02.06.2020 r.

Powierzenie po duńsku, czyli jak przy pomocy klocków w art. 28 ust. 3 stworzyć umowę powierzenia?

Od czasu wejścia w życie RODO minęło już ponad dwa lata. 25 maja 2018 roku umowa powierzenia była niemalże całkowicie nieznana biznesowi, a idea zawierania umowy w przypadkach przetwarzania danych osobowych w imieniu zlecającego dopiero nabierała na znaczeniu – mimo, że samo umowne powierzanie danych osobowych było obowiązkiem jeszcze przed obowiązywaniem stosowania RODO (na podstawie ustawy o ochronie danych osobowych z 29 sierpnia 1997 r.). Na początku wiedza o obowiązku zawierania umów powierzenia była przekazywana głównie za pośrednictwem dużych, międzynarodowych spółek, pragnących realizować obowiązki nałożone przez europejską centralę grupy kapitałowej. Obecnie umowy powierzenia na stałe zagościły w porządku biznesowym, stanowiąc nieodłączny element wielu umów współpracy, np. pośrednictwa, dropshippingu, czy hostingu. Wzory umów, jak i standardy bezpieczeństwa, roznoszą się sektorowo, dlatego wielkość firmy czy skala procesów przetwarzania nie ma znaczenia - umowy powierzenia są już stosowane zarówno przez duże spółki, jak i przez jednoosobowe działalności gospodarcze. Przez ostatnie dwa lata powstało wiele wzorów umów powierzenia wykorzystywanych w ramach:

- grup kapitałowych,
- spółek,
- sektorów biznesowych (np. hosting),
- obowiązków prawnych (np. sektor bankowy).

Czy najnowszy wzór standardowych klauzul umownych stworzonych przez duński organ przyniesie rewolucję w podejściu do zawierania umów powierzenia? Czy IOD oraz sam biznes powinni wyciągnąć wnioski na podstawie duńskich wzorów?

Umowa szyta na miarę, czy umowa dla każdego?

Jak należy skonstruować umowę powierzenia? Największą popularnością w Polsce cieszą się umowy powierzenia zawierające elastyczne i luźne terminy, np.:

- “w przypadku naruszenia procesor ma poinformować o naruszeniu bez zbędnej zwłoki”,
- “procesor zobowiązuje się do podejmowania wszelkich środków wymaganych na mocy art. 32 RODO”,

- “umowa powierzenia jest zawierana w celu realizacji umowy głównej”.

Najczęściej raz stworzony wzór, jest modyfikowany przez powierzającego tylko poprzez zmianę zakresu danych i kategorii osób, których te dane dotyczą. Niewątpliwie istotnym powodem stosowania takiej formy jest przeświadczenie o możliwości ustnego uregulowania szczegółów w przypadku wystąpienia danej sytuacji, np. naruszenia, a także braku negatywnych doświadczeń związanych ze współpracą z podmiotem przetwarzającym.

Polska praktyka znacząco różni się od formy proponowanej przez Datatilsynet (Duńska Agencja Ochrony Danych). Według propozycji tego organu wszelkie kwestie, które mogą budzić wątpliwość lub spory, powinny zostać uregulowane w sposób dokładny. Bardzo rzadko możemy ujrzeć umowy powierzenia, w których strony regulują kwestie postępowania na wypadek wydania przez administratora niezgodnych z prawem poleceń, zaś Datatilsynet proponuje nie tylko uregulowanie niniejszego zagadnienia, lecz także możliwość **przewidzenia i rozważenia przez strony konsekwencji takich działań**.

Konsekwentność w stosowaniu pisemnej formy jak i przestrzegania zasady rozliczalności towarzyszy nam na każdym kroku w proponowanym wzorze. Celem przetwarzania danych nie jest wykonanie umowy, zaś zakresem - dane konieczne do jej realizacji. Według Datatilsynet, zarówno:

- cel,
- **charakter,**
- zakres,
- kategorie,
- **czas,**

powinny zostać opisane w sposób szczegółowy. Jest to forma występująca w Polsce, jednakże nie będąca standardem. **Ulokowanie kwestii “charakterystycznych” dla danej umowy w załącznikach jest rozwiązaniem bardzo korzystnym,** nie tylko ze względu na realizację zasady rozliczalności, lecz także z powodu ułatwienia pracy dla IOD, który w szybki sposób jest w stanie zweryfikować czego dotyczy dana umowa, i jakie kwestie należy zweryfikować.

Bardzo ciekawym zagadnieniem jest **całkowite wyodrębnienie umowy powierzenia od innych umów łączących strony.** Nie ujrzymy w niniejszym dokumencie takich słów jak:

- umowa główna,
- aneks,
- przetwarzanie do czasu rozwiązania umowy głównej.

Umowa powierzenia ma być “**samowystarczalna**”. Zgodnie z art. 5 RODO i zasadą rozliczalności, strony są zobowiązane do wykazania przestrzegania RODO, a w szczególności art. 28 RODO. Jest to znacząca różnica od praktyki polskiej - opierania zapisów umowy powierzenia, w tym jej trwania, zakresu i celu, a często nawet i zasad odpowiedzialności, w zależności do umowy głównej. Stosowanie takiej formy zapewnia

większą elastyczność, np. w sytuacjach, gdy umowa pisemna nie stanowi podstawy powierzenia (chociażby regulamin). Wskazanie, iż przetwarzanie trwa "przez cały okres świadczenia usług" pozwala także na brak konieczności jej aneksowania lub uchylenia w przypadku zmian zasad współpracy.

Dokładne uregulowanie kwestii przetwarzania w umowie nie oznacza, iż zasady przetwarzania nie mogą być modyfikowane – powierzającemu wciąż przysługuje prawo do wydawania poleceń przez cały okres współpracy, **jednakże należy je udokumentować i przechowywać pisemnie lub w formie elektronicznej.**

Bezpieczeństwo? To problem podmiotu przetwarzającego!

Bardzo częstą praktyką w umowach powierzenia, jest uregulowanie kwestii ochrony danych poprzez "zobowiązanie do przestrzegania art. 32- 36 RODO". Jest to na pierwszy rzut oka działanie wystarczające do zawarcia wiążącej umowy powierzenia, jednakże czy jest to działanie wystarczające dla zachowania bezpieczeństwa danych? **Należy pamiętać, iż podmiot przetwarzający ponosi odpowiedzialność za zachowanie bezpieczeństwa danych, jednakże nie oznacza to, że taki obowiązek zapewnienia bezpieczeństwa nie ciąży jednocześnie na administratorze. Administrator poprzez korzystanie z usług podmiotów przetwarzających oczekuje, że podmioty takie zapewnią bezpieczeństwo przetwarzanym danym tak, aby administrator mógł wykazać, że wobec danych osobowych zastosowane zostały adekwatne środki bezpieczeństwa.** W duńskich standardowych klauzulach znajdują się nie tylko przykłady, w jaki sposób można ustalić zasady audytu lub jak go przeprowadzić, lecz standardowe postanowienia umowne posiadają także bardzo rozbudowane zapisy dot. standardów bezpieczeństwa, których ma przestrzegać podmiot przetwarzający.

Uregulowanie w sposób szczególny zasad bezpieczeństwa dotychczas najczęściej występowało w sektorach objętych tajemnicą zawodową lub szczególnymi obowiązkami prawnymi, np. tajemnicą lekarską, bankową, czy telekomunikacyjną. Mając na uwadze, że naruszenie bezpieczeństwa może wiązać się z dotkliwymi skutkami dla podmiotu danych osobowych nie tylko w przypadku podmiotów „szczególnego" sektora, lecz także chociażby i w sektorze e-commerce, brak jest przesłanek do uznania, że obowiązek uregulowania w sposób znaczący bezpieczeństwa powinien występować tylko wśród spółek zobowiązanych do zachowania danych w tajemnicy na podstawie przepisów szczególnych. Nie należy traktować poleceń dotyczących wykorzystywania danych osobowych, jako nowego "zła koniecznego" do umów powierzenia, tylko jako zbiór dobrych praktyk, które pozwolą uniknąć sporów pomiędzy stronami w przypadku wystąpienia niepożądanych zdarzeń.

Ewolucja, dewolucja czy stabilizacja?

Czy jest to ewolucja? Wiele firm, w szczególności o międzynarodowych korzeniach, stosuje już bardzo zbliżone treścią wzorce. Wynika to głównie z podobieństwa pomiędzy duńską

propozycją, a standardowymi klauzulami umownymi zaakceptowanymi przez Komisję Europejską. Prowadzenie ewidencji dalszych podmiotów przetwarzających, jak i audytowanie podmiotów przetwarzających, było i wciąż jest standardem dla firm uznających rozliczalność i bezpieczeństwo, jako wartość nadrzędną.

Czy wprowadzi to zmiany w relacjach biznesowych? Stworzenie omawianych wzorców może stanowić krok w dobrym kierunku. Jest to pierwszy taki wzorzec, który pomoże wyznaczyć standardy powierzania danych osobowych. Będzie to szczególnie pomocne narzędzie dla wszystkich małych przedsiębiorców, niedoświadczonych w kwestiach ochrony danych osobowych, które być może uchroni małe działalności przed bardzo niekorzystnymi zapisami umownymi.

Polecenia dotyczące wykorzystania danych osobowych, zawarte w duńskim wzorze, mogą być dla wielu nowością, lecz także niedługo mogą stać się nowym standardem powierzania danych osobowych. Administrator na podstawie przeprowadzonej analizy ryzyka, np. opartej o wytyczne ENISA, będzie w stanie wskazać minimalne wymogi bezpieczeństwa, które podmiot przetwarzający musi przestrzegać.

Stabilizacja? W pewnym stopniu komentowane wzory mogą spowodować ustabilizowanie się kwestii powierzenia danych osobowych, co jest stanem pożądanym przez wielu IOD. Mając na uwadze ilość nieuregulowanych lub nieznanych kwestii, rewolucja nie jest tym, czego oczekują IOD. W praktyce bardziej pożądana jest właśnie stabilizacja. Pozwoli to na oszacowanie ryzyk, a także na skupienie się na innych równie ważnych aspektach ochrony danych.