Warszawa, 30.05.2022 r.

W jaki sposób prawidłowo zawiadomić o naruszeniu podmiot danych?

Zarządzanie incydentami ochrony danych osobowych w organizacji to jedno z większych wyzwań z jakimi mierzą się administratorzy i Inspektorzy Ochrony Danych od momentu funkcjonowania RODO. Obsługa incydentów wymaga podjęciu wielu działań ze strony administratora. W pierwszej kolejności musi być duża świadomość w organizacji takich sytuacji, aby móc szybko i skutecznie zidentyfikować potencjalne naruszenie. Z drugiej strony, już po stwierdzeniu, że do naruszenia doszło, administrator musi podjąć szybkie kroki w celu oceny potencjalnego ryzyka dla praw i wolności osób, których dane zostały naruszone. Administrator za pomocą różnego rodzaju metodologii, m.in. metodologii ENISA, ocenia poziom i skalę naruszeń. Finalna ocena ma bardzo duży wpływ na kolejne kroki administratora przy obsłudze naruszenia.

W przypadku, gdy naruszenie powoduje średnie ryzyko naruszenia praw i wolności, administrator zobowiązany jest do zawiadomienia o incydencie Prezesa Urzędu Ochrony Danych Osobowych w przeciągu 72h od momentu stwierdzenia naruszenia. Jest to bardzo krótki okres, który wymaga od administratora natychmiastowego działania i zarządzenie incydentem. W przypadku, gdy podczas oceny naruszenia, administrator stwierdzi wysokie ryzyko dla praw i wolności podmiotu danych, dodatkowym obowiązkiem będzie zawiadomienie podmiotu danych o naruszeniu jego danych osobowych.
W jaki sposób prawidłowo zawiadomić podmiot danych? O czym należy pamiętać? Na co zwraca uwagę PUODO? O tym poniżej.

Zawiadomienie podmiotu danych

Z doświadczenia pracy w roli Inspektora Ochrony Danych muszę stwierdzić, że podczas korespondencji z PUODO dotyczącą zgłoszonego naruszenia jednym z najczęstszych zastrzeżeń Urzędu jest sposób zawiadomienia podmiotów danych. PUODO zazwyczaj nakazuje ponowne zawiadomienie podmiotu danych wskazując na liczne uchybienia przy pierwszej komunikacji z osobą, której dane zostały naruszone.

Co do zasady zawiadomienie powinno być przekazane bezpośrednio podmiotowi danych. Może to odbywać się za pomocą wiadomości e-mail, SMS, wiadomości listownej. W przypadku, gdy ilość osób, które należy zawiadomić jest bardzo szeroka lub administrator nie posiada bezpośredniego kontaktu do tych osób wskazane jest zawiadamianie za pomocą: banerów na stronach internetowych, reklamy, komunikatu prasowego lub inną formą masowego przekazu. Zgodnie z zalecaniami Grupy Roboczej art. 29 w wytycznych dotyczących zgłaszania naruszeń ochrony zgodnie z rozporządzeniem 2016/679 (obecnie Europejska Rada Ochrony Danych) forma i sposób komunikacji wybrany przez administratora powinien gwarantować łatwość i dostępność informacji o zawiadomieniu.

Komunikat ten powinien być przekazany w jak najprostszej formie, która dokładnie pozwoli zrozumieć zaistniałe zagrożenie oraz co podmiot danych powinien zrobić, aby zabezpieczyć się przed skutkami naruszenia.

Co istotne, zgodnie z zasadą rozliczalności, administrator musi być w stanie wykazać przed organem nadzorczym, że w przypadku pojawienia się obowiązku zawiadomienia podmiotu danych, obowiązek ten został zrealizowany. Dlatego też ewentualne powiadomienia ustne, mimo, że nie są przez przepisy prawa zabronione, nie są rekomendowane.

Treść zawiadomienia – na co zwracać uwagę?

Art. 33 ust. 3 RODO wskazuje na elementy, które muszą znaleźć się w każdym zawiadomieniu o naruszeniu ochrony danych osobowych. W pierwszej kolejności wskazany jest tzw. opis charakteru naruszeń. Administrator prostym i jasnym językiem powinien wytłumaczyć podmiotowi danych co tak naprawdę się stało z jego danymi osobowymi. Informacja ta powinna zawierać informację czy doszło do kradzieży danych, czy do ich usunięcia, zgubienia, nieuprawnionego dostępu itd. Administrator powinien, w miarę możliwości, poinformować również o rodzaju i liczbie naruszonych danych.

W dalszej kolejności przepisy obligują do poinformowania o danych kontraktowych inspektora ochrony danych lub innego punktu kontaktowego. Jest to istotne, aby podmiot danych mógł w każdej chwili zgłosić się do administratora z pytaniem o większą ilość informacji dotyczącą naruszenia jego danych osobowych. Administrator powinien wyjaśnić osobie fizycznej wszelkie okoliczności związane z naruszeniem. Dane kontaktowe powinny zawierać imię, nazwisko, adres e-mail lub numer telefonu.

Dwie pozostałe przesłanki z art. 33 ust. 3 to:

a) Opis możliwych konsekwencji naruszenia,
b) Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszenia.

Oba przypadki wywołują liczne uwagi ze strony PUODO i są powodem, przez które Urząd nakazuje administratorom ponowne zawiadomienie podmiotów danych. W poradniku dotyczącym obowiązków administratorów związanych z naruszeniami ochrony danych osobowych (https://uodo.gov.pl/pl/134/1029) oraz w pismach kierowanych do administratorów, Urząd zwraca uwaga, że konsekwencje naruszeń muszą być wskazane wprost. Dodatkowo, powinny być opisane jasnym i zrozumiałym dla odbiorców językiem. Należy unikać takich sformułowań jak: „uszczerbek fizyczny", „strata finansowa", „kradzież tożsamości". Zdaniem PUODO takie sformułowania są niewystarczające. Opis tych konsekwencji musi odzwierciedlać realne ryzyko wynikające z naruszenia. Przykłady takich konsekwencji zdaniem Urzędu są następujące: „osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji

pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL" lub „Pani / Pana dane osobowe mogą być wykorzystywane do wzięcia na Pani / Pana dane pożyczki krótkoterminowej".

Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu / środki minimalizujące negatywne skutki naruszenia

Przy tworzeniu zawiadomienia ww. punkt rodzi liczne problemy dla administratora. Zdarza się dosyć często, że trudno jest wskazać realne środki, które administrator może podjąć, aby zaradzić naruszeniu. Należy jednak kategorycznie unikać sformułowań mówiących o dobrych intencjach administratora, poprawie w przyszłości, podjęciu czynności minimalizujących ryzyko (ale bez wskazania jakie to są czynności). Zdaniem PUODO mają to być opisane konkretne działania podjęte przez administratora po zaistnieniu naruszenia. Jako przykład PUODO podaje takie sformułowanie: „*W związku z zaistniałym naruszeniem ochrony danych osobowych dokonaliśmy zmian w zakresie procedury weryfikacji poprawności adresu korespondencyjnego oraz zwróciliśmy się do niewłaściwego odbiorcy o zwrot dokumentacji. Dokonaliśmy także poprawienia Pani danych kontaktowych w celu uniknięcia wystąpienia podobnego zdarzenia w przyszłości. Naruszenie ochrony danych zgłosiliśmy również Prezesowi UODO.*"

W przypadku środków minimalizujących negatywne skutki należy wskazać przykłady konkretnych działań, które podmiot danych może podjąć, aby uniknąć tych skutków. Te działania muszą być oczywiście dostosowane do charakteru danego naruszenia. Na przykład w przypadku naruszenia danych osobowych w postaci numeru telefonu i adresu e-mail świetnym przykładem takich środków będzie: ignorowanie wiadomości od nieznanych nadawców, nieklikanie w niezweryfikowane linki otrzymane za pomocą sms lub e-mail, blokowanie nieznanych numerów telefonu.

Tak pokrótce przedstawiają się obowiązki wynikające z konieczności zawiadomienia podmiotów danych o naruszeniu. Przygotowując zawiadomienie pamiętajmy o prostym i jasnym języku, bez używania skomplikowanych fraz. Istotne jest, aby informacja odpowiadała okolicznościom naruszenia. Unikajmy ogólnych sformułowań, używajmy określeń wskazujących na konkretne działania podjęte przez administratora.

Maciej Łukaszewicz – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.