

Rödl & Partner

Echo



Data: 14.02.2021

Dotyczy: [Rzeczpospolita](#)

NARUSZENIE OCHRONY DANYCH OSOBOWYCH: BŁĄD KLIENTA NIE USPRAWIEDLIWIA UBEZPIECZYCIELA

Przyczynienie się przez osobę fizyczną, której dane osobowe dotyczą, do wystąpienia naruszenia ochrony danych osobowych nie zwalnia administratora z obowiązku niezwłocznego zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

9 grudnia 2020 roku Prezes Urzędu Ochrony Danych Osobowych (decyzją o numerze DKN.5131.5.2020) nałożył na TUIR WARTA S.A. karę pieniężną w wysokości 85 588 złotych za naruszenie: art. 33 ust. 1 RODO, tj. za niezgłoszenie naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia oraz art. 34 ust. 1 RODO, tj. za niezawiadomienie o naruszeniu ochrony danych osobowych, bez zbędnej zwłoki osób, których dane dotyczą.

PUODO w maju 2020 roku otrzymał od osoby trzeciej zawiadomienie o naruszeniu, polegającym na przesłaniu pocztą elektroniczną wiadomości z polisą ubezpieczeniową, przez podmiot przetwarzający w stosunku do TUIR WARTA S.A. na adres e-mail nieuprawnionej osoby trzeciej. W wyniku naruszenia poufności, ujawnieniu uległy imiona, nazwiska, adresy zamieszkania lub korespondencyjne, numery PESEL, numery telefonów, adresy poczty elektronicznej oraz informacje dotyczące samochodu osobowego (przedmiot ubezpieczenia).

PUODO wezwał TUIR WARTA S.A. do wyjaśnienia, czy w związku ze zdarzeniem przeprowadzono analizę ryzyka naruszenia praw i wolności osób fizycznych pod kątem obowiązku zawiadomienia PUODO oraz osób fizycznych, których dane osobowe dotyczą.

W odpowiedzi TUIR WARTA S.A. wskazała, że nie doszło do naruszenia skutkującego koniecznością zawiadomienia Prezesa UODO, ponieważ:

1. klient sam podał błędny adres poczty elektronicznej, na który został wysłany dokument polisy ubezpieczeniowej,
2. nieuprawniony odbiorca zwrócił się do spółki, a więc można wnioskować, że jest on świadomy przepisów i wagi informacji, jakie otrzymał.

TUIR WARTA S.A. oceniła ryzyko naruszenia praw i wolności osób fizycznych, których dane osobowe dotyczą jako niskie. To stanowisko poparła również tym, że osoba trzecia została poproszona o usunięcie wiadomości zawierającej dane osobowe.

Prezes UODO w uzasadnieniu decyzji zaznaczył, że z naruszeniem ochrony danych mamy do czynienia zarówno w przypadku świadomego działania, jak również nieumyślnego. Błąd klienta, który przekazał agentowi nieprawidłowy adres poczty elektronicznej nie może mieć wpływu na ocenę zdarzenia i niezakwalifikowanie go jako naruszenia ochrony danych osobowych, gdyż zdarzenie skutkowało udostępnieniem danych osobowych osobie nieuprawnionej.

Ponieważ wskazane naruszenie poufności danych dotyczy numerów PESEL (oraz danych osobowych zwykłych) należy uznać, że może wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.

W sprawie toczyła się dalsza polemika w ramach prowadzonej korespondencji, w której TUIR WARTA S.A. najpierw kwestionowała fakt wystąpienia naruszenia ochrony danych osobowych, a na dalszym etapie brak wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą.

Ostatecznie TUIR WARTA S.A. dokonała formalnego zawiadomienia PUODO oraz osób fizycznych, których dane osobowe dotyczą, o naruszeniu dopiero po wszczęciu postępowania administracyjnego przez PUODO (po około pięciu miesiącach od stwierdzenia naruszenia).

Po analizie materiału dowodowego PUODO wydał decyzję o nałożeniu kary pieniężnej na TUIR WARTA S.A.

ZDANIEM AUTORA

Grzegorz Gęborek, radca prawny, manager w [gliwickim oddziale Rödl & Partner](#)

O wadze decyzji i jej wymiarze praktycznym może świadczyć to, że informacja o nałożeniu kary pieniężnej na TUIR WARTA S.A. została zamieszczona nie tylko na stronie internetowej Urzędu Ochrony Danych Osobowych, lecz także w newsletterze UODO dla IOD w styczniu 2021 r. Chociaż kara pieniężna nałożona przez PUODO nie należy do szczególnie wysokich, to należy pamiętać, że naruszenie dotyczyło danych osobowych zaledwie dwóch osób. Oprócz tego, że dane osobowe pozwalały na pełną identyfikację osób fizycznych, to stanowiły też pewną informację o stanie majątkowym tych osób z uwagi na to, iż polisy dotyczyły ubezpieczenia pojazdu.

Decyzja PUODO ma wymiar edukacyjny i stanowi ważną wskazówkę dla administratorów oraz inspektorów ochrony danych osobowych, którzy przeprowadzają analizę ryzyka i rozważają, czy dane naruszenie jest objęte obowiązkiem zgłoszenia do PUODO oraz powiadomienia osób fizycznych, których dane osobowe dotyczą. Jak można zauważyć, nazbyt pochopne lub błędne podjęcie decyzji, może wiązać się z nałożeniem kary przez PUODO.

Co więcej, w uzasadnieniu decyzji PUODO w sposób jasny zajął stanowisko co do sposobu oceny sytuacji, w których naruszenie ochrony danych osobowych jest wynikiem bezpośredniego działania bądź zaniechania osoby fizycznej, której dane osobowe dotyczą. W tym przypadku – podania niewłaściwych danych kontaktowych. W praktyce takie przypadki zapewne mogą występować często. Niemniej PUODO słusznie wskazał, że formalnie doszło do naruszenia poufności danych osobowych. Bez znaczenia pozostaje zatem przyczynienie się do wystąpienia naruszenia ochrony danych osobowych przez osoby fizyczne, których dane osobowe dotyczą czy nawet osoby trzecie. Administrator nie może też arbitralnie, z uwagi na takie przyczynienie się, decydować o niezawiadamianiu organu nadzoru osoby oraz osoby fizycznej, której dane osobowe zostały ujawnione.

O ile trudno polemizować w ogóle z formalnym wystąpieniem naruszenia ochrony danych osobowych w tym przypadku, to pewne wątpliwości może zawsze budzić obowiązek powiadomienia osoby fizycznej. W tym też przypadku PUODO kolejny raz kierował się utartym już podejściem do ochrony numerów PESEL. Z decyzji jasno wynika, że w przypadku ujawnienia choćby niewielkiej liczby numerów PESEL nie można w zasadzie przyjmować innego niż wysokie ryzyka naruszenia praw i wolności osób fizycznych.

Stanowisko PUODO zaprezentowane w przedmiotowej decyzji jest dość racjonalne – mając na uwadze, że podstawowym celem jest ochrona danych osobowych, a jednym z podstawowych obowiązków administratorów jest niezwłoczne zawiadamianie organu nadzoru o przypadkach naruszenia ochrony danych osobowych, które niosą za sobą ryzyko

naruszenia praw i wolności osób fizycznych. Refleksję może też budzić stanowisko adresata decyzji i pewna zawziętość w negacji swoich obowiązków, które ostatecznie zostały wykonane, ale ze zwłoką – co stało się podstawą nałożenia kary. Tym bardziej, że gdyby organ nadzoru i osoby fizyczne zostały zawiadomione o wystąpieniu naruszenia w terminie, to nie wystąpiłyby określone w decyzji podstawy ukarania.

W opinii autora, PUODO w ramach prowadzonej korespondencji wskazał możliwości weryfikacji swojego stanowiska przez TUiR WARTA S.A. oraz ostatecznego wykonania obowiązków jeszcze przed wszczęciem postępowania administracyjnego przez organ. W istocie PUODO kilkakrotnie wezwał TUiR WARTA S.A. do wykonania analizy pod kątem ryzyka naruszenia praw i wolności osób fizycznych niezbędnej do oceny, czy doszło do naruszenia ochrony danych skutkującego koniecznością zawiadomienia go oraz osób, których dotyczy naruszenie, a także przesłania wyjaśnień.