Procedura reagowania na naruszenia ochrony danych

Wersja	
Właściciel	
Data zatwierdzenia	
Data wejścia w życie	

Zatwierdzający	

SPIS TREŚCI

§ 1. DEFINICJE

1. **Administrator (ADO)** – spółka ..... z w.....;

2. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3. **Koordynator ds. RODO** – osoba, wyznaczona przez Administratora do pełnienia funkcji koordynatora ochrony danych;

4. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

5. **Pracownik** – osoba świadcząca pracę u Administratora - bez względu na formę zatrudnienia;

6. **Procedura** – niniejszy dokument;

7. **Przetwarzanie danych osobowych** – oznacza jakąkolwiek operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

8. **Podmiot przetwarzający (PP)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza lub będzie przetwarzał dane osobowe w imieniu Administratora;

9. **RODO** – 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 osobowych).

§ 2. CEL I ZAKRES PROCEDURY

1. Celem Procedury jest określenie zasad reagowania na naruszenia ochrony danych osobowych, obejmujących ich identyfikację, rejestrowanie, analizę, podejmowanie działań.

2. Procedura obowiązuje od dnia zatwierdzenia jej przez zarząd Administratora. Zmiany i przegląd Procedury dokonywane są przez Koordynatora ds. RODO.

§ 3. OBOWIĄZEK ZAPOZNANIA SIĘ Z PROCEDURĄ

Każdy Pracownik ma obowiązek zapoznania się z niniejszą Procedurą oraz stosowania się do jej postanowień.

§ 4. REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Administrator prowadzi we współpracy z Koordynatorem ds. RODO rejestr wszelkich naruszeń ochrony danych osobowych, a więc również tych które nie podlegają zgłoszeniu organowi nadzorczemu, ani nie wymagają powiadomienia osób, których dane osobowe dotyczą („**Rejestr**").

§ 5. POSTĘPOWANIE I ODPOWIEDZIALNOŚĆ PRACOWNIKÓW

1. Przed przystąpieniem do pracy Pracownik dokonuje sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy. Pracownicy zwracają szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próbę naruszenia ochrony danych osobowych.

2. Za okoliczności, które mogą wskazywać na naruszenie ochrony danych osobowych, uważa się w szczególności poniżej wskazane zdarzenia, które mogą prowadzić do nieuprawnionego zniszczenia, utracenia, zmodyfikowania, czy ujawnienia danych osobowych:
   1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, długotrwałe przerwy w zasilaniu);
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki pracowników polegające m.in. na wysłaniu wiadomości e-mail do nieodpowiedniego adresata, niezamierzone pomyłki administratora polegające m.in. na nieprawidłowym nadaniu uprawnień, awarie sprzętowe, błędy oprogramowania, uszkodzenie szaf, zamków, zgubienie urządzeń informatycznych lub zewnętrznych nośników pamięci zawierających dane osobowe);
   3) Zagrożenia zamierzone zewnętrzne i wewnętrzne (np. włamanie do szaf, archiwów lub systemów informatycznych, kradzież narzędzi informatycznych lub nośników zewnętrznych zawierających dane osobowe).

3. W przypadku zaistnienia okoliczności, które mogą wskazywać na naruszenie ochrony danych osobowych, każdy Pracownik zobowiązany jest do natychmiastowego ustnego poinformowania o tym fakcie Administratora lub Koordynatora ds. RODO oraz w razie potrzeby przesyłania wiadomość e-mail na adres: .....

przekazując następujące informacje:

1) Imię i nazwisko osoby zgłaszającej,
2) Datę i godzinę wykrycia potencjalnego naruszenia ochrony danych osobowych,
3) Data i godzina kiedy naruszenie miało miejsce,
4) Opis zdarzenia,
5) Rodzaj danych osobowych, których naruszenie dotyczy,
6) Liczba rekordów danych osobowych, których naruszenie dotyczy,
7) Kategoria i liczba osób, których naruszenie dotyczy,
8) Komunikaty oraz logi systemowe,
9) Zrzuty ekranu,
10) Informacje o ewentualnych świadkach zdarzenia.

4. Okoliczności naruszenia ochrony danych osobowych mogą być również zgłaszane automatycznie przez systemy monitorujące infrastrukturę teleinformatyczną. Monitorowanie może obejmować: warunki środowiskowe w serwerowni, wykorzystanie nośników wymiennych, występowanie złośliwego oprogramowania, logi kluczowych komponentów teleinformatycznych, próby włamania z sieci Internet.

5. Do czasu stwierdzenia naruszenia ochrony danych osobowych bądź jego braku, zgłaszający:
   1) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
   2) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
   3) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;
   4) Wykonuje wszelkie polecenia Administratora lub Koordynatora ds. RODO, w tym w szczególności te mające na celu ograniczenia skutków możliwego naruszenia bezpieczeństwa ochrony danych.

§ 6. POSTĘPOWANIE Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

1. Koordynator ds. RODO jest odpowiedzialny za przeprowadzenie analizy incydentu bezpieczeństwa. Analiza w szczególności obejmuje:
   1) Ocenę okoliczności wskazanych w zgłoszeniu, ze szczególnym uwzględnieniem stanu Systemu informatycznego w którym doszło do incydentu oraz wstępnie ocenia ryzyko naruszenia praw lub wolności osób fizycznych związane z incydentem;
   2) W razie zakwalifikowania zgłoszenia jako naruszenia ochrony danych osobowych - rekomenduje działania, jakie powinny zostać podjęte w celu zaradzenia naruszeniu lub zminimalizowania jego ewentualnych negatywnych skutków.

2. Jeżeli to możliwe, Koordynator ds. RODO, zabezpiecza materiał dowodowy mogących wskazać sprawców oraz sposób w jaki powstał incydent.

3. Kwalifikacji zgłoszenia w imieniu Administratora dokonuje Koordynator ds. RODO na

podstawie opracowanego formularza Excel. Koordynator ds. RODO rekomenduje zarządowi Administratora jedno z 3 rozwiązań lub kilka łącznie: (i) odnotowanie naruszenia w Rejestrze (ii) zgłoszenie do UODO (iii) zawiadomienie podmiotów danych.

4. W przypadku zakwalifikowania zgłoszenia jako naruszenia ochrony danych osobowych, Koordynator ds. RODO niezwłocznie informuje o tym Administratora, który bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, aby stwierdzone naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Administrator może w tym zakresie udzielić również Koordynatorowi ds. RODO odpowiedniego pełnomocnictwa.

5. W przypadku, w którym Administrator uzna, że jest mało prawdopodobne, aby stwierdzone naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych i zdecyduje się nie zgłosić naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, jest zobowiązany do przygotowania stanowiska zawierającego argumentacje dlaczego w jego opinii nie ma konieczności zgłaszania naruszenia.

6. W przypadku zgłoszenia naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, po upływie 72 godzin od stwierdzenia naruszenia do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.

7. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać co najmniej:
   1) Opis charakteru naruszenia, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, a także kategorie i przybliżoną liczbę rekordów danych osobowych, których dotyczy naruszenie;
   2) Imię i nazwisko oraz dane kontaktowe IOD, jeżeli został wyznaczony;
   3) Opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   4) Opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

8. Administrator dokumentuje wszelkie naruszenia ochrony danych. Rejestr zawiera:
   1) Datę naruszenia,
   2) Wskazanie osoby zgłaszającej naruszenie,
   3) Opis naruszenia,
   4) Przyczynę naruszenia,
   5) Opis możliwych skutków naruszenia,
   6) Opis zastosowanych środków zaradczych w celu minimalizacji zdarzenia,
   7) Podjęte działania,
   8) Środki zastosowane w celu uniknięcia naruszenia w przyszłości,
   9) Zastosowane środki bezpieczeństwa,
   10) Informacja o zawiadomieniu UODO,
   11) Informacja o powiadomieniu osoby, której dane dotyczą.

9. Jeżeli naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadomi osobę, której dane dotyczą o zaistniałym naruszeniu.

10. Zawiadomienie, o którym mowa w ust. 10 powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki o których mowa w ust. 8.

11. Zawiadomienie, o którym mowa w ust. 10 powyżej nie jest wymagane w przypadku, gdy:
    a) Administrator wdrożył odpowiednie środki techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie;
    b) Administrator zastosował środki eliminujące prawdopodobieństwa wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
    c) Wymagałoby ono niewspółmiernie dużego wysiłku. We wskazanym przypadku należy wydać publiczny komunikat lub zastosować podobny środek, tak aby osoby, których dane dotyczą zostały poinformowane w równie skuteczny sposób.

12. W przypadku stwierdzenia naruszenia ochrony danych osobowych przez Podmiot przetwarzający, Podmiot przetwarzający zgłasza je bez zbędnej zwłoki Administratorowi, który następnie przekazuje je Koordynatorowi ds. RODO.

13. Do zgłoszenia, o którym mowa w ust. 13 powyżej stosuje się odpowiednio § 6 niniejszej Procedury.