Wycieku danych osobowych nie wolno utajniać

Wdrożenie odpowiednich procedur, polityk i dokumentów wykonawczych pozwala dostosować codzienne funkcjonowanie firmy do standardów RODO. Jak jednak pokazuje praktyka, nawet ścisłe przestrzeganie RODO nie jest w stanie zapobiec wystąpieniu incydentu ochrony danych, podobnie jak zapinanie pasów i wyposażenie samochodu w poduszki powietrzne nie zapobiegnie wypadkowi. Grunt, aby wiedzieć, jak postąpić, gdy taki „RODO-wypadek" się przydarzy.

Incydent ochrony danych osobowych

Tytułowy „wyciek" danych to jedna z form incydentu ochrony danych osobowych. Wyciek danych stanowi naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Wystąpi on np. w sytuacji wykradzenia z biura firmy danych w postaci dokumentacji papierowej, znajdującej się w segregatorze. Najczęściej jednak dotyczy przełamania zabezpieczeń teleinformatycznych, np. włamania się do wewnętrznej sieci informatycznej firmy.
Przez ostatni rok częstymi ofiarami takich zdarzeń były firmy z branży e-commerce. Doszło do wielu przypadków wykradzenia danych osobowych klientów ze sklepów czy serwisów internetowych, nierzadko połączone z uzyskaniem nieuprawnionego dostępu do skrzynek pocztowych nieświadomych klientów lub ich kont bankowych. W praktyce do naruszenia równie często dochodzi w wyniku działania pracownika, np. w razie skopiowania danych na niezabezpieczony pendrive, a następnie jego zagubienia i rozpowszechnienia znajdujących się tam danych. Z taką sytuacją możemy mieć też do czynienia, jeżeli dojdzie do wysłania danych do niewłaściwie zabezpieczonej chmury. Przykładem jednego z głośniejszych wycieków danych w ostatnim czasie jest incydent ujawnienia danych ok. 339 miliona gości hotelów sieci Marriott International Inc. – Biuro Komisarza ds. danych osobowych w Wielkiej Brytanii poinformowało, iż zamierza ukarać firmę karą 99 mln funtów brytyjskich.

Ocena, czy doszło do naruszenia ochrony danych osobowych, stanowi pierwszy stopień działań rozpoznawczych. Jeżeli jest pozytywna – pociąga za sobą konieczność działań naprawczych, które mogą wymagać poinformowania osób, których dane dotyczą, lub organu ochrony danych (PUODO).

Incydenty ochrony danych osobowych w liczbach

Zgodnie ze statystykami prowadzonymi przez UODO, w ciągu roku od wejścia w życie RODO liczba zgłoszeń incydentów dotyczących naruszenia ochrony danych utrzymuje się na podobnym poziomie i wyniosła odpowiednio:

Firmy nie zgłaszają wszystkich zdarzeń, które należy uznać za incydenty. Są one jednak stałym elementem rzeczywistości i można zaryzykować stwierdzenie, że nieprędko się to zmieni. Rośnie natomiast liczba kontroli prowadzonych przez Prezesa UODO, w wyniku których w 2019 r. zaczęły pojawiać się pierwsze kary pieniężne. Już choćby z tego względu warto wiedzieć, co zrobić, gdy wydarzy się incydent.

Niezwłoczne zawiadomienie UODO

Po wykryciu, że w firmie doszło do naruszenia ochrony danych osobowych, niezbędne jest przede wszystkim natychmiastowe podjęcie doraźnych środków bezpieczeństwa i wyjaśnienie, co się stało. Obejmuje to zidentyfikowanie źródła i okoliczności naruszenia oraz zweryfikowanie wadliwych procedur bądź zabezpieczeń. Są to w dużym skrócie działania podejmowane wewnątrz organizacji, mające na celu „zatkanie wycieku".

Równolegle administrator powinien ustalić, czy w wyniku incydentu mogło dojść do naruszenia praw i wolności osób, których dane obejmowało zdarzenie. W dalszej kolejności musi sprawdzić, czy ma obowiązek zgłosić naruszenie Prezesowi UODO (np. czy naruszenie może skutkować stratami finansowymi czy nieuprawnionym dostępem do usług zewnętrznych, z których korzystają końcowe ofiary wycieku). Jeżeli zachodzi obowiązek zgłoszenia naruszenia Prezesowi UODO, należy działać niezwłocznie – nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.

W praktyce te obowiązki sprawiają sporo problemów. Przede wszystkim z uwagi na krótki czas, kiedy powinny być dokonane ustalenia – zwłaszcza jeśli do wycieku dojdzie w weekend albo w czasie urlopu osoby odpowiedzialnej za RODO. Problematyczna jest też nieostrość kryteriów, na podstawie których kwalifikuje się incydent do zgłoszenia.

To administrator dokumentuje okoliczności związane z naruszeniem ochrony danych (np. określa charakter naruszenia) i jego skutki (np. określenie przybliżonej liczby osób, których dotyczy naruszenia i możliwe konsekwencje naruszenia) oraz podjęte środki zaradcze. Konsekwencje nieprawidłowej oceny w pełni obciążają administratora – niezawiadomienie Prezesa UODO może pociągać za sobą konsekwencje administracyjne. Dlatego istotne jest wprowadzenie odpowiednich procedur i ich prawidłowe wdrożenie, zanim wystąpi incydent.

Zawiadomienie zainteresowanych

Jeżeli naruszenie ochrony danych osobowych wymagało zgłoszenia do Prezesa UODO, a ryzyko naruszenia praw lub wolności osób dotkniętych incydentem administrator określił jako wysokie, musi dodatkowo poinformować o sytuacji te osoby (co również wymaga zadeklarowania oraz opisu w odpowiednim formularzu udostępnianym przez UODO).

Może to oznaczać znaczne koszty, dlatego kluczowe jest odpowiednie zabezpieczenie danych. Jeżeli dane objęte wyciekiem byłyby zaszyfrowane w stopniu uniemożliwiającym ich odczyt, wysokie ryzyko raczej nie powstanie. Administrator może nie zawiadamiać osób, których dane dotyczą, również wtedy, gdy wymagałoby to niewspółmiernie dużego wysiłku.

(Nie)współmierny wysiłek

Analizując niedawną decyzję o nałożeniu przez Prezesa UODO pierwszej kary za nieprzestrzeganie RODO (decyzja z 15 marca 2019 r., ZSPR.421.3.2018) zalecana jest ostrożność w opieraniu się na przesłance „niewspółmiernie dużego wysiłku" dla przedsiębiorcy. W przywołanej decyzji Prezes UODO uznał, że wyliczone znaczne koszty wysłania zawiadomień pocztą nie uzasadniają, że takie zawiadomienia wymagałyby od przedsiębiorcy owego niewspółmiernie dużego wysiłku.

Czynności, jakie zostaną podjęte w ciągu pierwszych 72 godzin od chwili dowiedzenia się o incydencie ochrony danych osobowych, są kluczowe dla zarządzania ryzykiem, jakie może wystąpić w przyszłości. Odpowiednio szybka i trafna ocena ryzyka oraz podjęcie działań informacyjnych powinny uzupełniać działania wewnętrzne ukierunkowane na ustalenie okoliczności naruszenia i przerwanie stanu naruszeń.

Zdaniem autora

Incydent w obszarze ochrony danych osobowych zmusza do zmierzenia się z pewną barierą – firma zwykle chce zachować fakt naruszenia we względnej tajemnicy, zachować twarz przed klientami i kontrahentami. Takie działanie może jednak szkodzić jej renomie, skutkować podjęciem działań przez UODO, a nawet narazić na roszczenia cywilnoprawne ze strony nieostrzeżonych w porę osób, których dane były przedmiotem naruszenia. Z tą barierą należy się zmierzyć i ją przełamać dla wspólnego dobra firmy oraz jej klientów. W przypadku incydentów nie pojawia się pytanie „czy", ale „kiedy" – dlatego najważniejsza jest prewencja i odpowiednie zabezpieczenia.

Autor: Jan Molicki, radca prawny, Kancelaria Prawna Piszcz i Wspólnicy sp.k.