Załącznik do Polityki Ochrony Danych Osobowych

PROCEDURA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

I. STWIERDZENIE NARUSZENIA I ZGŁOSZENIE DO ORGANU

1. **Należy wszcząć niniejszą procedurę, jeśli doszło do naruszenia ochrony danych osobowych lub pojawi się podejrzenie, że mogło dojść do takiego zdarzenia.**

Typowe sytuacje, które mogą budzić podejrzenie, że mogło dojść do naruszenia:
Zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki
Fizyczna obecność w budynku lub pomieszczenia osób podejrzanie się zachowujących
Udostępnianie danych osobowych osobom nieupoważnionych
Telefoniczne próby wyłudzenia danych osobowych
E-maile zachęcające do ujawnienia identyfikatora i/lub hasła
Przechowywanie haseł do systemów w pobliżu komputera
Pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
Typowe naruszenia ochrony danych osobowych
Kradzież danych (np. m.in. kradzież zarówno w formie elektronicznej jaki i kradzież dokumentów papierowych, czy też fizycznych nośników danych)
Błąd ludzki (np. pozostawienie danych – w formie dokumentu lub nośnika fizycznego – poza obszarem przetwarzania bez możliwości kontroli osób, które mają dostęp do tak pozostawionych danych osobowych, omyłkowe przesłanie korespondencji zawierającej dane osobowe do podmiotu nieuprawnionego)
Incydent spowodowany zaniedbaniem (np. pracownik pozostawia niezabezpieczone dokumenty zawierające dane osobowe w miejscu, do którego mają dostęp osoby nieuprawnione do przetwarzania danych osobowych – efektem takiego działania jest utrata poufności danych)
Incydent spowodowany zaniechaniem (np. m.in. pracownik, pomimo tego, że dysponuje odpowiednimi środkami technicznymi np. zamykanymi szafkami, nie korzysta z nich w celu zabezpieczenia danych osobowych – efektem takiego działania jest kradzież danych)
Incydent spowodowany włamaniem do sieci lub do kont użytkowników stacji roboczych (np. m.in. pracownik używa hasła do stacji roboczej, które składa się z jego imienia i nazwiska)
Utrata kopii zapasowych (np. m.in. kradzież niezabezpieczonej kopii zapasowej)

2. W przypadku gdy Administrator współpracuje z innymi osobami (współpracownicy, zleceniobiorcy), osoby te są zobowiązane niezwłocznie powiadomić **Administratora**, jeśli doszło do naruszenia ochrony danych osobowych lub pojawi się podejrzenie, że mogło dojść do takiego zdarzenia

CO ZROBIĆ gdy stwierdzono naruszenie lub prawdopodobieństwo naruszenia ochrony danych?

KROK 1: ZMNIEJSZENIE SKUTKÓW

1. **Należy podjąć niezwłocznie czynności niezbędne dla powstrzymania niepożądanych skutków** zaistniałego zdarzenia uwzględniając także potrzebę ustalenia jego przyczyn lub sprawców.

KROK 2: USTALENIE RODZAJU NARUSZENIA

2. Należy określić:
    1) jaka jest waga naruszenia
    2) czy zdarzenie prowadzi lub skutkuje ryzykiem naruszenia prawa lub wolności osoby fizycznej
    3) czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu,
    4) czy zaistniałe naruszenie podlega obowiązkowi powiadomienia osoby, której dane dotyczą.

KROK 3: WPISAĆ NARUSZENIE DO REJESTRU NARUSZEŃ

3. Administrator prowadzi rejestr naruszeń. Wzór rejestru znajduje się w załączniku do Polityki Ochrony Danych.

KROK 4: GDY ZACHODZI RYZYKO, ŻE NARUSZENIE BĘDZIE SKUTKOWAŁO RYZYKIEM NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

4. Administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu** naruszenia – **zgłasza się je organowi nadzorczemu**.
5. Zgłoszenie dokonuje się przy wykorzystaniu formularza udostępnionego przez Urząd. Informacje o tym, jak zgłosić naruszenie znajdują się na stronie Urzędu Ochrony Danych Osobowych - uodo.gov.pl. [https://uodo.gov.pl/pl/134/233].
6. Jeżeli naruszenie zgłosi się po 72 godzinach, do takiego zgłoszenia należy załączyć wyjaśnienia ze wskazaniem powodu opóźnienia.
7. **Zgłoszenie do organu nadzorczego** zawiera:

1) charakter naruszenia ochrony danych osobowych wraz ze wskazaniem kategorii i przybliżonej liczby osób, których dane dotyczą oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

2) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie naruszenia, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,

3) opis możliwych konsekwencji naruszenia danych osobowych,

4) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.

KROK 5: GDY ZACHODZI WYSOKIE RYZYKO, ŻE NARUSZENIE BĘDZIE SKUTKOWAŁO

RYZYKIEM NARUSZENIA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH

8. Administrator **bez zbędnej zwłoki** zawiadamia osoby, których dane dotyczą, o takim naruszeniu.

9. Zawiadomienie powinno być sformułowane jasnym i prostym językiem i zawierać:

   1) imię i nazwisko oraz dane kontaktowe osoby, która posiada szczegółowe informacje odnośnie incydentu, a organizacja wyznaczyła ją do załatwiania spraw związanych z ochroną danych osobowych,
   2) opis możliwych konsekwencji naruszenia danych osobowych,
   3) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach opis środków możliwych do podjęcia w celu minimalizacji skutków naruszenia.

10. Przyjmuje się, że **zawiadomienie nie będzie wymagane gdy**:

   1) Administrator zastosował odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, tj. w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

   2) Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

   3) wymagałoby to niewspółmiernie dużego wysiłku – wówczas Administrator wyda publiczny komunikat lub zastosowany zostanie podobny środek, za pomocą osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Zawiadomienie może być wysłane drogą elektroniczną, tj. email lub pocztą.