PROCEDURA ZAWIADAMIANIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH
W BIURZE RACHUNKOWE VECTIGAL CONSULTING
EWA DĄBROWSKA

1. Klasyfikacja naruszenia
   1.1. Należy dokonać klasyfikacji naruszenia ochrony danych osobowych w oparciu o Procedurę wykrywania i klasyfikowania naruszeń ochrony danych osobowych,
   1.2. Należy określić, czy organizacja względem danych osobowych, których naruszenie miało miejsce jest:
      1.2.1. Administratorem danych osobowych,
      1.2.2. Podmiotem przetwarzającym.

Komórki odpowiedzialne: inspektor ochrony danych osobowych, administrator systemów informatycznych, obsługa prawna

2. Zawiadomienie o naruszeniu przez Administratora danych osobowych
   2.1. Administrator danych osobowych, w zależności od klasyfikacji naruszenia, jako:
      2.1.1. Naruszenie nieistotne – podmiot poprzestaje na wykonaniu czynności, o których mowa w punktach 3.2 – 3.4 Procedury wykrywania i klasyfikowania naruszeń ochrony danych osobowych,
      2.1.2. Naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych – podmiot, prócz czynności wskazanych w punkcie 2.1.1. dokonuje zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
      2.1.3. Zawiadomienie, o którym mowa w punkcie 2.1.2. musi co najmniej:
         2.1.3.1. 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;
         2.1.3.2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
         2.1.3.3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
         2.1.3.4. 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,
      2.1.4. Naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych – prócz czynności wskazanych w punktach 2.1.1. i 2.1.2. oraz z zastrzeżeniem punktu 2.3., dokonuje zawiadomienia o naruszeniu osoby, której dane dotyczą, które musi co najmniej:
         2.1.4.1. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

2.1.4.2. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

2.1.4.3. 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,

2.2. Zawiadomienie, o którym mowa w punkcie 2.1. należy sporządzić posługując się jasnym i prostym językiem opisując charakter naruszenia ochrony danych osobowych.

2.3. Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, w następujących przypadkach:

2.3.1. Administrator danych osobowych 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,

2.3.2. Administrator danych osobowych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

2.3.3. 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.

Komórki odpowiedzialne: inspektor ochrony danych osobowych

3. Zawiadomienie o naruszeniu przez Podmiot przetwarzający

3.1. Jeżeli organizacja jest Podmiotem przetwarzającym, po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi danych osobowych,

3.2. Należy wykonać czynności, o których mowa w punktach 3.2 – 3.4 Procedury wykrywania i klasyfikowania naruszeń ochrony danych osobowych.

Komórki odpowiedzialne: inspektor ochrony danych osobowych

4. Postanowienia końcowe

4.1. Procedura może zostać zmieniona przez organ zarządzający po uzyskaniu uprzedniego stanowiska komórki obsługi prawnej oraz inspektora ochrony danych osobowych.

4.2. Zmiana procedury wchodzi w życie z dniem jej ogłoszenia w sposób zwyczajowo przyjęty.

4.3. Procedura wchodzi w życie z dniem 25 maja 2018 roku.