Warszawa, 10.10.2022 r.

Powierzenie przetwarzania danych należy udokumentować – wnioski z kolejnej kary nałożonej przez UODO

UODO nałożył administracyjną karę pieniężną w kwocie 2,5 tys. zł na Sułkowicki Ośrodek Kultury. Powodem było powierzenie przetwarzania danych osobowych bez zawartej na piśmie umowy powierzenia oraz bez przeprowadzenia weryfikacji podmiotu przetwarzającego w zakresie oceny, czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych.

W toku postępowania wyjaśniającego prowadzonego przez UODO ustalono, że administrator powierzył przetwarzanie danych podmiotowi przetwarzającemu bez zawarcia stosownej umowy regulującej taką formę współpracy. Podmiot przetwarzający miał świadczyć na zlecenie administratora usługi polegające na prowadzeniu ksiąg rachunkowych, ewidencji i sporządzania raportów czy przechowywania dokumentacji. Zdaniem UODO błąd w nawiązaniu tej współpracy biznesowej nie polegał tylko na barku zawarcia umowy powierzenia, ale również braku przeprowadzenia weryfikacji podmiotu przetwarzającego.

UMOWA POWIERZENIA ORAZ WERYFIKACJA PODMIOTU PRZETWARZAJĄCEGO

Stosownie do art. 28 RODO[1] *jeżeli przetwarzanie ma być dokonywane w mieniu 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.* Ponadto *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 przetwarzani, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, prawa i obowiązki i prawa administratora.* ***Umowa lub inny akt prawny mają formę pisemną, w tym formę elektroniczną.***

Odpowiedzialność za wybór podmiotu przetwarzającego spoczywa na administratorze danych. To on, wiedząc, jakie dane zamierza powierzyć do przetwarzania podmiotowi trzeciemu oraz jakie operację będą przez taki podmiot wykonywane na danych, powinien tak zweryfikować podmiot aby mieć pewność, iż będzie on zapewniał odpowiednie bezpieczeństwo przekazanych danych za pomocą właściwych środków technicznych i organizacyjnych. Podpisanie umowy powierzenia powinno zostać poprzedzone gruntownym zbadaniem podmiotu przetwarzającego oraz analizą jego kompetencji. Taka weryfikacja i analiza najczęściej polega na przesłaniu formularza weryfikacyjnego. Może ona

[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)

również polegać na przedłożeniu administratorowi stosownej dokumentacji obowiązującej u procesora (np. polityka prywatności, warunki świadczenia usług, raporty z audytów, certyfikaty ISO). Następnie ich wnikliwa analiza powinna stać się podstawą decyzji czy z danym podmiotem powinna zostać zawarta umowa powierzenia. Taka analiza dokonywana przez administratora danych jest formą oceny ryzyka, która w dużej mierze będzie zależeć od rodzaju przetwarzanych danych i powinna być każdorazowy wykonana indywidualnie z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania a także zagrożenia dla praw i wolności osób fizycznych.

W tym miejscu administratorzy danych bardzo często zadają sobie pytanie na co zwrócić szczególną uwagę podczas weryfikacji podmiotu przetwarzającego. I tutaj z pomocą mogą nam przyjść wytyczne EROD 7/2020[2] w sprawie pojęć administratora i podmiotu przetwarzającego. Wnika z nich, iż elementami, które należy wziąć pod uwagę przy ocenie podmiotu przetwarzającego mogą być:

- fachowa wiedza podmiotu przetwarzającego w zakresie np. środków bezpieczeństwa i naruszeń ochrony danych;
- wiarygodność podmiotu przetwarzającego;
- stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania;
- reputacja podmiotu przetwarzającego na rynku.

Decyzja komu administrator powinien powierzyć przetwarzanie danych nie może być podejmowana pochopnie i bezpodstawnie gdyż konsekwencje nieprzemyślanej decyzji, braku odpowiedniej formy oraz treści umowy powierzenia mogą oddziaływać bezpośrednio na osoby fizyczne, których dane osobowe zostały powierzone do przetwarzania.

Bardzo istotnym i wymagającym podkreślenia jest fakt, iż weryfikacja podmiotu przetwarzającego nie kończy się w momencie w którym oba podmioty zawierają umowę powierzenia. Administrator powinien w odpowiednich ostępach czasu weryfikować gwarancje podmiotu przetwarzającego, a w stosownych przypadkach przeprowadzać audyty oraz inspekcje.

PODSUMOWANIE

UODO po raz kolejny zwraca uwagę administratorów na to jak istotna jest prawidłowa weryfikacja podmiotu przetwarzającego a następnie zawarcie z nimi umowy powierzenia. Podkreśla również, iż ograniczenie się do zawarcia takiej umowy w sytuacji, gdy jej treść odpowiada wyłącznie minimalnym wymogom określonym w art 28 RODO może zostać uznane za działanie niewystarczające i prowadzić do wszczęcia postępowania zakończonego karą.
Administrator jako podmiot, który decyduje o sposobach i celach przetwarzania, odpowiada za zapewnienie bezpieczeństwa danych osobowych. Prowadzi to do obowiązku sprawdzenia

[2] Wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO przyjęte 7 lipca 2021 r.

każdego podmiotu, któremu zamierzać powierzyć dane do przetwarzania. Z kolei konsekwencją takiego sprawdzenia powinna być ocena czy dany podmiot zapewnia gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Jeżeli ocena podmiotu przetwarzającego jest pozytywne kolejnym krokiem powinno być podpisanie umowy powierzenia, która będzie w jak najlepszym zakresie odzwierciedlała prawa i obowiązki stron a nie tylko ograniczała się do minimum wskazanego w przepisach. Na tym jednak nie koniec. Kolejnymi działaniami jakie powinien podjąć administrator to cykliczna weryfikacja podmiotu przetwarzającego, która w określonych przypadkach polegać może na przeprowadzaniu audytów czy inspekcji. Tylko w ten sposób administrator będzie miał pewność, iż wywiązuje się z nałożonych na niego obowiązków określonych przepisami prawa oraz, że dane, które zostały powierzone do przetwarzani nadal są bezpieczne.

Karolina Żebrowska - specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.