ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4211
PRZEGLĄD PRAWA I ADMINISTRACJI CXXXV
WROCŁAW 2023

https://doi.org/10.19195/0137-1134.135.16

RADOSŁAW MIESZAŁA
ORCID: 0000-0002-3281-7475

RYZYKO W KONTEKŚCIE ODPOWIEDZIALNOŚCI ADMINISTRATORA DANYCH OSOBOWYCH I PODMIOTU PRZETWARZAJĄCEGO A ZAWARCIE ZAPISÓW W UMOWIE POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH W CELU OGRANICZENIA ODPOWIEDZIALNOŚCI W ZAKRESIE NAKŁADANIA ADMINISTRACYJNYCH KAR PIENIĘŻNYCH W ROZUMIENIU ARTYKUŁU 83 RODO

Abstrakt: Niniejszy artykuł jest interdyscyplinarną pracą skupiającą się na dziedzinie prawa oraz zarządzania, konkretnie — zarządzania kontraktami, w której autor podjął próbę przedstawienia ryzyk związanych z zapisami w umowie powierzenia przetwarzania danych osobowych, jakich to zastosowanie może stanowić ograniczenie ryzyka w kontekście nałożenia administracyjnych kar pieniężnych w rozumieniu art. 83 RODO. Na wstępie w pracy zostaje przedstawione pojęcie administratora danych osobowych oraz podmiotu przetwarzającego, a także różnice między tymi podmiotami. Następnie poruszona zostaje kwestia umowy o powierzeniu danych osobowych oraz skutków ewentualnego braku wymaganych zapisów bądź umowy w ogóle. W ostatniej części przedstawiona jest analiza przypadków — tak zwanych *case study*, oraz wnioski, z jakich powodów dotyczących umów o powierzeniu danych osobowych zostały nałożone kary pieniężne w rozumieniu art. 83 RODO.

Słowa kluczowe: ryzyko a umowa o powierzeniu danych osobowych, zapisy w umowie o powierzeniu danych osobowych a ryzyko, ryzyko a umowy RODO, ryzyka w umowie o powierzeniu danych osobowych

1. ADMINISTRATOR DANYCH OSOBOWYCH ORAZ PODMIOT PRZETWARZAJĄCY A ODPOWIEDZIALNOŚĆ ZWIĄZANA Z PRZETWARZANIEM DANYCH OSOBOWYCH W ROZUMIENIU ROZPORZĄDZENIA O OCHRONIE DANYCH OSOBOWYCH

Rozróżnienie pomiędzy administratorem danych osobowych a podmiotem przetwarzającym dane osobowe oraz interakcje pomiędzy tymi podmiotami

odgrywają kluczową rolę w zakresie stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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) (dalej: rozporządzenie o ochronie danych osobowych lub RODO), przede wszystkim dlatego, że z takiego ustalenia wynika:

i) kto pierwszorzędnie ponosi odpowiedzialność za zgodność przetwarzania danych osobowych z prawem oraz

ii) w jaki sposób osoby, których dotyczą przetwarzane dane osobowe, mogą w praktyce egzekwować swoje prawa[1].

Sama zasada odpowiedzialności („rozliczalności") została uregulowana w art. 5 ust. 2 rozporządzenia o ochronie danych osobowych w następujący sposób: „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie («rozliczalność»)"[2]. Oprócz tego rozporządzenie o ochronie danych osobowych nakłada inne skonkretyzowane zasady dotyczące korzystania przez administratorów danych osobowych z podmiotów przetwarzających (na przykład administrator powinien korzystać wyłącznie z usług podmiotów przetwarzających, które w wystarczający sposób zapewniają gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych w taki sposób, ażeby przetwarzanie spełniało wymogi rozporządzenia o ochronie danych osobowych i chroniło prawa osób, których dane są przetwarzane)[3] oraz zasady dotyczące przetwarzania danych osobowych również w kontekście podmiotów przetwarzających (na przykład że ten zapewnia poufność danych oraz inne kwestie wynikające z umowy o przetwarzaniu danych osobowych, w tym że stosuje on odpowiednie środki techniczne i organizacyjne, zobowiązuje się do „asystowania" administratorowi danych osobowych w wywiązaniu się z obowiązków określonych w rozporządzeniu o ochronie danych osobowych[4], prowadzi rejestr wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu administratora — rejestr ten musi posiadać wyszczególnione przez rozporządzenie o ochronie danych osobowych informacje[5], obowiązek wyznaczenia inspektora danych osobowych w konkretnych przypadkach czy też powiadomienia administratora danych osobowych o naruszeniu ochrony danych osobowych[6]. Oprócz tego trzeba zaznaczyć, że rozporządzenie o ochronie danych osobowych

[1] European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020, s. 7.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 5 ust. 2.

[3] *Ibidem*, motyw 81 oraz art. 28 ust. 1.

[4] *Ibidem*, art. 28 ust. 3, art. 32.

[5] *Ibidem*, art. 32 ust. 2.

[6] *Ibidem*, art. 33 ust. 2.

nakłada na obydwa podmioty — podmiot przetwarzający oraz administratora danych osobowych — obowiązek zawarcia umowy o przetwarzaniu danych osobowych[7]. Niewątpliwie sam brak takiej umowy między podmiotem przetwarzającym a administratorem będzie naruszeniem artykułu 28 ust. 3 rozporządzenia o ochronie danych osobowych, za które to naruszenie co do zasady odpowiadać może zarówno administrator, jak i podmiot przetwarzający dane osobowe. Nie ulega zatem wątpliwości, że z zastrzeżeniem art. 3 RODO odpowiedni organ nadzorczy w zakresie ochrony danych osobowych, w takiej sytuacji, ma co do zasady możliwość, aby nałożyć karę administracyjną na administratora danych osobowych oraz podmiot przetwarzający, biorąc oczywiście pod uwagę stan faktyczny danej sprawy[8]. Może się jednak zdarzyć, że przykładowo administrator danych osobowych będzie znajdował się poza jurysdykcją rozporządzenia o ochronie danych osobowych, w takiej sytuacji to podmiot przetwarzający — o ile znajduje się w tej jurysdykcji — będzie jako jedyny odpowiedzialny za zawarcie umowy o przetwarzaniu danych osobowych w rozumieniu art. 28 ust. 3 RODO[9]. Biorąc to pod uwagę, umowa taka powinna nakładać pewne obowiązki na podmiot przetwarzający w taki sposób, aby był on zobowiązany w rozumieniu przepisów Unii Europejskiej czy też odpowiedniego państwa członkowskiego Unii Europejskiej w zakresie ich przestrzegania („Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora")[10]. Warto przy okazji tutaj nadmienić, że taka umowa musi zgodnie z RODO być zawarta na piśmie, dlatego też bez względu na to, czy względem danego prawa krajowego podmiot przetwarzający i administrator zawarli przykładową umowę ustną, która jest wiążąca — w rozumieniu RODO forma ta będzie niewystarczająca[11]. Rozporządzenie o ochronie danych osobowych definiuje rolę administratora w następujący sposób[12]: „administrator" oznacza osobę fizyczną

[7] *Ibidem*, art. 28 ust. 3, European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020, s. 30.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 28 ust. 3; European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020, s. 32.

[9] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR*, 12.11.2019, s. 12.

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 28 ust. 3.

[11] *Ibidem*, art. 28 ust. 9, European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR*, 12.11.2019, s. 5–6.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

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, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Z kolei według tego rozporządzenia podmiot przetwarzający jest definiowany w następujący sposób: „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora[13]. Już tutaj można zauważyć podstawową różnicę, która polega na tym, że administrator „ustala cele i sposoby przetwarzania danych osobowych", a więc jest głównym decydentem w tym zakresie, zaś podmiot przetwarzający czy też dalszy podmiot przetwarzający przetwarza dane osobowe w imieniu tego decydenta — administratora. Jak więc widać, to właśnie administrator odgrywa największą rolę, gdy chodzi o przetwarzanie danych osobowych. Definicja ta jest oparta na tej zawartej w akcie normatywnym poprzedzającym rozporządzenie o ochronie danych osobowych — dokładnie w art. 2 lit. d dyrektywy 95/46/WE[14], tak samo zresztą jak definicja podmiotu przetwarzającego[15]. Definicja administratora jest również poniekąd zbliżona do byłej już polskiej ustawy z 29 sierpnia 1997 roku[16], w której była mowa o „środkach przetwarzania", natomiast w unijnym rozporządzeniu — już o „sposobach przetwarzania", co jest główną różnicą tych definicji. Ustalenie, który podmiot w danej relacji jest administratorem danych osobowych, a który podmiotem przetwarzającym, jest kluczowe przede wszystkim ze względu na to, że większość wymogów określonych przepisami komentowanego rozporządzenia ciąży na administratorze, jego także pierwszorzędnie obarcza się odpowiedzialnością za naruszenie przepisów. Zgodnie z rozporządzeniem oraz doktryną administratorem jest podmiot[17]:

i) będący osobą fizyczną lub prawną, organem publicznym, jednostką lub innym podmiotem (w regulacyjnym uszczegółowieniu administratora opisuje się, że kategorią może być również „inny podmiot", co umożliwia szeroką wykładnię i relatywną swobodę, gdyż dzięki temu zapisowi za administratora można uznać

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, s. 1 z późn. zm.), art. 4 ust. 7.

[13] *Ibidem*, art. 4 ust. 8.

[14] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. UE. L. z 1995 r. Nr 281, s. 31 z późn. zm.), art. 2 lit. d.

[15] *Ibidem*, art. 2 lit. e.

[16] Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.).

[17] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, art. 4.

także podmiot, który nie mieści się w żadnej z wcześniej wymienionych kategorii podmiotowych[18],

ii) który samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych,

przy czym, zgodnie z poglądami Dominika Lubasza, Witolda Chomiczewskiego, Michała Czerniawskiego, Piotra Drobka, Urszuli Góral, Magdaleny Kuby, Pawła Makowskiego i Katarzyny Witkowskiej-Nowakowskiej, „cele i sposoby przetwarzania mogą być ustalane na poziomie przepisów prawa krajowego lub w prawie Unii", które to przepisy mogą także wyznaczać samego administratora[19]. Z opinii grupy roboczej ds. ochrony danych powołanej na mocy art. 29[20] wynika, że nie jest kluczowe, czy decyzja w sprawie ustalania celów i sposobów przetwarzania jest zgodna z prawem, ponieważ ewentualna ocena zgodności przetwarzania jest kwestią wtórną i może podlegać ewentualnej weryfikacji na innym etapie.

2. RYZYKO DOTYCZĄCE UMOWY O PRZETWARZANIU DANYCH OSOBOWYCH W KONTEKŚCIE UZNANIA PODMIOTU PRZETWARZAJĄCEGO ZA ADMINISTRATORA DANYCH OSOBOWYCH ORAZ NIEDOPEŁNIENIA OBOWIĄZKÓW ADMINISTRATORA DANYCH OSOBOWYCH — ANALIZA WYBRANYCH PRZYPADKÓW

Celem podkreślenia tego, jak ważne jest skuteczne ustalenie, która ze stron jest administratorem danych, oraz wykonanie w tym zakresie wszelkich potrzebnych działań, przede wszystkim zawarcia umowy o przetwarzaniu danych osobowych pomiędzy administratorem a podmiotem przetwarzającym, w niniejszej sekcji została przedstawiona analiza wybranych przypadków.

---

[18] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, art. 4; European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020, s. 3, 10.

[19] D. Lubasz, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, P. Makowski, K. Witkowska-Nowakowska, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, art. 4.

[20] 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 roku, s. 10; European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020, s. 10.

2.1. PRZYKŁAD WHATSAPP IRELAND LTD

Trzeba podkreślić, że w przypadku administratora danych osobowych, zgodnie z art. 82 ust. 2 RODO — jak już zostało wskazane — odpowiada on przedmiotowo w znacznie dalej idący sposób aniżeli podmiot przetwarzający. Zgodnie z tym przepisem:

> Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom[21].

Jak widać, zakres odpowiedzialności podmiotu przetwarzającego dane osobowe jest znacznie mniejszy aniżeli administratora danych osobowych. Nic w tym dziwnego, że podmiot przetwarzający powinien dążyć zatem do ograniczenia ryzyka, a więc pozostania przy statusie podmiotu przetwarzającego. Aby to zrealizować, podmiot przetwarzający zmuszony jest, zgodnie z art. 28 ust. 3 RODO, do zawarcia umowy z administratorem danych osobowych. Bardzo ważne przy tym jest, aby umowa ta zawierała wszystkie konieczne, wymagane przez art. 28 ust. 3 RODO przesłanki. W innym wypadku umowa taka nie będzie poprawnie zawarta, w związku z czym podmiot przetwarzający narazi się na ryzyko uznania go za administratora danych osobowych. Najlepszym przykładem „ku przestrodze" jest jedna z najwyższych kar, jakie zostały kiedykolwiek nałożone w związku z RODO. Mowa tutaj o karze nałożonej na irlandzką spółkę kojarzącą się z jedną z najbardziej popularnych aplikacji (komunikatorów) na świecie w branży mediów i telekomunikacji, to jest — spółce WhatsApp Ireland Ltd. Grzywna, jaką nałożono, wyniosła aż 225 milionów euro. Z informacji podanych w decyzji wydanej przez irlandzki organ odpowiedzialny za ochronę danych osobowych nr IN-18-12-2 wynika, że komisja ta — o nazwie Komisja Ochrony Danych (dalej: KOD) — ogłosiła w dniu 2 września 2021 roku zakończenie dochodzenia związanego z RODO, które przeprowadziła w sprawie irlandzkiej spółki WhatsApp Ireland Ltd. Dochodzenie KOD rozpoczęło się 10 grudnia 2018 roku i zbadało, czy spółka ta wywiązała się ze swoich obowiązków w zakresie przejrzystości związanej z regulacją RODO w odniesieniu do dostarczania informacji i ich przejrzystości zarówno użytkownikom, jak i osobom niekorzystającym z usługi oferowanej przez WhatsApp Ireland Ltd (dalej: WhatsApp). Dotyczy to informacji przekazywanych osobom, których dane dotyczą, na temat przetwarzania informacji między WhatsApp a innymi firmami Facebooka. Po długim i kompleksowym dochodzeniu KOD przedłożył projekt decyzji wszystkim zainteresowanym organom nadzorczym na mocy art. 60

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 82 ust. 2.

GDPR w grudniu 2020 roku. KOD otrzymał następnie zastrzeżenia od ośmiu organów nadzorczych, nie był w stanie osiągnąć porozumienia z organami nadzorczymi w sprawie przedmiotu zastrzeżeń i w dniu 3 czerwca 2021 roku uruchomił proces rozstrzygania sporów (art. 65 GDPR).

W dniu 28 lipca 2021 roku Europejska Rada Ochrony Danych (EDPB) przyjęła wiążącą decyzję, o której powiadomiono KOD. Decyzja ta zawierała wyraźną instrukcję, która wymagała od KOD ponownej oceny i zwiększenia proponowanej grzywny na podstawie wielu czynników zawartych w decyzji EDPB, a po ponownej ocenie KOD nałożyła na spółkę WhatsApp grzywnę w wysokości 225 milionów euro. Oprócz nałożenia grzywny administracyjnej KOD nałożyła również na WhatsApp naganę wraz z nakazem doprowadzenia przetwarzania danych do zgodności z przepisami poprzez podjęcie określonych działań naprawczych. EDPB opublikował decyzję na podstawie art. 65 oraz decyzję końcową na swojej stronie internetowej.

Z punktu 39b omawianej tutaj decyzji wydanej przez KOD jednoznacznie wynika, że prowadzący dochodzenie sformułował pogląd, że przetwarzając dane osobowe osób niebędących użytkownikami, spółka WhatsApp czyniła to jako administrator danych osobowych, a nie podmiot przetwarzający. Ten pogląd oparty był na tym, że przepis określony w art. 28 ust. 3 RODO wymaga, aby wszelkie przetwarzanie (przez podmiot przetwarzający działający w imieniu administratora) było uregulowane „umową lub innym aktem prawnym". Stwierdzono zatem, że takiej umowy nie było, fakt ten natomiast stanowił, że WhatsApp nie powinien być uznany za podmiot przetwarzający, a za administratora danych osobowych, co wymagało spełnienia obowiązków administratora danych osobowych, których WhatsApp nie spełnił, i w związku z tym nałożona została opisywana w tej kwestii grzywna. Przykład ten w bardzo bezpośredni sposób pokazuje, jak ważne jest to, aby między administratorem a podmiotem przetwarzającym była zawarta odpowiednia umowa o przetwarzaniu danych osobowych. Zawarcie jej „w ogóle" jest kluczowym elementem ograniczenia ryzyka.

Relacja między administratorem danych a podmiotem przetwarzającym musi być określona w formie pisemnej umowy[22] lub innego prawnie wiążącego aktu. Jest to konieczne, aby zapewnić przejrzysty podział obowiązków i odpowiedzialności zarówno wewnętrznie (pomiędzy administratorami i podmiotami przetwarzającymi), jak i zewnętrznie (wobec osób, których dane dotyczą, i organów regulacyjnych)[23]. W innym wypadku (bez takiej umowy), jak widać po niniejszej decyzji, podmiot przetwarzający może w łatwy sposób uzyskać status

[22] Bez uszczerbku dla „każdej indywidualnej umowy między nimi, administrator i podmiot przetwarzający mogą również zarządzać wymogami art. 28 ust. 3 i 4 poprzez standardowe klauzule umowne, które Komisja Europejska wydała lub organ nadzorczy przyjął na mocy art. 28 ust. 8", tak w: Millard/Kamarinou, [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Article 28 GDPR, s. 606 (Oxford 2020).

[23] *Ibidem*.

administratora danych osobowych, gdyż zgodnie z art. 28 ust. 3 lit. a RODO podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora[24]. Zgodnie z art. 28 ust. 3 GDPR zasadnicza treść takiej umowy składa się z ośmiu elementów: 1) przedmiot, 2) czas trwania przetwarzania, 3) charakter[25], 4) cel przetwarzania, 5) rodzaj danych osobowych, 6) kategorie osób, których dane dotyczą, oraz 7) obowiązki i prawa administratora[26]. Druga część art. 28 ust. 3 GDPR zawiera listę elementów, które muszą być szczegółowo przewidziane w umowie między administratorem a podmiotem przetwarzającym.

2.2. PRZYKŁAD DEDALUS BIOLOGIE

Inny przykład niedawnej grzywny nałożonej na podstawie braku tak zwanej umowy z art. 28 GDPR został nałożony we Francji na firmę Dedalus Biologie[27]. W dniu 23 lutego 2021 roku w prasie ujawniono ogromny wyciek danych dotyczących prawie 500 tysięcy osób, który dotyczył firmy Dedalus Biologie. W ten sposób rozpowszechniono w internecie nazwisko, imię, numer ubezpieczenia społecznego, nazwisko lekarza przepisującego leki, datę badania, ale także informacje medyczne tych osób. Zgodnie z informacjami zawartymi w decyzji francuskiego Urzędu Ochrony Danych Osobowych nr SAN-2022-009 z dnia 15 kwietnia 2022 roku kara pieniężna w wysokości 1500 tysięcy 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 przetwa-

---

[24] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 28 ust. 3 lit. a.

[25] W zakresie charakteru przetwarzania, podmiot przetwarzający może otrzymać pewną swobodę w kwestii sposobów przetwarzania, por. N. Bertermann, [w:] E. Ehmann, M. Selmayr, *Datenschutz-Grundverordnung*, Article 28 GDPR, margin number 20 (Warszawa 2018) with reference to WP29, "Opinion 1/2010 on the concepts of controller and processor", 00264/10/EN WP 169, 16.02.2010, s. 17.

[26] Aby określić prawa i obowiązki administratora, przykładowo właśnie te aspekty należy określić. Zgodnie z RODO tylko administrator danych decyduje o usunięciu, poprawieniu i dostępie do danych osobowych. W szczególności administrator jest również odpowiedzialny za sprawdzenie ogólnej dopuszczalności i zgodności z prawem przetwarzania i musi wydać wystarczające instrukcje (rozumie się, że sposobem wydania tych instrukcji są przede wszystkim zapisy w umowie lub też to, w jaki sposób będzie realizowane wydawanie instrukcji). Administrator danych osobowych ma więc za zadanie być transparentny wobec osoby, której dane dotyczą, w zakresie przetwarzania danych osobowych tej osoby — por. J. Hartung, [w:] J. Kühling, B. Buchner, *DS-GVO BDSG, art. 25 GDPR*, numer marginesu 66 (Warszawa 2020).

[27] Délibération SAN-2022-009 issued by Commission nationale de l'informatique et des libertés concerning the company DEDALUS BIOLOGIE, dated 5.04.2022, Légifrance.

rzaniu 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 działa 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. Podmiot przetwarzający nie zakwestionował tego naruszenia, twierdził jednak, że nie jest wyłącznie odpowiedzialny, ponieważ art. 28 ust. 3 GDPR nakłada obowiązki zarówno na podmiot przetwarzający, jak i administratora danych, aby taką umowę zawrzeć. Zgodnie z punktem nr 35 oraz 36 decyzji nakładającej karę[28]

> 35. Komisja Ograniczona zauważa, że fakt, iż obowiązek wynikający z art. 28 ust. 3 GDPR ciąży zarówno na administratorze danych, jak i na przetwarzającym, nie ma wpływu na istnienie odpowiedzialności podwykonawcy. Zauważa, że to sama spółka przekazuje laboratoriom swoje własne ogólne warunki sprzedaży, które służą jako ramy umowne zgodnie z RODO. 36. Po drugie, Organ zauważa, że ogólne warunki sprzedaży zaproponowane przez DEDALUS BIOLOGY w momencie, gdy laboratoria przyjmują jej usługę, przekazane przez spółkę w ramach procedury kontrolnej, nie zawierają żadnego z oświadczeń wymaganych przez art. 28 RODO. Podobnie zauważa, że wymagane informacje nie pojawiają się również w umowach o konserwację przesłanych do CNIL, zawartych między przedsiębiorstwem a laboratoriami. Tytułem ilustracji, umowa serwisowa zawarta między NETIKA SAS (dawna nazwa DEDALUS BIOLOGY) a spółką […], w dniu 13 września 2019 roku, z pewnością zawiera część poświęconą danym osobowym, która jednak nie spełnia wymogów art. 28 RODO i odnosi się do nieaktualnych przepisów ustawy o ochronie danych osobowych. Komisja Ograniczona zauważa również, że przykładowa umowa o pomocy i konserwacji, przedstawiona przez spółkę delegacji CNIL podczas kontroli na miejscu w dniu 1 marca 2021 roku, nie zawiera obowiązkowych informacji zgodnie z art. 28 RODO. Jeśli zawiera ona sekcję poświęconą danym osobowym, nie spełnia to wymogów tego artykułu.

Przykład ten pokazuje, że obowiązek wynikający z art. 28 ust. 3 RODO, a konkretnie — zawarcie umowy o powierzeniu danych osobowych pomiędzy podmiotem przetwarzającym a administratorem danych osobowych spoczywa na obu stronach i niewłaściwe jest tutaj doszukiwanie się ograniczenia odpowiedzialności jednej ze stron (w tym konkretnym przypadku chodziło o podmiot przetwarzający), z tego powodu, że druga strona nie wyszła z inicjatywą zawarcia takiej umowy. Obie strony umowy są więc zobowiązane do zawarcia między sobą umowy, zanim takie przetwarzanie danych osobowych nastąpi.

---

[28] Commission nationale de l'informatique et des libertés, Délibération SAN-2022-009 concerning the company DEDALUS BIOLOGIE dated 15.04.2022, Légifrance, pkt 35, 36.

2.3. PRZYKŁAD FIRMY COSMOTE

Kolejny przykład związany jest ze spółką Cosmote Mobile Telecommunications SA będącą częścią grupy firm o nazwie OTE — również w bardzo precyzyjny sposób pokazuje, jak ważne jest zawarcie umowy o powierzeniu danych osobowych między administratorem a podmiotem przetwarzającym dane osobowe.

Grecki Urząd Ochrony Danych (ang. Hellenic Data Protection Authority, dalej: HDPA) opublikował w dniu 31 stycznia 2022 roku decyzję nr 4/2022[29], w której nałożył na Cosmote Mobile Telecommunications SA karę pieniężną w wysokości 6 milionów euro za naruszenie RODO, w następstwie naruszenia danych dotyczącego wycieku danych o połączeniach abonentów. HDPA zważył na to, że Cosmote Mobile Telecommunications SA zgłosiła naruszenie danych do HDPA i w związku z żądaniem HDPA 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 do 5 września 2020 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, rzecz jasna, 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[30].

Brak ustalenia ról oraz dookreślenia celów i sposobów przetwarzania albo przekazania pewnej autonomii podmiotowi przetwarzającemu przekazanych przez administratora danych osobowych co do sposobu przetwarzania danych osobowych

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

[30] *Ibidem*, s. 17–19, 39–40, 43.

czy choćby wstępnych instrukcji przetwarzania danych osobowych w umowie o przetwarzaniu danych osobowych może powodować uznanie podmiotu przetwarzającego jako administratora danych osobowych[31] na bazie art. 28 ust. 10 RODO[32]: „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". W takiej sytuacji, jak wynika z przepisu, wszelka odpowiedzialność podmiotu pozostaje bez zmian, a podmiot przetwarzający traci swój uprzywilejowany status w zakresie odpowiedzialności i podlega wszystkim obowiązkom administratora określonym w RODO[33]. Fakt potrzeby określenia w umowie o przetwarzaniu danych osobowych wyżej określonych kwestii (sposób przetwarzania danych osobowych, cele, instrukcje) w celu zmniejszenia ryzyka — przede wszystkim w kontekście art. 28 ust. 10 RODO — podmiotu przetwarzającego wynika również z tego, co pisze w komentarzu do RODO Marlena Sakowska-Baryła:

> Jeśli natomiast podmiot przetwarzający naruszy ramy dysponowania danymi osobowymi, ingerując w cele i sposoby przetwarzania bez udziału, wiedzy i zgody administratora, i naruszy w ten sposób RODO, jego działanie kwalifikować należy jako niezgodne z prawem, a on sam będzie ponosił odpowiedzialność jak administrator[34],

jak i Paweł Litwiński:

> Natomiast w sytuacji, gdy procesor naruszy tę zasadę i samodzielnie (bez wiedzy i zgody administratora) określi cele i sposoby przetwarzania (bez odpowiedniej podstawy w umowie lub innym akcie prawnym albo też poleceniu wydanym przez administratora), zgodnie z art. 28 ust. 10 RODO taki podmiot przetwarzający będzie ponosił odpowiedzialność jak administrator danych w odniesieniu do tego przetwarzania w sytuacji naruszenia przepisów RODO. Pomimo że polskie tłumaczenie posługuje się sformułowaniem „uznaje się", chodzi jednak nie o zmianę administratora danych, tylko o rozszerzenie zakresu odpowiedzialności procesora[35].

Litwiński również słusznie podkreśla, że zostało to potwierdzone także w polskim orzecznictwie:

> Z powyższego wynika zatem, że strona skarżąca miała dostęp do danych osobowych przetwarzanych w ramach monitoringu wizyjnego w związku z bieżącym administrowaniem nieruchomością, a także decydowała o celach i sposobach przetwarzania danych. Nie wynikało to jednak z umowy o administrowanie częścią wspólną zawartą ze Wspólnotą Mieszkaniową […], z umowy

---

[31] W. Spoerr, [w:] H. Wolff, S. Brink, *BeckOK Datenschutzrecht, Article 28 GDPR*, margin number 104 (Warszawa 2021).

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, art. 28 ust. 10.

[33] W. Spoerr, [w:] H. Wolff, S. Brink, *BeckOK Datenschutzrecht, Article 28 GDPR*, margin number 104.

[34] *Komentarz do artykułu 28 RODO*, red. M. Sakowska-Baryła, Warszawa 2018, Nb 29.

[35] P. Litwiński, *Komentarz do artykułu 28 RODO*, Warszawa 2021, Nb 18.

powierzenia przetwarzania danych osobowych z dnia […] maja 2018 roku, ani z procedur wewnętrznych dotyczących zarządzania systemem monitoringu. Jak już wyżej wskazano, w sytuacji, gdy podmiot przetwarzający dane osobowe naruszy ogólne rozporządzenie o ochronie danych przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (art. 28 ust. 10). Podejmowanie decyzji o celach i sposobach przetwarzania danych należy do sfery uprawnień administratora danych. Jeżeli w tę sferę bezprawnie ingeruje podmiot przetwarzający, wchodząc w zakres zastrzeżony administratorowi, to art. 28 ust. 10 ww. rozporządzenia nakazuje uznać podmiot przetwarzający za administratora w odniesieniu do tego przetwarzania. Oznacza to, że podmiot przetwarzający odpowiada w tym zakresie za naruszenie przepisów rozporządzenia tak jak administrator[36].

Jak widać, wojewódzki sąd administracyjny w przytaczanym powyżej przypadku zaznacza, że strona skarżąca przetwarzała dane osobowe oraz decydowała o celach i sposobach tego przetwarzania danych osobowych w ramach monitoringu, ale nie wynikało to z umowy powierzenia przetwarzania danych osobowych, a w związku z tym uznało się ją jako administratora w odniesieniu do ponoszenia odpowiedzialności — jak wynika z art. 28 ust. 10 RODO. Trzeba więc stwierdzić, że gdyby jednak te czynności wynikały z umowy powierzenia przetwarzania danych osobowych, a więc innymi słowy — była ku temu podstawa w tej umowie lub poleceniu wydanym na podstawie tej umowy, to *a contrario* ocena odpowiedzialności podmiotu przetwarzającego plasowałaby się inaczej, a mianowicie — podmiot ten nie ponosiłby odpowiedzialności tak jak administrator danych osobowych, co *de facto* zminimalizowałoby ryzyko tego podmiotu.

3. PODSUMOWANIE

Oryginalnym wkładem autora niniejszego artykułu było udowodnienie na wybranych przykładach, jak zawarcie umowy o przetwarzaniu danych osobowych w odpowiedni sposób pozwala ograniczyć ryzyko podmiotów biorących udział w przetwarzaniu tych danych. Jak się okazuje, zawarcie umowy o powierzeniu danych osobowych oraz odpowiednich zapisów w tej umowie w znaczący sposób ogranicza odpowiedzialność obu podmiotów, a w szczególności podmiotu przetwarzającego. Bardzo „w punkt" pokazuje to pierwszy przypadek wymieniony w niniejszym artykule, gdzie między innymi w związku z brakiem umowy oraz ustaleniem w niej ról podmiotów WhatsApp Ireland LTD został uznany za administratora danych osobowych, a co za tym idzie — jego odpowiedzialność oraz obowiązki były znacznie szersze, niż gdyby został on uznany za podmiot

[36] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 27 października 2020 roku, II SA/Wa 310/20; P. Fajgielski, [w:] *Komentarz do rozporządzenia nr 2016/679 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)*, Warszawa 2022, art. 28.

przetwarzający. Drugi przypadek wskazuje, że obowiązek zawarcia samej umowy spoczywa na obu stronach. Daje to więc możliwość organowi nadzorczemu, rozumianemu w ujęciu art. 51 RODO, nałożenia kary za brak umowy czy też odpowiednich zapisów w tej umowie zarówno na podmiot przetwarzający, jak i administratora danych osobowych. Trzeci przypadek również podkreśla, jak ważne jest samo zawarcie umowy i odpowiednich zapisów w niej, aby ograniczyć ryzyko — zarówno administratora danych osobowych, jak i podmiotu przetwarzającego. Przykłady te, jak i sama literatura dotycząca analizy RODO, potwierdzają, że zapisy dotyczące umowy o powierzeniu danych osobowych mają niebagatelny wpływ zarówno na odpowiedzialność podmiotu przetwarzającego, jak i administratora. Ograniczeniem badań jest ilość wydanych decyzji przez organy nadzorcze w rozumieniu art. 51 RODO, zważywszy na to, że RODO jest regulacją, która relatywnie niedawno weszła w życie. Perspektywą dalszych badań jest klasyfikacja ryzyk, o których mowa w niniejszym artykule.

RISK IN THE CONTEXT OF THE LIABILITY OF THE DATA CONTROLLER AND DATA PROCESSOR AND THE INCLUSION OF PROVISIONS IN THE DATA PROCESSING AGREEMENT TO LIMIT LIABILITY FOR THE IMPOSITION OF ADMINISTRATIVE FINES UNDER ARTICLE 83 OF THE GDPR

Summary

The article deals with the risks in the context of the responsibility of the data controller and data processor and the connection of these risks to the inclusion of relevant provisions in the personal data processing agreement(s) to limit responsibility for the imposition of administrative penalties under the article 83 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR). At the outset, the paper introduces the concept of the data controller and the data processor and the differences between these entities. Then the issue of the data processing agreement and the consequences of the possible absence of the required provisions or of the agreement itself is addressed. The final section presents an analysis and conclusions as to which reasons relating to data processing agreement have resulted in fines imposed according to the Article 83 of the GDPR.

Keywords: risk versus personal data agreement, provisions in personal data agreement vs. risk, risk vs. GDPR agreements, risks in personal data agreement

BIBLIOGRAFIA

Bertermann N., [w:] E. Ehmann, M. Selmayr, *Datenschutz-Grundverordnung, Article 28 GDPR*, München 2018.

Commission nationale de l'informatique et des libertés, Délibération SAN-2022-009 concerning the company DEDALUS BIOLOGIE dated 15.04.2022, Légifrance.

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

Délibération SAN-2022-009 issued by Commission nationale de l'informatique et des libertés concerning the company DEDALUS BIOLOGIE, dated 5.04.2022, Légifrance.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. UE. L. z 1995 r. Nr 281, s. 31 z późn. zm.).

European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2.09.2020.

European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR*, 12.11.2019.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 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)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

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 roku.

Hartung J., [w:] J. Kühling, B. Buchner, *DS-GVO BDSG*, *C.H. Beck 2020*, Auflage 3, München 2020.

Kamarinou D., [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, Cambridge 2021.

Komentarz do artykułu 28 RODO, red. M. Sakowska-Baryła, Warszawa 2018.

Litwiński P., *Komentarz do artykułu 28 RODO*, Warszawa 2021.

Lubasz D., Chomiczewski W., Czerniawski M., Drobek P., Góral U., Kuba M., Makowski P., Witkowska-Nowakowska K. [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018.

Spoerr W., [w:] H. Wolff, S. Brink, *DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz*, München 2021.

Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.).

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 27 października 2020 roku, II SA/Wa 310/20.