ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

NARUSZENIA OCHRONY DANYCH OSOBOWYCH
Stwierdzenie naruszenia i zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych (PUODO)

Część 2

MATERIAŁ SZKOLENIOWY PRZYGOTOWANY PRZEZ CZŁONKÓW KOMISJI DS. OCHRONY DANYCH OSOBOWYCH DZIAŁAJĄCEJ PRZY ŚZGiP (6/13)

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

STWIERDZENIE NARUSZENIA

W przypadku zaistnienia naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości nie później niż w terminie **72 godzin po stwierdzeniu naruszenia** - zgłasza je organowi nadzorczemu (czyli Prezesowi Urzędu Ochrony Danych Osobowych), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Istotny (krytyczny niejako) jest zatem **moment stwierdzenia naruszenia.** Należy uznać, że administrator **„stwierdza”** wystąpienie naruszenia w momencie, w którym uzyskał **wystarczającą dozę pewności** co do tego, że doszło lub mogło dojść do wystąpienia incydentu bezpieczeństwa, który doprowadził lub mógł doprowadzić do naruszenia poufności, integralności lub dostępności przetwarzanych danych osobowych.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

„STWIERDZENIE” – MOMENT NARUSZENIA

Okoliczności zdarzenia, będą warunkowały to, czy faktycznie doszło do naruszenia ochrony danych i wskazywały kiedy można uznać, że administrator „stwierdził” wystąpienie określonego naruszenia. Jednakże do każdego przypadku należy podejść indywidualnie, gdyż nie zawsze sytuacja będzie klarowna i jednoznaczna. W niektórych przypadkach stwierdzenie samego wystąpienia naruszenia (w tym określenie momentu jego stwierdzenia) będzie łatwe i przejrzyste, a w innych może nastręczać sporo trudności.

Kluczowe jest zatem, aby sprawnie i możliwie szybko dokonać weryfikacji danej sytuacji (danego zdarzenia) w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak - by podjąć działania zaradcze i w razie konieczności zgłosić naruszenie do PUODO.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

PRZYKŁADY

1. W przypadku utraty pamięci USB zawierającej niezaszyfrowane dane osobowe ustalenie, czy nieuprawnione osoby uzyskały dostęp do tych danych, okazuje się często niemożliwe. Niemniej jednak, mimo że administrator może nie być w stanie ustalić, czy w danym przypadku doszło do naruszenia dotyczącego poufności danych, taki przypadek musi zostać zgłoszony, ponieważ można z wystarczającą dozą pewności stwierdzić, że doszło do naruszenia dotyczącego dostępności danych, a samo naruszenie poufności danych jest wysoce prawdopodobne; w tym kontekście przyjmuje się, że administrator „stwierdził” wystąpienie naruszenia w momencie, w którym zdał sobie sprawę z utraty pamięci USB.

2. Administrator wykrywa potencjalne włamanie do swojej sieci. Administrator sprawdza systemy w celu ustalenia, czy bezpieczeństwo danych osobowych przechowywanych w tym systemie zostało narażone na szwank, po czym potwierdza, że faktycznie tak się stało. Ponownie, ponieważ administrator uzyskał dowody jednoznacznie świadczące o wystąpieniu naruszenia, nie można mieć żadnych wątpliwości co do tego, że „stwierdził” wystąpienie takiego naruszenia.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

JAK POSTĘPOWAĆ W SYTUACJI PODEJRZENIA ZAISTNIENIA INCYDENTU BEZPIECZEŃSTWA?

Po otrzymaniu pierwszej informacji o potencjalnym, możliwym naruszeniu ochrony danych osobowych (np. od osoby fizycznej, organizacji medialnej lub z innego źródła) lub po samodzielnym wykryciu incydentu bezpieczeństwa, zasadne jest, by administrator przeprowadził krótkotrwałe postępowanie (weryfikację i analizę okoliczności), aby ustalić, czy faktycznie doszło lub mogło dojść do naruszenia ochrony danych.

Zasadniczo, do momentu zakończenia tego postępowania, **nie można** uznać, że administrator **„stwierdził”** wystąpienie naruszenia.

Niemniej jednak i w tym przypadku mogą pojawić się trudności interpretacyjne ze względu na możliwą złożoność sytuacji i trudności w jednoznacznym wskazaniu momentu stwierdzenia przez administratora zaistniałego naruszenia.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Przykłady incydentów bezpieczeństwa i określenia momentu jego zaistnienia.

1. Pracownik poczty (listonosz) dostarczający przesyłkę z Urzędu Miasta wykonał telefon do Wydziału z informacją o zagubieniu przesyłki. Pracownik Wydziału przekazał informację Inspektorowi Ochrony Danych. Inspektor po przeanalizowaniu stanu faktycznego skontaktował się z placówką pocztową i otrzymał informację, że nie nastąpiło oficjale zgłoszenie incydentu na poczcie. Po tygodniu od zdarzenia okazało się, że przesyłka nie została zagubiona.

2. Wydział rejestruje brak otrzymania zwrotnego potwierdzenia odbioru. Występuje z reklamacją do placówki pocztowej. Operator pocztowy uznaje reklamację i stwierdza, że przesyłka została zgubiona. Pismo z odpowiedzią na reklamację zostaje przekazane do Kancelarii Urzędu Miasta, a następnie do wydziału merytorycznego. Jednakże w wydziale merytorycznym okazuje się, iż pracownik odpowiedzialny jest nieobecny. W konsekwencji przesyłka pozostaje nieotwarta przez dwa tygodnie od daty zarejestrowania jej w Kancelarii. Po powrocie pracownik tego samego dnia zgłasza incydent bezpieczeństwa do Inspektora Ochrony Danych.
W przedmiotowej sprawie datą, którą należy brać pod uwagę jako początek konieczności uruchomienia procedury weryfikacyjnej pod kątem zaistnienia naruszenia danych osobowych jest pieczęć z datą wpływu do Kancelarii Urzędu Miasta. Ponadto, warto zwrócić uwagę na istotny w tej sprawie brak zastępowalności pracowników. Okazuje się bowiem, że w przedmiotowej sprawie brak zachowania ciągłości działania miał krytyczny wpływ na rozpoczęcie procedury weryfikacji.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Dziękujemy za uwagę.

Komisja ds. Ochrony Danych Osobowych

https://silesia.org.pl/struktura/komisje/komisja-ds-ochrony-danych-osobowych/