Postępowanie w przypadku naruszenia ochrony danych osobowych

CEL PROCEDURY

Sprecyzowanie i wdrożenie jednolitej i przejrzystej procedury postępowania w przypadku naruszenia ochrony danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1. IOD w zakresie:
   1) oceny czy zgłoszenie stanowi naruszenie ochrony danych osobowych:
      a) jeżeli tak – czy może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych i w związku z tym wymaga zgłoszenia organowi nadzorczemu,
      a) czy zidentyfikowane naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co wiąże się z obowiązkiem zawiadomienia osób, których dane dotyczą;
   2) dokumentowania spraw z zakresu naruszeń;
   3) przygotowania dokumentów wymaganych przez UODO w związku ze zgłaszaniem naruszenia przez administratora.
2. Kierujący komórką organizacyjną w zakresie:
   1) zgłaszania IOD zdarzeń noszących znamiona incydentu lub naruszenia, które wystąpiły w komórce organizacyjnej;
   2) współdziałania z IOD w przypadku wystąpienia zdarzenia mogącego stanowić naruszenie ochrony danych osobowych w zakresie wyjaśnienia przyczyn i okoliczności;
   3) informowania we współpracy z IOD osób, których dane dotyczą o naruszeniu, w przypadku zaistnienia takiej konieczności;
   4) wdrożenia działań minimalizujących niekorzystne skutki wystąpienia zdarzenia mogącego stanowić naruszenie ochrony danych osobowych oraz działań zaradczych na przyszłość.
3. Administrator systemu informatycznego (ASI) – w przypadku gdy naruszenie dotyczy systemów informatycznych, współdziała z IOD.
4. Pracownicy – w zakresie zgłaszania podejrzenia naruszenia lub naruszenia danych osobowych.

POSTANOWIENIA OGÓLNE PROCEDURY

Procedura dotycząca postępowania w przypadku naruszeń ochrony danych osobowych realizowana jest w dwóch etapach:

1) wewnętrznym, którego celem jest ustalenie, czy zgłoszone zdarzenie jest naruszeniem oraz w jaki sposób zidentyfikowane zdarzenie wpłynie na ryzyko dla praw i wolności osób fizycznych;
2) zewnętrznym, którego celem jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego oraz poinformowanie osoby, której dane dotyczą, w przypadku gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

RODZIAŁ I – ETAP WEWNĘTRZNY

1. Każdy użytkownik, który stwierdził lub podejrzewa wystąpienie zdarzenia, które może stanowić naruszenie ochrony danych osobowych, ma obowiązek zgłosić ten fakt na piśmie bezpośredniemu przełożonemu oraz na adres:iodo@mrips.gov.pl.
2. W przypadku gdy zgłoszenie dotyczy systemów informatycznych zgłoszenie należy przekazać równocześnie do DI, zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Informacji w obszarze IT.
3. Zgłoszenie zdarzenia mogącego stanowić naruszenie ochrony danych osobowych powinno zawierać:
   1) opisanie symptomów naruszenia ochrony danych osobowych;
   2) określenie okoliczności i czasu, w jakim prawdopodobnie nastąpiło naruszenie ochrony danych osobowych;
   3) określenie okoliczności i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   4) określenie istotnych informacji, które mogą wskazywać na przyczynę naruszenia;
   5) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
4. Stwierdzenie naruszenia następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie, które może prowadzić do naruszenia bezpieczeństwa danych osobowych.
5. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, ASI w porozumieniu z IOD podejmuje niezbędne działania zabezpieczające, niezwłocznie po otrzymaniu informacji, o której mowa w ust. 3. Szczegółowe zasady postępowania określone są w Polityce Bezpieczeństwa Informacji w obszarze IT.
6. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego odpowiednie czynności zabezpieczające podejmuje IOD, tj. w szczególności:
   1) nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji Dyrektora Generalnego Ministerstwa;
   2) działa w celu wyjaśnienia okoliczności zdarzenia;
   3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.
7. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana jest jako naruszenie obowiązków pracowniczych.
8. O każdym naruszeniu skutkującym zgłoszeniem do UODO informowany jest Minister i Dyrektor Generalny Ministerstwa.
9. Rejestr zdarzeń, incydentów i naruszeń prowadzi IOD. Rejestr jest co najmniej raz w roku i na każde żądanie przedstawiany Ministrowi i Dyrektorowi Generalnemu Ministerstwa.

ROZDZIAŁ II – ETAP ZEWNĘTRZNY

1. Zgłoszenie naruszenia ochrony danych osobowych opracowuje IOD według wzoru określonego przez Prezesa Urzędu Ochrony Danych Osobowych.
2. Zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu dokonuje Administrator bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
4. W przypadku stwierdzenia w toku dalszych czynności, że do naruszenia nie doszło, informację o tym należy przekazać organowi nadzorczemu w ramach uzupełnienia zgłoszenia, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą.
6. Za realizację obowiązku wskazanego w ust. 5 odpowiada kierujący komórką organizacyjną, w której wystąpiło naruszenie ochrony danych osobowych.
7. Zawiadomienie należy przygotować jasnym i prostym językiem.
8. Zawiadomienie osób których dane dotyczą o naruszeniu nie jest wymagane, jeżeli w Ministerstwie:
    1) wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie;
    2) zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
    3) zawiadomienie takie wymagałoby niewspółmiernie dużego wysiłku; w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.