

UREGULOWANIE STOSUNKU POWIERZENIA

Każda współpraca pomiędzy podmiotami, polegająca na wykonywaniu czynności na danych osobowych, które to czynności określa jeden z tych podmiotów (administrator danych osobowych), a wykonuje je drugi w jego imieniu (podmiot przetwarzający), musi zostać uregulowana umową powierzenia.

Zdarza się, że podmioty powierzając dane, nie do końca zdają sobie sprawę, że dana czynność jest właśnie powierzeniem danych osobowych. Do takich sytuacji należy np. hosting, przechowywanie dokumentów, itp. Zapominamy, że zgodnie z definicją „przetwarzania”, przechowywanie danych jest również ich przetwarzaniem. Wydawać by się mogło, że przetwarzanie danych to wykonywanie na tych danych konkretnych operacji, ale nie tylko. Nawet samo ich przeglądanie jest już ich przetwarzaniem. Kolejnym przykładem niezidentyfikowania stosunku powierzenia jest kwestia przetwarzania np. danych służbowych pracowników. RODO nie rozdziela danych osobowych na dane prywatne i służbowe. Definicja danych osobowych mówi o zidentyfikowaniu lub o możliwości zidentyfikowania osoby fizycznej po tych danych, a po danych służbowych jak najbardziej jest możliwe zidentyfikowanie konkretnej osoby.

Jeżeli już zidentyfikujemy stosunek powierzenia danych przy danej współpracy, to oczywiście powinniśmy podpisać umowę powierzenia. Możliwe jest to jednak nie tylko podpisanie umowy powierzenia, ale i sama współpraca, wyłącznie z podmiotem, który spełnia wymogi RODO. Nie wystarczy samo oświadczenie umowne o spełnianiu takich wymogów. My, jako podmiot, który ma zamiar powierzyć dane do dalszego przetwarzania innemu podmiotowi, powinniśmy go pod tym kątem odpowiednio zweryfikować – przeanalizować zapisy na stronie internetowej podmiotu, jeżeli taką posiada, przekazać do wypełnienia i podpisania kwestionariusz weryfikacyjny, a jeżeli jakieś informacje wzbudzą naszą wątpliwość, poprosić o udostępnienie przykładowych dokumentów potwierdzających zgodność z RODO albo nawet przeprowadzić audyt sprawdzający. Taka weryfikacja powinna następować cyklicznie również po rozpoczęciu współpracy.

Niestety z naszego doświadczenia wynika, że często zdarza się powierzenie danych bez odpowiedniej weryfikacji podmiotu lub po jego negatywnej weryfikacji, ale takie przypadki, jako Inspektorzy Ochrony Danych (IOD) u naszych Klientów, zawsze pozostawiamy do decyzji biznesowej obarczonej ryzykiem konsekwencji. Te konsekwencje mogą wystąpić ze strony organu nadzorczego (PUODO) lub skutkować negatywnymi skutkami związanymi z nieprawidłowym przetwarzaniem danych przez podmiot przetwarzający (np. wyciek danych i związane z nim straty finansowe lub wizerunkowe).