PROCEDURA

reagowania i oceny naruszeń bezpieczeństwa danych osobowych

Data wprowadzenia procedury:

Data wycofania procedury:

**Podmioty realizujące:**

1. Inspektor Ochrony Danych (IOD).
2. Administrator Systemów Informatycznych (ASI).
3. Administratora Danych Osobowych (ADO).
4. Pracownik.

**Naruszenie**

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa 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.

**Wszczęcie postępowania i działania**

Inspektor Ochrony Danych na podstawie zgłoszenia podejmuje działania mające na celu:

* ograniczenie do minimum negatywnych skutków zdarzenia;
* wyjaśnienie okoliczności zdarzenia;
* sporządzenie raportu z podjętych czynności;
* zgłoszenia (w przypadkach naruszeń skutkujących ryzykiem naruszenia praw lub wolności osób fizycznych) Prezesowi Urzędu Ochrony Danych Osobowych, Administratorowi Danych (w przypadku przetwarzania danych w imieniu innego podmiotu – w roli procesora);
* zgłaszania (w przypadku naruszeń może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych) osoby/osób, których dane uległy naruszeniu;
* poinformowania kierownictwa jednostki o stwierdzonym naruszeniu w celu podjęcia stosowanych działań naprawczych.

Inspektor Ochrony Danych w ramach powyższych działań ma prawo do podejmowania wszelkich dopuszczalnych prawem działań, w szczególności:

* żądania wyjaśnień od osób zatrudnionych przez Administratora Danych Osobowych;
* nakazania przerwania pracy przy przetwarzaniu danych osobowych;
* żądania podjęcia niezwłocznych działań przez ASI.

W przypadku naruszenia bezpieczeństwa danych osobowych działania, określonych w niniejszej procedurze powinny mieć pierwszeństwo przed innymi poleceniami.

**Postępowanie**

1. **Stwierdzenie naruszenia**. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, każdy pracownik, który stwierdzi naruszenie ma obowiązek zgłoszenia tego faktu Inspektorowi Ochrony Danych Osobowych niezwłocznie i stosować się do jego wskazówek.
2. **Analiza.** W przypadku wykrycia przez Administratora naruszenia ochrony danych osobowych dokonuje sie analizy pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych wynikiem, której może być stwierdzenie naruszenia lub incydentu.
3. **Naruszenie**. W przypadku stwierdzenia, iż jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (**naruszenie**),
   1. naruszenie nie wymaga zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych,
   2. naruszenie nie wymaga zgłaszania osobie, której dane osobowe naruszono,
   3. ocenę prawdopodobieństwa uzasadnia się i udokumentowuje, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze
   4. naruszenie zostaje wpisane do ewidencji naruszeń (oznaczając jako „naruszenie”).
4. **Incydent.** W przypadku stwierdzenia, iż jest prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (**incydent**):
   1. naruszenie wymaga zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych;
   2. ocenę prawdopodobieństwa uzasadnia się i udokumentowuje, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;
   3. naruszenie zostaje wpisane do ewidencji naruszeń (oznaczając jako „naruszenie”);
   4. przeprowadza się ocenę pod kątem konieczności jej zgłoszenia osobie, której dane dotyczą (zgodnie z pkt. 7 poniżej) i podejmuje na tej postawie stosowne, kroki.
5. **Informowanie Prezesa Urzędu Ochrony Danych Osobowych o incydencie.** Incydent należy zgłosić Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia. W przypadku przetwarzania danych osobowych w imieniu Administratora danych osobowych (jako procesor) Incydent należy zgłosić Administratorowi w terminie przewidzianym w umowie z Administratorem.
6. **Zgłoszenie.** Zgłoszenie musi obejmować, co najmniej, następujące elementy:
   1. 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;
   2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4. 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.

- jeżeli, i w zakresie, w jakim, informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

- zgłoszenia dokonuje Administrator danych osobowych we współpracy z Inspektorem Ochrony Danych.

1. **Informowanie osoby, której danych dotyczy Incydent.** Incydent należy zgłosić osobie, której dane dotyczą w przypadku stwierdzenia, iż Incydent może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby. Zgłoszenia należy dokonać bez zbędnej zwłoki.
2. **Zawiadomienie.** Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia zdanych osobowych oraz zawiera przynajmniej informacje i środki:
   1. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   2. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   3. 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.

- zgłoszenia dokonuje Administrator danych osobowych we współpracy z Inspektorem Ochrony Danych.

1. **Wyjątki.** Zawiadomienie, o którym mowa w powyżej, nie jest wymagane, w następujących przypadkach:
   1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
   3. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.