**Załącznik nr 16 do Polityki Ochrony danych**

**Procedura postępowania w przypadku zaistnienia zagrożenia (incydentu) ochrony danych osobowych**

1. **INFORMACJA OGÓLNA**

**Naruszenie ochrony danych osobowych** to zgodnie z definicją zawartą w art. 4 RODO 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

W przypadku naruszenia praw i wolności osoby, której dane dotyczą Administrator może być obowiązany w trybie art. 33 RODO w terminie 72 godzin do zgłaszania naruszenia do Prezesa Urzędu Ochrony Danych Osobowych. Kwalifikacja zgłoszenia naruszenia podlegającego zgłoszeniu wymaga każdorazowo przeprowadzenia analizy pod kątem naruszenia praw i wolności osoby, której dane dotyczą. Jednocześnie, zgodnie z art. 34 jeżeli naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

Nie każdy incydent bezpieczeństwa (czyli pojedyncze niepożądane lub niespodziewane zdarzenie z bezpieczeństwa informacji lub szereg takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych oraz zagrażają bezpieczeństwu informacji) stanowi naruszenie prawa i wolności osoby, której dane dotyczą.

Myśląc o zachowaniu bezpieczeństwa informacji zawsze musimy pamiętać o konieczności jednoczesnego zachowania trzech podstawowych zasad tj.:

1. integralności informacji polegającej na zapewnieniu jej kompletności i dokładności;
2. poufności informacji charakteryzującej się tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom;
3. dostępności informacji czyli właściwości bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu

Do typowych przykładów naruszenia bezpieczeństwa danych osobowych wymagających bezpośredniej reakcji, jak również zgłoszenia zgodnie z obowiązującą procedurą w zakresie zgłaszania naruszeń bezpieczeństwa, możemy zaliczyć:

niszczenie dokumentów w stopniu umożliwiającym otworzenie danych (np. bez użycia niszczarki)

ustawienie monitora pozwalające na wgląd osobom postronnym,

nie stosowanie wygaszacza i blokady ekranu po odejściu od komputera,

ujawnienie swojego osobistego hasła drugiemu użytkownikowi programu, systemu

pozostawienie w miejscu widocznym hasła do komputera ( przysłowiowa „żółta karteczka”),

pozostawienie niezabezpieczonego pomieszczenia, szafy etc po opuszczeniu pomieszczenia

pozostawienie w pomieszczeniu gdzie są przechowywane dane osobowe osoby nieupoważnionej bez nadzoru,

udzielenie telefonicznych informacji o danych osobowych bez zweryfikowania osoby dzwoniącej i podstawy udzielenia tej informacji,

otrzymanie mail o treści prowokującej do ujawnienia hasła, potwierdzenia rzekomej transakcji, informacji o przesłanej fakturze z adresu innego niż pierwotnie widoczny na liście,

zagubienie, kradzież laptopa, smartfona, dysków przenośnym lub innych nośników danych osobowych (np. pendrive, CD-room ), dokumentacji papierowej,

zagubienie korespondencji papierowej przez operatora pocztowego lub nosząca ślady otwarcia przed zwróceniem jej do dostawcy,

przesłanie maila do wielu adresatów zewnętrznych bez zastosowani kopii ukrytej ( sytuacji nie dotyczy konwersacji prowadzonej w ramach grupy roboczej realizującej konkretne działania gdzie wskazane jest poinformowanie wszystkich o realizowanym procesie),

przesłanie mailem danych osobowych do niewłaściwego adresata,

ujawnienie śladów wskazujących na próbę włamania do pomieszczenia,

ataki hackerskie, które nie zostały zablokowane przez stosowany w ADMINISTRATOR system antywirusowy,

inne zdarzenia mające lub mogące mieć wpływ na naruszenie bezpieczeństwa danych osobowych.

Oprócz naruszeń obejmujących celowe lub przypadkowe działania człowieka należy również zaliczyć:

* 1. zdarzenia losowe (zewnętrzne) – pożar obiektu lub pomieszczenia, zalanie wodą, utratę zasilania, utratę łączności,
	2. zdarzenia losowe (wewnętrzne) – awaria serwera, komputera, twardego dysku, oprogramowania.

Przykładami naruszeń praw i wolności są:

1. uszczerbek fizyczny

2. szkoda majątkowa lub niemajątkowa, a w szczególności

a) dyskryminacja,

b) kradzież tożsamości lub oszustwo dotyczące tożsamości,

c) naruszenie dobrego imienia,

d) naruszeniem poufności danych osobowych chronionych tajemnica zawodową,

e) nieuprawnione odwróceniem pseudonimizacji

e) pozbawienie przysługujących praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi

f) wszelka inną znaczną szkoda gospodarcza lub społeczna;

1. **PROCEDURA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU**
2. Biorąc pod uwagę powyższe za **naruszenie ochrony danych osobowych** (dalej określonej jako „naruszenie”) uznaje się przypadki, gdy:
	1. stwierdzono naruszenie zabezpieczenia systemu informatycznego,
	2. stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
	3. miał miejsce przypadek utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe,
	4. stwierdzono inne, nie wymienione okoliczności, takie jak zdarzenia losowe, czy umyślne i nieumyślne incydenty, na podstawie których jednak można wnosić, iż doszło do sytuacji, w której do danych osobowych mogła uzyskać dostęp osoba nieupoważniona.
3. Każdy Pracownik Administratora, który stwierdzi lub podejrzewa wystąpienie zagrożenia dla ochrony danych osobowych lub fakt naruszenia ochrony danych osobowych, zobowiązany jest (w pierwszej kolejności) do natychmiastowego, osobistego poinformowania o tym swojego bezpośredniego przełożonego (dopuszczalna jest droga telefoniczna), a w razie jego braku Dyrektora oraz, w razie jego wyznaczenia, Inspektora Ochrony Danych.
4. Informacja, o której mowa w pkt 2, powinna być dodatkowo przekazana pisemnie lub w formie wiadomości mailowej niezwłocznie po stwierdzeniu okoliczności, o których mowa w pkt 1.
5. Informacja, o której mowa w pkt 3 musi uwzględniać co najmniej
	* + możliwie precyzyjny opis okoliczności zagrożenia lub naruszenia i podjętych działań w reakcji na te okoliczności,
		+ podanie orientacyjnego terminu wystąpienia okoliczności zagrożenia lub naruszenia oraz orientacyjny czas ich trwania,
		+ wyszczególnienie zagrożonych lub naruszonych danych (jeśli to możliwe),
		+ informację kto, kiedy i w jaki sposób został powiadomiony dotychczas o fakcie wystąpienia okoliczności zagrożenia lub naruszenia, jakie były wstępne decyzje osób, które zostały powiadomione oraz kto posiada informacje o okolicznościach naruszenia lub zagrożenia,
		+ dane osoby zgłaszającej.
6. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych administratora danych, bezpośredni przełożony Pracownika, który stwierdził lub podejrzewa wystąpienie zagrożenia dla ochrony danych osobowych lub fakt naruszenia ochrony danych osobowych, a w razie jego braku sam pracownik powinien:
	1. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
	2. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
	3. udokumentować wstępnie zaistniałe naruszenie,
	4. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora danych.
7. Każde zgłoszone naruszenie bezpieczeństwa informacji Administrator danych zobowiązany odnotować w rejestrze naruszeń.
8. Administrator danych oraz osoby przez niego wskazane, jeśli stwierdziły lub uzyskały informację wskazującą na wystąpienie okoliczności zagrożenia lub naruszenia ochrony danych osobowych zobowiązani są do podjęcia natychmiast wspólnych działań mających na celu:
	1. zabezpieczenie danych osobowych przed ich naruszeniem lub przed dalszym ich naruszaniem,
	2. ustalenie zakresu i przyczyn zagrożenia lub naruszenia, i jego ewentualne skutki,
	3. ustalenie skutków i wielkości szkód, jakie mogły wystąpić na skutek wystąpienia okoliczności zagrożenia lub naruszenia,
	4. ustalenie kręgu osób odpowiedzialnych za wystąpienie okoliczności zagrożenia lub naruszenia,
	5. ustalenie zbioru danych osobowych, które uległy zagrożeniu lub naruszeniu,
	6. ustalenie rodzajów danych osobowych, które uległy zagrożeniu lub naruszeniu,
	7. ustalenie kręgu osób fizycznych, których dane osobowe uległy zagrożeniu lub naruszeniu,
	8. zabezpieczeniu ewentualnych dowodów zagrożenia lub naruszenia,
	9. przedsięwzięcia działań naprawczych mających na celu usunięcie stanu zagrożenia lub skutków naruszenia,
	10. przygotowanie strategii mającej na celu zapobieżeniu wystąpienia okoliczności zagrażania lub naruszania danych osobowych w przyszłości.
9. Administrator jeśli stwierdził lub uzyskał informację wskazującą na wystąpienie okoliczności zagrożenia lub naruszenia ochrony danych osobowych zobowiązany jest ponadto do niezwłocznego:
	1. jeżeli zasoby Systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
	2. podjęcia działań mających na celu zapobieżeniu wystąpienia okoliczności zagrażania lub naruszania danych osobowych w przyszłości,
	3. podjęcie działań kontrolnych, mających na celu sprawdzenie ewentualnej możliwości wystąpienia w przyszłości okoliczności zagrożenia lub naruszenia danych osobowych,
	4. zainicjowania ewentualnych działań dyscyplinarnych,
	5. szczegółowego odnotowania, w specjalnie w tym celu prowadzonym rejestrze (o którym mowa w pkt 5 powyżej), wszelkich informacji związanych z wystąpieniem okoliczności zagrożenia lub naruszenia danych osobowych, a w szczególności informacji uzyskanych na podstawie działań, o których mowa w pkt 4 i 6, i odnotowaniu rodzajów podjętych działań
10. W przypadku stwierdzenie naruszenia skutkującego naruszeniem praw i wolności osoby, której dane dotyczą Administrator danych **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** zobowiązany jest do zgłoszenia tego faktu do organowi nadzorczemu, którym jest Prezes Urzędu Ochrony Danych Osobowych.
11. **Zgłoszenia**, o którym mowa w pkt 9 **nie dokonuje się**, jeżeli ADO stwierdzą, że naruszenie ochrony danych osobowych **nie skutkowało naruszeniem praw i wolności osób fizycznych**.
12. Zgłoszenie naruszenia, o którym mowa w pkt 9, musi co najmniej zawierać:
	1. typ zgłoszenie (wstępne, jednorazowe-kompletne, uzupełniające),
	2. dane podmiotu zgłaszającego czyli ADMINISTRATORA obejmujące dane teleadresowe, dane osób uprawnionych do reprezentacji,
	3. dane kontaktowe inspektora ochrony danych (jeżeli został powołany) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
	4. czas naruszenia, sposób stwierdzenia naruszenia,
	5. charakter naruszenia (brak zachowania poufności, integralności lub dostępności),
	6. rodzaj naruszenia (zagubienie lub kradzież urządzenia, nośnika danych, dokumentacji papierowe, stwierdzenie nieuprawnionego dostępu do informacji, phishing, niezamierzona publikacja, przesłanie informacji do niewłaściwej osoby, ujawnienie danych osobom nieuprawnionym),
	7. przyczyny naruszenia,
	8. kategorie danych osobowych w zakresie danych podstawowych (np. dane identyfikacyjne, numer PESEL lub inny krajowy numer identyfikacyjny, dane kontaktowe, dane ekonomiczne i finansowe (np. historie transakcji, numery rachunków bankowych), oficjalne dokumenty (np. dowód osobisty, akt notarialny), dane lokalizacyjne (np. miejsce zamieszkania, GPS), szczególnych kategorii danych, wyroków skazujących, czynów zabronionych,
	9. kategorie osób ( np. pracownicy, użytkownicy, klienci (obecni i potencjalni)),
	10. przybliżona liczbę wpisów danych,
	11. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
	12. opis możliwych konsekwencji naruszenia ochrony danych osobowych.

Zgłoszenie dokonywane jest zgodnie z instrukcją zawartą na stronie <https://uodo.gov.pl/pl/134/233>, na formularzu zgłoszenia naruszenia ochrony danych osobowych.

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Wzór zawiadomienia stanowi załącznik nr 16 do Polityki ochron danych.
2. Zawiadomienie, o którym mowa w pkt 12 formułowane jest prostym i zrozumiałym językiem
i dokonywane jest przy pomocy wiadomości elektronicznej oraz zawiera:
	1. imię i nazwisko oraz dane kontaktowe Inspektora Danych Osobowych (jeżeli został powołany) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
	2. opis możliwych konsekwencje naruszenia ochrony danych osobowych,
	3. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Zawiadomienie, o którym mowa w ust. 12 nie jest wymagane, w następujących przypadkach:
4. Administrator wdrożył 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,
5. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
6. 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.
7. W sytuacji kiedy Administrator jest podmiotem przetwarzającym po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w wyznaczonym w umowie powierzenia czasie tak aby administrator danych (nasz klient) miał możliwość zgłoszenia naruszenia w wyznaczonym przez organ nadzorczy w terminie 72h od godziny zajścia zdarzenia.