# **Cel procedury**

 Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości
w funkcjonowaniu Zakładu, spowodowanych nieuprawnionym ujawnieniem danych osobowych, udostępnieniem lub umożliwieniem dostępu do nich osobom nieupoważnionym, zabraniem danych przez osobę nieupoważnioną, uszkodzeniem lub usunięciem,
a w szczególności:

* 1. nieautoryzowany dostęp do danych,
1. nieautoryzowane modyfikacje lub zniszczenie danych,
2. udostępnienie danych nieautoryzowanym podmiotom,
3. nielegalne ujawnienie danych,
4. pozyskiwanie danych z nielegalnych źródeł.

# **Klasyfikacja naruszeń**

 Naruszenia ze względu na ich występowanie możemy podzielić na:

1. zdarzenia losowe **zewnętrzne**, których występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów (np. klęski żywiołowe, przerwy w zasilaniu);
2. zdarzenia losowe **wewnętrzne**, których występowanie może doprowadzić
do zniszczenia danych, zakłócenia ciągłości pracy systemu, może nastąpić naruszenie poufności danych (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu);
3. zdarzenia zamierzone, celowe i świadome, niepowodujące uszkodzenia infrastruktury technicznej i zakłóceń ciągłości pracy możemy podzielić na:
4. nieuprawniony dostęp do bazy danych z zewnątrz
5. nieuprawniony dostęp do bazy danych z sieci wewnętrznej
6. nieuprawniony transfer danych
7. pogorszenie funkcjonowania sprzętu i oprogramowania np. działania wirusów
8. bezpośrednie zagrożenie materialnych składników systemu np. kradzież sprzętu.

# **Zgłaszanie naruszeń związanych z bezpieczeństwem informacji**

 W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a następnie postępować stosownie do podjętej przez niego decyzji.

 Pracownicy jednostki mają obowiązek zgłaszać zauważone przez siebie naruszenia oraz notować wszystkie szczegóły związane z naruszeniami.

Zgłoszenie powinno zawierać:

1. imię i nazwisko zgłaszającego,
2. określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
3. określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
4. określenie znanych zgłaszającemu sposobów zabezpieczenia systemu
oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

 Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń
w jednostce jest ………………

# **Postępowanie z naruszeniami**

 Osoba, która otrzymała zgłoszenie dokonuje wstępnej identyfikacji zdarzenia
i po konsultacji z Inspektorem Ochrony Danych Osobowych dokonuje jego kwalifikacji
jako naruszenie niskie lub wysokie. W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi ***załącznik nr 1*** do niniejszej Procedury. Naruszenia zakwalifikowane jako wysokie podlegają zgłoszeniu do organu nadzorczego niezwłocznie, jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia.

1. charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
2. miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
3. liczba referatów/komórek organizacyjnych dotkniętych incydentem,
4. identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
5. możliwości rozszerzania się incydentu i sposoby jego ograniczania,
6. szacowany poziom szkód,
7. szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
8. skutki organizacyjne i prawne (wstępny szacunek).

 Po dokonanej analizie Administrator zgłasza naruszenie do organu nadzorczego (wzór zgłoszenia stanowi ***załącznik nr 2*** do niniejszej Procedury),
oraz jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (wzór zawiadomienia stanowi ***załącznik nr 3*** do niniejszej Procedury). Zawiadomienie osoby nie jest wymagane jeśli Administrator wdrożył odpowiednie techniczne

i organizacyjne środki, które uniemożliwią osobom nieuprawnionym dostęp do danych, zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Z zawiadomienia, o którym mowa nie należy stosować gdy wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak wypadku należy opublikować ogłoszenie, zastosować inny, równie skuteczny środek.

 Jeżeli z jakiegokolwiek powodu nie uda się przekazać zgłoszenia w tym terminie,
do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia. Jeżeli Administrator
nie zawiadomił jeszcze o naruszeniu osób, których ono dotyczy, organ nadzorczy może
mu to nakazać.

 Dodatkowo naruszenia mogą być wykorzystywane przez Inspektora Ochrony Danych podczas szkoleń pracowniczych jako przykład tego, co może się wydarzyć, jak unikać ich
w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowywania poufności.

Załącznik nr 1:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Data naruszenia** | **Kategoria osób, których dane zostały naruszone** | **Kwalifikacja naruszenia****(niskie lub wysokie)** | **Zastosowane środki zaradcze** | **Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)** | **Zawiadomienie osoby której dane dotyczą****(dotyczy lub nie dotyczy)** |
| **1.** |  |  |  |  |  |  |
| **2.** |  |  |  |  |  |  |
| **3.** |  |  |  |  |  |  |
| **4.** |  |  |  |  |  |  |

Załącznik nr: 2

….........................dnia…….

Urząd Ochrony Danych Osobowych

……………………………………..

**Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu**

Na podstawie obowiązku wynikającego z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie
o ochronie danych)

|  |  |
| --- | --- |
| Data Naruszenia |  |
| Liczba osób których dane dotyczą |  |
| Liczba wpisów danych osobowych i kategoria tych danych |  |
| Dane Inspektora Danych osobowych |  |
| Dane Organu Nadzorczego |  |
| Charakter Naruszenia: |  |
| Konsekwencje naruszenia: |  |
| Zastosowane i proponowane środki zaradcze: |  |

……….……………………………………………….

(Podpis Administratora)

Załącznik nr: 3

………………….dnia ………………roku

Pan/Pani ……………………

………………………………

………………………………

**ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH**

 Na podstawie obowiązku wynikającego z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie
o ochronie danych) w związku z naruszeniem Pana/Pani danych osobowych w zakresie …………. Zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie…………………………..

 Urząd podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

 Celem uzyskania dodatkowych informacji należy kontaktować się z ..........................

…………………………………….

 (Podpis Administratora)