PROCEDURA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH W STOWARZYSZENIU ZWIĄZEK GMIN I POWIATÓW SUBREGIONU PÓŁNOCNEGO

§1

Niniejsza procedura obowiązuje wszystkich pracowników zatrudnionych u Administratora danych oraz inne osoby, które stwierdzą naruszenie/podejrzenia naruszenia, o ile zostały zapoznane z niniejszą Procedurą.

§2

1. Użytkownik jest zobowiązany NIEZWŁOCZNIE powiadomić:

   1) Dyrektora Biura
   2) Bezpośredniego przełożonego lub osobę go zastępującą,
   3) inną osobę wyznaczoną przez Administratora danych,

   - jeśli stwierdzi, że doszło do naruszenia ochrony danych osobowych lub będzie miał podejrzenie, że mogło dojść do takiego zdarzenia. Typowe sytuacje, o których użytkownik powinien powiadomić wskazano w tabeli w §4.

2. Do czasu przybycia na miejsce osoby z ust. 1 należy:

   1) O ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej lub innej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   5) przygotować opis incydentu,
   6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia osób z ust. 1.

3. Administrator danych lub osoba z ust. 1 wyznaczona przez Administratora danych po otrzymaniu zawiadomienia, o którym mowa w ust 1, powinna niezwłocznie:

   a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
   b) podjąć działania chroniące przed ponownym lub dalszym naruszeniem.

oraz w zależności od okoliczności dotyczących naruszenia

c) sporządzić notatkę z przeprowadzonych oględzin miejsca zdarzenia,
d) wykonać kopię obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem ochrony danych osobowych
e) sporządzić kopie zapisów rejestru systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu,
f) podjąć inne czynności niezbędne do należytego udokumentowania okoliczności naruszenia ochrony danych osobowych i ustalenia okoliczności naruszenia.

5. Administrator danych określa wagę naruszenia oraz ocenia czy naruszenie skutkuje ryzykiem naruszenia prawa lub wolności osoby fizycznej, w tym czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu i powiadomieniu osoby, której dane dotyczą.
6. W sytuacji gdy zachodzi ryzyko, iż naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza się je organowi nadzorczemu.
7. Jeżeli naruszenie zgłosi się po 72 godzinach, do takiego zgłoszenia należy załączyć wyjaśnienia ze wskazaniem powodu opóźnienia.
8. Procedura powyżej dotyczy także zgłoszenia naruszenia przez Procesora z tym zastrzeżeniem, że w określaniu informacji z ust. 5 może brać udział także Procesor.
9. W przypadku stwierdzenia naruszeń danych osobowych względem danych, co do których ……. [nazwa organizacji] jest Procesorem, ……. [nazwa organizacji] zgłasza bez zbędnej zwłoki takie naruszenia właściwemu podmiotowi, który w takim przypadku jest administratorem danych.
10. 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.

11. Zgłoszenie do organu nadzorczego następuje w sposób przewidziany przepisami prawa.
12. Administrator danych prowadzi rejestr naruszeń.

13. Wzór rejestru naruszeń danych osobowych stanowi załącznik do niniejszej Procedury.

§3

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się osoby, których dane dotyczą, o takim naruszeniu.
2. Zawiadomienie powinno być sformułowane jasnym i prostym językiem, a ponadto powinno zawierać następujące elementy takie jak:
    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.
3. Przyjmuje się, że zawiadomienie nie będzie wymagane gdy:
    1) Administrator danych 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 danych zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    3) wymagałoby to niewspółmiernie dużego wysiłku – wówczas Administrator danych 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 tradycyjną.

§4

Tabela poniżej zawiera przykładowe naruszenia ochrony danych osobowych, jakie mogą wystąpić.

Typowe sytuacje, które mogą budzić podejrzenie, że mogło dojść do naruszenia ochrony danych osobowych:
Ślady na drzwiach, oknach i szafach wskazują na próbę włamania
Zniszczenie dokumentacji zawierającej dane osobowe bez użycia niszczarki
Fizyczna obecność w budynku lub pomieszczenia osób podejrzanie się zachowujących
Wynoszenie danych osobowych w wersji papierowej i/lub elektronicznej na zewnątrz firmy bez upoważnienia Administratora danych
Udostępnianie danych osobowych osobom nieupoważnionych w formie papierowej, elektronicznej i ustnej
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 lub stacji roboczych, włamanie do siedziby organizacji, tj. ingerencja w fizyczny obszar przetwarzania danych osobowych)
Błąd ludzki (np. m.in. 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, pozostawienie osoby nieupoważnionej w obrębie przetwarzania danych osobowych bez nadzoru)
Sabotaż (np. m.in. działania byłego lub obecnego pracownika mające na celu wykreowanie incydentu bezpieczeństwa np. poprzez umieszczenie danych osobowych w publicznych serwisach internetowych)
Oszustwo (np. m.in. pracownik organizacji udostępnia dane osobowe podmiotom nieupoważnionym w celu osiągnięcia dodatkowych korzyści finansowych)
Incydent spowodowany zaniedbaniem (np. m.in. pracownik pozostawia niezabezpieczone dokumenty zawierające dane osobowe po godzinach pracy 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 pojawieniem się osób nieupoważnionych w obszarze przetwarzania danych osobowych (np. kurier dostarczający przesyłki, wskutek złego ustawienia monitora stacji roboczych, ma wgląd do przetwarzanych danych osobowych i wykonuje zdjęcia ekranu, a następnie publikuje je w sieci Internet – efektem takiego działania jest utrata poufności danych)
Incydent spowodowany awaria sprzętu/brak zasilania (np. m.in. wskutek braku zasilania fizyczny obszar przetwarzania danych osobowych zostanie pozbawiony energii elektrycznej, a co za tym idzie urządzeń alarmowych, co ułatwia dokonanie kradzieży)
Incydent spowodowany wirusem (np. m.in. pracownik instaluje na stacji roboczej samowolnie nieautoryzowane oprogramowanie, które zawiera wirusy)

Incydent spowodowany złośliwym oprogramowaniem (jw)
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)

Załącznik nr 1 do Procedury

REJESTR NARUSZEŃ DLA ADMINISTRATORA DANYCH

Data stwierdzenia naruszenia (data, godzina)	
Osoba, która stwierdziła/zgłosiła naruszenie	
Okoliczności naruszenia ochrony danych osobowych:	
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:	
Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane przez Administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków	
Środki proponowane przez Administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków	
Czy zgłoszono naruszenie do osoby, której dane dotyczą? Jeśli nie, wskazać powód braku zawiadomienia	
Czy naruszenie było zgłoszone do organu nadzorczego? *Jeśli tak, to kiedy? Można załączyć dokument zgłoszenia*.	
Załączniki:	