Rödl & Partner

Echo

Data: 19.03.2020

Źródło: Rzeczpospolita

# WYSOKA KARA ZA NARUSZENIA ZASADY POUFNOŚCI DANYCH OSOBOWYCH - DECYZJA UODO

Aneta Siwek, prawnik Gliwice, Rödl & Partner

Administrator i podmiot przetwarzający zobowiązani są ocenić stopień bezpieczeństwa przetwarzania danych i uwzględnić ryzyko wiążące się z przetwarzaniem. Zastosowanie wysokiej kary pieniężnej ma skutecznie doprowadzić do stosowania przez podmiot środków technicznych i organizacyjnych, które zapewnią przetwarzanym danym stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą oraz wadze zagrożeń towarzyszącym procesom przetwarzania danych.
Tak orzekł prezes Urzędu Ochrony Danych Osobowych w decyzji z 10 września 2019 r.

W listopadzie 2018 r. spółka z o.o. z siedzibą w K (dalej: spółka) zgłosiła prezesowi UODO dwa naruszenia ochrony danych osobowych, które dotyczyły uzyskania przez osobę nieuprawnioną dostępu do bazy danych klientów sklepów internetowych należących do spółki oraz uzyskania przez osobę nieupoważnionego dostępu do danych klientów.

W listopadzie 2018 r. spółka została poinformowana przez klientów o otrzymywaniu wiadomości tekstowych informujących o konieczności dokonania dodatkowej opłaty. Spółka zawiadomiła policję i zamieściła na stronie internetowej informację ostrzegającą o fałszywych smsach. Taka sama informacja była przez spółkę wysyłana do klientów e-mail em oraz sms.

W styczniu 2019 r. dokonano w spółce kontroli. Ustalono, że spółka jako administrator naruszyła zasadę poufności danych wyrażonej art. 5 ust. 1 lit. f rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO).

W czerwcu 2019 r. prezes UODO wszczął z urzędu postępowanie administracyjne. Pełnomocnik spółki złożył wyjaśnienia, w których wskazał listę zastosowanych środków bezpieczeństwa, a także potwierdził monitorowanie przez spółkę potencjalnych zagrożeń i wdrażanie metod zapewnienia bezpieczeństwa. W ocenie organu, w sposób niewystarczający oceniono zdolność do ciągłego zapewnienia poufności oraz nie uwzględniono ryzyka związanego z uzyskaniem nieuprawnionego dostępu.

W ocenie prezesa UODO spółka zastosowała środki techniczne i organizacyjne, które przyczyniły się w ograniczonym stopniu do wypełnienia wymogów z art. 32 rozporządzania 2016/679, gdyż przewidywalne ryzyka nie zostały odpowiednio zminimalizowane i ograniczone w czasie przetwarzania, a nałożenie kary pieniężnej na spółkę jest konieczne i uzasadnione wagą oraz charakterem, zakresem zarzucanych spółce naruszeń.

## KOMENTARZ EKSPERTA

Aneta Siwek, prawnik w gliwickim biurze Rödl & Partner

Na mocy decyzji prezesa UODO, spółka została ukarana dotychczas najwyższą w Polsce karą pieniężną, nałożoną w związku z naruszeniem przepisów w zakresie ochrony danych

osobowych w wysokości 2 830 410 zł, równowartość 660 000 euro, według średniego kursu euro ogłoszonego przez NBP w tabeli kursów na 28 stycznia 2019 r.

Spółka została ukarana tak wysoką karą pieniężną wobec stwierdzenia naruszenia zasady poufności danych, wyrażonej w art. 5 ust. 1 lit. f RODO, a odzwierciedlonej w postaci obowiązków określonych w art. 24 ust. 1, art. 25 ust. 1 oraz art. 32 ust. 1 lit. b i d, art. 32 ust. 2 RODO, naruszenia zasad legalności, rzetelności i przejrzystości, wyrażonych w art. 5 ust. 1 lit. a RODO oraz zasady rozliczalności, wyrażonej w art. 5 ust. 2, uszczegółowionych w art. 6 oraz 7 rozporządzenia RODO.

Powodem nałożenia na spółkę kary było niewywiązanie się z obowiązku polegającego na zapewnieniu doboru skutecznych środków technicznych i organizacyjnych na poziomie kontroli dostępu i uwierzytelniania. Spółce zarzucono też nieskuteczne monitorowanie potencjalnych zagrożeń dla praw i wolności, których dane są przetwarzane. Spółka nie była w stanie wykazać, od kiedy zbierała dane osobowe użytkowników w celu ułatwienia wypełniania przyszłych wniosków ratalnych oraz nie przedstawiła klauzul i oświadczeń o wyrażeniu zgody na przetwarzanie przedmiotowych danych.

Za najpoważniejsze uznane zostało naruszenie zasady poufności, w myśl której dane powinny być przetwarzane w sposób zapewniający bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).

Rozporządzenie zawiera katalog środków technicznych i organizacyjnych, jakie administrator i podmiot przetwarzający zobowiązani są wdrożyć w celu zapewnienia dostosowanego do poziomu ryzyka bezpieczeństwa danych. Do katalogu powyższych środków zalicza się m.in. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów usług przetwarzania oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 lit. b i d RODO).

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, administrator i podmiot przetwarzający zobowiązani są uwzględnić ryzyko wiążące się z przetwarzaniem. W szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 ust. 2 RODO).

Niezapewnienie optymalnego poziomu bezpieczeństwa przetwarzanych danych przesądziło o uzyskaniu do nich dostępu przez osoby nieupoważnione. W konsekwencji, wobec niektórych użytkowników korzystających z usług spółki, powzięte zostały niebezpieczne ataki phishingowe zmierzające do wyłudzenia danych uwierzytelniających do rachunków bankowych. Z raportów publikowanych przez CERT Polska wynika, że phishing to kategoria incydentów aktualnie najczęstsza i najbardziej wyróżniająca się na tle innych zagrożeń bezpieczeństwa informatycznego, a ich odsetek utrzymuje się od 2016 r. na poziomie ponad 40 proc. (w 2018 r. – odsetek tego typu incydentów wyniósł 44 proc.).

Zważywszy na skalę przetwarzanych danych ich zakres i kontekst przetwarzania, w ocenie prezesa UODO, spółka nie wywiązała się z obowiązku zapewnienia odpowiednich środków bezpieczeństwa gwarantujących skuteczną ochronę przetwarzanym danym. Z decyzji wynika, że spółka tylko w ograniczonym stopniu spełniła wymagania w zakresie ochrony danych, a zastosowane przez nią środki nie przyczyniły się do optymalnego obniżenia poziomu ryzyka.

Niewątpliwie wdrożenie właściwych środków bezpieczeństwa zapewniających niezbędny poziom ochrony danych, znacznie zminimalizowałoby ryzyko uzyskania do nich nieuprawnionego dostępu oraz naruszenia praw i wolności użytkowników i w tym zakresie stanowisko prezesa UODO należy uznać za słuszne. Uzasadnione wątpliwości budzi wysokość kary, która spełniłaby rolę również w niższym wymiarze.