

Warszawa, dn. 9.05.2024 r.

## Odpowiedzialność finansowa w grupie kapitałowej i nadzór nad procesami

Podmioty działające w ramach grup kapitałowych bardzo często dzielą się informacjami. Kiedy wymiana dotyczy danych osobowych, z zasady niezbędne jest spełnienie wymagań określonych w przepisach o ich ochronie. Nadzór nad procesami w grupie kapitałowej jest w gruncie rzeczy bardzo trudny. Jest to zauważalne zjawisko ukazujące się podczas audytu RODO. Zazwyczaj, nie zdajemy sobie sprawy z powagi sytuacji nałożenia kar finansowych oraz jej wysokości. Największym praktycznym zagrożeniem w tym zakresie wydaje się być zbyt powierzchowne podejście do tematu i automatyczne przyjęcie, że wszystkie procesy w grupie są wspólne i oznaczają współadministrację. W praktyce rzadko ten model będzie odpowiadał wszystkim przepływom danych w grupie, a dodatkowo nie jest najkorzystniejszy biznesowo ze względu na wspólną odpowiedzialność wszystkich administratorów.

Warto pamiętać, że mimo funkcjonowania poszczególnych spółek w grupie, każda z nich pozostaje odrębnym podmiotem w świetle prawa. Czy zatem spółki wymieniające się danymi osobowymi wewnątrz grupy po wejściu w życie RODO mogą korzystać ze swobody wymiany danych?

Właśnie swobodny przepływ danych pomiędzy spółkami w grupie jest podstawą ich funkcjonowania. Struktura holdingowa (przypominająca na ogół drzewo genealogiczne) wymaga, żeby członkowie holdingu wiedzieli o sobie wiele. Skoro spółka - matka kieruje działalnością spółek - córek, a te z kolei – ich spółek zależnych, to spółki te naturalnie wchodzi w posiadanie określonych informacji często zawierających dane osobowe.

Z punktu widzenia ochrony danych osobowych istotne jest natomiast poprawne przeprowadzenie mapowania przepływu danych oraz istnienie podstawy prawnej ich przetwarzania, a także realizacja obowiązków informacyjnych względem osób, których dane dotyczą. Przetwarzanie danych osobowych przez spółki z grupy musi się mieścić w ramach wyznaczonych przez przepisy o ochronie danych osobowych. W większości grup przedsiębiorstw współistnieje jednocześnie kilka różnych procesów i podstaw przetwarzania danych.

Może być to obszar współadministrowania, gdzie cele i sposoby przetwarzania ustalane są wspólnie. Dodatkowo, np. jeśli czynności administracyjne są zlecone do jednego podmiotu z grupy, to powstaje stosunek powierzenia przetwarzania danych, a podmiot wspierający działa jako procesor. Podmioty z grupy udostępniają także dane podmiotowi centralnemu, jako osobnemu administratorowi.

Istnieje popularne przeświadczenie, że samo występowanie powiązania kapitałowego lub osobowego pomiędzy spółkami jest wystarczającą podstawą do wymiany danych osobowych. Mówi się zazwyczaj o możliwości powołania się na uzasadniony interes każdej ze spółek w

przesyłaniu danych w ramach grupy, do wewnętrznych celów administracyjnych. W praktyce najczęściej chodzi o dane pracowników, klientów i kontrahentów.

Oczywiście nie oznacza to, że wszystkie dane osobowe można swobodnie przekazywać wewnątrz grupy. Każdorazowo trzeba identyfikować legalność przekazania danych innym członkom grupy, w szczególności w zakresie istnienia realnego celu przetwarzania. Jeżeli udostępnienie danych nie będzie możliwe, należy rozważyć zawarcie między spółkami umowy o współpracy wraz z umową powierzenia przetwarzania danych osobowych.

Przykład: Jedną ze spółek z Grupy Kapitałowej stanowi tzw. Centrum Wszechświata dla pozostałych spółek. W związku z tym w Centrum Wszechświata dochodzi do przetwarzania danych osobowych pracowników czy kontrahentów, których administratorem są inne spółki z Grupy - jest zatem podwykonawcą usług świadczonych na rzecz innych spółek (czyli w świetle RODO jest procesorem). W takim przypadku należy określić w jaki sposób dojdzie do przekazania danych przez spółki z Grupy na rzecz Centrum Wszechświata – należy zawrzeć umowę powierzenia przetwarzania danych lub kwestia ta powinna wynikać z wiążących reguł korporacyjnych.

### **Nadzór nad procesami – co może pomóc?**

W procesie identyfikacji procesów przetwarzania danych i ich podstaw prawnych (mapowanie) z pomocą może przyjść w szczególności rejestr czynności przetwarzania danych, stworzony dla każdej ze spółek z grupy. Kolejnym krokiem powinno być wypracowanie zgodnych z przepisami procedur w zakresie przepływu informacji i wkomponowanie ich w całość regulacji obowiązujących w grupie.

Procedury powinny być jednak skrojone na miarę konkretnej grupy. Stos dokumentów „do szuflady”, pomijających specyfikę danej organizacji, nie spełni swojej roli.

RODO przewiduje przy tym możliwość przyjęcia przez grupy tzw. wiążących reguł korporacyjnych, które stanowią polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający. Co ważne, wiążące reguły korporacyjne powinny być przyjmowane przez międzynarodowe grupy kapitałowe, tj. takie, które posiadają siedziby nie tylko na terytorium UE, ale również w państwie trzecim.

### **Więcej o karach**

Tak jak wskazuje wyżej, nadzór nad całością nie jest łatwy. Wymiana danych między Spółkami często prowadzona jest w dużym chaosie. Brak koordynacji nad tym, może spowodować nałożenie wysokich kar finansowych przewidzianych w RODO.

Przepisy RODO przewidują dwie kategorie kar finansowych, które zależne są od rodzaju przewinienia.

UODO może nałożyć karę w wysokości:

- do 10 lub 20 mln euro,
- do 2 lub 4% całkowitego rocznego obrotu firmy z poprzedniego roku.

Co ważne, wysokość kary dla Spółki, mimo że stanowi odrębny twór prawny, liczona jest na podstawie 2 lub 4 % całkowitego rocznego obrotu firmy z poprzedniego roku, a więc grupy kapitałowej.

Przetwarzanie i wzajemne udostępnianie danych osobowych w ramach grupy kapitałowej, poza zarysowanymi powyżej ułatwieniami prawnymi, pociąga za sobą również pewne wyzwania. Przede wszystkim niełatwa może okazać się identyfikacja przez członków grupy całości procesów przetwarzania danych w poszczególnych spółkach oraz sytuacji wzajemnego udostępniania danych (tzw. mapowanie).

**Olga Skotnicka** – dyrektor operacyjny w iSecure Legal, ekspert ds. ochrony danych osobowych w iSecure Sp. z o.o.