

**Wewnętrzne procedury ograniczania/naprawiania naruszeń ochrony danych osobowych.**

1. Koordynator ds. RODO jest odpowiedzialny za przeprowadzenie analizy incydentu bezpieczeństwa.

Analiza w szczególności obejmuje:

1) Ocenę okoliczności wskazanych w zgłoszeniu, ze szczególnym uwzględnieniem stanu Systemu informatycznego w którym doszło do incydentu oraz wstępnie ocenia ryzyko naruszenia praw lub wolności osób fizycznych związane z incydem;

2) W razie zakwalifikowania zgłoszenia jako naruszenia ochrony danych osobowych - rekomenduje działania, jakie powinny zostać podjęte w celu zaradzenia naruszeniu lub zminimalizowania jego ewentualnych negatywnych skutków.

2. Jeżeli to możliwe, Koordynator ds. RODO, zabezpiecza materiał dowodowy mogących wskazać sprawców oraz sposób w jaki powstał incydent.

3. Kwalifikacji zgłoszenia w imieniu Administratora dokonuje Koordynator ds. RODO na podstawie opracowanego formularza Excel. Koordynator ds. RODO rekomenduje zarządowi Administratora jedno z 3 rozwiązań lub kilka łącznie:

(i) odnotowanie naruszenia w Rejestrze

(ii) zgłoszenie do UODO

(iii) zawiadomienie podmiotów danych.

4. W przypadku zakwalifikowania zgłoszenia jako naruszenia ochrony danych osobowych, Koordynator ds. RODO niezwłocznie informuje o tym Administratora, który bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, aby stwierdzone naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Administrator może w tym zakresie udzielić również Koordynatorowi ds. RODO odpowiedniego pełnomocnictwa.

5. W przypadku, w którym Administrator uzna, że jest mało prawdopodobne, aby stwierdzone naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych i zdecyduje się nie zgłosić naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, jest zobowiązany do przygotowania stanowiska zawierającego argumentację dlaczego w jego opinii nie ma konieczności zgłaszania naruszenia.

6. W przypadku zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, po upływie 72 godzin od stwierdzenia naruszenia do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.

7. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać co najmniej:

1) Opis charakteru naruszenia, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, a także kategorie i przybliżoną liczbę rekordów danych osobowych, których dotyczy naruszenie;

2) Imię i nazwisko oraz dane kontaktowe IOD, jeżeli został wyznaczony;

3) Opis możliwych konsekwencji naruszenia ochrony danych osobowych;

4) Opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

8. Administrator dokumentuje wszelkie naruszenia ochrony danych. Rejestr zawiera:

1) Datę naruszenia,

2) Wskazanie osoby zgłaszającej naruszenie,

3) Opis naruszenia,

4) Przyczynę naruszenia,

- 5) Opis możliwych skutków naruszenia,
  - 6) Opis zastosowanych środków zaradczych w celu minimalizacji zdarzenia,
  - 7) Podjęte działania,
  - 8) Środki zastosowane w celu uniknięcia naruszenia w przyszłości,
  - 9) Zastosowane środki bezpieczeństwa,
  - 10) Informacja o zawiadomieniu UODO,
  - 11) Informacja o powiadomieniu osoby, której dane dotyczą.
9. Jeżeli naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadomi osobę, której dane dotyczą o zaistniałym naruszeniu.
10. Zawiadomienie, o którym mowa w ust. 10 powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki o których mowa w ust. 8.
11. Zawiadomienie, o którym mowa w ust. 10 powyżej nie jest wymagane w przypadku, gdy: a) Administrator wdrożył odpowiednie środki techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie; b) Administrator zastosował środki eliminujące prawdopodobieństwa wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; c) Wymagałoby ono niewspółmiernie dużego wysiłku. We wskazanym przypadku należy wydać publiczny komunikat lub zastosować podobny środek, tak aby osoby, których dane dotyczą zostały poinformowane w równie skuteczny sposób.
12. W przypadku stwierdzenia naruszenia ochrony danych osobowych przez Podmiot przetwarzający, Podmiot przetwarzający zgłasza je bez zbędnej zwłoki Administratorowi, który następnie przekazuje je Koordynatorowi ds. RODO.