Zarządzenie nr 5/2021
Dyrektora Suwalskiego Ośrodka Kultury z dnia 8.02.2021 r.
w sprawie wprowadzenia Polityki bezpieczeństwa informacji
oraz Instrukcji zarządzania systemem informatycznym służącym
do przetwarzania danych osobowych

Na podstawie § 3 ust. 5 pkt 3 regulaminu organizacyjnego Suwalskiego Ośrodka Kultury, ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej (tekst jedn. Dz. U. z 2020r. poz 194 z późn. zm.) oraz na postawie 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) zarządzam, co następuje:

§ 1

1. Wprowadza się „Politykę bezpieczeństwa informacji Suwalskiego Ośrodka Kultury" oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".
2. Polityka bezpieczeństwa Suwalskiego Ośrodka Kultury stanowi załącznik nr 1do niniejszego Zarządzenia.
3. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi załącznik nr 2 do niniejszego Zarządzenia.

§ 2

Polityka bezpieczeństwa określa zbiór zasad obowiązujących przy przetwarzaniu danych osobowych we wszystkich zbiorach administrowanych przez Suwalski Ośrodek Kultury w Suwałkach zgodnie z Rozporządzeniem 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).

§ 3

Wykonanie Zarządzenia powierzam Zastępcy Dyrektora – Ignacemu Ołowiowi oraz Inspektorowi Ochrony Danych – Dorocie Skłodowskiej i zobowiązuję do zapoznania z treścią niniejszego Zarządzenia wraz z załącznikami wszystkich pracowników Suwalskiego Ośrodka Kultury.

§ 4

Traci moc Zarządzenie nr 8/2018 dnia 24 maja 2018 r. Dyrektora Suwalskiego Ośrodka Kultury w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji wraz z załącznikami oraz Instrukcji zarządzania systemem informatycznym Suwalskiego Ośrodka Kultury.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Suwalskiego Ośrodka Kultury
Alicja Astrauskiewicz

Załącznik nr 1 do Zarządzenia nr 5/2021
z dnia 08.02.2021 r.
Dyrektora Suwalskiego Ośrodka Kultury

Polityka bezpieczeństwa informacji Suwalskiego Ośrodka Kultury

Ewidencja zasobów

1. Wyjaśnienie używanych pojęć:
a) dane osobowe – wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
b) baza danych osobowych – każdy zbiór danych o charakterze osobowym,
c) Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, a zwłaszcza te, które wykonuje się w systemach informatycznych,
d) Inspektor Ochrony Danych – osoba monitorująca przestrzeganie bezpieczeństwa przetwarzania danych osobowych,
e) bezpieczeństwo systemu informatycznego – wdrożenie przez administratora danych osobowych lub inną osobę przez niego wyznaczoną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed dostępem, modyfikacją, ujawnieniem, pozyskiwaniem lub zniszczeniem,
f) nośniki danych osobowych – dyski twarde komputerów, płyty CD lub DVD, dyski zewnętrzne, pamięć flash, itp.,
g) pracownicy – osoby zatrudnione w Ośrodku na umowę o pracę i/lub współpracownicy.

Rozdział 1

Postanowienia ogólne

1. Polityka bezpieczeństwa informacji w Suwalskim Ośrodku Kultury, zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych, w szczególności w wykazach, listach wycieczek/wyjazdów, uczestników konkursów/ festiwali oraz w innych zbiorach ewidencyjnych zgodnie z Rozporządzeniem 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)
2. Suwalski Ośrodek Kultury zwany dalej „Ośrodkiem" realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby te dane były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z planem pracy Ośrodka, celów,
c) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

3. Dane osobowe w Ośrodku Kultury przetwarzane są w budynkach znajdujących się przy ul. T. Noniewicza 71, Papieża Jana Pawła II 5 oraz Andrzeja Wajdy 3 w Suwałkach.

4. Polityka zawiera:
a) wykaz zbiorów danych osobowych przetwarzanych w Ośrodku wraz z opisami struktury zbiorów i sposobów ich przetwarzania (załącznik nr 1 do Polityki bezpieczeństwa Informacji),
b) wykaz pomieszczeń, w których przetwarzane są dane osobowe w sposób tradycyjny i z użyciem stacjonarnego sprzętu komputerowego (załącznik nr 2 do Polityki bezpieczeństwa informacji),
c) rejestr czynności przetwarzania danych osobowych (załącznik nr 3 do Polityki bezpieczeństwa informacji

Rozdział 2

Opis zagrożeń naruszających ochronę danych osobowych

Rodzaje zagrożeń naruszających ochronę danych osobowych:
1. Zagrożenia losowe:
a) zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu prądu) – ich wystąpienie może prowadzić do utraty danych lub ich zniszczenia lub uszkodzenia,
b) wewnętrzne (np., awarie sprzętowe) – w wyniku ich wystąpienia może dojść do zniszczenia danych.
2.Zagrożenie zamierzone (świadome i celowe naruszenie poufności danych).

Rozdział 3

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności przetwarzanych danych osobowych

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
a) wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz. W ośrodku obowiązują ścisłe procedury dotyczące odbioru i zwrotu kluczy do pomieszczeń. Klucze znajdują się w zamykanej szafie, do której dostęp ma osoba pełniąca dyżur na Informacji. Każda czynność związana z odbiorem i zwrotem kluczy jest rejestrowana. W Galerii Sztuki Stara Łaźnia ponadto klucze znajdują się w szafie z podwójnym zabezpieczeniem elektronicznym, którą można otworzyć wyłącznie za pomocą spersonifikowanej karty magnetycznej z potwierdzeniem indywidualnym kodem. Pobranie i zwrot klucza są odnotowywane przez system. Ponadto wejście do pomieszczeń chronionych również wymaga zastosowania spersonifikowanej karty magnetycznej.
b) w SOK funkcjonuje system alarmowy, który zostaje włączony przez uprawnionego pracownika, który opuszcza Ośrodek jako ostatni (budynek T. Noniewicza 71 oraz Galerii Sztuki Stara Łaźnia), natomiast w budynku przy ul. Papieża Jana Pawła II 5 - nadzór fizyczny przez całą dobę .
2. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
a) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii, odtwarzane są dane i system operacyjny
b) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie gaśnic
3. Organizacyjną ochronę danych osobowych i ich przetwarzania realizuje się poprzez:
   a) zapoznanie każdego pracownika z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem do pracy przy ich przetwarzaniu,

b) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych osobowych oraz form zabezpieczenia pomieszczeń i budynku, sprzętu,
c) upoważnienie osób do przetwarzania danych osobowych (załącznik nr 4 do Polityki bezpieczeństwa informacji),
d) upoważnienie osób do przebywania w obszarze przetwarzania danych osobowych (załącznik nr 5 do Polityki bezpieczeństwa informacji),
e) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik nr 6 do Polityki bezpieczeństwa informacji),
f) prowadzenie ewidencji osób upoważnionych do przebywania w obszarze przetwarzania danych osobowych (załącznik nr 7 do Polityki bezpieczeństwa informacji).

Rozdział 4

Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy 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) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
2. Niniejsza „Polityka bezpieczeństwa" służąca do przetwarzania danych osobowych w Suwalskim Ośrodku Kultury wchodzi w życie z dniem podpisania.

DYREKTOR
Suwalskiego Ośrodka Kultury
Alicja Andrulewicz

Załącznik nr 2 do Zarządzenia nr 5/2021
z dnia 08.02.2021 r.
Dyrektora Suwalskiego Ośrodka Kultury

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Rozdział I

Postanowienia ogólne

1. 1.Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Suwalskim Ośrodku Kultury zwanym dalej „Ośrodkiem".
2. Instrukcja została opracowana zgodnie z Rozporządzeniem 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) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenia Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
3. Dyrektor Ośrodka wykonuje obowiązki administratora danych osobowych i administratora systemów informatycznych, a funkcję Inspektora Ochrony Danych sprawuje wyznaczony pracownik w odniesieniu do prowadzonych w Ośrodku zbiorów danych.
4. W systemach informatycznych służących do przetwarzania danych osobowych w Ośrodku stosuje się środki bezpieczeństwa na poziomie wysokim.

Rozdział II

Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym.

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez Inspektora Ochrony Danych z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Ośrodku wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych.
3. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na przekazaniu dostępu do hasła oraz ustalenia zakresu

dostępnych danych. Inspektor ochrony Danych jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział III

Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Użytkownik uzyskuje dostęp do danych osobowych wyłącznie po podaniu hasła zaraz po włączeniu komputera.
2. Hasło składa się co najmniej z 8 znaków.
3. Hasło powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalnej. (tzw. silne hasło)
4. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy.
5. Hasło należy zmieniać co najmniej raz na miesiąc, zmiany są systemowe lub programowe, przeprowadzane na bieżąco oraz w miarę potrzeby.
6. Użytkownik nie może udostępniać osobom nieuprawnionym hasła dostępu oraz osobom nieuprawnionym dostępu do swojego stanowiska pracy.
7. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło.
8. Hasła do firmowej poczty elektronicznej nie mogą być zapisane na stałe w programie pocztowym komputera.
9. Zabrania się instalowania oprogramowania nieznanego pochodzenia bez zgody administratora.

Rozdział IV

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu

1. Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego lub programu pocztowego.
2. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane. Kończąc pracę użytkownik obowiązany jest wyłączyć sprzęt komputerowy. Monitor z danymi wrażliwymi nie może stać przy oknie, do którego możliwy jest dostęp dla osób postronnych.

Rozdział V

Korzystanie z bankowości internetowej.

1. Do dokonywania operacji związanych z obsługą bankowości internetowej, dostępu do konta Ośrodka i wykonywania jakichkolwiek operacji, upoważnieni są wyłącznie główny księgowy i osoby upoważnione przez Dyrekcję.
2. Zabrania się przechowywania haseł dostępu do konta na biurku, w dokumentacji, razem z osobistym kluczem do konta (token), zapisywania w notatkach, w pamięci komputera na dyskach. Hasła i login należy zapamiętać.

3. Osobisty klucz do konta (token) każda z osób, główny księgowy i inne osoby upoważnione, przechowują w sposób należycie zabezpieczony, zapewniający nieużycie przez osoby trzecie. Po wylogowaniu się z banku, w czasie godzin pracy, token zamykany jest na klucz w kontenerach przy biurkach, a na zakończenie dnia pracy, w szafie pancernej.
4. Główny księgowy wprowadza wszelkie dane, które następnie zatwierdza Dyrektor.
5. Zabrania się korzystania z bankowości internetowej na komputerze, na którym stwierdzono źle działającą ochronę, oprogramowanie lub inne problemy.
6. W czasie wykonywania operacji bankowych, zabrania się odchodzenia od komputera, przyjmowania rozmów telefonicznych i załatwiania innych spraw.

Rozdział VI

Tworzenie kopii zapasowych zbiorów danych.

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie cyklicznie (nie rzadziej niż raz na pół roku) kopii zapasowych.
2. Kopie zapasowe przechowywane są na dysku zewnętrznym w szafie pancernej.
3. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
4. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
5. Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego danych osobowych.

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator danych osobowych.
2. System antywirusowy zainstalowany jest w każdym komputerze, systemy operacyjne mogą zawierać dodatkowe/wewnętrzne programy antywirusowe.
3. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym lub programie pocztowym.
4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora bezpieczeństwa informacji.
6. Aktualizacje systemu/programu antywirusowego przeprowadzane są systemowo, programowo, cyklicznie oraz w razie potrzeby.

Rozdział VIII

Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych.

1. Dane osobowe przetwarzane w Ośrodku mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania na mocy 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) oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek chyba, że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Ośrodkowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Dokładna kopia danych osobowych przesłanych do Zakładu Ubezpieczeń Społecznych przechowywana jest w bazie danych programu "PROGMAN WOLTERS KLUWER." w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia dokumentu, datą wysłania zestawu.
5. Dokładna kopia danych osobowych przesłanych do banku przechowywana jest w bazie danych systemu bankowości elektronicznej do wejścia, której konieczne jest wprowadzenie loginu i hasła.

Rozdział IX

Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych.

1. Wszelkie prace związane z naprawami sprzętu komputerowego wykonywane są przez firmę zatrudnioną na podstawie umowy z klauzulą powierzenia przetwarzania danych osobowych i zachowaniem tajemnicy.
2. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora danych osobowych.

DYREKTOR
Suwalskiego Ośrodka Kultury
Alicja Andrulewicz

Załącznik nr 1 do Polityki bezpieczeństwa informacji

WYKAZ ZBIORÓW SUWALSKIEGO OŚRODKA KULTURY

NAZWA ZBIORU DANYCH OSOBOWYCH	ADMINISTRATOR DANYCH OSOBOWYCH/DZIAŁ	DATA WPISU d.o.	DATA USUNIĘCIA d.o.	PODSTAWA PRAWNA PRZETWARZANIA d.o.	CEL PRZETWARZANIA d.o.	ZAKRES DANYCH	SPOSÓB GROMADZENIA d.o.	Komu udostępniane są d.o.

Wykaz pomieszczeń, w których przetwarzane są dane osobowe w Suwalskim Ośrodku Kultury w Suwałkach.

L.p.	*Adres*	*Pomieszczenie/nazwa*	*Uwagi*

REJESTR CZYNNOŚCI PRZETWARZANIA		
Lp.	**Opis pola informacyjnego**	**Dane**
1.	Nazwa i dane kontaktowe administratora danych:	
2.	Dane kontaktowe IODO:	
3.	Jednostka organizacyjna (dział):	
	Proces 1	
1.	Cel przetwarzania danych:	
2.	Kategorie osób, których dane dotyczą:	
3.	Kategorie danych przetwarzane w procesie:	
4.	Źródła danych:	
5.	Kategorie odbiorców danych:	
6.	Państwo trzecie, do którego przekazuje się dane:	
7.	Planowany termin usunięcia danych:	
8.	Opis zabezpieczeń technicznych i organizacyjnych:	
	Proces 2	
1.	Cel przetwarzania danych:	
2.	Kategorie osób, których dane dotyczą:	
3.	Kategorie danych przetwarzane w procesie:	
4.	Kategorie odbiorców danych:	
5.	Źródła danych:	
6.	Państwo trzecie, do którego przekazuje się dane:	
7.	Planowany termin usunięcia danych:	
8.	Opis zabezpieczeń technicznych i organizacyjnych:	

WZÓR

Suwałki, ...

Suwalski Ośrodek Kultury
ul. Papieża Jana Pawła II 5, 16-400 Suwałki

Sz. Pani/Pan

.....

.....

UPOWAŻNIENIE NR.....
DO PRZETWARZANIA DANYCH OSOBOWYCH

I.

Na podstawie art. 29 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)

z dniem ..... udzielam polecenia i upoważniam Panią/Pana*) :

.....

(imię i nazwisko)

zatrudnioną/zatrudnionego w Suwalskim Ośrodku Kultury

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku:

.....

(zajmowane stanowisko)

polegającego w szczególności na*):

1. zbieraniu,
2. utrwalaniu,
3. organizowaniu,
4. porządkowaniu,
5. przechowywaniu,

6. adaptowaniu lub modyfikowaniu,
7. pobieraniu,
8. przeglądaniu,
9. wykorzystywaniu,
10. ujawnianiu poprzez przesłanie, rozpowszechnianiu lub innego rodzaju udostępnianiu,
11. dopasowywaniu,
12. łączeniu,
13. ograniczaniu,
14. usuwaniu,
15. niszczeniu;
16. inne

II.

Upoważniam Panią/Pana*) do przetwarzania kategorii danych osobowych/zbiorów danych osobowych , w szczególności *):

1. nazwisko i imię,
2. numer PESEL,
3. numer dowodu osobistego,
4. NIP, REGON,
5. adres zamieszkania, w tym numer domu, ulica i kod pocztowy,
6. województwo, powiat, gmina, miejscowość,
7. adres miejsca pracy, stanowisko służbowe,
8. telefon kontaktowy,
9. adres e-mail
10. inne ..... (wpisać),

III.

Upoważnienie jest ważne do odwołania oraz wygasa z chwilą ustania Pana/Pani*) zatrudnienia w Suwalskim Ośrodku Kultury na stanowisku: .....

IV.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w każdej formie, w tym tradycyjnej i elektronicznej lub innej prawnie dopuszczalnej.

V.

Obowiązek zachowania powyższych informacji w tajemnicy, w tym w szczególności danych osobowych powierzonych do przetwarzania, istnieje od chwili udzielenia niniejszego upoważnienia, przez okres zatrudnienia, jak również po ustaniu zatrudnienia.

VI.

1. Osoba upoważniona obowiązana jest przetwarzać dane osobowe przekazane Jej do

przetwarzania w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administartora Danych - Suwalskiego Ośrodka Kultury.

2. Osoba upoważniona zobowiazuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem, przepisami 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, przepisami obowiązującej na terenie RP ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Suwalskim Ośrodku Kultury wewnętrznymi regulacjami w sprawie ochrony danych osobowych.
3. Naruszenie obowiązków o których mowa w niniejszym upoważnieniu może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów obowiązującej na terenie RP ustawy o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

....

data i podpis Upoważnionej/go

data i podpis osoby upoważnionej do reprezentowania Administratora (Dyrektor)

*) *niepotrzebne skreślić*

OŚWIADCZENIE

1. Oświadczam, że zapoznałam/łem się z obowiazującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Suwalskim Ośrodku Kultury. Przyjmuję do wiadomości obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.
2. Jestem świadoma/my obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia lub po ustaniu zatrudnienia.

.....

data i podpis Upoważnionej/go

rozdzielnik : 4 egzemplarze w oryginale (dokumentacja kadrowa, Administrator x 2, osoba upoważniona)

Załącznik nr 5 do Polityki bezpieczeństwa informacji

WZÓR

Suwałki dn. .....

Suwalski Ośrodek Kultury
Ul. Papieża Jana Pawła II 5, 16-400 Suwałki

Pan/Pani...
Dział....
Suwalskiego Ośrodka Kultury

UPOWAŻNIENIE NR
DO PRZEBYWANIA W OBSZARZE
PRZETWARZANIA DANYCH

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), z dniem 24 .05.2018 r. udzielam polecenia upoważniam Pana/Panią .....

Zatrudnioną/nego w Suwalskim Ośrodku Kultury do przebywania w obszarze przetwarzania danych osobowych w zakresie niezbędnym do wykonywania obowiązków służbowych i prac zleconych na stanowisku:

.....

Upoważnienie jest ważne do odwołania.

....
(data i podpis osoby upoważnionej) (podpis Administratora Danych Osobowych)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp)*	Data nadania upoważnienia	Data ustania upoważnienia	Numer upoważnienia
1.						
2.						
3.						
4.						
5.						

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA OSOBOWYCH

L.p.	**Imię i nazwisko**	**Stanowisko/komórka organizacyjna**	**Zakres** *(określenie, do jakich zbiorów dana osoba ma dostęp)*	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Numer upoważnienia**
1.						
2.						
3.						
4.						
5.						