

Obieg informacji w grupach kapitałowych

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.

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?

Swobodna wymiana danych

Wymiana danych osobowych w grupach spółek jest istotna z uwagi na złożony proces raportowania m.in. o stanie finansów czy przedsięwzięć biznesowych spółek poszczególnych szczebli. Dodatkowo spółki w grupie dzielą się kompetencjami i zadaniami. Ze względu na digitalizację, wiele danych przetwarzanych jest też przy użyciu systemów ERP czy też CRM, a w takich systemach zasadniczo nie jest identyfikowane, która spółka z grupy jest administratorem danych osobowych. Czy z uwagi na wejście w życie RODO takie praktyki są sprzeczne z prawem?

Trzeba pamiętać, że to 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. Dzieje się tak np., gdy jako wspólnicy:

- głosują na zgromadzeniach wspólników lub walnych zgromadzeniach spółek zależnych, czy
- wykonują prawo kontroli wspólnika w spółce-córce, analizując jej księgi i dokumenty, żądając wyjaśnień od zarządu itd.

Po wejściu w życie RODO spółki nadal mogą dzielić się kompetencjami. Na przykład spółka produkcyjna nadal może odpowiadać za stworzenie zaplecza produkcyjnego dla pozostałych spółek z grupy, spółka dystrybucyjna wciąż może prowadzić sprzedaż, spółka pracownicza – udostępniać pozostałym spółkom pracowników, a spółka rachunkowa – nadal może świadczyć usługi księgowe itd. 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.

Podstawa przetwarzania

Przetwarzanie danych osobowych przez spółki z grupy musi się mieścić w ramach wyznaczonych przez przepisy o ochronie danych osobowych. W zależności jednak od tego, jakie dane są przetwarzane (jaki rodzaj danych), możliwe jest ich przetwarzanie na podstawie tzw. prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit f RODO). Takim interesem może być potrzeba przekazywania danych osobowych przez

administratora, którym jest jedna ze spółek z grupy, innym jej członkom – np. w celach administracyjnych (tworzenie raportów, analiz), przetwarzania danych klientów w programie CRM, do którego dostęp mają różne spółki z grupy, czy też danych pracowników poszczególnych spółek w celach sprawozdawczych.

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: Jedna ze spółek z Grupy Kapitałowej stanowi tzw. Centrum usług wspólnych (CUW) dla pozostałych spółek. W związku z tym w CUW dochodzi do przetwarzania danych osobowych pracowników czy kontrahentów, których administratorem są inne spółki z Grupy - CUW 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 CUW – należy zawrzeć umowę powierzenia przetwarzania danych lub kwestia ta powinna wynikać z wiążących reguł korporacyjnych.

Jeden inspektor, wspólne reguły

Ustawodawca unijny przewidział pewne ułatwienia dla podmiotów funkcjonujących jako grupa przedsiębiorstw (tytułem objaśnienia: RODO nie posługuje się terminem „grupa kapitałowa”, a „grupa przedsiębiorstw”, która oznacza przedsiębiorstwo sprawujące kontrolę i przedsiębiorstwa przez nie kontrolowane). Grupa przedsiębiorstw może np. wyznaczyć jednego inspektora ochrony danych osobowych (IODO), jeśli można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej. W przypadku wyznaczenia jednego IODO dla grupy kapitałowej, każda ze spółek musi dokonać jego odrębnego zgłoszenia do UODO (Urząd Ochrony Danych Osobowych).

Przykład: Spółki z Grupy Kapitałowej postanowiły wyznaczyć jednego wspólnego IODO. Spółka – matka postanowiła dokonać jednego zgłoszenia do UODO dla wszystkich spółek z Grupy. Takie postępowanie jest nieprawidłowe. Aby skutecznie wyznaczyć IODO, każda ze spółek z Grupy Kapitałowej musi dokonać odrębnego zgłoszenia do UODO.

Kolejnym ułatwieniem jest możliwość przyjęcia wspólnych reguł korporacyjnych z zakresu ochrony danych osobowych.

Aby skutecznie wdrożyć te reguły, w pierwszej kolejności należy zapanować nad obiegiem danych wewnątrz grupy przez dokonanie tzw. mapowania przepływu danych.

Pomoże mapowanie procesów

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 muszą być

jednak skrojone na miarę konkretnego koncernu i „użyteczne”. 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.

Informacje o członkach organów

Dane członków organów mogą być swobodnie przetwarzane w ramach grupy kapitałowej. Wynika to stąd, że istnieje prawnie uzasadniony interes poszczególnych spółek do przetwarzania tych danych.

Natomiast mimo, że dane członków zarządu czy rady nadzorczej są jawne (są publikowane w KRS), nie jest tak, że każdy może je przetwarzać. Jeśli dane członków organów spółek są zbierane przez podmioty trzecie (np. agencje marketingowe), a następnie przetwarzane w określonym celu (np. składania oferty handlowej), podmiot, który się tym zajmuje, musi wypełnić określone obowiązki. Często jest to uzyskanie zgody na takie działania (dotyczy to prowadzenia działań marketingowych) oraz wypełnienie obowiązku informacyjnego. Za niedopełnienie tych obowiązków organ nadzoru może nałożyć karę. Potwierdził to UODO w decyzji z 15 marca 2019 r. (ZSPR.421.3.2018).

Autorzy:

Nastazja Lisek, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.

Anna Hoffmann, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.