

ZARZĄDZENIE NR 14/2025
DYREKTORA SUWALSKIEGO OŚRODKA KULTURY
z dnia 15 września 2025 r.

**w sprawie wprowadzenia Procedury reagowania na naruszenia ochrony
danych osobowych w Suwalskim Ośrodku Kultury**

Na podstawie § 3 ust.5 pkt 3 Regulaminu Organizacyjnego Suwalskiego Ośrodka Kultury, ustawy z dnia 25 października 1991r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz.U. z 2024 r.poz. 87 ti.) oraz na podstawie 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, dalej:RODO) (Dz.Urz.UE.L Nr 119 str. 1) , zarządzam co następuje:

§ 1.

Wprowadzam Procedurę reagowania na naruszenia ochrony danych w Suwalskim Ośrodku Kultury.

§ 2.

Wykonanie Zarządzenia powierzam Zastępcy Dyrektora Suwalskiego Ośrodka Kultury oraz kierownikom komórek organizacyjnych Suwalskiego Ośrodka Kultury.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor Suwalskiego
Ośrodka Kultury

Ignacy Ołów

Załącznik do zarządzenia nr 14/2025
Dyrektora Suwalskiego Ośrodka Kultury
z dnia 15 września 2025 r.

Procedura reagowania na naruszenia ochrony danych osobowych w Suwalskim
Ośrodku Kultury

Wersja	1
Właściciel	Suwalski Ośrodek Kultury
Data zatwierdzenia	15.09.2025 r.
Data wejścia w życie	15.09.2025 r.
Zatwierdzający	

SPIS TREŚCI

§ 1.	
DEFINICJE.....	3
§ 2.	
CEL I ZAKRES PROCEDURY.....	4
§ 3.	
POSTĘPOWANIE I ODPOWIEDZIALNOŚĆ PRACOWNIKÓW ORAZ WSPÓŁPRACOWNIKÓW.....	4
§ 4.	
POSTĘPOWANIE Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH.....	5
§ 5.	
REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH.....	6
§ 6.	
ZAWIADOMIENIE OSÓB, KTÓRYCH DANE OSOBOWE PODLEGAŁY NARUSZENIU.....	7
§ 7.	
NARUSZENIE OCHRONY DANYCH OSOBOWYCH PRZEZ PODMIOT PRZETWARZAJĄCY.....	7
§ 8.	
POSTANOWIENIA KOŃCOWE.....	7

§ 1.

DEFINICJE Przyjmuje się, że określenia użyte w Procedurze reagowania na naruszenia ochrony danych należy rozumieć w następujący sposób:

1. **Administrator (ADO)** - Suwalski Ośrodek Kultury z siedzibą w Suwałkach;

2. **Dane osobowe (Dane)** - 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. **Inspektor Ochrony Danych Osobowych** - osoba, wyznaczona przez Administratora do monitorowania tematów związanych z ochroną Danych osobowych i zarządzania nimi;

4. **Naruszenie ochrony Danych osobowych (Naruszenie)** - 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** — osoby zatrudnione przez Administratora w oparciu o umowę o pracę;

6. **Współpracownik** - osoby fizyczne wykonujące na rzecz Administratora usługi na innej podstawie niż stosunek pracy oraz osoby fizyczne wykonujące na rzecz Administratora usługi prowadzące na własny rachunek działalność gospodarczą;

7. **Procedura** — niniejsza Procedura reagowania na naruszenia ochrony Danych;

8. **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;

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

10. **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);

11. **Rejestr** - rejestr Naruszeń ochrony Danych osobowych prowadzony przez Administratora.

§ 2.

CEL

I ZAKRES

PROCEDURY

Celem Procedury jest określenie zasad reagowania na Naruszenia ochrony Danych osobowych, obejmujących ich identyfikację, rejestrowanie, analizę oraz podejmowanie dalszych działań zaradczych.

§ 3.

POSTĘPOWANIE I ODPOWIEDZIALNOŚĆ PRACOWNIKÓW ORAZ WSPÓŁPRACOWNIKÓW

1. Przed przystąpieniem do pracy lub świadczenia usług, Pracownik lub Współpracownik dokonuje sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy lub świadczenia usług. Pracownicy oraz Współpracownicy zwracają szczególną uwagę, czy nie zaszły okoliczności wskazujące na Naruszenie lub próbę Naruszenia ochrony Danych osobowych.

2. Za okoliczności, które mogą wskazywać na wystąpienie Naruszenia ochrony Danych osobowych, uważa się w szczególności poniżej wskazane zdarzenia, które mogą prowadzić do nieuprawnionego zniszczenia, utracenia, zmodyfikowania, czy ujawnienia Danych osobowych nieuprawnionym osobom, tj.:

- 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 lub ujawnienie dokumentów zawierających Dane osobowe osobie nieuprawnionej, 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 oraz Współpracownik zobowiązany jest do natychmiastowego ustnego poinformowania o tym fakcie Administratora lub Inspektora Ochrony Danych Osobowych, a następnie przesłania zgłoszenia w formie wiadomości e-mail na adres: olszewska.kancelaria@gmail.com lub sok@soksuwalki.eu

4. Zgłoszenie, o którym mowa w ust. 3 powyżej, powinno zawierać wszystkie informacje znane osobie dokonującej zgłoszenia, w tym:

- 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.

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

6. Do czasu stwierdzenia Naruszenia ochrony Danych osobowych bądź jego braku, Pracownik lub Współpracownik, który dokonał zgłoszenia:

- 1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy lub świadczenia usług, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów Naruszenia bądź innych dowodów;
- 2) zabezpiecza elementy systemu informatycznego lub dokumentacji, 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 osobowych.

§ 4.

POSTĘPOWANIE Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

1. Inspektor Ochrony Danych Osobowych 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 incydem;
- 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, Inspektor Ochrony Danych Osobowych , zabezpiecza materiał dowodowy mogący wskazać sprawców oraz sposób w jaki powstał incydent. Zabezpieczenie materiału dowodowego może być realizowane przykładowo przez:

- a) wykonanie kopii nośników Danych;
- b) zabezpieczenie logów z urządzeń sieciowych, serwerów, itp.;
- c) odłączenie urządzeń od sieci.

3. Kwalifikacji zgłoszenia w imieniu Administratora dokonuje Inspektor Ochrony Danych Osobowych na podstawie opracowanego formularza Excel. Inspektor Ochrony Danych Osobowych rekomenduje Administratorowi jedno z 3 rozwiązań lub kilka łącznie:

- a) odnotowanie naruszenia w Rejestrze;
- b) zgłoszenie do UODO;
- c) zawiadomienie podmiotów Danych — w zależności od stwierdzonego poziomu naruszenia praw lub wolności osób, których Dane zostały objęte Naruszeniem.

4. W przypadku zakwalifikowania zgłoszenia jako Naruszenia ochrony Danych osobowych, Inspektor Ochrony Danych Osobowych 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 Inspektor Ochrony Danych Osobowych 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 udokumentowania okoliczności oraz przyczyn odstąpienia od zgłoszenia Naruszenia do organu nadzorczego.

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 OD, jeżeli został wyznaczony lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- 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.

§ 5.

1. Administrator prowadzi we współpracy z Inspektorem Ochrony Danych Osobowych Rejestr wszelkich zidentyfikowanych Naruszeń ochrony Danych osobowych, a więc również tych które nie podlegają zgłoszeniu organowi nadzorcemu, ani nie wymagają powiadomienia osób, których Dane dotyczą.

2. Rejestr zawiera:

- 1) datę stwierdzenia Naruszenia,

- 2) sposób stwierdzenia Naruszenia (w tym źródło pozyskania informacji o wystąpieniu Naruszenia),
- 3) datę rozpoczęcia oraz zakończenia Naruszenia,
- 4) charakter Naruszenia (Naruszenie poufności / integralności / dostępności Danych);
- 5) opis Naruszenia, w tym okoliczności Naruszenia,
- 6) przyczynę Naruszenia,
- 7) kategorię Danych, których dotyczy Naruszenie,
- 8) kategorię osób, których Dane zostały objęte Naruszeniem,
- 9) liczbę osób, których mogło dotyczyć Naruszenie,
- 10) opis możliwych skutków Naruszenia,
- 11) ocenę poziomu ryzyka naruszenia praw lub wolności osób fizycznych,
- 12) opis zastosowanych środków zaradczych w celu minimalizacji zdarzenia,
- 13) środki zastosowane w celu uniknięcia Naruszenia w przyszłości,
- 14) informacja o zawiadomieniu UODO lub przyczyny uzasadniające odstępianie od dokonania zawiadomienia,
- 15) informacja o powiadomieniu osoby, której Dane dotyczą lub przyczyny uzasadniające odstępianie od powiadomienia osób, których Dane dotyczą.

§ 6.

ZAWIADOMIENIE OSÓB, KTÓRYCH DANE OSOBOWE PODLEGAŁY NARUSZENIU

1. 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.

2. Zawiadomienie, o którym mowa w ust. 1 powyżej, jasnym i prostym językiem opisuje charakter Naruszenia ochrony Danych osobowych oraz zawiera przynajmniej informacje i środki o których mowa w § 4 ust. 7 powyżej.

3. Zawiadomienie, o którym mowa w ust. 1 powyżej nie jest wymagane w przypadku, gdy:

- a) Administrator wdrożył odpowiednie środki techniczne i organizacyjne 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.

§ 7.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH PRZEZ PODMIOT PRZETWARZAJĄCY

1. W przypadku stwierdzenia Naruszenia ochrony Danych osobowych przez Podmiot przetwarzający, Podmiot przetwarzający zgłasza je bez zbędnej zwłoki Administratorowi, który następnie przekazuje je Inspektorowi Ochrony Danych Osobowych. Administrator podpisując umowę powierzenia z Podmiotem przetwarzającym zobowiązany jest dopilnować, aby taki obowiązek był nałożony na Podmiot przetwarzający.

§ 8.

POSTANOWIENIA KOŃCOWE

1. Każdy Pracownik oraz Współpracownik ma obowiązek zapoznania się z Procedurą oraz stosowania jej postanowień.

2. Procedura wchodzi w życie w dniu jej zatwierdzenia przez Administratora. Procedura podlega cyklicznej weryfikacji pod kątem aktualności oraz zgodności z regulacjami prawnymi i dobrymi praktykami.

3. Procedura nie narusza obowiązujących u Administratora odrębnych procedur, polityk, instrukcji lub innych dokumentów regulujących kwestie związane z ochroną Danych osobowych oraz stanowi element zasad ochrony Danych osobowych u Administratora.

do Procedury reagowania na naruszenia ochrony danych w Suwalskim Ośrodku Kultury, wprowadzonej Zarządzeniem Dyrektora Suwalskiego Ośrodka Kultury nr 14/2025 z dnia 15 września 2025 r.

Zgłoszenie Naruszenia ochrony Danych osobowych w Suwalskim Ośrodku Kultury Prezesowi Urzędu Ochrony Danych Osobowych

1	Kategoria naruszenia	
2	Kategoria danych osobowych, których dotyczy naruszenie	
3	Przybliżona liczba osób których dane dotyczą	
4	Imię nazwisko oraz dane kontaktowe IOD	
5	Opis możliwych konsekwencji Naruszenia ochrony Danych osobowych	
6	Opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia Naruszeniu ochrony Danych osobowych, w tym środków w celu zminimalizowania ewentualnych negatywnych skutków Naruszenia.	

do Procedury reagowania na naruszenia ochrony danych w Suwalskim Ośrodku Kultury, wprowadzonej Zarządzeniem Dyrektora Suwalskiego Ośrodka Kultury nr 14/2025 z dnia 15 września 2025 r. REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH w Suwalskim Ośrodku Kultury

L.p.	Rodzaj danych w rejestrze		Dane udokumentowane w rejestrze na podstawie materiału zgromadzonego w toku postępowania wyjaśniającego zgłoszenie naruszenia danych osobowych
1.	Data stwierdzonego naruszenia		
2.	Sposób stwierdzenia Naruszenia (w tym źródło pozyskania informacji o wystąpieniu Naruszenia)		
3.	Data	rozpoczęcia naruszenia	
		zakończenia naruszenia	
4.	Charakter naruszenia	naruszenie poufności	
		naruszenie integralności	
		naruszenie dostępności	
5.	Opis Naruszenia, w tym okoliczności Naruszenia		
6.	Kategoria osób, których Dane zostały objęte Naruszeniem		
7.	Liczbę osób, których mogło dotyczyć Naruszenie		
8.	Opis możliwych skutków Naruszenia		
9.	Ocenę poziomu ryzyka naruszenia praw lub wolności osób fizycznych		
10.	Opis zastosowanych środków zaradczych w celu minimalizacji zdarzenia,		
11.	Środki zastosowane w celu uniknięcia Naruszenia w przyszłości		
12.	Informacja o zawiadomieniu UODO lub przyczyny uzasadniające odstąpienie od dokonania zawiadomienia		
13.	Informacja o powiadomieniu osoby, której Dane dotyczą lub przyczyny uzasadniające odstąpienie od powiadomienia osób, których Dane dotyczą		