portal Facebook. Działo się to za pomocą tzw. „ciasteczek" (z ang. *cookies*), a więc plików zawierających pewne informacje – w każdym z nich zapisany był unikalny kod użytkowania, który był aktywny dwa lata i który był przechowywany przez Facebook na urządzeniach gości. Taki unikalny kod mógł być powiązany z użytkownikami zarejestrowanymi na Facebooku, a ich dane były zbierane za każdym razem, kiedy dany fanpage był odwiedzany, z tym że ani portal Facebook, ani firma Wirtschaftsakademie nie powiadomiła gości strony internetowej o takim przechowywaniu (przetwarzaniu) danych, a konkretniej danych osobowych. Jednym z głównych wniosków w wyroku TSUE było, co następuje: „Art. 2 lit. d dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych należy interpretować w ten sposób,

że pojęcie «administratora danych» w rozumieniu tego przepisu obejmuje administratora fanpage'a prowadzonego na portalu społecznościowym" (Wyrok, 2018c).

Trybunał Sprawiedliwości Unii Europejskiej orzekł, iż mimo że sam fakt korzystania z portalu społecznościowego nie powoduje, że użytkownik staje się administratorem danych odpowiedzialnym za przetwarzanie danych osobowych, to administrator strony, czyli ten, który tworzy fanpage, wyraża zgodę na politykę użytkowania, politykę tzw. *cookies*, określa cele i promuje swoją działalność, a co za tym idzie, ma wpływ na przetwarzanie danych osobowych w celu sporządzenia przez portal Facebook raportu statystycznego dotyczącego strony, którą administruje, zanonimizowania użytkowników korzystających z nich lub też nie. Zgodnie z tym orzeczeniem zostało stwierdzone, co następuje: „Wprawdzie statystyki dotyczące użytkowników sporządzone przez Facebook są przekazywane wyłącznie administratorowi fanpage'a w formie zanonimizowanej, nie zmienia to jednak faktu, że sporządzanie tych statystyk opiera się na wcześniejszym gromadzeniu za pomocą plików cookies instalowanych przez Facebook na komputerach lub na wszelkich innych urządzeniach osób odwiedzających tę stronę i na przetwarzaniu danych osobowych tych osób w celach statystycznych. Dyrektywa 95/46 nie wymaga w żadnym razie, by w przypadku wspólnej odpowiedzialności kilku podmiotów w zakresie tego samego przetwarzania każdy miał dostęp do odnośnych danych osobowych" (Wyrok, 2018c, pkt 38). Tym samym administrator takiego fanpage'a, zgodnie z tym orzeczeniem, jest współadministratorem danych osobowych w rozumieniu RODO, wraz zresztą z portalem Facebook na podstawie art. 2 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (jak wynika z tego orzeczenia) (Wyrok, 2018c). Warto pokreślić, tak jak wynika to też z treści wytycznych, że podczas gdy orzeczenia te zostały wydane na zasadzie interpretacji koncepcji współadministratorów, bazując jeszcze na wyżej opisanej dyrektywie, a nie RODO, wciąż pozostają one właściwe i mają zastosowanie w rozumieniu RODO, ponieważ elementy dotyczące identyfikacji, ustalenia, w jakich przypadkach dany podmiot jest administratorem danych osobowych, pozostają po uchyleniu dyrektywy 95/46/CE (Dyrektywa, 1995) takie same (Wyrok, 2018c, pkt 38, s. 16-17).

Wracając jeszcze do kwestii braku konieczności posiadania dostępu do danych osobowych, aby zostać uznanym za administratora danych osobowych, należy podkreślić, że w tej sprawie jeden z administratorów danych osobowych, konkretnie Wirtschaftsakademie Schleswig-Holstein GmbH, uczestniczył w przetwarzaniu danych osobowych, o czym mówi treść orzeczenia w następujący sposób: „podejmując działania polegające na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, w określeniu celów i sposobów przetwarzania danych osobowych osób odwiedzających jego fanpage" (Wyrok, 2018c, pkt 39).

Właśnie z tego względu Wirtschaftsakademie Schleswig-Holstein GmbH został uznany za administratora danych osobowych, a właściwie współadministratora danych osobowych ze spółką Facebook Ireland Limited, a przez to wraz z tą spółką ponosił na poziomie Unii Europejskiej wspólną odpowiedzialność w związku z przetwarzaniem danych osobowych (wówczas jeszcze w rozumieniu art. 2 lit. d dyrektywy 95/46/CE), gdyż zgodnie z orzeczeniem: „Okoliczność, iż administrator fanpage'a korzysta z platformy oferowanej przez Facebook i z usług na niej dostępnych, nie zwalnia go bowiem z jego obowiązków w dziedzinie ochrony danych osobowych" (Wyrok, 2018c, pkt 40). Pogląd taki jest zbieżny również z tym prezentowanym przez grupę roboczą „Artykułu 29" (Zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołany jako ciało doradcze na podstawie art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych). Zgodnie z tym poglądem brak możliwości bezpośredniego wywiązania się ze wszystkich obowiązków administratora danych, takich jak zapewnienie prawa dostępu, nie wyklucza możliwości bycia administratorem (Opinia, 2010, s. 23). W związku właśnie z takimi okolicznościami wcześniej dyrektywa (zgodnie z opinią rzecznika generalnego Yves'a Bota w sprawie Wirtschaftsakademie Schleswig-Holstein (Opinia, 2017, pkt 62), a teraz RODO stanowi, że odpowiedzialność może ponosić łącznie kilka osób. Należy również pamiętać, że zgodnie z opinią grupy roboczej „Artykułu 29" udział stron w określaniu celów i sposobów przetwarzania w kontekście wspólnej kontroli może przyjmować różne formy i nie musi być taki sam (Opinia, 2010, s. 35).

Kolejnym przykładem, który pokazuje, czy konieczny jest bezpośredni dostęp do danych osobowych, aby zostać uznanym przykładowo za podmiot przetwarzający, a przez to naprowadza na interpretację odpowiedzialności stron, jest ten udostępniony przez Europejską Radę Ochrony Danych w wytycznych w sprawie ustalania pojęć „administrator danych osobowych" i „podmiot przetwarzający". Opisuje on przypadek usług hostingowych (EDPB, 2020, s. 15). Sytuacja tam opisana przedstawia przykład, w którym podmiot A zleca usługę hostingową (podmiotowi H) do przechowywania zaszyfrowanych danych (w tym danych osobowych) na serwerach podmiotu H. W związku z tym, że podmiot H nie ustala, czy dane, które przechowuje na swoim serwerze, są danymi osobowymi, ani nie przetwarza tych danych osobowych w żaden inny sposób i przetwarza je na zlecenie podmiotu A, podmiot H powinien zostać uznany jako podmiot przetwarzający dane osobowe. Europejska Rada Ochrony Danych nadmienia o konieczności (EDPB, 2020, s. 15):

- przekazania przez podmiot A odpowiednich instrukcji podmiotowi H, jak np. wymagane techniczne i organizacyjne środki bezpieczeństwa;
- zawarcia umowy o powierzaniu danych osobowych zgodnie z art. 28 ust. 3 RODO;

- wsparcia podmiotu A przez podmiot H w zapewnieniu koniecznych środków bezpieczeństwa;
- powiadomienia podmiotu A przez podmiot H w przypadku jakiegokolwiek naruszenia danych osobowych.

Co warto zaznaczyć, chyba najważniejszym etapem w procesie rozpoczynania przetwarzania danych osobowych między dwoma podmiotami jest odpowiednia decyzja w zakresie ustalenia ról tych podmiotów, a konkretnie decyzja w sprawie uznania danego podmiotu za administratora danych osobowych czy też podmiotu przetwarzającego. Jak widać, różne niuanse decydują o tym, jaka rola powinna być przyjęta przez dany podmiot. Ważne zatem dla ograniczania nieprzewidzianego ryzyka jest zorientowanie się przez dany podmiot, który przetwarza dane osobowe, czy aby na pewno przyjął odpowiednią rolę, a w konsekwencji zastosował się do wymogów regulacji RODO w zależności od tego, jaką rolę powinien przyjąć.

Literatura przedmiotu, którą wskazano powyżej, oraz ryzyka, które się zmaterializowały, jednoznacznie wskazują na konsekwencje opisanego błędnego określenia roli administratora danych osobowych albo podmiotu przetwarzającego dla organizacji. Jednym z przykładów ryzyk, które się zmaterializowały, jest nałożenie kary finansowej na firmę Cosmote. Grecki Urząd Ochrony Danych (z ang. Hellenic Data Protection Authority; dalej jako: HDPA) opublikował w dniu 31 stycznia 2022 r. decyzję nr 4/202229 (Decyzja, 2022a), nakładającą na Cosmote Mobile Telecommunications SA karę pieniężną w wysokości 6 mln euro za naruszenie rozporządzenia o ochronie danych osobowych, w konsekwencji naruszenia danych dotyczącego wycieku danych o połączeniach abonentów. HDPA zauważył, że Cosmote Mobile Telecommunications SA zgłosiła naruszenie danych do HDPA oraz przedstawiła odpowiednią dokumentację, z której wynikało, że Grecka Organizacja Telekomunikacyjna SA, grupa OTE, powinna być zaangażowana w badanie incydentu, w szczególności w odniesieniu do wdrożonych środków bezpieczeństwa. Naruszenie obejmowało trzydziestogigabajtowy plik danych osobowych dotyczący połączeń abonentów w okresie od 1 września 2020 r. do 5 września 2020 r. z jednego z serwerów firmy Cosmote Mobile Telecommunications SA. Plik zawierał dane abonentów – milionów osób – i składał się z następujących danych: numer telefonu, współrzędne stacji bazowej, oznaczenie IMEI, oznaczenie IMSI, informacje na temat czasu trwania połączenia, informacje na temat operatora, informacje dotyczące planu abonamentowego, wieku, płci oraz średniego przychodu na użytkownika. Zgodnie z treścią decyzji nakładającej karę pieniężną na firmę Cosmote Mobile Telecommunications SA zarówno ona, jak i podmiot przetwarzający dane nie okazały dowodu, że strony te ustaliły między sobą podział ról w kontekście przetwarzania danych osobowych. W niniejszym przypadku tamtejszy organ nadzorujący powołał się na brak umowy o przetwarzaniu (powierzeniu) danych osobowych zgodnie z art. 28 RODO lub też art. 26 RODO (umowy w przypadku współadministratorów danych osobowych), która zgodnie z przepisami RODO zawiera ustalenie takich kwestii.

Współpraca tych dwóch podmiotów i podział odpowiedzialności powinny być oparte albo na podstawie art. 26 RODO w przypadku odpowiedzialności wspólnej (współadministratorów), albo w umowie lub innym akcie prawnym na podstawie art. 28 RODO w przypadku powierzenia przetwarzania danych. Jak się okazało w trakcie badania sprawy przez HDPA, żadna z takich umów nie została zawarta (Decyzja, 2022a, s. 17-19, 39-40, 43; Mieszała, 2024).

Inny przykład niedawnej grzywny nałożonej na podstawie braku tzw. umowy z art. 28 RODO, a przez to brak określenia ról administratora danych osobowych oraz podmiotu przetwarzającego został nałożony we Francji na firmę Dedalus Biologie (Decyzja, 2022b). W dniu 23 lutego 2021 r. w prasie ujawniono ogromny wyciek danych dotyczących prawie 500 tysięcy osób. Dotyczył on firmy Dedalus Biologie. W ten sposób rozpowszechniono w Internecie nazwisko, imię, numer ubezpieczenia społecznego, nazwisko lekarza przepisującego leki, datę badania, a także informacje medyczne tych osób. Zgodnie z informacjami zawartymi w decyzji Commission Nationale de l'Informatique et des Libertés (francuskiego odpowiednika Urzędu Ochrony Danych Osobowych) nr SAN-2022-009 z dnia 15 kwietnia 2022 r. kara pieniężna w wysokości 1500 tys. euro została nałożona na dostawcę rozwiązań w zakresie oprogramowania działającego jako podmiot przetwarzający dane dla laboratoriów analiz medycznych – Dedalus Biologie – w związku z naruszeniem danych prawie 500 tysięcy osób, których dane dotyczą, w tym z naruszeniem między innymi art. 28 RODO (brak zawarcia umowy o przetwarzaniu danych osobowych). Miejscowy inspektor danych osobowych uznał, że Dedalus Biologie był podmiotem przetwarzającym zgodnie z art. 4 ust. 8 GDPR, ponieważ dostarczył laboratoriom narzędzia ułatwiające realizację przetwarzania i działał wyłącznie w imieniu i na odpowiedzialność laboratoriów. Na podstawie tego francuski organ uznał, że przetwarzający naruszył art. 28 ust. 3 GDPR, ponieważ umowa między nim a administratorem (administratorami) nie zawierała niezbędnych informacji wymaganych przez art. 28 ust. 3 GDPR. Na przykład jedna z umów odwoływała się do nieaktualnych przepisów francuskiej ustawy o ochronie danych osobowych. Commission Nationale de l'Informatique et des Libertés wyjaśnił, że samo istnienie sekcji dotyczącej danych osobowych nie spełnia wymogów art. 28 ust. 3 GDPR.

Podsumowanie

Artykuł miał za zadanie zilustrować za pomocą wybranych przykładów, że ryzyko błędnego ustalenia roli danego podmiotu, który przetwarza dane osobowe, występuje mimo wielu wytycznych oraz regulacji wynikających z RODO. Oryginalnym wkładem autora niniejszego opracowania było udowodnienie na wybranych przykładach, jak różnego rodzaju niuanse mogą wpływać na ustalenie roli danego podmiotu, który przetwarza dane osobowe, za administratora danych osobowych

czy też podmiot przetwarzający, a w konsekwencji znajomość których niuansów przyczynia się do ograniczenia ryzyka popełnienia pomyłki w tym zakresie. Ponadto autor udowadnia, na wskazanych przykładach, że mają miejsce pomyłki czy też ryzyko związane z błędnym ustaleniem roli danego podmiotu, który przetwarza dane osobowe, czy też generalnie problemy z identyfikacją właściwej roli danego podmiotu. Jak się okazuje w wymienionych wyżej przypadkach, nierzadko zdarza się, że podmioty przyjmują te role błędnie, mimo odpowiednich wytycznych czy też zasad wynikających z samej regulacji RODO. Konsekwencją takich błędnych ustaleń mogą być kary finansowe nakładane przez organy nadzorujące przestrzeganie przepisów RODO (organy ochrony danych poszczególnych państw członkowskich Unii Europejskiej). Oprócz tego dany podmiot, w przypadku błędnego przyjęcia roli, musi zastosować się do wszystkich przepisów nawiązujących do roli, którą powinien przyjąć, co nierzadko wiąże się – w szczególności w przypadku dużych organizacji – z długotrwałym procesem wdrażania odpowiednich procedur, aby wypełnić te obowiązki. Przykłady te oraz sama literatura dotycząca analizy RODO potwierdzają, że odpowiednie ustalenie ról podmiotów, które przetwarzają dane osobowe, mają niebagatelny wpływ zarówno na odpowiedzialność, jak i obowiązki wynikające z RODO. Ograniczeniem badań jest liczba wydanych decyzji przez organy nadzorcze w rozumieniu art. 51 RODO czy też wyroków Trybunału Sprawiedliwości Unii Europejskiej dotyczących RODO, zważywszy na to, że RODO jest regulacją, która relatywnie niedawno weszła w życie. Perspektywą dalszych badań jest dalsza klasyfikacja ryzyk związanych z RODO.

BIBLIOGRAFIA

[1] Bielak-Jomaa, E., Lubasz, D. (red.), 2018. *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa: Wolters Kluwer.

[2] Decyzja, 2022a. Decyzja w sprawie nałożenia grzywny za naruszenie danych osobowych i niezgodne z prawem przetwarzanie danych, wydana przez Grecki Urząd Ochrony Danych, nr 4.

[3] Decyzja, 2022b. Decyzja SAN-2022-009 wydana przez Commission Nationale de L'Informatique et des Libertés dot. Dedalus Biologie, 5.04.2022, Légifrance.

[4] Dyrektywa, 1995. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 23.11.1995).

[5] EDPB, 2020. European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted on 2 September 2020.

[6] Grupa, 2010. Grupa Robocza ds. Ochrony Danych powołana na mocy art. 29, Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający", przyjęta w dniu 16 lutego 2010 r.

[7] Mieszała, R., 2023. Ryzyko w kontekście odpowiedzialności administratora danych osobowych i podmiotu przetwarzającego a zawarcie zapisów w umowie powierzenia przetwarzania danych osobowych w celu ograniczenia odpowiedzialności, *Przegląd Prawa i Administracji*, t. CXXXV.

[8] Opinia, 2010. Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjęta przez grupę roboczą „Artykułu 29" w dniu 16 lutego 2010 r. (00264/10/PL, WP 169).

[9] Opinia, 2017. Opinia rzecznika generalnego Yves'a Bota w sprawie Wirtschaftsakademie Schleswig-Holstein.

[10] Opinia, 2018. Opinia rzecznika generalnego Michala Bobeka przedstawiona w dniu 19 grudnia 2018 r. w sprawie C-40/17 Fashion ID GmbH & Co. KG przeciwko Verbraucherzentrale NRW eV przy udziale Facebook Ireland Limited, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Oberlandesgericht Düsseldorf – wyższy sąd krajowy w Düsseldorfie, Niemcy).

[11] Rozporządzenie, 2016. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 4.05.2016).

[12] Sakowska-Baryła, M., 2015. *Prawo do ochrony danych osobowych*, Wrocław: Presscom Sp. z o.o.

[13] Sakowska-Baryła, M. (red.), 2018. *Komentarz do artykułu 28 RODO*, Warszawa: C.H. Beck.

[14] Wolff, H., Brink, S., 2021, *BeckOK Datenschutzrecht, Article 28 GDPR, margin number 104.*

[15] Wyrok, 2014. Wyrok Trybunału Sprawiedliwości UE w sprawie *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, C-212/13, ECLI:EU:C:2014:2428.

[16] Wyrok, 2018a. Wyrok Trybunału Sprawiedliwości UE w sprawie Świadków Jehowy, C-25/17, ECLI:EU:C:2018:551.

[17] Wyrok, 2018b. Wyrok Trybunału Sprawiedliwości UE w sprawie *Vera Egenberger przeciwko Evangelisches Werk für Diakonie und Entwicklung eV*, C-414/16, ECLI:EU:C:2018:257.

[18] Wyrok, 2018c. Wyrok Trybunału Sprawiedliwości UE (wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Bundesverwaltungsgericht – Niemcy) – *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI:EU:C:2018:388.

[19] Wyrok, 2019. Wyrok Trybunału Sprawiedliwości UE w sprawie Fashion ID, C-40/17, ECLI:EU:C:2019:629.