Art. 33 RODO nakłada na Administratora Danych obowiązek zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych („Prezes Urzędu"; nazwa polskiego organu nadzorczego została określona w projekcie ustawy o ochronie danych osobowych).

W przypadku naruszenia ochrony danych osobowych Administrator Danych nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je Prezesowi Urzędu. Zgłoszenie nie jest wymagane, gdy Administrator Danych przeprowadzi analizę incydentu i stwierdzi, że mało prawdopodobne jest, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego po upływie 72 godzin Administrator Danych zobowiązany jest dołączyć wyjaśnienie przyczyn opóźnienia.

Zgłoszenie naruszenia powinno zawierać następujące informacje:

- charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane zostały naruszone,
- dane Inspektora Ochrony Danych - imię i nazwisko oraz dane kontaktowe lub oznaczenie innego punktu kontaktowego,
- możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki techniczne i organizacyjne zastosowane lub proponowane przez Administratora Danych w celu zaradzenia naruszeniu ochrony danych osobowych.

Administrator Danych jest zobowiązany do dokumentowania naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych. Dokumentacja ta musi pozwolić Prezesowi Urzędu na weryfikowanie prawidłowości postępowania administratora w tym zakresie.

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Art. 34 RODO określa sposób zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator Danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o zaistniałym naruszeniu.

Zawiadomienie musi być napisane prostym i zrozumiałym językiem, opisywać charakter naruszenia oraz zawierać informacje podane Prezesowi Urzędu w zgłoszeniu naruszenia.

Zawiadomienie osoby, której naruszenie dotyczy, nie jest wymagane, gdy:

- 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,
- administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby 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.