

*Załącznik nr 7 do Zarządzenia Nr 25/2025 Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa zmieniającego zarządzenie w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Agencji Restrukturyzacji i Modernizacji Rolnictwa*

*Załącznik nr 8 do Polityki bezpieczeństwa informacji w ARiMR*

## **REGULAMIN ZARZĄDZANIA INCYDENTAMI**

### **Spis treści:**

§ 1. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji.....	2
§ 2. Postępowanie z incydentami .....	2
§ 3. Ograniczanie skutków incydentu .....	4
§ 4. Odtwarzanie systemu informacyjnego .....	5
§ 5. Działania po zakończeniu incydentu .....	6
§ 6. Rejestrowanie informacji o incydentach .....	6
§ 7. Gromadzenie materiału dowodowego .....	7
<i>Załącznik nr 1 do Regulaminu - Instrukcja zabezpieczania komputerów.....</i>	<i>8</i>
<i>Załącznik nr 2 do Regulaminu - Wzór protokołu zabezpieczenia materiału dowodowego ..</i>	<i>10</i>
<i>Załącznik nr 3 do Regulaminu - Wzór raportu z incydentu .....</i>	<i>12</i>
<i>Załącznik nr 4 do Regulaminu – Procedura postępowania w sytuacji naruszenia ochrony danych osobowych .....</i>	<i>15</i>

## **§ 1.**

### **Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji**

1. Wszyscy pracownicy Agencji oraz pracownicy reprezentujący Podmiot zewnętrzny, którzy mają dostęp do systemów informacyjnych Agencji i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury Agencji dotyczące bezpieczeństwa informacji.
2. Zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji opisane zostały w Regulaminie użytkownika.
3. Osoba dokonująca zgłoszenia jest informowana przez Inspektora Bezpieczeństwa Informacji/Administradora Zabezpieczeń Fizycznych/Help Desk ARiMR o wyniku obsługi zgłoszenia.
4. Administrator Systemu/Administrator Zabezpieczeń Fizycznych ma obowiązek zareagować na alarm wygenerowany przez moduł automatycznego powiadamiania w systemach wykrywania włamań (systemów teleinformatycznych oraz elektronicznych systemów zabezpieczeń). W razie zidentyfikowania zagrożenia naruszenia bezpieczeństwa ochrony danych osobowych Administrator Systemu/Administrator Zabezpieczeń Fizycznych niezwłocznie informuje Inspektora Ochrony Danych, przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania.
5. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi Podmiotom zewnętrznym, powiadamianie Administratora Systemu/Administradora Zabezpieczeń Fizycznych/Inspektora Bezpieczeństwa Informacji/ Inspektora Ochrony Danych o zdarzeniu odbywa się na zasadach określonych w umowie o świadczeniu usług.
6. W celu zapewnienia prawidłowości i kompletności zgłaszania oraz obsługi zdarzeń związanych z bezpieczeństwem informacji, dyrektor komórki właściwej ds. bezpieczeństwa informacji dokonuje:
  - 1) comiesięcznych analiz z użyciem raportów tworzonych w ramach realizacji umów z Podmiotami zewnętrznymi;
  - 2) przeglądu zdarzeń z wykorzystaniem, udostępnionych przez komórkę właściwą ds. informatyki, narzędzi monitorujących środowisko teleinformatyczne Agencji w czasie rzeczywistym.

## **§ 2.**

### **Postępowanie z incydentami**

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych lub pracownik Help Desk ARiMR dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
  - 1) zdarzenie niemające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna;
  - 2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej;
  - 3) awaria techniczna czasowo blokująca dostępność informacji;
  - 4) incydent niskiej kategorii - związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności i poufności, nie generujący kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego Agencji;

- 5) incydent średniej kategorii – związany z naruszeniem bezpieczeństwa informacji wywołujący którykolwiek z poniższych skutków:
    - a) pośrednie lub bezpośrednie zatrzymanie realizacji jakiegokolwiek procesu ustawowego,
    - b) straty finansowe nieprzekraczające kwoty 139 tys. €,
    - c) konsekwencje prawne,
    - d) utratę wizerunku;
  - 6) incydent wysokiej kategorii - związany z naruszeniem bezpieczeństwa informacji, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów Agencji; skutki tego incydentu powodują uruchomienie PZCD i wznowienie funkcjonowania w Zapasowych Miejscach Pracy; incydemntem wysokiej kategorii jest również incydent, którego skutki mogą spowodować straty przekraczające kwotę 139 tys. €.
2. W przypadku zdarzenia związanego z naruszeniem ochrony danych osobowych należy postępować zgodnie z wytycznymi zawartymi w załączniku nr 4 do niniejszego regulaminu. Inspektor Ochrony Danych na podstawie przekazanej dokumentacji dokonuje oceny zdarzenia związanego z naruszeniem zasad ochrony danych osobowych i stwierdza, czy doszło do wysokiego ryzyka związanego z naruszeniem danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do przekazania informacji oraz opinii w wyznaczonym przez Inspektora Ochrony Danych terminie.
  3. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa informacji mogą świadczyć:
    - 1) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
    - 2) niestabilna praca systemu teleinformatycznego;
    - 3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
    - 4) nowe „podejrzane” (nieznane) konta użytkowników;
    - 5) wysoka aktywność kont, które długo pozostawały niewykorzystane;
    - 6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
    - 7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
    - 8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Agencji (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).
  4. O zdarzeniu noszącym znamiona incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych/pracownik Help Desk ARiMR powiadamia niezwłocznie Inspektora Bezpieczeństwa Informacji (IBI), który dokonuje ostatecznej jego klasyfikacji.
  5. Inspektor Bezpieczeństwa Informacji, we współpracy z Administratorem Systemu oraz, jeśli zachodzi taka potrzeba, z Administratorem Zabezpieczeń Fizycznych, przeprowadza analizę incydentu.
  6. Analiza incydentu uwzględnia następujące kryteria:
    - 1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego;

- 2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.);
  - 3) liczba jednostek/komórek organizacyjnych Agencji, zakres zasobów dotkniętych incydem;
  - 4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydem związanym z bezpieczeństwem informacji;
  - 5) możliwości rozszerzania się incydemu i sposoby jego ograniczania;
  - 6) szacowany poziom szkód finansowych;
  - 7) rodzaj ujawnionej informacji (jeśli ma zastosowanie – np. dane osobowe);
  - 8) szacunkowy czas, po którym skutki incydemu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji;
  - 9) skutki organizacyjne i prawne (wstępny szacunek).
7. W przypadku, gdy incydent ma skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej Agencji, lub gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydemu jako incydemu wysokiej kategorii, Inspektor Bezpieczeństwa Informacji powiadamia niezwłocznie dyrektora komórki właściwej ds. bezpieczeństwa informacji, który następnie informuje niezwłocznie Prezesa Agencji.
8. W przypadku, gdy zasięg incydemu wykracza poza system teleinformatyczny Agencji, Administrator Systemu, w porozumieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi Podmiotami zewnętrznymi, może przekazać do Podmiotu zewnętrznego informacje o incydencie zawierające:
- 1) typ zdarzenia;
  - 2) informacje o odległym systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników;
  - 3) wszystkie zapisy z rejestrów zdarzeń w określonym przedziale czasowym;
  - 4) inne informacje określone w umowie z Podmiotem zewnętrznym.
9. W przypadku, gdy rodzaj i zasięg incydemu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Prezes Agencji.

### **§ 3.**

#### **Ograniczanie skutków incydemu**

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych prowadzi bieżącą dokumentację incydemu. Dokumentacja ta w szczególności obejmuje:
  - 1) wszystkie zdarzenia zachodzące w systemie informacyjnym (zapisy systemowych dzienników audytu zdarzeń i dzienników audytu, lub zapisy z elektronicznych systemów zabezpieczeń);
  - 2) wszystkie podejmowane działania (opatrzone datą i czasem);
  - 3) wszystkie przeprowadzone rozmowy (osoba rozmówcy, data i czas zdarzenia, treść rozmowy).
2. Dokumentacja incydemu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowanie przy postępowaniu z incydemem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe

(zgodnie z rygorami tworzenia materiału dowodowego), bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

3. Administrator Systemu/Administrator Zabezpieczeń Fizycznych przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowania źródła naruszenia bezpieczeństwa. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
4. W przypadku, gdy działania opisane w ust. 3 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Agencji, Administrator Systemu/Administrator Zabezpieczeń Fizycznych przedstawia decyzję do akceptacji Prezesa Agencji, wraz z rekomendacją dyrektora komórki właściwej ds. bezpieczeństwa informacji.
5. Rekomendacja dyrektora komórki właściwej ds. bezpieczeństwa informacji uwzględnia:
  - 1) uzależnienie Agencji od systemu teleinformatycznego (jak długo Agencja może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu);
  - 2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych Agencji na ujawnienie w przypadku utrzymywania się stanu naruszenia zabezpieczenia;
  - 3) stopień uświadomienia użytkowników (jaka może być reakcja użytkowników na anormalne zachowanie się systemu – np. niemożność zarejestrowania się, wyłączenie niektórych funkcji, itp.);
  - 4) konieczność schwytania i ewentualnego ukarania sprawcy (przy założeniu, że istnieją okoliczności umożliwiające takie działanie);
  - 5) konieczność angażowania zasobów systemu informatycznego (jaka część i jak długo);
  - 6) aspekt finansowy, organizacyjny i ludzki podejmowanych działań (jak długo działanie ma trwać, w jakim stopniu zakłóca normalne funkcjonowanie Agencji, jakie są tego koszty).
6. Przy ograniczaniu skutków incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji, może korzystać z konsultantów zewnętrznych, jeśli Agencja wcześniej zawarła w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji Agencji.

#### **§ 4.**

#### **Odtwarzanie systemu informacyjnego**

1. Z zastrzeżeniem ust. 4, Administrator Systemu przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.
2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Zapewnienia Ciągłości Działania ARiMR, odtwarzanie systemu jest realizowane w oparciu o procedury opisane w tym planie.
3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemu ma uzasadnioną pewność, że nie zawiera źródła incydentu.
4. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
5. Prezes Agencji, po zasięgnięciu opinii dyrektora komórki właściwej ds. bezpieczeństwa informacji i Administratora Systemu, może podjąć decyzję o podjęciu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

## **§ 5.**

### **Działania po zakończeniu incydentu**

1. Inspektor Bezpieczeństwa Informacji, przy wsparciu Administratora Systemu, Właścicieli Procesów / Właścicieli Zasobów, Administratora Zabezpieczeń Fizycznych, sporządza raport z incydentu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego regulaminu oraz wprowadza do Rejestru Incydentów Bezpieczeństwa Informacji (RIBI) prowadzonego przez dyrektora właściwej komórki np. bezpieczeństwa informacji.
2. Jeśli zachodzi taka potrzeba, to Administrator Systemu/ Administrator Zabezpieczeń Fizycznych sporządza dodatkowy raport techniczny, stanowiący załącznik do raportu wskazanego w ust. 1 i zawierający co najmniej:
  - 1) rejestr incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań;
  - 2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód);
  - 3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu;
  - 4) kopię dziennika pracy systemu z okresu trwania incydentu;
  - 5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu;
  - 6) zakres informacji technicznych przekazanych Podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.
3. Dyrektor komórki właściwej np. bezpieczeństwa informacji, sporządza okresowy przegląd incydentów i przedstawia go Komitetowi.
4. Dyrektor komórki właściwej np. bezpieczeństwa informacji przedkłada Prezesowi Agencji rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości.

## **§ 6.**

### **Rejestrowanie informacji o incydentach**

1. Dyrektor komórki właściwej np. bezpieczeństwa informacji prowadzi rejestr incydentów zawierający następujące informacje:
  - 1) opis incydentu;
  - 2) datę i godzinę zgłoszenia incydentu;
  - 3) dane identyfikujące osobę zgłaszającą;
  - 4) dane osoby przekazującej informację o incydencie;
  - 5) datę zarejestrowania incydentu;
  - 6) dane identyfikujące osobę rejestrującą incydent;
  - 7) informację o zgromadzonych materiałach dowodowych;
  - 8) informacje dotyczące sposobu postępowania z incydemem.

2. Dyrektor komórki właściwej np. bezpieczeństwa informacji prowadzi analizy i statystyki incydentów.
3. Dyrektor komórki właściwej np. bezpieczeństwa informacji zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

## **§ 7.**

### **Gromadzenie materiału dowodowego**

1. Na każdym etapie postępowania z incydem, dyrektor komórki właściwej np. bezpieczeństwa informacji nadzoruje prawidłowość gromadzenia materiału dowodowego.
2. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.
3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:
  - 1) dla dokumentów papierowych – oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu;
  - 2) dla zapisów utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie (np. poza siedzibą Agencji).
4. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w załączniku nr 1 do niniejszego regulaminu.
5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w załączniku nr 2 do niniejszego regulaminu.
6. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z incydem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, NIE WŁĄCZAJ GO.
3. Jeśli urządzenie jest włączone, NIE próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotuj wszystkie parametry połączeń komputera:
  - 1) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS;
  - 2) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
4. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
5. Następnie ODŁĄCZ WSZYSTKIE KABLE ZEWNĘTRZNE KOMPUTERA. Zanotuj czas odłączenia kabli.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych. ZAPŁOMBUI WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Agencję albo opis jego indywidualnych cech. Wpisz do PROTOKOŁU wykonane czynności (Załącznik nr 2 do Regulaminu zarządzania incydentami).
7. Pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp.).
8. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, taśmy streamera, płyty CD, DVD oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (płyty CD itp.). PAKUJ, NUMERUJ poszczególne paczki, PŁOMBUI I OPISZ W PROTOKOLE. Wpisz do PROTOKOŁU wykonane czynności.
9. Załadaj od użytkownika spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem - okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli użytkownik nie ma spisu oprogramowania, to załadaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokołu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.
10. Załadaj od użytkownika przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych (np. FK). Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Załadaj od użytkowników i administratora podania parametrów dostępu do BIOS-u, systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejęcia parametrów dostępu do protokołu.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.

**Uwagi końcowe:**

- 1) Sprawdź przed odesłaniem zgodność numerów zabezpieczonych materiałów i dowodów z treścią protokołu (zwróć uwagę na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach),
- 2) Skontaktuj się z odpowiednią komórką organizacyjną Agencji w celu zorganizowania przewozu i badań zabezpieczonych materiałów.

**PAMIĘTAJ:**

**NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA ANI ZAWARTOŚCI NOŚNIKÓW  
DANYCH.**

**KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA  
WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE  
INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.**

## PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>

Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>

Świadek 3: <imię i nazwisko, niezależny ekspert>

### I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu: .....	
Dokument elektroniczny	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu: .....	
Kopia zapasowa	<input type="checkbox"/>	System operacyjny <input type="checkbox"/> Nazwa i wersja systemu: .....	Aplikacja <input type="checkbox"/> Nazwa i wersja aplikacji: .....
		Baza danych <input type="checkbox"/> Nazwa i wersja bazy: .....	Oznaczenie nośnika .....
Obraz dysku	<input type="checkbox"/>	Lokalizacja dysku (adres IP/IPX): ..... Typ i nr seryjny dysku: .....	
Pliki konfiguracyjne i/lub systemowe	<input type="checkbox"/>	System operacyjny <input type="checkbox"/> Nazwa i wersja systemu: .....	Aplikacja <input type="checkbox"/> Nazwa i wersja aplikacji: .....
		Baza danych <input type="checkbox"/> Nazwa i wersja bazy: .....	Nazwa(y) Pliku(ów) ..... .....
Kopie zawartości dzienników (logów) zdarzeń .....	<input type="checkbox"/>	System operacyjny <input type="checkbox"/> Nazwa i wersja systemu: .....	Aplikacja <input type="checkbox"/> Nazwa i wersja aplikacji: .....
		Baza danych <input type="checkbox"/> Nazwa i wersja bazy: .....	Nazwa(y) Pliku(ów) ..... .....
Kopia zawartości skrzynki pocztowej	<input type="checkbox"/>	zewnętrzna <input type="checkbox"/>	wewnętrzna <input type="checkbox"/>
		Nazwa skrzynki pocztowej: .....	Za okres od: .....

## II. Opis czynności

*(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))*

## III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:

„....., Egzemplarz nr 1”

„....., Egzemplarz nr 2”

*(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)*

## IV. Zabezpieczenie materiału dowodowego

*(opisać sposób zabezpieczenia jednego z egzemplarzy)*

.....  
.....  
.....

Protokół sporządził: .....

Podpisano:

Świadek 1	.....
Świadek 2	.....
Świadek 3	.....

## DANE OSOBY ZGŁASZAJĄCEJ

Nr telefonu ..... e-mail .....

[illegible]

Podpis osoby zgłaszającej .....

**B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU**

(wypełnia osoba rozpatrująca zgłoszenie incydentu)

DANE OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU - ADMINISTRATOR SYSTEMU/ ADMINISTRATOR  
ZABEZPIECZEŃ FIZYCZNYCH/ IBI

Imię i nazwisko..... Stanowisko .....

Adres .....

Nr telefonu ..... e-mail .....

**INFORMACJE O INCYDENCIE**

Data i czas zajścia incydentu .....

Data i czas wykrycia incydentu .....

Data i czas zgłoszenia incydentu .....

Czy incydent jest zakończony?                      TAK                      ☐                      NIE                      ☐

Jeśli tak, to jak długo trwał (dni/godziny/minuty)? .....

Jeśli nie, należy określić jak długo już trwa? .....

Kogo powiadomiono z KIEROWNICTWA? .....

**OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO**

.....

.....

.....

.....

.....

.....

Załączniki (materiał dowodowy):

1. ....
2. ....
3. ....

**OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA**

.....

.....

.....

.....

.....

Imię i Nazwisko .....

Data .....

Podpis .....

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE INCYDENTU  
(wypełnia osoba prowadząca postępowanie wyjaśniające – IBI w Centrali/OR)

Data rozpoczęcia postępowania ws. incydentu .....

Data zakończenia incydentu (jeśli jest zakończony) .....

Data zamknięcia skutków incydentu .....

Data zakończenia postępowania ws. incydentu .....

Data przedstawienia incydentu na KSBI .....

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU  
(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

.....

.....

.....

.....

.....

.....

WNIOSKI I REKOMENDACJE  
(w tym zalecenia dotyczące zmian w SZBI)

.....

.....

.....

.....

.....

.....

.....

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

.....

.....

.....

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko .....	Imię i Nazwisko .....
Stanowisko .....	Stanowisko .....
Data .....	Data .....
Podpis .....	Podpis .....

## **I. Cel Procedury i osoby odpowiedzialne za realizację określonych zadań**

1. Celem Procedury jest opracowanie i wdrożenie w Agencji jednolitych zasad postępowania w przypadku naruszenia ochrony danych osobowych, tj. zasad oceny, ewidencji i notyfikacji naruszeń ochrony danych osobowych, spełniających wymogi RODO.
2. Każdy pracownik, stażysta, wolontariusz, praktykant, osoba realizująca zadania na podstawie umowy cywilnoprawnej oraz pracownicy Podmiotu zewnętrznego, którzy stwierdzili lub podejrzewają wystąpienie zdarzenia, które stanowi naruszenie ochrony danych osobowych, mają obowiązek zgłoszenia tego faktu na zasadach określonych w niniejszej Procedurze.
3. Jeśli niniejsza Procedura nie stanowi inaczej, zadania opisane w jej treści realizuje w imieniu Administratora wyznaczony pracownik lub Inspektor Ochrony Danych oraz Administrator Systemu.

## **II. Zasady ogólne**

1. Sposób postępowania w przypadku naruszenia ochrony danych osobowych, określony i wprowadzony niniejszą Procedurą obejmuje dwa etapy, tj.:
  - 1) ustalenie, czy zgłoszone zdarzenie wypełnia znamiona naruszenia oraz w jaki sposób zidentyfikowane zdarzenie wpłynie na ryzyko dla praw i wolności osób fizycznych;
  - 2) zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych) oraz poinformowanie osoby, której dane dotyczą, w przypadku, gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.
2. Administrator zapewnia, że podmioty przetwarzające dane na zlecenie Administratora zobowiązały się do informowania Administratora o naruszeniach dotyczących powierzonych im do przetwarzania danych osobowych, a także zobowiązały się do współpracy przy wyjaśnianiu okoliczności naruszenia, w szczególności do udzielania na żądanie Administratora wszelkich informacji dotyczących naruszenia.

## **III. Definicja naruszenia ochrony danych osobowych**

1. Naruszenie ochrony danych osobowych oznacza:
  - 1) 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;
  - 2) utratę atrybutów bezpieczeństwa informacji, tj. poufności, integralności, dostępności oraz rozliczalności. Takie sytuacje są często skutkiem błędu ludzkiego (np. błędne zaadresowanie korespondencji), nieprawidłowego działania urządzenia (np. automatyczne, przedwcześnie wykasowanie części bazy danych), zdarzenia losowego (takiego jak pożar), a tylko w skrajnych przypadkach – rażącego niedbalstwa lub umyślnego działania (np. kradzież bazy danych).
2. Stwierdzone naruszenie ochrony danych osobowych może zostać zakwalifikowane jako:
  - 1) naruszenie dotyczące poufności danych – polega ono na nieuprawnionym lub przypadkowym ujawnieniu lub dostępie do danych osobowych;

- 2) naruszenie dotyczące integralności danych – polega ono na nieuprawnionym lub przypadkowym zmodyfikowaniu danych osobowych (zmianie treści danych);
  - 3) naruszenie dotyczące dostępności danych – polega ono na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych.
3. W zależności od okoliczności zdarzenia dane naruszenie może zostać zakwalifikowane do więcej niż jednej ze wskazanych w ust. 2 kategorii naruszeń ochrony danych osobowych.
4. Naruszeniem zasad ochrony danych osobowych jest w szczególności:
- 1) nieuprawnione zniszczenie danych osobowych – sytuacja, w której dane osobowe przestają istnieć (np. skasowanie) lub przestają istnieć w formie nadającej się do użytku przez Administratora;
  - 2) utrata danych osobowych – sytuacja, w której Administrator utracił kontrolę nad danymi lub dostęp do nich, lub nie jest już w ich posiadaniu (np. kradzież laptopa służbowego lub zgubienie dysku przenośnego);
  - 3) nieuprawnione zmodyfikowanie danych osobowych (np. nadpisanie, pomieszenie);
  - 4) nieuprawnione ujawnienie danych osobowych (np. przesłanie na błędny adres);
  - 5) nieuprawnione uzyskanie dostępu do danych osobowych (np. kradzież bazy danych).
5. O wystąpieniu naruszenia ochrony danych osobowych mogą świadczyć w szczególności następujące sytuacje, które wymagają wyjaśnienia, tj.:
- 1) uszkodzenia fizyczne nieznanego pochodzenia stacji roboczych, drzwi, zamków, skrytek;
  - 2) niestandardowe komunikaty wyświetlane na ekranie urządzeń;
  - 3) znaczne spowolnienie działania systemu informatycznego;
  - 4) błędy w funkcjonowaniu systemu informatycznego (brak możliwości logowania, niedostępność funkcji, modułów lub aplikacji systemowych);
  - 5) przedłużający się brak możliwości odnalezienia określonych dokumentów, nośników danych lub urządzeń służących do przetwarzania danych (np. komputera, telefonu).

#### **IV. Postępowanie w przypadku wystąpienia naruszenia ochrony danych osobowych**

1. Każdy pracownik, stażysta, wolontariusz, praktykant, osoba realizująca zadania na podstawie umowy cywilnoprawnej oraz pracownik Podmiotu zewnętrznego jest zobowiązany do niezwłocznego zgłaszania bezpośrednio przełożonemu lub bezpośrednio Inspektorowi Ochrony Danych, każdego zdarzenia, które może stanowić naruszenie ochrony danych osobowych. W przypadku, gdy zgłoszenie dotyczy systemu teleinformatycznego, informację w tym zakresie należy również przekazać Administratorowi Systemu. Jeśli natychmiastowe zgłoszenie nie jest możliwe, pracownik powinien podjąć działania zmierzające do zgłoszenia naruszenia w terminie nie dłuższym niż 4 godziny od czasu zidentyfikowania sytuacji mogącej wypełniać znamiona naruszenia.
2. Zgłoszenie, o którym mowa w ust. 1 winno być sporządzone według wzoru, który stanowi załącznik nr 1 do niniejszej Procedury. Zgłoszenie winno być dokonane w formie pisemnej oraz przekazane na adres: [iod@arimr.gov.pl](mailto:iod@arimr.gov.pl). Do zgłoszenia należy załączyć sporządzoną wagę naruszenia za pomocą kalkulatora wagi (opracowanego na podstawie wzoru zamieszczonego na portalu wewnętrznym ARiMR przez Inspektora Ochrony Danych), notatkę zawierającą wyjaśnienia osoby powodującej naruszenie (osoby, która swoim działaniem lub zaniechaniem przyczyniła się do naruszenia ochrony danych osobowych) oraz opisującą szczegółowo

zdarzenie ze wskazaniem zabezpieczonych materiałów, dokumentów lub innych dokumentów związanych ze zdarzeniem (o ile dotyczy). Do zgłoszenia należy również dołączyć wszelkie dokumenty, o których mowa w zdaniu poprzednim. W przypadku, gdy naruszenie będzie podlegało zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych (PUODO), pracownik prowadzący postępowanie wyjaśniające zobowiązany jest do przesłania do Inspektora Ochrony Danych wypełnionego zgłoszenia do PUODO wg wzoru zamieszczonego na stronie internetowej PUODO, w terminie uzgodnionym z Inspektorem Ochrony Danych.

3. W przypadku, gdy waga naruszenia wyliczona w oparciu o kalkulator, o którym mowa w pkt 2, zostanie określona na poziomie co najmniej średnim, wówczas w Rejestrze Incydentów Bezpieczeństwa Informacji należy zakwalifikować zdarzenie jako incydent co najmniej średniej kategorii.
4. Dyrektor komórki organizacyjnej w Centrali albo wyznaczony przez niego pracownik oraz Dyrektor Oddziału Regionalnego za pośrednictwem Inspektora Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w każdej zgłoszonej sytuacji, w której naruszenia ochrony danych nie można wykluczyć. Postępowanie wyjaśniające powinno być wszczęte niezwłocznie po otrzymaniu zgłoszenia.
5. Celem postępowania wyjaśniającego jest zebranie informacji, w tym materiałów i dokumentów niezbędnych do ustalenia wszystkich okoliczności zdarzenia, jego przyczyn i możliwych skutków, określenie na ich podstawie czy doszło do naruszenia (stwierdzenie naruszenia) oraz wypełnienie Rejestru naruszeń ochrony danych osobowych (po stwierdzeniu, że naruszenie ochrony danych osobowych miało miejsce). Stwierdzenie naruszenia następuje w chwili, gdy na podstawie zebranych informacji można racjonalnie przyjąć, że do naruszenia doszło lub z dużym prawdopodobieństwem doszło (gdy Administrator ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych).
6. W celu zebrania potrzebnych informacji osoba prowadząca postępowanie wyjaśniające, może kontaktować się z pracownikami i osobami trzecimi, żądać od nich wyjaśnień, uzyskiwać dostęp do dokumentów, pomieszczeń, urządzeń i schowków.
7. Na podstawie informacji uzyskanych w toku postępowania wyjaśniającego osoba prowadząca postępowanie wyjaśniające przeprowadza ocenę wagi naruszenia, na podstawie kalkulatora wagi naruszenia, udostępnionego na portalu wewnętrznym ARiMR, w zakładce ochrona danych osobowych – „Wytyczne”, w wyniku której ustala:
  - 1) czy jest prawdopodobne, że stwierdzone naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych;
  - 2) czy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
8. Przy przeprowadzaniu oceny, o której mowa w ust. 7, brane są pod uwagę okoliczności naruszenia, w tym jego ciężar, skala i możliwy negatywny wpływ na sytuację podmiotów danych, a także prawdopodobieństwo nastąpienia tego negatywnego wpływu. W szczególności uwzględnia się:
  - 1) rodzaj naruszenia, tj. czy doszło do nieuprawnionego ujawnienia, utraty, zniszczenia, zmodyfikowania, czy nieuprawnionego uzyskania dostępu – wpływa głównie na ocenę rodzajów możliwych negatywnych konsekwencji naruszenia;
  - 2) rodzaj, poziom wrażliwości i skalę danych, których dotyczy naruszenie, w szczególności czy naruszenie dotyczy danych szczególnych kategorii – wpływa głównie na ocenę możliwych negatywnych konsekwencji naruszenia;
  - 3) czy dane można łatwo powiązać z osobą fizyczną (tj. czy dane osobowe objęte naruszeniem pozwalają na identyfikację osób, czy inne dane osobowe tych osób są

publicznie dostępne, czy łatwo można dokonać połączenia danych osobowych objętych naruszeniem z innymi danymi osobowymi publicznie dostępnymi) – wpływa głównie na ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych;

- 4) wagę potencjalnych konsekwencji dla podmiotów danych;
  - 5) specjalne cechy podmiotów danych – wpływa głównie na ocenę możliwych negatywnych konsekwencji naruszenia;
  - 6) liczbę podmiotów danych, których dotyczy naruszenie – wpływa głównie na ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.
9. Przyjmuje się, że zachodzi wysokie prawdopodobieństwo naruszenia praw lub wolności osób, których dane osobowe dotyczą, jeżeli naruszenie dotyczy:
- 1) danych osobowych szczególnych kategorii lub informacji o ukaraniu lub zastosowanych środkach karnych;
  - 2) danych osobowych umożliwiających kradzież tożsamości, tj. co najmniej:
    - a) imię i nazwisko, PESEL;
    - b) imię i nazwisko, adres zamieszkania, numer telefonu oraz adres e-mail;
    - c) loginów oraz haseł, niezależnie od tego, do jakich zasobów;
  - 3) szerokiego zakresu danych.
10. Po przeprowadzeniu oceny wagi naruszenia oraz przygotowaniu zgłoszenia zgodnie z załącznikiem nr 1 do przedmiotowej Procedury, osoba prowadząca postępowanie wyjaśniające przekazuje niezwłocznie, nie później niż 24 godziny od zaistnienia zdarzenia sporządzone dokumenty, podpisane przez Dyrektora komórki organizacyjnej w Centrali/OR wraz z notatką osoby powodującej naruszenie do Inspektora Ochrony Danych. Wraz ze zgłoszeniem należy przekazać zabezpieczone materiały, dokumenty lub inne dokumenty związane z naruszeniem (o ile dotyczy).
11. Inspektor Ochrony Danych po otrzymaniu podpisanej przez Dyrektora komórki organizacyjnej w Centrali/OR dokumentacji dotyczącej naruszenia ochrony danych osobowych dokonuje analizy zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do przekazania informacji oraz opinii w wyznaczonym przez Inspektora Ochrony Danych terminie.
12. W wyniku analizy Inspektor Ochrony Danych stwierdza czy jest prawdopodobne, że zdarzenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
13. W przypadku stwierdzenia ryzyka naruszenia praw i wolności osób fizycznych Inspektor Ochrony Danych informuje o tym Prezesa ARiMR.
14. Inspektor Ochrony Danych odpowiada za przygotowanie zgłoszenia stwierdzonego naruszenia ochrony danych osobowych, w oparciu o projekt zgłoszenia przesłany przez pracownika prowadzącego postępowanie wyjaśniające, w którym wystąpiło ryzyko naruszania praw i wolności osób fizycznych, do organu nadzorczego (Prezesa Urzędu Ochrony Danych Osobowych).
15. Zgłoszenie dokonywane jest zgodnie z wymogami określonymi w art. 33 RODO. Zgłoszenia dokonuje się przez dedykowane kanały komunikacji dostarczone przez PUODO. Zgłoszenia należy dokonać niezwłocznie, nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. Jeśli przekazanie kompletu informacji nie jest możliwe w tym czasie, należy przesłać część informacji, wskazując jednocześnie rodzaj informacji, które zostaną uzupełnione, i termin tego

uzupełnienia. W przypadku uchybienia terminowi należy dokonać zgłoszenia, wyjaśniając powody niedotrzymania terminu.

16. Poinformowanie osób, których dane dotyczą powinno nastąpić niezwłocznie po zaistniałym naruszeniu. Zawiadomienie należy przygotować jasnym i prostym językiem. Zawiadomienie winno spełniać wymogi art. 34 RODO. W każdym przypadku projekt zawiadomienia podlega konsultacji z Inspektorem Ochrony Danych. Jeśli wyczerpujące określenie podmiotów danych, których dotyczy naruszenie, nie jest możliwe, Administrator zamieszcza informację na swojej stronie internetowej lub przekazuje ją w inny sposób, który maksymalizuje szansę dotarcia informacji do odpowiednich podmiotów danych.
17. Inspektor Ochrony Danych pełni nadzór nad właściwym dokonaniem procesu poinformowania przez odpowiednie jednostki, komórki organizacyjne Agencji osób, których naruszenia danych osobowych dotyczy naruszenie.
18. Wszelkie czynności podejmowane w ramach postępowania wyjaśniającego winny być dokumentowane, np. w postaci notatki służbowej. Notatki oraz materiały i dokumenty zgromadzone w ramach prowadzonego postępowania wyjaśniającego są przechowywane przez czas niezbędny do wyjaśnienia okoliczności naruszenia, co obejmuje także ewentualne czynności podejmowane przez organ nadzorczy (Prezesa Urzędu Ochrony Danych Osobowych) lub sąd (do czasu ostatecznych rozstrzygnięć), a następnie jeszcze przez okres przewidziany w przepisach o archiwizacji.
19. Po zakończeniu badania naruszenia Administrator zobowiązany jest do niezwłocznego:
  - 1) zastosowania środków bezpieczeństwa w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia;
  - 2) zastosowania środków bezpieczeństwa w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą.
20. Kierownik komórki lub jednostki organizacyjnej, w której naruszenie miało miejsce, informuje Inspektora Ochrony Danych o podjętych czynnościach, o których mowa w ust. 19, i przekazuje potwierdzenie ich dokonania.
21. Inspektor Ochrony Danych w razie potrzeby rekomenduje zastosowanie innych lub dodatkowych środków ochrony przetwarzanych danych osobowych.
22. Inspektor Ochrony Danych przedstawia dwa razy w roku informacje o naruszeniach ochrony danych osobowych Komitetowi Sterowania Bezpieczeństwem Informacji.

## **V. Rejestr naruszeń ochrony danych osobowych**

1. Inspektor Ochrony Danych Osobowych prowadzi Rejestr naruszeń ochrony danych osobowych w formie elektronicznej.
2. Każdy przypadek naruszenia ochrony danych osobowych powinien zostać wpisany również do Rejestru Incydentów Bezpieczeństwa Informacji, prowadzonego przez Dyrektora komórki właściwej ds. bezpieczeństwa informacji i opisany zgodnie z systematyką tego rejestru. Wpisu naruszenia do rejestru dokonuje Inspektor Bezpieczeństwa Informacji.
3. Informacje zamieszczone w rejestrach wskazanych w ust. 1 i 2 mogą zostać udostępnione organowi nadzorczemu na jego żądanie.
4. Nie rzadziej niż jeden raz w roku Dyrektor komórki właściwej ds. bezpieczeństwa informacji dokonuje analizy wpisów w Rejestrze Incydentów Bezpieczeństwa Informacji w celu:

- 1) oceny skuteczności środków technicznych i organizacyjnych zabezpieczenia danych osobowych;
- 2) zidentyfikowania powtarzających się naruszeń;
- 3) zaplanowania, w zależności od wyników oceny, działań zmierzających do poprawy środków organizacyjnych i technicznych zabezpieczenia danych osobowych.

LP.	PYTANIE	ODPOWIEDŹ
<b>Oznaczenie podmiotu zgłaszającego naruszenie i osoby kontaktowej</b>		
1.	Nazwa jednostki/ komórki organizacyjnej ARiMR zgłaszającej naruszenie (np. OR 12; Centrala DB)	
2.	Imię, nazwisko, adres e-mail, numer telefonu, stanowisko służbowe osoby kontaktowej po stronie zgłaszającego naruszenie)	
<b>Opis naruszenia</b>		
3.	Nazwa i rola podmiotu, u którego doszło do naruszenia – administrator danych / procesor (należy wskazać rolę)	
4.	Opis naruszenia (należy podać możliwie jak najbardziej szczegółowy opis naruszenia i jego okoliczności)	
5.	Data wykrycia naruszenia oraz czas, przez jaki naruszenie miało miejsce, o ile naruszenie miało charakter ciągły	
6.	W jaki sposób dowiedziano się o naruszeniu?	
7.	Jeśli od stwierdzenia naruszenia do zgłoszenia upłynęło więcej niż 24 godziny, należy opisać powody opóźnienia w raportowaniu	
8.	Jakie są prawdopodobne przyczyny naruszenia?	
9.	Jakie są potencjalne konsekwencje i niekorzystne skutki dla osób, których naruszenie dotyczy?	

LP.	PYTANIE	ODPOWIEDŹ
<b>Zakres danych objętych naruszeniem</b>		
10.	Jakich kategorii osób dotyczy naruszenie? (np. beneficjentów ARiMR, pracowników ARiMR, pracowników Podmiotów zewnętrznych, z którymi współpracuje ARiMR)	
11.	Ilu (w przybliżeniu) osób dotknęło naruszenie?	
12.	Jakich danych osobowych dotyczyło naruszenie? (należy wskazać możliwie szczegółowo przynajmniej kategorie danych np. imię i nazwisko, numer PESEL, adres zamieszkania, jeśli naruszenie dotyczyło danych szczególnych kategorii np. dane o stanie zdrowia, przynależność do związków zawodowych, lub danych o karalności, należy ten fakt wskazać,	
13.	Jaka jest skala naruszenia?  (należy wskazać, ilu w przybliżeniu wpisów danych / rekordów dotyczy naruszenie)	
<b>Opis podjętych i planowanych działań</b>		
15.	Jakie kroki podjął lub zamierza podjąć Administrator w celu minimalizacji niekorzystnych skutków naruszenia dla osób, których ono dotknęło?	
16.	Jakie kroki podjął lub zamierza podjąć Administrator, aby zapobiec analogicznym do naruszenia zdarzeniom w przyszłości?	