Procedura postępowania w przypadku naruszenia ochrony danych osobowych

CEL PROCEDURY

Sprecyzowanie i wdrożenie w Urzędzie 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,
      b) 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.

2. **Pracownik wyznaczony przez Administratora** do kontaktów z IOD:

   1) ewentualne zgłaszanie naruszeń w imieniu Administratora do organu nadzorczego, w porozumieniu z IOD;
   2) ewentualne informowanie (zawiadamianie) osób, których dane dotyczą o wystąpieniu naruszenia, w imieniu Administratora, w porozumieniu z IOD;
   3) ewentualne podejmowanie odpowiednich czynności zabezpieczających, w porozumieniu z Administratorem oraz IOD;
   4) prowadzenie dokumentacji *z* zakresu naruszeń *(raport o naruszeniu, rejestr naruszeń ochrony danych, zgłoszenie naruszenia, informacja o wystąpieniu naruszenia itp.).*

3. Administrator systemu informatycznego (**ASI**) - w sytuacji gdy naruszenie dotyczy systemów informatycznych, współdziała z IOD.

4. Inny **pracownicy** Urzędu - 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: **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. **Zewnętrznym**, którego celem jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego oraz poinformowanie osoby, której dane dotyczą, wv przypadku gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.

POSTANOWIENIA SZCZEGÓLOWE PROCEDURY

ROZDZIAŁ I - ETAP WEWNETRZNY

1. Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, którzy stwierdzili lub podejrzewają wystąpienie zdarzenia, które stanowi naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu na piśmie Administratorowi. W przypadku gdy zgłoszenie dotyczy systemów informatycznych stosowną informację należy przekazać również ASI.

2. Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:
   1) opisanie oznak naruszenia ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) określenie istotnych informacji mogących wskazywać na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

3. Stwierdzenie naruszenia następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych. W celu identyfikacji naruszenia, muszą być spełnione łącznie trzy przesłanki:
   1) naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie;
   2) skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
   3) naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

4. 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.

5. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego i ma związek z naruszeniem zabezpieczeń fizycznych, odpowiednie czynności zabezpieczające, w porozumieniu z IOD, podejmuje wyznaczony przez Administratora pracownik Urzędu, tj.:
   1) nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji Administratora;
   2) działa w celu wyjaśnienie okoliczności zdarzenia;
   3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

6. Odmowa udzielenia wyjaśnień lub współpracy z wyznaczonym przez Administratora pracownikiem Urzędu oraz IOD, traktowana będzie jako naruszenie obowiązków pracowniczych.

7. Raport o naruszeniu danych osobowych opracowuje IOD według wzoru stanowiącego część niniejszej Procedury. Raport przedstawiany jest Administratorowi. Raport o naruszeniu danych osobowych jest przechowywany przez wyznaczonego przez Administratora pracownika Urzędu, wraz z pozostałą dokumentacją z zakresu naruszeń.

8. Każdy incydent związany z ochroną danych, przypadek naruszenia ochrony danych, odnotowywany jest w rejestrze naruszeń ochrony danych, który stanowi załącznik do niniejszej Procedury), prowadzonym przez wyznaczonego przez Administratora pracownika Urzędu.

ROZDZIAŁ II - ETAP ZEWNETRZNY

1. W przypadku gdy naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, musi być ono zgłoszone organowi nadzorczemu bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

2. Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialna lub niematerialna szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:
   1) dyskryminacja,
   2) kradzież tożsamości lub oszustwo dotyczące tożsamości,
   3) nadużycia finansowe,
   4) straty finansowe,
   5) nieuprawnione cofniecie pseudonimizacji,
   6) utrata poufności danych osobowych chronionych tajemnicą zawodową,
   7) naruszenie dobrego imienia,
   8) inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

3. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane dotyczące zdrowia, dane dotyczące życia seksualnego, - należy uznać, że występuje duże prawdopodobieństwo szkody, o której mowa w ust. 2.

4. W przypadku konieczności dokonania zgłoszenia naruszenia do organu nadzorczego pismo w tej sprawie przygotowuje wyznaczony przez Administratora pracownik Urzędu, w porozumieniu z IOD. W zgłoszeniu takim, zgodnie z art. 33 RODO, należy w szczególności:
   1) opisać 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) wskazać imię i nazwisko oraz dane kontaktowe IOD;
   3) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisać środki zastosowane lub proponowane w Urzędzie w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. Jeżeli informacji, o których mowa w ust. 2, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki w następujący sposób:
   1) po dokonaniu pierwszego zgłoszenia można przekazywać na bieżąco organowi nadzorczemu aktualne informacje;
   2) w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

6. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

7. 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. Rekomenduje się następującą klasyfikację oceny powagi naruszeń praw i wolności osób fizycznych, na poziomie od 1 do 4, gdzie:
   - 1 to **ograniczone naruszenie** (osoba, której dane dotyczą, nic odczuje wpływu lub zetknie się z niewielka liczbą niedogodności, które łatwo może przezwyciężyć),
   - 2 to **naruszenie** (osoba, której dane dotyczą, nie odczuje wpływu lub zetknie się z niewielka liczbą niedogodności, które łatwo może przezwyciężyć),
   - 3 to **znaczące naruszenie** (osoby, których dane dotyczą, mogą napotkać znaczące konsekwencje, które powinny móc przezwyciężyć mimo realnych i dużych trudności),
   - 4 to **najwyższy stopień naruszenia** (osoba, której dane dotyczą, może napotkać poważne i nieodwracalne konsekwencje, których może nie być w stanie przezwyciężyć).

8. Za realizację obowiązku wskazanego w ust. 7 odpowiada wyznaczony przez Administratora pracownik Urzędu, w porozumieniu z IOD.

9. Zawiadomienie należy przygotować jasnym i prostym językiem (art. 34 RODO). Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.

10. Zawiadomienie, o którym mowa w ust. 7, nie jest wymagane, w następujących przypadkach:
   1) w Urzędzie wdrożono 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) w Urzędzie zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   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.

11. Należy wykazać przed organem nadzorczym, że został Spełniony przynajmniej jeden z warunków wskazanych w ust. 10 w przypadku braku powiadomienia osób, których dane naruszono.

„WZÓR” Miejscowość, dnia ……

Raport o naruszeniu danych osobowych

Miejsce, czas i data naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych

……

Osoby powodujące naruszenie *(które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych):*

……

Charakter naruszenia - stwierdzone nieprawidłowości (*nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych, wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania):*

……

Informacje o danych, które zostały lub mogły zostać ujawnione *(nazwa czynności procesu przetwarzania, w ramach którego doszło do naruszenia chrony danych):*

……

Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

……

Kategorie danych osobowych, których dotyczy naruszenie (zwykle, szczególne): ……

Kategorie osób, których dane dotyczą, dotkniętych naruszeniem: ……

Liczba osób, których dane dotyczą, dotkniętych naruszeniem: ……..

Środki bezpieczeństwa zastosowane przed naruszeniem: ……..

Krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacji, w tym ochrony danych osobowych *(przebieg zdarzenia, opis zachowania uczestników. podjęte działania):*

……

Możliwe konsekwencje naruszenia dla Urzędu lub osób zainteresowanych:

……

Zalecenia naprawcze w celu przywrócenia stanu zgodnego z prawem, zminimalizowania negatywnych skutków, zminimalizowania ryzyka wystąpienia analogicznego naruszenia w przyszłości:

……

Ocena pod katem zgłoszenia naruszenia organowi nadzorczemu (art.33 RODO):

……

Ocena pod kątem zawiadomienia osób, których dane dotyczą, o naruszeniu (art.34 RODO):

……

Sporządzający raport *(imię i nazwisko, funkcja):* ***Zapoznałem się:***

(czytelny podpis) *(czytelny podpis Administratora)*

„WZÓR”

REJESTR
naruszeń ochrony danych osobowych

L.p	Informacje o wystapieniu zdarzenia i stwierdzeniu naruszenia			Okolicznośći naruszenia		
	Data zdarzenia	Data i zródlo uzyskania informacji	Data i godzina stwierdzenia naruszenia	Charakter naruszenia	Kategorie osób /Przyblizona Liczba osób,których dane dotycza (jezeli to mozliwe)	Kategoria danych:zwykle,szczegóine i liczba wpisów (jezeli to mozliwe)
1.	2.	3.	4.	5.	6.	7.

Skutki naruszenia	Srodki napraweze i zaradeze			Zgloszenie naruszenia organowi nadzorczemu PUODO			Uwagi
Opis konsekwencji naruszcnia	Czy poinformowano osoby których dane dotycza?(jesli tak, to w jaki sposób,jesli nie,to dlaczcgo)	Dzialania naprawcze	Dzialania zaradcze	Czy dokonano zgloszenia (jesli nie,przyczyna niedokonania zgloszenia)	Data zgloszenia	Data zgloszenia uzupelniajacego	Np. o poinformowaniu CERT Polska,organów scigania
8.	9.	10.	11.	12.	13.	14.	15.