Powierzenie przetwarzania danych osobowych w świetle ogólnego rozporządzenia o ochronie danych

Aleksandra Pyka[1]

Celem niniejszego opracowania jest przedstawienie instytucji powierzenia przetwarzania danych osobowych w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[2], które zostało uregulowane w art. 28. Powołany przepis określa w szczególności wymogi dotyczące wyboru podmiotu przetwarzającego dane na zlecenie, jak również elementy obligatoryjne umowy bądź innego instrumentu prawnego, który regulowałby omawianą instytucję powierzenia przetwarzania danych osobowych.

Uwagi wstępne

Powierzenie przetwarzania danych osobowych nie jest instytucją nową[3], gdyż zostało wprowadzone w art. 31 ustawy z 29.8.1997 r. o ochronie danych osobowych[4], który stanowił, iż administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Obecnie powierzenie przetwarzania danych osobowych zostało znacznie szerzej uregulowane w art. 28 RODO. Jak stanowi ust. 1 tego przepisu, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą (tzw. podmiotów danych). Niniejszy przepis reguluje instytucję powierzenia przetwarzania danych osobowych w świetle stosowanego od 25.5.2018 r. ogólnego rozporządzenia. Powołana podstawa prawna powierzenia przetwarzania danych nie zawiera definicji powierzenia[5]. Celem niniejszej publikacji jest przedstawienie instytucji powierzenia przetwarzania danych w odniesieniu do przepisów ogólnego rozporządzenia, a także w aspekcie praktycznym.

Podmiot, któremu powierzono przetwarzanie

W myśl art. 4 pkt 8 RODO pod pojęciem podmiotu przetwarzającego należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Charakterystyczne dla tego podmiotu jest więc przetwarzanie danych osobowych na zlecenie. Podmiot przetwarzający nie może przetwarzać danych osobowych w innym celu niż wskazany w umowie powierzenia lub innym instrumencie prawnym[6].

Podmiotem przetwarzającym dane osobowe na zlecenie może być zarówno osoba fizyczna (w tym osoba fizyczna prowadząca działalność gospodarczą), osoba prawna (np. spółka prawa handlowego, stowarzyszenie, fundacja), podmiot publiczny (np. Centrum Usług Wspólnych), jak i jednostka lub inny podmiot (w tym tzw. ułomna osoba w myśl art. 331 § 1 KC). Ogólne rozporządzenie wskazuje, iż administrator korzysta z usług podmiotu przetwarzającego. Można postawić tezę, że nie każdy podmiot, który świadczy określone usługi, może być stroną umowy (lub innego instrumentu prawnego) powierzenia przetwarzania danych. Podmiot ten powinien zapewniać wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi ogólnego rozporządzenia, a także chroniło prawa osób, których dane dotyczą. Podmiot przetwarzający nie determinuje procesu przetwarzania danych tak jak administrator (nie ustala celów i sposobów przetwarzania, nie podejmuje samodzielnie decyzji odnośnie do wyboru podmiotu, któremu dane osobowe będą podpowierzone). Administrator oddelegowuje realizację określonej usługi, która wiąże się z przetwarzaniem danych osobowych, podmiotowi cechującemu się profesjonalizmem. Wydaje się również, że nie ma przeszkód, aby współadministratorzy powierzyli przetwarzanie danych jednemu podmiotowi. Prawodawca wskazał, iż „administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających,

[1] Autorka jest inspektorem ochrony danych w Katolickim Uniwersytecie Lubelskim Jana Pawła II, koordynatorem ds. ochrony danych osobowych w Towarzystwie Przyjaciół KUL oraz doktorantką na Wydziale Prawa, Prawa Kanonicznego i Administracji KUL.

[2] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO lub rozporządzenie ogólne.

[3] *P. Litwiński*, *P. Barta*, *M. Kawecki*, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, s. 473.

[4] Dz.U. z 2016 r. poz. 922 ze zm.

[5] *K. Witkowska-Nowakowska*, Podmiot przetwarzający, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 634.

[6] *J. Sobczak*, Dane osobowe przetwarzane w chmurze obliczeniowej, Informacja w Administracji Publicznej 2017, Nr 2, s. 34.

które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania" (motyw 81 preambuły ogólnego rozporządzenia). W tym miejscu należy dodać, że art. 32 RODO – dotyczący bezpieczeństwa przetwarzania – stanowi *explicite*, że zapewnienie odpowiednich środków technicznych i organizacyjnych (celem zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku przetwarzania) jest również obowiązkiem podmiotu przetwarzającego dane na zlecenie. Podmiot ten nie powinien zatem wyłącznie opierać się na zaleceniach administratora, lecz każdorazowo analizować, czy istotnie wdrożone środki techniczne i organizacyjne zapewniają odpowiedni poziom bezpieczeństwa. Stwierdzenie naruszenia ochrony danych, które nastąpiło w wyniku działania bądź zaniechania podmiotu przetwarzającego po zawarciu umowy powierzenia przetwarzania (lub innego instrumentu prawnego), nie może prowadzić do kwestionowania wyboru ww. podmiotu przez administratora w kontekście niespełniania kryterium „profesjonalizmu". Jak wskazuje się w piśmiennictwie, „nie sposób zgodzić się z tego rodzaju wnioskowaniem, gdyż oznaczałoby to sprowadzenie sprawdzenia statusu podmiotu, któremu administrator zamierza powierzyć przetwarzanie, do dokonywania oceny jego postępowania po zawarciu umowy (z perspektywy ewentualnych naruszeń), a w konsekwencji prowadziłoby do możliwości zakwestionowana profesjonalnego statusu praktycznie wobec każdego podmiotu, który przed zawarciem umowy oceniony został jako podmiot zapewniający odpowiednie zabezpieczenie przetwarzanych danych"[7].

Warto nadmienić, że powierzenie przetwarzania danych osobowych nie wymaga zgód osób, których dane dotyczą[8]. Niemniej realizując obowiązek informacyjny, administrator – na podstawie art. 13 ust. 1 lit. e) oraz art. 14 ust. 1 lit. e) RODO – jest zobowiązany poinformować o odbiorcach danych lub kategoriach odbiorców, jeżeli istnieją. Odwołując się do słownika pojęć zawartego w art. 4 pkt 9 RODO – podmiot przetwarzający dane na zlecenie jest odbiorcą danych, choć nie wynika to literalnie z samej definicji odbiorcy.

Posługiwanie się przez prawodawcę zwrotem „podmiot przetwarzający" może nasuwać wątpliwości interpretacyjne[9]. Pod tym pojęciem rozumieć można zarówno osoby przetwarzające dane z polecenia administratora (*vide* art. 29 RODO), jak i inne podmioty, które w operacjach przetwarzania danych osobowych odgrywają określoną rolę (w tym inni odbiorcy oraz organy publiczne, którym udostępniono dane w ramach konkretnego postępowania zgodnie z prawem UE lub prawem państwa członkowskiego).

Stosunku powierzenia przetwarzania danych osobowych nie należy pojmować jako formy zależności bądź podległości. W przypadku gdy dojdzie do powierzenia przetwarzania danych osobowych, podmiot ten może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający (*vide* art. 28 ust. 3 lit. a RODO). Decyzyjność w relacjach powierzenia przetwarzania danych jest charakterystyczna przede wszystkim dla administratora. Podmiot przetwarzający dane na zlecenie może jednak niezwłocznie poinformować administratora, że w jego ocenie wydane polecenie stanowi naruszenie ogólnego rozporządzenia bądź innych przepisów Unii lub państwa członkowskiego o ochronie danych.

Obowiązki podmiotu, któremu powierzono przetwarzanie

Podmiot przetwarzający dane na zlecenie jest obowiązany do identyfikowania ryzyka związanego z przetwarzaniem danych osobowych, a także stosowania odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Prawodawca dostrzegł potrzebę określenia obowiązków spoczywających również na podmiocie przetwarzającym, o czym stanowi motyw 79 preambuły RODO: „Ochrona praw i wolności osób, których dane dotyczą, oraz 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 (...)". Ponadto podmiot przetwarzający jest zobowiązany informować administratora o obowiązku przekazania danych do państwa trzeciego lub organizacji międzynarodowej, jeżeli wynika to z przepisów prawa UE lub prawa państwa członkowskiego (art. 28 ust. 3 RODO). Każdy podmiot przetwarzający dane na zlecenie jest zobowiązany prowadzić zgodnie z art. 30 ust. 2 RODO rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

[7] *P. Fajgielski*, Glosa do wyroku SN z 1.6.2017 r., CSK 597/16, OSP 2018, Nr 10.

[8] Takie stanowisko podniósł organ nadzorczy (GIODO – obecnie PUODO) w sprawie toczącej się przed WSA w Warszawie (wyrok z 20.12016 r., II SA/Wa 1190/15, Legalis).

[9] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 342.

Wymogi dotyczące treści umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego

Ogólne rozporządzenie – w przeciwieństwie do ustawy z 1997 r. – określa dosyć istotne wymogi dotyczące treści umowy powierzenia przetwarzania danych osobowych lub innego instrumentu, w ramach którego administrator powierza przetwarzanie. Obowiązująca przez przeszło 20 lat ww. ustawa wskazywała w art. 31 obligatoryjne elementy umowy powierzenia, do których zaliczyć należało zakres i cel przetwarzania. Obecnie ogólne rozporządzenie znacząco rozbudowało obligatoryjne wymogi dotyczące treści powierzenia. Umowa bądź inny instrument prawny (porozumienie administracyjne, ogólne warunki ubezpieczenia etc.)[10] powinny zawierać postanowienia dotyczące przedmiotu i czasu trwania przetwarzania, jego charakteru i celu, rodzaju danych osobowych, a także kategorii osób, których dane dotyczą, oraz obowiązków i praw administratora (*vide* art. 28 ust. 3 RODO). Prawodawca określił również enumeratywny katalog postanowień, które powinny być obligatoryjnie zawarte w umowie lub innej formie powierzenia. Mając na uwadze treść ww. normy prawnej, można stwierdzić, że elementy obligatoryjne stanowią swoistego rodzaju *essentialia negotii*, które powinny być zawarte w umowie o charakterze cywilnoprawnym, lecz również w każdej innej formie (w tym w porozumieniu administracyjnym).

Powierzając przetwarzanie danych osobowych, administrator powinien zobowiązać procesora do przetwarzania danych jedynie na udokumentowane polecenie. Odnosi się to również do przekazywania danych poza teren Europejskiego Obszaru Gospodarczego. Podmiot przetwarzający dane na zlecenie jest jednak zwolniony z konieczności działania z polecenia, jeśli obowiązek przetwarzania danych wynika z prawa UE bądź państwa członkowskiego, któremu podlega ten podmiot. Przetwarzanie na podstawie udokumentowanego polecenia administratora wzmacnia rolę podmiotu, który ustala cele i sposoby przetwarzania danych, tym samym znacząco ograniczając autonomiczność procesora. Powierzenie przetwarzania danych osobowych uregulowane w określonej formie prawnej powinno odnosić się również do kwestii środków technicznych i organizacyjnych. Podmiot przetwarzający dane osobowe na zlecenie jest zobowiązany do podjęcia wszelkich środków wymaganych na mocy art. 32 RODO, tj. zabezpieczeń adekwatnych do ryzyka związanego z przetwarzaniem danych osobowych. Jak stanowi art. 28 ust. 3 lit. e) RODO, procesor powinien w miarę swych możliwości pomagać administratorowi wywiązać się z obowiązku realizowania uprawnień osób, których dane dotyczą – określonych w rozdziale III. Ogólne rozporządzenie nie wskazuje, czy świadczenie pomocy przez podmiot przetwarzający ma charakter odpłatny, jednak wydaje się, że nie ma przeszkód, aby kwestię dotyczącą wypłaty ekwiwalentu pieniężnego uregulować szczegółowo w samej umowie powierzenia przetwarzania danych lub w innym instrumencie prawnym, zwłaszcza w sytuacji gdy wsparcie ze strony podmiotu przetwarzającego może znacząco wpływać na działalność tego podmiotu. Podmiot, któremu powierzono przetwarzanie danych osobowych, jest zobowiązany pomagać administratorowi również w wypełnianiu obowiązków określonych w art. 32–36 RODO. Umowa lub inny instrument prawny powinny regulować również kwestię zakończenia współpracy pomiędzy procesorem a administratorem w zakresie dotyczącym zwrotu danych osobowych lub ich usunięcia. Postanowienia umowy odmienne od przepisów prawa UE lub prawa państwa członkowskiego dotyczącego dalszego przetwarzania danych po zakończeniu korzystania z usług procesora będą nieważne, a odpowiednie zastosowanie znajdą właściwe regulacje normatywne. Warto wskazać w formie przykładu przepis ustawodawstwa krajowego, który wyłącza swobodę uregulowania zakończenia współpracy pomiędzy administratorem a podmiotem przetwarzającym dane na zlecenie. Zgodnie z art. 24 ust. 7 ustawy z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[11], w przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, określonemu w ust. 1, który powierzył przetwarzanie danych osobowych[12]. Wyłączona zostaje zatem *ex lege* możliwość usunięcia danych osobowych.

Forma powierzenia przetwarzania danych osobowych

Warto zwrócić uwagę na tezę przedstawioną w piśmiennictwie na gruncie ustawy o ochronie danych osobowych z 1997 r., według której „Umowa w sprawie powierzenia przetwarzania danych innemu podmiotowi nie została w przepisach Ustawy [z 1997 r. o ochronie danych osobowych] sprecyzowana odnośnie do jej rodzaju. Brak także szczególnej regulacji tej umowy w przepisach prawa cywilnego. Ten stan prawny zostawia swobodę wyboru, ale wydaje się, że umowa

[10] Warto zwrócić uwagę, iż w doktrynie pojawiło się stanowisko, zgodnie z którym pod pojęciem innego instrumentu prawnego rozumieć należy również tzw. delegację ustawową. Zob. *M. Ujejski*, Ukształtowanie wzajemnych stosunków administratorów i procesorów w ramach administracji publicznej, Informacja w Administracji Publicznej 2018, Nr 1, s. 21.

[11] T.j. Dz.U. z 2019 r. poz. 1127 ze zm.

[12] *M. Kamiński*, Powierzenie przetwarzania osobowych danych medycznych a perspektywy prowadzenia dokumentacji medycznej w postaci elektronicznej, Prawo Mediów Elektronicznych 2008, Nr 8, s. 7.

powierzająca przetwarzanie danych osobowych powinna być kwalifikowana jako umowa o świadczenie usług, nienormowana w sposób szczególny"[13]. Powierzenie przetwarzania danych może nastąpić niewyłącznie w formie postanowienia zawartego w nienazwanej umowie o świadczenie usług. Równie właściwą formą będzie zawarcie w pełni odrębnej umowy powierzenia przetwarzania danych, która ma charakter akcesoryjny w stosunku do umowy o świadczenie usług. Zarówno z perspektywy prawa cywilnego przyjęcie formy aneksu, jak i odrębnej umowy powierzenia przetwarzania danych nie wiąże się z żadnymi reperkusjami. Warto nadmienić, iż budzi wątpliwość twierdzenie, według którego dopuszczalne jest aneksowanie umowy zawartej w wyniku udzielenia zamówienia publicznego w trybie ustawy z 29.1.2004 r. – Prawo zamówień publicznych[14]. W sytuacji gdy w umowie o świadczenie usług nie zawarto postanowień dotyczących powierzenia przetwarzania danych osobowych, wątpliwe jest zawarcie aneksu do tejże umowy. Właściwe będzie argumentowanie, że powierzenie przetwarzania w formie aneksu narusza treść art. 144 ust. 1 PrZamPubU (dot. zmian postanowień zawartej umowy lub umowy ramowej w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy). Nie ma natomiast przeszkód, aby aneksować inne umowy, które nie zostały zawarte w wyniku udzielenia zamówienia publicznego przeprowadzonego na podstawie ustawy Prawo zamówień publicznych, jeśli przepisy nie stanowią inaczej. Dla potwierdzenia słuszności tej tezy warto odnieść się do orzecznictwa sądów administracyjnych. Jak wynika z tezy wyroku WSA w Krakowie z 28.2.2018 r.[15]: „art. 144 ust. 1 PrZamPubU nie wskazuje, jakie zmiany umowy w sprawie zamówienia publicznego należy traktować jako istotne, jednak zmiana zamówienia publicznego w czasie jego trwania może być uznana za istotną, jeżeli wprowadza ona warunki, które – gdyby zostały ujęte w ramach pierwotnej procedury udzielania zamówienia – umożliwiłyby dopuszczenie innych oferentów niż ci, którzy zostali pierwotnie dopuszczeni, lub umożliwiłyby dopuszczenie innej oferty niż ta, która została pierwotnie dopuszczona". Mając na uwadze powyższe, należy zwrócić uwagę, iż taka wykładnia art. 144 ust. 1 PrZamPubU może wywoływać wątpliwości interpretacyjne. Problematyka dotyczy sytuacji, w której w drodze aneksu zamawiający wraz z wykonawcą uregulowaliby postanowienia dotyczące powierzenia, przy czym wykonawca, jako podmiot przetwarzający dane na zlecenie, nie spełniałby choćby kryterium z art. 28 ust. 3 lit. c RODO (podjęcie wszelkich środków – technicznych i organizacyjnych – wymaganych na mocy art. 32), czy też korzysta z usług innego podmiotu przetwarzającego, który nie zapewnia przestrzegania m.in. warunków dotyczących stosowania odpowiednich środków technicznych i organizacyjnych. Istotna byłaby zatem zmiana wprowadzona w formie aneksu w postaci powierzenia przetwarzania danych wówczas, gdy pozostali oferenci (pierwotnie dopuszczeni) spełnialiby kryteria określone w ogólnym rozporządzeniu. Oznacza to, iż dopuszczalność aneksowania umowy o świadczenie usług zawartej w trybie określonym w ww. ustawie nie jest jednoznaczna. Ponadto „za niedopuszczalne na gruncie prawa zamówień publicznych w związku z treścią art. 140 PrZamPubU należy, o czym wspominano szeroko wcześniej, uznać wszelkie zmiany do umowy powodujące rozszerzenie zakresu świadczenia wykonawcy poza zakres określony w przedmiocie zamówienia"[16].

Według art. 28 ust. 9 RODO „umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną"[17]. Forma pisemna (bądź elektroniczna) nie została zastrzeżona przez prawodawcę unijnego dla celów dowodowych (*ad probationem*). Niedochowanie rygoru zastrzeżenia formy szczególnej – pisemnej lub elektronicznej – skutkować będzie nieważnością umowy (*ad solemnitatem*). Zmiana postanowień umowy, wypowiedzenie czy też rozwiązanie umowy powierzenia przetwarzania danych osobowych powinno również nastąpić w formie pisemnej lub elektronicznej, choć nie wynika to wprost ze wskazanego powyżej przepisu. Odnosząc się do nieważności czynności prawnej, warto nadmienić, iż wątpliwości może budzić także zawieranie umów powierzenia przetwarzania danych osobowych z mocą wsteczną (retroaktywnie) – zarówno w formie aneksu, jak i odrębnej umowy. Ogólne rozporządzenie nie odnosi się jednak do zawierania umów powierzenia przetwarzania danych osobowych z mocą wsteczną.

W przypadku podmiotów publicznych (tj. w relacji pomiędzy tymi podmiotami) powierzenie przetwarzania nie może nastąpić w formie umowy cywilnoprawnej[18]. Zawarcie w świetle Kodeksu cywilnego umowy nienazwanej nie ma zastosowania w stosunkach pomiędzy podmiotami prawa administracyjnego. Kodeks cywilny reguluje stosunki cywilnoprawne między osobami fizycznymi a osobami prawnymi (*vide* art. 1 KC). W tym przypadku właściwe jest powierzenie

[13] *R. Golat*, Przekazywanie przez pracodawców przetwarzania danych osobowych innym podmiotom, Sł. Prac. 2011, Nr 8, s. 11–14.

[14] T.j. Dz.U. z 2019 r. poz. 1843 ze zm.; dalej jako: PrZamPubU.

[15] I SA/Kr 930/17, Legalis.

[16] *J. Olszewska-Stompel*, *M. Stompel*, Prawo zamówień publicznych. Wybór najkorzystniejszej oferty i zawieranie umów, Lex/el. 2013.

[17] Zawarcie umowy w formie ustnej nie spełnia wymogu określonego w art. 28 ust. 9 RODO. Warto nadmienić, że zagadnienie to było poruszane także na gruncie dotychczas obowiązującej ustawy z 1997 r. o ochronie danych osobowych. Zob. *D. Fleszer*, Zakres przetwarzania danych osobowych w działalności gospodarczej, Warszawa 2008, s. 238 i 239.

[18] Warto poczytać szerzej na temat powierzenia przetwarzania pomiędzy podmiotami publicznymi na gruncie ustawy z 1997 r. o ochronie danych osobowych. Zob. *P. Barta*, Powierzenie przetwarzania danych osobowych w sektorze publicznym po zmianach w ustawie o ochronie danych osobowych wprowadzonych ustawą 500+, Informacja w Administracji Publicznej 2016, Nr 2, s. 43–47. Zob. *T. Osiej*, Dopuszczalność zawierania umów powierzenia przetwarzania danych osobowych w administracji publicznej, Informacja w Administracji Publicznej 2015, Nr 3, s. 25–27.

przetwarzania danych osobowych w drodze porozumienia administracyjnego[19].

Podpowierzenie

Na gruncie poprzednio obowiązującej ustawy nie uregulowano instytucji podpowierzenia, jednak nie stanowiło to przeszkody, aby taka konstrukcja była stosowana. Aktualna pozostaje definicja podpowierzenia przytoczona przez *G. Sibigę*, który wskazuje, że „przez podpowierzenie przetwarzania danych osobowych będziemy rozumieli sytuację, w której podmiot, któremu powierzono przetwarzanie danych na podstawie art. 31 OchrDanOsobU (przetwarzający, *processor*), dalej powierza ich przetwarzanie kolejnemu podmiotowi lub podmiotom (podwykonawca, *subprocessor*)"[20]. Jak stanowi 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". Korzystanie z usług innego podmiotu przez procesora nie jest dozwolone. Przesłanką wyłączającą zakaz podpowierzenia jest szczegółowa lub ogólna zgoda wyrażona przez administratora. Niekiedy postanowienia umowne wskazują, że formą akceptacji ze strony administratora jest niewniesienie sprzeciwu w przeciągu określonego czasu (np. 7 dni). Administrator kształtuje strukturę powierzenia poprzez dobór podmiotu przetwarzającego dane na zlecenie oraz podmiotu, któremu podpowierzono przetwarzanie. Niemniej odpowiedzialność za przetwarzanie podpowierzonych danych osobowych spoczywa na procesorze, o czym była mowa wyżej. Warto nadmienić, że niedopuszczalne są postanowienia umowy, według których odpowiedzialność za działania lub zaniechania podmiotu, któremu podpowierzono przetwarzania danych, spoczywa na administratorze. W przypadku scedowania ww. odpowiedzialności w drodze postanowień umowy lub innego instrumentu prawnego tracą one swą moc, a tym samym zastosowanie znajduje wskazany powyżej art. 28 ust. 4 RODO. Należy podać w wątpliwość stwierdzenie, że „z podpowierzeniem nie będziemy mieli natomiast do czynienia w sytuacji, gdy administratora danych łączy bezpośrednia umowa z podwykonawcą, obok umowy z przetwarzającym, którego też łączy umowa z podwykonawcą"[21]. Oznacza to, że realizując określone zadanie w imieniu administratora, podmiot przetwarzający nie mógłby podpowierzyć przetwarzania danych podmiotowi, z którym administrator zawarł bezpośrednio umowę. Eliminowałoby to zatem z obrotu – w konstrukcji podpowierzenia – podmioty, którym już powierzono przetwarzanie danych. *Subprocessor* musiałby dysponować wiedzą, którym podmiotom administrator powierzył przetwarzanie danych.

Odpowiedzialność podmiotu przetwarzającego na zlecenie

Administrator nie ponosi już odpowiedzialności za działania (bądź zaniechania) podmiotu przetwarzającego na zlecenie dane osobowe, gdyż procesor może również być adresatem decyzji wydanej przez Prezesa Urzędu Ochrony Danych Osobowych[22]. Odpowiedzialność podmiotu przetwarzającego nie jest zatem ograniczona do odpowiedzialności cywilnej z tytułu niewykonania lub nienależytego wykonania umowy (w przypadku umów cywilnoprawnych), lecz dotyczy również odpowiedzialności za niezgodne z prawem przetwarzanie danych (obszar prawa administracyjnego), a także odpowiedzialności karnej na gruncie ustawy z 10.5.2018 r. o ochronie danych osobowych[23]. Powierzenie procesorowi przetwarzania danych osobowych zwalnia administratora z odpowiedzialności spoczywającej na tym podmiocie na gruncie ogólnego rozporządzenia. W zasadzie odpowiedzialność ta zostaje scedowana na podmiot przetwarzający. Odmiennie kształtuje się odpowiedzialność za podpowierzenie przetwarzania danych osobowych. Zgodnie z art. 28 ust. 4 RODO „jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym". Korzystając z metody prawnoporównawczej, z całą pewnością można stwierdzić, że kwestia uregulowania obowiązków spoczywających na procesorze została znacznie szerzej uregulowana w ogólnym rozporządzeniu, aniżeli było to w poprzednim stanie prawnym[24].

[19] W nawiązaniu do poczynionych uwag warto nadmienić, że zgodnie z wyrokiem NSA z 6.7.2004 r. (FSK 228/04, Legalis) „Przepisy prawa cywilnego regulują stosunki cywilnoprawne pomiędzy osobami fizycznymi i osobami prawnymi. Nie znajdują one zastosowania dla oceny skuteczności czynności jakie podejmują organy egzekucyjne w wykonawczym postępowaniu podatkowym, a więc postępowaniu o charakterze publicznoprawnym".

[20] *G. Sibiga*, Podpowierzenie przetwarzania danych osobowych, MoP 2012, Nr 7, s. 31.

[21] *J. Byrski*, Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46 i w ogólnym rozporządzeniu o ochronie danych, MoP 2016, Nr 20, s. 36–37.

[22] *P. Litwiński*, Ochrona danych osobowych w ogólnym postępowaniu administracyjnym, Warszawa 2009, s. 109.

[23] T.j. Dz.U. z 2019 r. poz. 1781 ze zm.

[24] Dla przykładu można odnieść się do poprzednio obowiązującej ustawy z 1997 r. o ochronie danych osobowych. Zob. Obowiązki przy powierzeniu przetwarzania danych [w:] *M. Krekora*, *M. Świerczyński*, *E. Traple*, Prawo farmaceutyczne. Zagadnienia regulacyjne i cywilnoprawne, Warszawa 2008, s. 208–209.

W piśmiennictwie podkreślana jest również odpowiedzialność cywilnoprawna podmiotu przetwarzającego dane na zlecenie, gdyż „(…) można stwierdzić, że naruszenie przepisów RODO może w szczególności narazić procesora na roszczenia (w tym odszkodowawcze na podstawie przepisów powszechnego prawa cywilnego o deliktach) w związku z naruszeniem dóbr osobistych (prawa do prywatności) podmiotu danych”[25].

Z całą pewnością należy zanegować możliwość przeniesienia administracyjnej kary pieniężnej nałożonej na administratora lub podmiot przetwarzający dane na zlecenie przez Prezesa Urzędu Ochrony Danych Osobowych w drodze decyzji administracyjnej, jako jedno z postanowień umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego. Wydaje się, że nie jest również dopuszczalne uregulowanie w umowie powierzenia przetwarzania możności zwolnienia z administracyjnej kary pieniężnej nawet przed wydaniem decyzji administracyjnej przez organ nadzorczy. Warto przy tym nadmienić, że administracyjne kary pieniężne nakładane mogą być jedynie w zależności od okoliczności każdego indywidualnego przypadku (art. 83 ust. 2 RODO). Niekiedy w umowach powierzenia przetwarzania danych pojawiają się stwierdzenia, że administrator ponosi wyłączną odpowiedzialność za określenie celów i sposobów, w jakich dane osobowe są lub mają być przetwarzane. Tak sformułowane postanowienie umowy jest niezgodne z art. 28 ust. 10 RODO, że bez uszczerbku dla art. 82, 83 i 84 RODO, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Centrum Usług Wspólnych jako podmiot publiczny przetwarzający dane na zlecenie

Centrum Usług Wspólnych jako jednostka obsługująca może być utworzona m.in. na podstawie art. 10a ustawy z 8.3.1990 r. o samorządzie gminnym[26], który stanowi, iż „Gmina może zapewnić wspólną obsługę, w szczególności administracyjną, finansową i organizacyjną: 1) jednostkom organizacyjnym gminy zaliczanym do sektora finansów publicznych, 2) gminnym instytucjom kultury, 3) innym zaliczanym do sektora finansów publicznych gminnym osobom prawnym utworzonym na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego – zwanym dalej „jednostkami obsługiwanymi”. W świetle art. 10b ust. 1 SamGminU wspólną obsługę może prowadzić m.in. jednostka organizacyjna gminy, która w ramach realizacji zadań związanych ze wspólną obsługą administracyjną, finansową i organizacyjną, może przetwarzać dane osobowe. Centrum Usług Wspólnych, jako jednostka obsługująca, będzie przetwarzać dane osobowe jako podmiot, któremu powierzono przetwarzanie danych osobowych, jednakże jest to tzw. ustawowe powierzenie przetwarzanie danych. Wykonywanie ww. zadań nie będzie wymagało zawarcia odrębnego porozumienia administracyjnego regulującego kwestie powierzenia przetwarzania danych osobowych. Ogólne rozporządzenie nie definiuje pojęcia „innego instrumentu prawnego”, niemniej art. 10d SamGminU stanowiący, iż „jednostka obsługująca jest uprawniona do przetwarzania danych osobowych przetwarzanych przez jednostkę obsługiwaną w zakresie i celu niezbędnych do wykonywania zadań w ramach wspólnej obsługi tej jednostki”, należy zakwalifikować jako „inny instrument prawny”. W formie przykładu warto wskazać, iż Centrum Usług Wspólnych będzie legitymowało się statusem podmiotu przetwarzającego dane na zlecenie m.in. wówczas, gdy będzie przetwarzać dane osobowe na potrzeby prowadzenia dokumentacji związanej z dowozem niepełnosprawnych dzieci do szkół. Zgodnie z art. 39 ust. 4 ustawy z 14.12.2016 r. – Prawo oświatowe[27] obowiązkiem gminy jest zapewnienie bezpłatnego transportu i opieki w czasie przewozu do szkoły uczniom niepełnosprawnym. Jest to zadanie własne gminy, a realizacja zadania w postaci prowadzenia dokumentacji związanej z obowiązkiem zapewnienia bezpłatnego transportu do szkół uczniom niepełnosprawnym może być powierzona jednostce obsługującej. Podmiot ten stanie się wówczas podmiotem przetwarzającym dane na zlecenie.

Podsumowanie

Powierzenie przetwarzania danych osobowych – jak już wskazano na początku – nie jest instytucją nową. W zupełności nieprawidłowe jest twierdzenie, że powierzenie zostało uregulowane dopiero w ogólnym rozporządzeniu. Ten akt normatywny nie zmienił znacząco istoty powierzenia przetwarzania danych osobowych. Analizując przepisy, można jedynie stwierdzić, iż prawodawca unijny znacznie szerzej uregulował tę instytucję. Mając na uwadze całokształt uwag poczynionych w niniejszym artykule, należy nadmienić, że umowa powierzenia lub inny instrument prawny nie mogą zawierać postanowień mających na celu wyeliminowanie bądź obejście przepisów ogólnego roz-

[25] *M. Gomularz*, *E. Laskowska*, Wpływ ogólnego rozporządzenia o ochronie danych na zasady prowadzenia baz danych – problemy praktyczne na styku prawa prywatnego i publicznego, [w:] Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, *M. Kawecki*, *T. Osieja* (red.), Warszawa 2017, s. 86.

[26] T.j. Dz. U. z 2019 r. poz. 506 ze zm.; dalej jako: SamGminU.

[27] T.j. Dz.U. z 2019 r. poz. 1148 ze zm.

porządzenia. Z rozwagą należy również analizować, czy istotnie określony stosunek można zakwalifikować jako powierzenie przetwarzania danych osobowych, gdyż niesie to za sobą daleko idące konsekwencje, jak przykładowo możliwość przeprowadzania audytów czy inspekcji przez administratora.

Słowa kluczowe: RODO, administrator, procesor, przetwarzanie, dane osobowe.

Entrusting the processing of personal data in the light of GDPR

The purpose of this article is to present the institution of entrusting the processing of personal data in the light of regulation of the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of protection of natural persons in regard to processing of personal data and free movement of such data and repealing Directive 95/46/EC (GDPR), which has been regulated in article 28. Directive specifies requirements regarding election of an entity to process data on request, and also obligatory elements of a contract, or another legal instrument, which would regulate the institution in question of entrusting the processing of personal data.

Keywords: GDPR, controller, processor, processing, personal data.