Warszawa, dn. 10.09.2024 r.

Zawarcie i negocjacja umowy powierzenia – co i jak administrator może weryfikować u procesora?

WSTĘP

W dzisiejszym artykule zamierzamy przeanalizować praktyczne problemy występujące podczas negocjowania umów powierzenia pomiędzy procesorem a administratorem danych. W wielu umowach administrator wprost zobowiązuje procesora do udostępnienia mu wszelkich polityk bezpieczeństwa i ochrony danych osobowych, a także innej dokumentacji potwierdzającej zgodność procesora z przepisami RODO. Administrator przede wszystkim chce zabezpieczyć się pod kątem wyboru „odpowiedniego i zaufanego" dostawcy w zakresie jego zgodności z przepisami RODO. Z drugiej strony wielu procesorów niechętnie przystaje na takie postanowienia, a następnie na ewentualne udostępnianie swojej dokumentacji. Podmioty przetwarzające nie chcą dzielić się swoimi zasobami, dokumentacją oraz politykami. Wielu z nich twierdzi, że jest to element, który można zakwalifikować pod tzw. „tajemnicę przedsiębiorca". Z kolei dla administratorów danych, którzy ponoszą główna odpowiedzialność za przetwarzanie danych – samo oświadczenie procesora o istnieniu takiej dokumentacji bywa niewystarczające. Co w takim razie na to przepisy samego Rozporządzenia? Wyjściem do dalszych rozważań jest brzmienie art. 28 ust. 3 lit h. RODO, który brzmi następująco: Umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

„udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule *oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich."*

Wydaje się, że brzmienie wskazanego wyżej przepisu nie pozostawia wątpliwości w zakresie uprawnień administratora. Oczywiście same postanowienia może dokładnie regulować dana umowa powierzenia. Poniżej postaramy się bliżej przyjrzeć się możliwościom po stronie procesora w zakresie ewentualnej negocjacji wskazanych punktów.

I. Europejska Rada Ochrony Danych (EROD) wskazuje, że administratorowi mogą zostać udostępnione odpowiednie fragmenty rejestrów podmiotu

przetwarzającego dotyczące czynności przetwarzania. Podmiot przetwarzający powinien przekazać wszelkie informacje na temat sposobu, w jaki będzie przetwarzać dane w imieniu administratora. Informacje takie powinny obejmować informacje na temat funkcjonowania wykorzystywanych systemów, środków bezpieczeństwa, sposobu spełniania wymogów zatrzymywania danych, lokalizacji danych, przekazywania danych, tego, kto ma dostęp do danych i kto jest ich odbiorcą, podwykonawców przetwarzania danych itd.[1] EROD komentując art. 28 ust. 3 lit. h) RODO potwierdza sam obowiązek przekazywania informacji przez procesora (np. fragmentów danego rejestru), lecz nie przesądza, w jakiej formie ma to nastąpić. Można z tego wywnioskować, że przekazanie do wglądu pełnej dokumentacji i umożliwienie sporządzenia z niej kopii nie jest jedyną opcją spełnienia obowiązku z art. 28 ust. 3 lit. h) RODO. Co za tym idzie, nie stanowi to bezwzględnego obowiązku po stronie procesora i nie jest wykluczone, że Podmiot przetwarzający może sporządzić stosowne wyciągi, opisy lub fragmentów pewnych dokumentów, potwierdzające spełnienie obowiązków określonych w art. 28 RODO.

II. Istotne stanowisko w zakresie interpretacji przepisu art. 28 ust. 3 lit. h RODO zajął Prezes Urzędu Ochrony Danych Osobowych.[2] Zdaniem PUODO, administrator powinien mieć możliwość sprawdzenia komu powierza dane osobowe oraz w jaki sposób będą one przetwarzane. Prawo dostępu do takich informacji oraz przeprowadzania audytów przysługuje administratorowi również w trakcie realizacji umowy powierzenia. W tym celu w art. 28 ust. 3 lit. h RODO na podmiot przetwarzający zostały nałożone obowiązki udostępniania administratorowi wszelkich informacji potwierdzających spełnienie wymogów RODO, a także umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniania się do nich. Administrator jest bowiem zobowiązany do stałej kontroli, czy podmiot przetwarzający przetwarza dane zgodnie z prawem. Kontrole te mogą być przeprowadzane również doraźnie np. w przypadku wystąpienia naruszenia ochrony powierzonych danych osobowych. Zatem jakiekolwiek inne

[1] Wytyczne EROD 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO Wersja 2.0 Przyjęta 7 lipca 2021 r., s. 44-45

[2] Czy administrator musi kontrolować podmiot przetwarzający? https://uodo.gov.pl/pl/225/1213

postanowienia umowy powierzenia, które w istocie ograniczałyby ww. prawa administratora należałoby uznać za niezgodne z RODO. Podobnie należy ocenić utrudnianie lub ograniczanie administratorowi możliwości przeprowadzania kontroli u podmiotu przetwarzającego lub ograniczanie jej zakresu. Nieudostępnienie dokumentacji lub pewnego zakresu dokumentacji rodzi ryzyko stwierdzenia przez PUODO utrudnienia lub ograniczenia możliwości prowadzenia kontroli przez administratora. Również sami administratorzy mogą postawić sobie na szczycie priorytetów bardzo dokładną weryfikację podmiotu przetwarzającego ze względu na kary, jakie pojawiły się do tej pory za brak takiej weryfikacji np.: https://uodo.gov.pl/pl/138/2304.

III. Podobny przypadek badany był w sprawie naruszenia przepisów RODO przez Krajową Szkołę Sądownictwa i Prokuratury. PUODO badało m.in. realizację obowiązków administratora w zakresie art. 28 ust. 1 i art. 28 ust. 3 lit. h RODO pod kątem wyboru podmiotu przetwarzającego dającego gwarancję odpowiednich zabezpieczeń. Prezes UODO, w oparciu o przedłożoną dokumentację, jak i wyjaśnienia złożone przez KSSiP, z punktu widzenia ww. przepisów, nie dopatrzył się okoliczności, które pozwoliłyby stwierdzić, że procesor nie zapewniał wystarczających gwarancji dla bezpieczeństwa danych osobowych oraz nie udostępniał administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał administratorowi przeprowadzanie audytów, w tym inspekcji.[3] Pomimo, że w tym przypadku PUODO nie stwierdziło naruszenia art. 28 ust. 3 lit. h RODO, to organ podczas postępowania badał czy podmiot przetwarzający udostępniał administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał administratorowi przeprowadzanie audytów, w tym inspekcji. Trzeba mieć na uwadze, że administratorzy przy negocjowaniu umów powierzenia mogą powoływać się na ten fakt. Brak jest też w decyzji wskazania jakie konkretnie dokumenty lub dokumentacja została przedłużona przez administrator w zakresie realizacji przez procesora obowiązków z art. 28 ust. 3 lit. h RODO.

[3] https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020

Niemniej, fragmenty tej decyzji wskakują, że PUODO może wnikliwie badać realizację obowiązków przewidzianych w art. 28 ust. 3 lit. h RODO – stąd też można spodziewać się, że administrator będzie wymagał od procesora przedstawienia stosownej dokumentacji – i będzie miał ku temu uzasadnione argumenty.

IV. PUODO w decyzji nakładającej administracyjną karę pieniężna na ID FINANSE w uzasadnieniu faktycznym wskazał w jaki sposób *realizowany* był obowiązek przewidziany w art. 28 ust. 3 lit. h RODO, *tj.: „Odnosząc się do realizacji prawa kontroli z art. 28 ust. 3 lit. h rozporządzenia 2016/679, Spółka wskazała, że podmiot przetwarzający niezwłocznie udzielał administratorowi informacji na temat zdarzenia z (...) lutego 2020 r., jak również na przestrzeni całego okresu obowiązywania umowy powierzenia regularnie odbywały się rozmowy telefoniczne, telekonferencje i wzajemne, bezpośrednie wizyty. Ponadto podmiot przetwarzający udzielił Spółce odpowiedzi na pytania w ramach szczegółowego kwestionariusza weryfikującego przestrzeganie postanowień umownych. Wypełniony kwestionariusz stanowi załącznik do pisma z (...) czerwca 2020 r."*[4] PUODO w uzasadnieniu prawnym do tej decyzji stwierdził, że organ nie dopatrzył się okoliczności, które pozwoliłyby stwierdzić, że podmiot przetwarzający nie zapewniał wystarczających gwarancji dla bezpieczeństwa danych osobowych oraz nie udostępniał administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał Spółce przeprowadzanie audytów, w tym inspekcji. Można z tego wnioskować, że zdaniem PUODO warunek udostępniania wszelkich informacji niezbędnych do przestrzegania postanowień art. 28 RODO może być realizowany m.in. poprzez bieżący kontakt, wyjaśnienia, regularne spotkanie i omawianie bieżących problemów. PUODO nie wskazał w decyzji, że obowiązek wykazywania zgodności z art. 28 ust. 3 lit. h RODO polega na konieczności udostępnienia przez procesora polityk ochrony danych osobowych oraz innych dokumentów związanych z systemem ochrony danych osobowych. Z

[4] DKN.5130.1354.2020, Decyzja w sprawie nałożenia kary pieniężnej w związku z naruszeniem przepisów o ochronie danych osobowych - Decyzja Prezes Urzędu Ochrony Danych Osobowych, LEX

drugiej strony te fragmenty decyzji wskazują jak szeroko można ten obowiązek interpretować i jak wiele czynności można wykonywać, aby go spełnić.

Podsumowanie

Szczegółowe warunki umowy powierzenia, w tym prowadzenia audytów, pozostawione są do uzgodnienia między stronami, na zasadzie swobody zawierania umów. Udostępnienie dokumentacji czy polityk administratorowi nie ma więc charakteru bezwzględnego obowiązku wynikającego z przepisów. Jako że uzgodnienia muszą mieć charakter dwustronny, wymagane jest takie rozwiązanie, które zadowoli również podmiot przetwarzający. Administrator w tym przypadku nie może jednostronnie narzucać rozwiązań (umowa ma charakter dwustronny). Tak samo procesor może zwracać uwagę podczas negocjacji, że udostępnienie dokumentacji ochrony danych osobowych będzie naruszeniem tajemnicy przedsiębiorstwa oraz obowiązujących procedur w organizacji. Niemniej, procesor powinien podjąć w tym zakresie, wszelkie możliwe działania, aby wykazać, że udostępnia administratorowi informacje niezbędne do spełnienia wymagań art. 28 RODO (np. wypełnienia kwestionariuszy, udostępnianie fragmentów procedur lub polityk, bieżący kontakt z administratorem, regularna weryfikacja realizacji umowy powierzenia etc.).

Jednak, bez względu na zasadę swobody umowy – mając na względzie powyższą analizę i stanowiska organów nadzorczych - trzeba brać pod uwagę, z perspektywy podmiotu przetwarzającego, że administrator będzie dążyć do możliwości dokładnej weryfikacji zgodności podmiotu z przepisami RODO. Art. 28 ust. 3 lit. h RODO sam w sobie daje konkretne uprawnienia do możliwości weryfikacji administratorowi zgodności z RODO poprzez udostępnianie wszelkich informacji w tym zakresie. Do ustalenia zostają już „szczegóły" – w jaki sposób procesor będzie udostępniał informacje niezbędne do wykazania spełnienia obowiązków z RODO. W relacjach administrator – procesor, to jednak rolę znacznie silniejszą odgrywa administrator. Wynika to z faktu realizacji celów biznesowych, w których to zazwyczaj procesor jest podwykonawcą świadczącym usługi na rzecz zleceniodawcy. Dodatkowo, administrator - na gruncie RODO - jest tym podmiotem najbardziej odpowiedzialnym i w jego interesie leży też jak najszersze zabezpieczenie swoich interesów. To na administratorze wprost ciąży obowiązek dokładnej weryfikacji podmiotu, któremu powierzy pewien zakres usług. Administrator ma obowiązek wybrać podmiot, który daje odpowiednie gwarancje zgodności z przepisami RODO. Bardzo dużo argumentów przy negocjacjach umowy powierzenia jest po stronie administratora.

Wniosek dla podmiotów przetwarzających? Dobrze przygotowana dokumentacja ochrony danych osobowych, skrupulatnie przeprowadzone analizy ryzyka i oceny skutków przetwarzania danych osobowych oraz stały monitoring bieżących procesów to dzisiaj podstawa, także dla bieżącej działalności gospodarczej spółki pełniejącej role podmiotu przetwarzającego. Bez tych elementów może dochodzić do niezawierania umów powierzenia, a jednocześnie do umów o świadczeniu danej usługi, co wpływa już operacyjną działalność gospodarczą.

Maciej Łukaszewicz – radca prawy, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.