**INISTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTU NA DANYCH OSOBOWYCH**

**§ 1**

**Definicje**

1. **Administrator danych osobowych (Administrator) -** …[[1]](#footnote-1)
2. **Incydent mogący skutkować naruszeniem ochrony danych osobowych** (**Incydent**) – oznacza każde zaburzenie w procesie przetwarzania danych osobowych.
3. **Inspektor ochrony danych osobowych (IOD) –** osoba, wykonująca zadania określone w art. 39 Rodo[[2]](#footnote-2), skutecznie zgłoszona do Urzędu Ochrony Danych Osobowych;
4. **Naruszenie ochrony danych osobowych (Naruszenie)** - oznacza 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. **Organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych.

**§ 2**

**Zakres przedmiotowy i podmiotowy Instrukcji**

1. Niniejsza Instrukcja określa tryb postępowania w przypadku wystąpienia u Administratora Incydentu lub stwierdzenia Naruszenia ochrony danych osobowych.
2. Niniejsza Instrukcja określa obowiązki w zakresie Incydentów oraz Naruszeń ochrony danych osobowych wszystkich pracowników i innych osób mających dostęp do danych osobowych przetwarzanych u Administratora na podstawie umów cywilnoprawnych oraz osób odbywających praktykę lub staż.

**§ 3**

**Postępowanie w przypadku Incydentu**

1. Źródłem informacji o wystąpieniu Incydentu mogą być zarówno pracownicy jak i osoby świadczące usługi na podstawie umowy cywilnoprawnej lub osoby odbywające praktykę lub staż oraz osoby trzecie.
2. Każda osoba, która uzyskała informację o wystąpieniu Incydentu lub informację o podejrzeniu wystąpienia takiego Incydentu ma obowiązek niezwłocznie zgłosić ją do IOD [[3]](#footnote-3)oraz [[4]](#footnote-4)…
3. Adresat powiadomienia o Incydencie niezwłocznie uzupełnia informacje niezbędne do zarządzenia Incydentem, w szczególności odnotowując:
   1. dokładny opis i przebieg zdarzenia z podaniem daty i godziny,
   2. ilość danych, zakres danych, kategorie danych osobowych a w szczególności informację czy Incydentowi podlegają dane administrowane czy też powierzone …,[[5]](#footnote-5)
   3. opis kroków podjętych dotychczas w celu zminimalizowania negatywnych skutków Incydentu.

**§ 4**

**Kwalifikacja Incydentu**

1. Po otrzymaniu informacji o wystąpieniu Incydentu, IOD, a w przypadku jego nieobecności osoba zastępująca IOD, ustala, czy Incydent wyczerpuje znamiona naruszenia ochrony danych osobowych i przekazuje ocenę Zarządowi[[6]](#footnote-6) Administratora wraz ze swoją rekomendację dalszego postępowania w sprawie.
2. Zarząd Administratora niezwłocznie, nie później jednak niż w terminie 24 godzin od otrzymania rekomendacji IOD podejmuje decyzję w przedmiocie jej wdrożenia.
3. IOD w celu określenia i oceny wagi Incydentu ma prawo żądać udokumentowanych wyjaśnień od każdej osoby mającej związek z Incydentem, jak również pozyskiwać dowody potwierdzające składane wyjaśnienia, takie jak logi do systemów, zrzuty ekranu, umowy z kontrahentami i inne dokumenty.

**§ 5**

**Postępowanie w sytuacji stwierdzania Naruszenia ochrony danych osobowych**

1. Stwierdzenie Naruszenia następuje chwili zatwierdzenia rekomendacji IOD przez Zarząd, o ile w treści rekomendacji zawarto informację, że okoliczności Incydentu wskazują, że do Naruszenia doszło.
2. Jeżeli Zarząd nie wypowie się w zakresie rekomendacji IOD w terminie 24 godzin od jej otrzymania przyjmuje się, że stwierdzenie Naruszenia nastąpiło z upływem tego terminu.
3. W przypadku stwierdzenia Naruszenia IOD:
4. dokonuje oceny wagi naruszenia,
5. ustala przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy Naruszenie,
6. identyfikuje wszystkie podmioty uczestniczące w procesie przetwarzania danych osobowych, którego dotyczy Naruszenie,
7. Jeżeli z Naruszeniem wiąże się ryzyko naruszenia praw i wolności osób fizycznych, należy zgłosić je Organowi nadzorczemu w terminie 72 godzin od jego stwierdzenia. W przypadku, gdy ryzyko to jest określane jako wysokie, należy również powiadomić o nim osoby, których dane dotyczą.
8. Jeżeli jest mało prawdopodobne by Naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych, nie jest wymagane jego zgłoszenie Organowi nadzorczemu, ani powiadamianie osób, których dane dotyczą. Prowadzone są jednak działania zaradcze, a Naruszenie dokumentowane jest w rejestrze Incydentów i Naruszeń.
9. W sytuacji, gdy dotychczasowe czynności wyjaśniające nie pozwalają na dokonanie jego kompletnego zgłoszenia w terminie określonym w ust. 4 powyżej, wówczas dokonuje się wstępnego zgłoszenia Naruszenia, a po uzyskaniu kolejnych, istotnych informacji o Naruszeniu dokonuje niezwłocznie zgłoszenia uzupełniającego.

**§ 6**

**Zawiadomienie osoby, której dane dotyczą, o Naruszeniu ochrony danych osobowych**

1. Jeżeli ryzyko naruszenia praw i wolności osób fizycznych wynikające z Naruszenia określono jako wysokie, Administrator zobowiązany jest do niezwłocznego powiadomienia osoby, której dane dotyczą o Naruszeniu.
2. W powiadomieniu o Naruszeniu znajduje się co najmniej:
3. opis charakteru Naruszenia,
4. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego,
5. opis prawdopodobnych konsekwencji Naruszenia,
6. opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia Naruszeniu, w tym w stosownych przypadkach proponowanych osobie środków zaradczych w celu zminimalizowania przez nią negatywnych skutków Naruszenia.
7. Dowody potwierdzające powiadomienie osoby, której dane dotyczą archiwizowane są razem z rejestrem Naruszeń.

**§ 7**

**Dokumentowanie Naruszeń**

1. Osoba wyznaczona przez Administratora prowadzi rejestr Incydentów oraz Naruszeń ochrony danych wraz ze związaną z Incydentami i Naruszeniami dokumentacją, zebranymi dowodami i korespondencją.
2. Każdemu wpisowi w rejestrze nadaje się indywidualną sygnaturę.
3. Rejestr jest na bieżąco aktualizowany i udostępniany Organowi nadzorczemu na jego żądanie.
4. Nie rzadziej niż jeden raz w roku IOD analizuje wpisy rejestru w celu:
5. oceny skuteczności środków technicznych i organizacyjnych zabezpieczenia danych osobowych,
6. zidentyfikowania powtarzających się Naruszeń,
7. decyzji w przedmiocie wykonania audytu określonego procesu przetwarzania danych osobowych.

# Wykaz załączników:

* Załącznik nr 1 – Wzór rejestru Naruszeń i Incydentów ochrony danych osobowych.

1. ## Proszę uzupełnić pełną nazwę podmiotu.

   [↑](#footnote-ref-1)
2. ## Rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.)

   [↑](#footnote-ref-2)
3. Rekomenduje się utworzenie dedykowanego adresu e-mail do zgłaszania Incydentów, np.: [incydenty@nazwa.pl](mailto:incydenty@nazwa.pl) z dostępem do skrzynki dla IOD i innych zainteresowanych stron. [↑](#footnote-ref-3)
4. ## Proszę uzupełnić zgodnie ze strukturą podmiotu.

   [↑](#footnote-ref-4)
5. Proszę o podanie nazwy podmiotu. Celowo unikam tutaj użycia terminu „Administrator” gdyż w przypadku powierzenia nasz podmiot będzie procesorem danych, nie ich administratorem. [↑](#footnote-ref-5)
6. Proszę zmienić zgodnie ze strukturą podmiotu. [↑](#footnote-ref-6)