1 mln złotych za nieprzestrzeganie RODO – kontrowersyjna decyzja UODO

W dniu 26 marca 2019 roku Prezes UODO dr Edyta Bielak – Jomaa podczas zorganizowanej konferencji prasowej poinformowała o nałożeniu – na podstawie decyzji nr ZSPR.421.3.2018 wydanej w dniu 15 marca 2019r. (dalej Decyzja) na podmiot przetwarzający dane osobowe dostępne z publicznych rejestrów m.in. CEIDG oraz KRS, kary za nieprzestrzeganie RODO w wysokości 943 tys. zł. Jest to pierwsza kara nałożona przez polski organ nadzoru za nieprzestrzeganie postanowień RODO. Pierwsza, i do tego tak wysoka kara jest z pewnością złą prognozą nie tylko dla podmiotów, które pomimo upływu kilku miesięcy od dnia wejścia w życie RODO nadal nie przygotowały organizacji do ww. przepisów ale również dla podmiotów, które co prawda przygotowały się do RODO jednak nie wypełniły wstecz obowiązku informacyjnego.

Pierwsza „ofiara" za nieprzestrzeganie RODO

Pierwszą „ofiarą" RODO padł podmiot przetwarzający dane osobowe w celach zarobkowych, które dostępne były w publicznych rejestrach tj. Centralnej Ewidencji i Informacji Działalności Gospodarczej (CEiDG), Rejestru Przedsiębiorców Krajowego Rejestru Sądowego oraz Bazy REGON Głównego Urzędu Statystycznego. Pomimo przetwarzania danych osobowych, podmiot ten nie wypełnił – zdaniem organu nadzorczego - zgodnie z RODO obowiązku informacyjnego wobec osób, których dane przetwarzał. Administrator wypełnił obowiązek informacyjny jedynie wobec osób, których posiadał adres e-mail, natomiast obowiązek informacyjny – jak wskazano w Decyzji - nie został wypełniony wobec osób fizycznych prowadzących działalność gospodarczą, co do których Spółka nie posiadała adresu e-mail w swojej bazie danych, przy czym dotyczy to zarówno przedsiębiorców, którzy aktualnie prowadzą działalność gospodarczą bądź tę działalność zawiesili jak i tych, którzy tej działalności już nie prowadzą, lecz prowadzili ją w przeszłości. Prezes UODO w uzasadnieniu podjętej decyzji wskazała m.in., że podmiot miał świadomość o ciążącym na nim obowiązku informacyjnym, jednak z uwagi na wysokie koszty tego obowiązku nie wypełnił. Istotne w niniejszej sprawie są liczby – podmiot przetwarzał w dedykowanym systemie dane ok. 6 mln osób tj. 3.59 mln osób fizycznych prowadzących aktualnie jednoosobową działalność i 2,33 mln osób fizycznych prowadzących w przeszłości działalność gospodarczą. Obowiązek informacyjny został wypełniony jedynie wobec ok. 682 tys. osób, odnośnie których spółka posiadała adresy e-mail (spółka przesłała treść obowiązku informacyjnego na podane adresy e-mail). Wobec pozostałych osób, obowiązek nie został wypełniony. Z uwagi na skalę przetwarzania danych, UODO zdecydował się podjąć decyzję o nałożeniu na ten podmiot kary w postaci: dopełnienia przez podmiot obowiązku podania informacji określonych w art. 14 ust 1 i 2 RODO również wobec osób, których danych podmiot nie posiadał oraz administracyjnej kary pieniężnej w wysokości 943 tys. zł.

Dlaczego podmiot pomimo tego, że – jak wskazał UODO - wiedział o ciążącym na nim obowiązku informacyjnym postanowił go nie wypełnić? Jak wynika z treści decyzji podmiot powoływał w toku postępowania kontrolnego prowadzonego przez UODO następujące argumenty:

1) informacje o przetwarzaniu danych osobowych znajdowały się na stronie internetowej podmiotu,
2) podmiot nie posiadał numerów telefonów do osób, których dane przetwarzał wobec czego nie mógł wypełnić tego obowiązku telefonicznie (a nawet jeżeli posiadał numery telefonów spółka powoływała się na wysokie koszty tej operacji),
3) dane przetwarzane przez spółkę są danymi publicznie odstępnymi zgromadzonymi w oficjalnych, publicznych rejestrach, zakres tych danych jest wąski a ryzyko dla praw i wolności osób, których dane dotyczą, związane z ich przetwarzaniem – niskie,
4) koszt poinformowania osób, których dane dotyczą z wykorzystaniem poczty tradycyjnej spółka wyceniła na ok 33mln zł,
5) realizacja obowiązku informacyjnego tj. indywidualny kontakt z każdą osobą powodowałby „nadmierny wysiłek" – spółka uznała, że może skorzystać z wyłączenia określonego w przepisie art. 14 ust. 5 lit. b RODO.

Powyższe argumenty nie przekonały jednak organu nadzoru, który zdecydował się nałożyć na Spółkę karę.

Kosztowny obowiązek informacyjny

Nieprawidłowości stwierdzone przez UODO dotyczą kwestii wypełnienia przez podmiot obowiązku informacyjnego, który wielu przedsiębiorcom po wejściu w życie przepisów ogólnego rozporządzenia o ochronie danych osobowych daje się we znaki. RODO wymaga aby administrator w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielił osobie wszelkich informacji o przetwarzaniu jej danych osobowych. Zakres przekazywanych informacji przez administratora – w zależności od sposobu pozyskania tych danych – został określony w przepisie art. 13 i art. 14 RODO. Możliwość nieinformowania osób, których dane dotyczą o przysługujących im prawach dotyczy sytuacji, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami lub udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Na tą przesłankę powołał się ukarany podmiot. Czy wysokie koszty wypełnienia obowiązku informacyjnego albo adresowanie korespondencji listownie do ok. 6,5 mln osób (wobec tylu osób spółka dysponuje wyłącznie adresami korespondencyjnymi) uzasadniają spełnienie przesłanki „niewspółmiernie dużego wysiłku", wobec czego indywidualne przesłanie treści obowiązku informacyjnego nie jest konieczne? Należy zauważyć, że koszty wypełnienia obowiązku poprzez przesłanie do każdej z tych osób listu stanowiłyby połowę rocznego przychodu spółki. W uzasadnieniu Decyzji organ nadzoru wskazał, że w 2017 roku spółka osiągnęła przychód netto ze sprzedaży w wysokości ok 29 mln zł. Przy założeniu, że spółka miałaby wysłać do każdej z osób, której dane posiada (a nie dysponuje adresami e-mail tylko korespondencyjnymi), to wypełnienie obowiązku informacyjnego poprzez wysłanie do tych osób przesyłki listowej nierejestrowanej kosztowałoby spółkę 16mln 900tys zł. (koszt przesyłki listowej nierejestrowanej to 2,60 zł, a spółka miałaby wysłać obowiązek informacyjny wobec 6.5mln zł). Natomiast spełnienie obowiązku informacyjnego za pomocą przesyłki rejestrowanej (z potwierdzeniem odbioru), dzięki czemu spółka mogłaby udowodnić fakt wysłania obowiązku informacyjnego do osób, których dane dotyczą kosztowałby podmiot

aż 33 mln 800 tys. zł, co oznacza, że jest to kwota wyższa niż przychody netto. W decyzji co prawda wskazano, że z przepisu art. 14 RODO nie wynika, aby prawodawca nałożył obowiązek wysłania informacji o przetwarzaniu danych przesyłką poleconą, ale konieczne jest aby administrator spełnienie takiego obowiązku wykazał. A jak lepiej wykazać fakt wysłania obowiązku informacyjnego pocztą jak nie poprzez zachowanie dowodu nadania przesyłki pocztowej?

UODO nie rozumie biznesu

Pomimo tego, że w uzasadnieniu Decyzji organ nadzoru wskazał wysokość przychodów spółki w roku poprzedzającym, niż w roku w którym przeprowadzono kontrolę (kontrola była przeprowadzana w 2018 roku), to jednak organ nadzoru w ogóle nie wziął pod uwagę jak koszty wypełnienia obowiązku informacyjnego (wysłania treści obowiązku informacyjnego listownie) mogłyby wpłynąć na prowadzenie działalności przez ten podmiot. Twierdzenia organu nadzoru, że powoływanie się na „wielomilionowe koszty" wypełnienia obowiązku informacyjnego oznacza de facto, że spółce należy przypisać umyślność działania jest niedorzeczne. Tym bardziej, że organ sam stwierdził, że nie ustalono aby po stronie osób, których dane dotyczą powstała jakakolwiek szkoda. Co również istotne, zauważyć trzeba, że tak wysoka kara została wymierzona nie z uwagi na wyciek danych a z uwagi na rzekome niewypełnienie formalizmu. Zastanawiające jest zatem jak dużą karę wymierzyłby organ, gdyby doszło do wycieku danych.

Co równie istotne, UODO nie pochyliło się nad jeszcze jedną, bardzo ważną kwestią a mianowicie momentu zapisania „rekordów" (danych osób fizycznych) w bazie Spółki. Jeżeli nastąpiło to przed dniem 25 maja 2018r. tj. przed wejściem w życie RODO, to należy się zastanowić czy zasadne jest powoływanie się przez organ nadzoru na treść motywu 171, który wskazuje, że „przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów". Organ nadzoru nie pochylił się nad tym, że obowiązek informacyjny powstaje w momencie pozyskiwania danych osobowych, jeżeli administrator pozyskuje je w sposób bezpośredni od osoby, której dane dotyczą (art. 13 RODO). Natomiast jeżeli dane te nie są pozyskiwane w sposób bezpośredni – tak jak w niniejszej sprawie – to konieczność poinformowania aktualizuje się – zgodnie z przepisem art. 14 ust 3 lit a) – c) RODO: w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych; jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu. Całkowicie zasadne wydaje się stwierdzenie, że po wejściu w życie RODO nie było konieczne wypełnienie obowiązku informacyjnego wstecz, zgodnie z zasadą, że prawo nie działa wstecz.

Ewentualne nałożenie kary na podmiot wobec niewypełnienia obowiązku informacyjnego powinno zatem dotyczyć wyłącznie osób, których dane spółka pozyskała po 25 maja 2018r. a nie osób których dane posiadała i przetwarzała przed wejściem w życie RODO.

Nie pozostaje nic innego jak obserwować dalszy przebieg niniejszej sprawy. Podmiot z pewnością odwoła się od decyzji do sądu. Być może zasadne byłoby skierowanie pytania prejudycjalnego do do Trybunału Sprawiedliwości Unii Europejskiej w zakresie właściwej wykładni pojęcia „nadmiernych wysiłków" i oceny czy w jego zakres wchodzą także nadmierne koszty, które de facto mogą spowodować zakończenie prowadzenia biznesu.

Co więcej fakt, że oprócz nałożenia kary administracyjnej UODO zobowiązało podmiot do wypełnienia obowiązku informacyjnego wstecz oznacza, że organ ten nie pozostawia złudzeń w zakresie dość surowego podejścia do kwestii zapewnienia przetwarzania danych osobowych zgodnie z prawem w zakresie spełnienia przez administratorów wszelkich formalizmów nawet jeżeli osoby, których dane dotyczą nie poniosły szkody.

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