4 istotne obszary, na które administrator powinien zwrócić szczególną uwagę przy powierzeniu przetwarzania danych

Czym jest powierzenie przetwarzania danych osobowych?

Z powierzeniem przetwarzania danych osobowych mamy do czynienia w sytuacji, w której podmiot będący administratorem danych osobowych powierza podmiotowi zewnętrznemu (podmiotowi przetwarzającemu) przetwarzanie danych w związku z realizacją przez ten podmiot określonych usług na rzecz administratora, takich jak np. rachunkowość, archiwizacja dokumentów, IT, monitoring, w określonych przypadkach rekrutacja pracowników na rzecz administratora.

RODO[1] nie zawiera definicji powierzenia przetwarzania danych osobowych. Jego istota została jednak ujęta w art. 28 ust. 1 RODO, zgodnie z którym *„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 niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą”.* Podmiot zewnętrzny nie decyduje, w przeciwieństwie do administratora, o celach i sposobach przetwarzania danych osobowych, a przetwarzanie danych osobowych przez ten podmiot, w ramach powierzenia, dokonywane jest w imieniu administratora.

Obowiązki administratora

1) Weryfikacja kontrahenta

Administrator przy wyborze podmiotu, któremu zleca wykonanie określonej usługi musi kierować się nie tylko rzetelnością świadczonej w konkretnym obszarze usługi, lecz przede wszystkim zapewnieniem przez taki podmiot wystarczających gwarancji spełnienia wymogów RODO i ochrony praw osób, których dane dotyczą. W jaki sposób administrator może sprostać temu obowiązkowi? Administrator powinien przeprowadzić audyt ww. podmiotu np. poprzez wysłanie ankiety lub kwestionariusza weryfikacyjnego, w ramach której podmiot zewnętrzny udzieli informacji w odniesieniu do kluczowych kwestii związanych z zapewnieniem bezpieczeństwa przetwarzania danych osobowych, takich jak np. przyjęte i obowiązujące polityki ochrony danych osobowych, udzielenie pracownikom i współpracownikom posiadającym dostęp do danych osobowych stosownych upoważnień, zobowiązanie ww. osób do zachowania poufności, rodzaje systemów i sposób zabezpieczania danych osobowych w środowisku teleinformatycznym, sposób fizycznego przechowywania dokumentów, czy np. stosowana jest tzw.

[1] 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 RODO)

„zasada czystego biurka” – to tylko niektóre przykładowe elementy, które powinien zawierać formularz weryfikacyjny kontrahenta.

2) Podpisanie umowy powierzenia przetwarzania danych osobowych

Kolejnym etapem, oprócz zawarcia umowy głównej o świadczenie konkretnej usługi, jest zawarcie umowy powierzenia przetwarzania danych osobowych. Umowa taka najczęściej stanowi umowę odrębną w stosunku do umowy głównej. W praktyce zdarzają się jednak sytuacje, kiedy umowa powierzenia jest częścią umowy o świadczenie konkretnej usługi.

Zgodnie z art. 28 ust. 3 RODO, *„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, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, prawa i obowiązki i prawa administratora.”*

W świetle RODO, umowa powierzenia powinna mieć formę pisemną, w tym formę elektroniczną (przy czym RODO nie definiuje formy elektronicznej) oraz stanowić, że zewnętrzny podmiot wykonujący daną usługę (podmiot przetwarzający):

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (co dotyczy także przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej);
b) zapewnia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub aby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki dotyczące bezpieczeństwa przetwarzania danych osobowych;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mówi RODO, w tym podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora; zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych było zgodne z RODO;
e) w miarę możliwości pomaga administratorowi (z uwzględnieniem charakteru przetwarzania), poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
f) pomaga administratorowi wywiązać się z obowiązków określonych w RODO z uwzględnieniem charakteru przetwarzania oraz dostępnych mu informacji;
g) po zakończeniu świadczenia usług, które dotyczą przetwarzania, usuwa lub zwraca administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie (chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych);
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków wynikających z RODO oraz umożliwia

administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Powyższy katalog obowiązków podmiotu przetwarzającego ma charakter otwarty. Z punktu widzenia zabezpieczenia interesu administratora, umowa powierzenia w sposób szczegółowy i wyczerpujący powinna określać obowiązki leżące po stronie podmiotu przetwarzającego, a także uprawnienia przysługujące administratorowi.

3) Bieżąca weryfikacja kontrahenta

Administrator jako podmiot odpowiedzialny za bezpieczeństwo przetwarzania danych osobowych, w tym współpracę z kontrahentem, zapewniającym wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO, powinien weryfikować kontrahenta nie tylko przed nawiązaniem współpracy, lecz także w jej trakcie.

4) Prowadzenie rejestru umów powierzenia

Rejestr umów powierzenia może ułatwić administratorowi zarządzanie procesem powierzenia przetwarzania danych osobowych, a tym samym ułatwić wywiązanie się z obowiązków wynikających z RODO, w szczególności w sytuacji, w której administrator ma zawarte umowy powierzenia z wieloma podmiotami przetwarzającymi.

Emilia Dudzińska – specjalista ds. ochrony danych osobowych