|  |  |
| --- | --- |
| **Identyfikator dokumentu:** | IPPN |
| **Nazwa dokumentu:** | Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych lub zaistnienia zagrożeń dla ochrony danych |
| **Data:**  |  |
| **Wersja** | 1 |
| **Autor dokumentu:** | Justyna Chomicz |
| **Właściciel dokumentu:** | Joanna Lotko |
| **Osoba zatwierdzająca:** | Joanna Lotko |
| **Sposób zatwierdzenia** | elektronicznie (email) |

**Spis treści**

[Rozdział 1: Cel i zakres instrukcji 2](#_Toc532853240)

[Rozdział 2: Obowiązek zgłoszenia naruszenia ochrony danych osobowych 2](#_Toc532853241)

[Rozdział 3: Zgłaszanie podejrzanych sytuacji 3](#_Toc532853242)

[Rozdział 4: Przykładowe zdarzenia wymagające zgłoszenia 3](#_Toc532853243)

[Rozdział 5: Reagowanie na zgłoszenia 4](#_Toc532853244)

[Rozdział 6: Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych 5](#_Toc532853245)

[Rozdział 7: Naruszenie ochrony danych osobowych – odpowiedzialność 6](#_Toc532853246)

[Rozdział 8: Spis załączników 6](#_Toc532853247)

[Rozdział 9: Dokumenty powiązane 6](#_Toc532853248)

[Rozdział 10: Historia wersji 6](#_Toc532853249)

# Rozdział 1: Cel i zakres instrukcji

1. Celem Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych (zwanej dalej „Instrukcją”) jest ustalenie zasad i procedur reagowania w przypadku wystąpienia zdarzenia będącego naruszeniem ochrony danych osobowych. Ponadto Instrukcja ma na celu wprowadzenie środków pozwalających ja szybką i skuteczną reakcję na naruszenia ochrony danych osobowych.
2. Instrukcja zawiera procedurę zgłaszania naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.
3. Instrukcja jest bezpośrednio powiązana z dokumentem Polityki Bezpieczeństwa (tj.„PB Polityka Bezpieczeństwa Informacji i Danych Osobowych”).
4. Instrukcja powinna być wykorzystywana w powiązaniu z dokumentem Polityki Bezpieczeństwa.
5. Naruszenie ochrony danych osobowych 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;
6. Zakres niniejszej Instrukcji obejmuje przypadki przetwarzania danych osobowych zarówno w systemach informatycznych jak i w wersji papierowej. W szczególności instrukcja obejmuje:
	1. wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz papierowe, w których przetwarzane są dane osobowe podlegające ochronie;
	2. wszystkie lokalizacje - budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie;
7. Do stosowania zasad określonych przez Instrukcję zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, współpracownicy oraz wykonawcy.
8. Za koordynację działań związanych z reakcją na naruszenia danych osobowych jest odpowiedzialna osoba wskazana w dokumencie, stanowiącym załącznik do Polityki Bezpieczeństwa, tj. „PB\_01 Lista kontaktowa ochrony danych osobowych” zwana dalej koordynatorem. W przypadku powołania Inspektora Ochrony Danych (IOD), koordynatorem tym staje się IOD.

# Rozdział 2: Obowiązek zgłoszenia naruszenia ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, administrator danych osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
	1. opisywać 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;
	2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
	3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
	4. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli – i w zakresie, w jakim – informacji, o których mowa powyżej, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
5. Administrator danych osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego rozdziału.
6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

# Rozdział 3: Zgłaszanie podejrzanych sytuacji

1. Każdy pracownik lub współpracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych lub zagrożenia dla ochrony danych osobowych, jest zobowiązany niezwłocznie zgłosić to osobie odpowiedzialnej za koordynację działań związanych z naruszeniami danych osobowych, wskazanej w dokumencie „PB\_01 Lista kontaktowa ochrony danych osobowych” jako koordynator. Jeśli kontakt z koordynatorem nie jest możliwy w rozsądnym czasie, to pracownik zgłasza naruszenie swojemu bezpośredniemu przełożonemu, a jeśli i to nie jest możliwe to członkowi zarządu.
2. Każdy pracownik i współpracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .
3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia koordynatora lub innej osoby upoważnionej przez koordynatora lub administratora (lub jeżeli został powołany inspektora ochrony danych osobowych).

# Rozdział 4: Przykładowe zdarzenia wymagające zgłoszenia

Do zdarzeń, które wymagają zgłoszenia należą m.in.:

* ślady na drzwiach, oknach lub szafach, które wskazują na włamanie lub próbę włamania;
* wyrzucenie dokumentów z danymi osobowymi w stopniu zniszczenia umożliwiającym ich odczytanie (np. bez użycia niszczarki);
* pozostawienie danych osobowych w drukarce, na ksero, a tym samym potencjalne udostępnienie danych osobowych osobom nieupoważnionym;
* pozostawienie bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe;
* niezablokowanie stanowiska pracy w sposób uniemożliwiający dostęp do treści wyświetlanych na ekranie w przypadku opuszczenia stanowiska pracy,
* nieprawidłowe ustawienie monitorów, które powoduje, iż osoby postronne mogą zapoznać się z treścią informacji wyświetlanych na monitorach,
* wynoszenie danych osobowych zapisanych na nośnikach/ urządzeniach bądź utrwalonych na papierze bez zgody administratora;
* przypadki udostępnienia danych osobowych w formie papierowej lub elektronicznej osobom nieupoważnionym;
* kradzież komputerów, nośników elektronicznych lub dokumentów papierowych z danymi osobowymi;
* zgubienie lub kradzież nośnika/ urządzenia zawierającego dane osobowe,
* skuteczne telefoniczne próby wyłudzenia danych osobowych,
* pozostawienie dokumentacji papierowej zawierającej dane osobowe lub nośników zawierających dane osobowe w niezabezpieczonej lokalizacji,
* utrata korespondencji papierowej zawierającej dane osobowe przez operatora pocztowego,
* zwrócenie do nadawcy otwartej korespondencji pocztowej zawierającej dane osobowe,
* maile zachęcające do ujawnienia identyfikatora i/lub hasła;
* oznaki infekcji wirusem komputerowym lub podejrzane zachowanie komputera;
* złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych,
* uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak email czy komunikator internetowy (phishing),
* nieprawidłowa anonimizacja danych,
* nieprawidłowe usunięcie danych/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora,
* niezamierzona publikacja danych,
* zapisanie hasła do systemu informatycznego/komputera na kartce,
* nieuzasadnione ujawnienie hasła do systemu informatycznego zawierającego dane osobowe,
* ujawnienie zabezpieczeń i procedur ochrony danych osobowych osobom nieuprawnionym;
* przypadki podłączenia się do sieci IT osób nieuprawnionych,
* utrata kontroli nad kopią danych osobowych,
* przechowywanie haseł do systemów informatycznych w pobliżu komputera.

# Rozdział 5: Reagowanie na zgłoszenia

1. Osoba odpowiedzialna za koordynację działań związanych z naruszeniami danych osobowych, wskazana w dokumencie „PB\_01 Lista kontaktowa ochrony danych osobowych” jako koordynator:
	1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy;
	2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem;
	3. jeśli zachodzi taka potrzeba, nawiązuje kontakt ze specjalistami wewnętrznymi lub zewnętrznymi (na przykład specjalistami IT), zasięga potrzebnych opinii i proponuje działania zaradcze i naprawcze, ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych osobowych;
	4. dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport używając załącznika „IPPN\_01 Formularz raportu ze zdarzenia” lub formularza organu nadzorczego oraz uzupełnia dokument „IPPN\_02 Rejestr zdarzeń naruszenia i zagrożenia ochrony danych osobowych”;
	5. ocenia czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, a jeśli tak, to powiadamia o tym zarząd i w ciągu 72h od wykrycia naruszenia, zgłasza naruszanie organowi nadzorczemu. Jeśli nie można dotrzymać terminu 72h, to zgłoszenie do organu nadzorczego jest uzupełniane o przyczyny opóźnienia;
	6. jeśli dane których dotyczy naruszenie są przetwarzane w wyniku ich powierzenia przez inny podmiot, naruszenie bez zbędnej zwłoki zgłaszane jest administratorowi danych;
	7. jeśli zachodzi taka potrzeba, to w porozumieniu z zarządem powiadamia organy ścigania.

# Rozdział 6: Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w Rozdziale 2 ust. 3 lit. b), c) i d) niniejszej Instrukcji.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach:
	1. 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;
	2. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
	3. 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

# Rozdział 7: Naruszenie ochrony danych osobowych – odpowiedzialność

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami może zostać wszczęte postępowanie dyscyplinarne lub porządkowe. Ponadto osoba ta ponosi odpowiedzialność na zasadach ogólnych za wszelkie szkody, które w związku z jej zachowaniem/naruszeniem poniósł Administrator.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków lub naruszenie obowiązków umownych (w przypadku umowy cywilnoprawnej). Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę/zleceniodawcę/zamawiającego o zrekompensowanie poniesionych strat.

# Rozdział 8: Spis załączników

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **Tytuł dokumentu** | **Typ dokumentu** |
| IPPN\_01 | Formularz raportu ze zdarzenia naruszenia ochrony danych osobowych lub zaistnienia zagrożeń dla ochrony danych | Wewnętrzny |
| IPPN\_02  | Rejestr zdarzeń naruszenia i zagrożenia ochrony danych osobowych | Wewnętrzny poufny |

# Rozdział 9: Dokumenty powiązane

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **Tytuł dokumentu** | **Typ dokumentu** |
| PB | Polityka Bezpieczeństwa Informacji i Danych Osobowych | Wewnętrzny |

# Rozdział 10: Historia wersji

|  |  |  |  |
| --- | --- | --- | --- |
| **Wersja** | **Data** | **Autor** | **Opis zmian** |
| 1 | 06.12.2018 | Justyna Chomicz | Pierwsza wersja |