ROLA PODMIOTU PRZETWARZAJĄCEGO W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH NA GRUNCIE RODO

Przepisy RODO nakładają na administratorów danych osobowych szereg obowiązków, takich jak konieczność zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu czy zawiadamiania o nich podmiotów danych. To na administratorach spoczywa główny ciężar odpowiedzialności za wykonanie ww. zadań, jednak istotną rolę w tym procesie odgrywają również podmioty przetwarzające. Jakie działania powinny one podejmować, aby we współpracy z administratorami prawidłowo realizować obowiązki wynikające z występujących naruszeń?

„Podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Stosownie do art. 28 ust. 3 RODO przetwarzanie to odbywa się na podstawie umowy lub innego instrumentu prawnego, określającego przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora. Art. 28 ust. 3 lit. f) RODO wskazuje zaś, że podmiot przetwarzający pomaga administratorowi wywiązać się z zadań określonych w art. 32-36 RODO (a zatem m.in. z obowiązku notyfikacji, o którym mowa w art. 33 RODO, oraz zawiadomienia osób, których dane dotyczą, w trybie art. 34 RODO), co należy uwzględnić w ramach ww. ustaleń.

Obowiązek zgłoszenia naruszenia administratorowi

W myśl art. 33 ust. 2 RODO po stwierdzeniu naruszenia ochrony danych osobowych podmiot przetwarzający ma obowiązek bezzwłocznego poinformowania o nim administratora.
Warto zauważyć, że podmiot przetwarzający nie jest zobowiązany do dokonania oceny ryzyka wynikającego z naruszenia – to administrator powinien przeprowadzić analizę ryzyka w związku z zaistniałym incydentem i podjąć decyzję o ewentualnym zgłoszeniu go organowi nadzorczemu (więcej na ten temat w „Biuletynie UODO" nr 7-8/07-08/23, s. 16) oraz zawiadomieniu osób, których dane dotyczą. W geszi podmiotu przetwarzającego pozostaje ustalenie, czy doszło do naruszenia, a jeśli tak – zgłoszenie tego faktu administratorowi. Prawodawca unijny nie przedstawił w ramach przepisów RODO precyzyjnych wytycznych w zakresie treści i formy takiego zgłoszenia, a także konkretnego terminu na jego dokonanie (przepis wskazuje wyłącznie, że trzeba to zrobić „bez zbędnej zwłoki"). Mając jednak na uwadze przytoczony powyżej obowiązek wynikający z art. 28 ust. 3 lit. f) RODO, należy przyjąć, iż działanie to powinno mieć na celu wsparcie administratora w wykonywaniu jego zadań, a więc dostarczać mu co najmniej tych informacji, o których mowa w art. 33 ust. 3 lit. a) RODO, jak również umożliwiać dochowanie przez niego terminu na zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, wynoszącego 72 godziny.

Pomoc w zawiadomieniu o naruszeniu osób, których dane dotyczą

Zgodnie z art. 34 ust. 1 RODO jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o nim osoby, których dane dotyczą. Praktyka pokazuje jednak, że w niektórych sytuacjach to podmiot przetwarzający dysponuje informacjami niezbędnymi do prawidłowego dokonania zawiadomienia, takimi jak istotne szczegóły dotyczące incydentu czy dane kontaktowe osób objętych naruszeniem. W świetle powyższego sprawnie funkcjonująca komunikacja między administratorem a podmiotem przetwarzającym może okazać się niezbędna, aby we właściwy sposób wypełnić obowiązki związane z zawiadamianiem o naruszeniu objętych nim osób.

Współpraca administratora i podmiotu przetwarzającego

W celu zminimalizowania ryzyka wystąpienia ewentualnych nieprawidłowości, w ramach realizacji zadań wynikających z naruszeń ochrony danych osobowych, strony zawierające umowę powierzenia powinny precyzyjnie określić warunki współpracy w tym obszarze. Wypracowanie dobrych praktyk i spójnych procedur może poskutkować lepszą komunikacją, usprawniając reakcję na występujące incydenty. Warto jednak pamiętać, że ustalenia te nie wpływają na prawną odpowiedzialność administratora w przypadku naruszenia art. 33 lub 34 RODO, które skutkować może nałożeniem administracyjnej kary pieniężnej.