ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

NARUSZENIA OCHRONY DANYCH OSOBOWYCH
Część 1

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

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Czym są incydenty bezpieczeństwa i naruszenia ochrony danych?

Incydent bezpieczeństwa informacji to zaistniałe zdarzenie, które może mieć wpływ na bezpieczeństwo informacji tj. każdy stwierdzony fakt udostępnienia lub umożliwienia dostępu do informacji osobie nieupoważnionej, nieuprawnionego ujawnienia informacji, utraty, uszkodzenia, zniszczenia jej nośnika lub jakiegokolwiek elementu zabezpieczenia. Incydent taki może dotyczyć sfery technicznej, organizacyjnej czy też informatycznej.

Naruszenie ochrony danych osobowych to rodzaj incydentu bezpieczeństwa oznaczający naruszenie bezpieczeństwa danych osobowych - prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

„INCYDENT + DANE OSOBOWE = NARUSZENIE”

Generalnie, aby doszło do naruszenia ochrony danych osobowych, zaistniały incydent musi dotyczyć danych osobowych w jakikolwiek sposób przetwarzanych, a jego skutkiem może być przede wszystkim zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp
do danych i najczęściej jest on skutkiem złamania zasad bezpieczeństwa.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Naruszenie ochrony danych osobowych może dotyczyć:

- **poufności danych -** naruszanie w rezultacie którego dochodzi do nieuprawnionego (celowego lub przypadkowego) ujawnienia lub dostępu do danych,
- **integralności danych** - naruszanie w rezultacie którego dochodzi do nieuprawnionego (celowego lub przypadkowego) zmodyfikowania danych,
- **dostępności danych** - naruszanie w rezultacie którego dochodzi do nieuprawnionego (celowego lub przypadkowego) zniszczenia danych lub uniemożliwienia do nich dostępu.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

JAK POSTĘPOWAĆ W SYTUACJI ZAISTNIENIA INCYDENTU BEZPIECZEŃSTWA?

Każda osoba, która stwierdziła zaistnienie incydentu bezpieczeństwa, była jego sprawcą lub świadkiem, zobligowana jest do niezwłocznego zgłoszenia takiego zdarzenia do bezpośredniego przełożonego. Dalszy sposób postępowania wyznaczają procedury wewnętrzne wdrożone w urzędzie.

UWAGA!

W związku z koniecznością podjęcia określonych działań naprawczych oraz wynikających z przepisów prawa, istotna jest szybka reakcja na zaistniały incydent i jego natychmiastowe zgłoszenie. W sytuacji jakichkolwiek wątpliwości należy w każdym przypadku kontaktować się z bezpośrednim przełożonym lub Inspektorem Ochrony Danych. Nie należy przy tym obawiać się zgłoszenia incydentu - to z jednej strony obowiązek prawny, ale także i moralny - dbałość o bezpieczeństwo osób, których dane dotyczą.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Dalszy sposób postępowania w sytuacji zaistnienia naruszenia ochrony danych osobowych.

Naruszenia ochrony danych wymagają kompleksowych i spójnych działań administratora danych w celu zarówno wdrożenia działań naprawczych jak i wykonania obowiązków prawnych w tym zakresie, na które składa się przede wszystkim ocena wagi takiego naruszenia, zawiadomienie organu nadzorczego oraz powiadomienie osób, których dane dotyczą.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

ZAWIADOMIENIE ORGANU NADZORCZEGO

W przypadku 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.

Zgłoszenie musi co najmniej:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Uwaga!

Administrator ma obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności takiego naruszenia, jego skutki oraz podjęte działania zaradcze.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

ZAWIADOMIENIE PODMIOTU DANYCH - CZYLI OSOBY, KTÓREJ DANE DOTYCZĄ

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o zaistniałym naruszeniu osobę, której dane dotyczą. Zawiadomienie takie powinno jasnym i prostym językiem opisywać charakter naruszenia, możliwe konsekwencje oraz środki zastosowane lub proponowane w celu zaradzenia naruszeniu, a także wskazywać dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji.

Zawiadomienie powinno zostać jak najszybciej przekazane osobom, których dane dotyczą, aby mogły one zwiększyć swą czujność i wdrożyć także odpowiednie środki ochrony swej prywatności, a w konsekwencji zminimalizować ryzyko niekorzystnych skutków typu np. utrata tożsamości, kradzież danych, utrata dostępu do poczty internetowej i portali internetowych czy też utrata środków finansowych.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Przykłady incydentów bezpieczeństwa i naruszeń ochrony danych osobowych.

- zagubienie, kradzież dokumentów papierowych, korespondencji lub dokumentów elektronicznych, a także nośników danych,
- przesłanie informacji (listu, e-maila) do niewłaściwego adresata,
- ujawnienie, przekazanie danych osobie nieuprawnionej,
- nieuprawniony lub zbyt szeroki dostęp do informacji,
- zniszczenie dokumentacji,
- wydanie klucza do biura osobie nieuprawnionej,
- pozostawianie pomieszczeń biurowych bez nadzoru,
- zgubienie lub znalezienie kluczy, karty do pomieszczeń urzędu,
- umożliwienie osobie nieuprawnionej dostępu do strefy chronionej,
- ujawnienie hasła do systemów informatycznych,
- awarie i błędy systemu kontroli dostępu lub karty dostępowej,
- awarie sprzętu lub oprogramowania,
- włamanie do systemu teleinformatycznego np. skuteczny atak wirusowy,
- zblokowanie dostępu do dokumentacji elektronicznej wskutek złośliwego oprogramowania,
- wszelkie formy kradzieży sprzętu przetwarzającego informacje,
- umożliwienie dostępu do sprzętu i systemów informatycznych urzędu osobom nieuprawnionym,
- skuteczne ataki socjotechniczne na pracowników urzędu,
- brak właściwego nadzoru nad osobami trzecimi,
- nieuprawniony lub zbyt szeroki dostęp do informacji,
- brak zapisów o zachowaniu poufności w umowach z podmiotami zewnętrznymi,
- brak umów powierzenia przetwarzania danych osobowych, jeżeli ma to uzasadnienie,
- sytuacje losowe lub nieprzewidziane oddziaływania czynników zewnętrznych np. pożar, zalanie, włamanie do budynku.

ŚLĄSKI ZWIĄZEK
GMIN I POWIATÓW

Dziękujemy za uwagę.

Komisja ds. Ochrony Danych Osobowych

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