

<b>Administrator Danych</b>	Centrum Kultury „Karolinka” w Radzionkowie
<b>Dyrektor</b>	Justyna Konik
<b>Inspektor Ochrony Danych</b>	Tomasz Nolewajka
<b>Data wprowadzenia dokumentu</b>	25 maja 2018 roku

## POLITYKA OCHRONY DANYCH OSOBOWYCH

### **Preambuła:**

Na podstawie art. 24 ust. 1 Unijnego Rozporządzenia Ochrony Danych Osobowych (RODO)<sup>1</sup>, Dyrektor Centrum Kultury „Karolinka” w Radzionkowie wprowadza niżej opisane środki techniczne i organizacyjne, mające na celu bezpieczne przetwarzanie danych osobowych.

„Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość).”

**RODO, art.5, ust.1, lit. a)**

„Administrator jest odpowiedzialny za przestrzeganie przepisów ust.1 i musi być w stanie wykazać ich przestrzeganie (rozliczalność).”

**RODO, art.5, ust.2.**

**Dyrektor**

DYREKTOR  
  
mgr Justyna Konik

<sup>1</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

## § 1

### DEFINICJE

Poprzez poniższe określenia należy rozumieć:

**RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

**Organ Nadzorczy** - Prezes Urzędu Ochrony Danych Osobowych.

**Administrator** – Centrum Kultury „Karolinka” w Radzionkowie

**Inspektor Ochrony Danych (IOD)** - Upoważniona przez Administratora osoba do realizowania w jego imieniu zadań wynikających z RODO.

**Obszar chroniony** - wydzielone pomieszczenia lub część pomieszczenia w Centrum Kultury „Karolinka” w Radzionkowie, gdzie dochodzi do przetwarzania danych osobowych.

**Upoważnieni** – pracownicy Centrum Kultury „Karolinka” lub inne osoby fizyczne świadczące usługi na rzecz Centrum Kultury „Karolinka” na podstawie umów cywilnoprawnych, a także podmioty zewnętrzne, którym Administrator udzielił upoważnienia i polecenia do przetwarzania danych osobowych lub upoważnienia do przebywania w pomieszczeniu, w którym znajduje się obszar chroniony.

**Nośnik cyfrowy** - urządzenie typu dysk twardy wewnętrzny lub zewnętrzny, pendrive, pamięci masowe serwerów, taśmy streamer, na których przetwarzane są dane osobowe.

**Nośnik danych** – arkusze papieru, wydruki i inne dokumenty w formie papierowej zawierające dane osobowe.

**Nośnik optyczny** – DVD, HD DVD, Blu-Ray

**Płyta kompaktowa** – CD-R, CD-RW

**Przetwarzanie** - oznacza 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.

**Dane osobowe** - oznaczają 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.

**Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

**Zgoda** - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

**Naruszenie danych** - 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.

**Zabezpieczenie cyfrowe** - wszelkie mechanizmy prowadzące do zabezpieczenia danych przetwarzanych w systemach informatycznych, a do których należy zaliczyć szyfrowanie danych, hasła dostępu, czytniki linii papilarnych, czytniki kart, tokeny.

**Norma DIN 66399** – procedury opisujące standardy niszczenia nośników danych.

**Jednostka** - osoba fizyczna, której dane osobową są przetwarzane.

**Uczestnik** – osoba korzystająca z usług Centrum Kultury „Karolinka” w Radzionkowie.

**Działania akcyjne** – zajęcia statutowe oraz dodatkowe prowadzone w Centrum Kultury „Karolinka” w Radzionkowie.

**Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji. Dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

**Systemy dziedzinowe** – systemy informatyczne w których dochodzi do procesu przetwarzania danych osobowych.

## § 2

### OBSZARY CHRONIONE

1. Do obszarów chronionych wlicza się niżej wymienione części pomieszczeń Centrum Kultury „Karolinka” w Radzionkowie :

Lokalizacja	Pomieszczenie
Plac Jana Pawła II Parter	Dział Impresaryjno-Techniczny – szafy, komputer, biurka (pom.nr 1) Dział Impresaryjno-Techniczny – szafy, komputery, biurka, serwer (pom.nr 2) Dział Tradycji i Dziedzictwa Kulturowego – szafy, komputer. Kasa – stanowisko komputerowe, szafa Portiernia - monitoring
Plac Jana Pawła II I piętro	Gabinet Dyrektor – szafy, biurko, komputer Dział Administracyjno-Gospodarczy

	Dział Finansowo-Księgowy – szafy, biurka, komputery
ul. Św. Wojciecha 118	Komputer (baza danych), biurko i szafa

2. Do wskazanych w punkcie 1 części obszarów chronionych mają dostęp upoważnieni, w zakresie wynikającym z treści upoważnienia wydanego przez Administratora.
3. W przypadku konieczności wydania upoważnienia dla celów przetwarzania danych osobowych Administrator wydaje upoważnienie wg wzoru określonego w **załączniku nr 1**.
4. W razie konieczności powierzenia przez Administratora przetwarzania danych osobowych, zawiera się umowę o powierzeniu przetwarzania danych osobowych wg wzoru stanowiącego **załącznik nr 2**.
5. W przypadku konieczności umożliwienia dostępu do pomieszczeń, w których znajduje się obszar chroniony, takich jak wykonywanie usług serwisowych, naprawczych, modernizacyjnych z innych powodów niż przetwarzanie danych Administrator wydaje zgodę wg **załącznika nr 16**.
6. Do wszystkich obszarów chronionych każdorazowo należy pobierać i zdawać klucze poprzez wpis w książce pobrań. Procedura dotyczy głównej siedziby Centrum Kultury „Karolinka”.
7. Personel sprzątający oraz pozostali pracownicy posiadają dodatkowy komplet kluczy w celu realizacji swoich obowiązków poza godzinami pracy. Pracownicy Ci podpisują oświadczenia o odpowiedzialności za właściwe i odpowiednie zabezpieczenie kluczy przed ich utratą, zgubieniem – **załącznik nr 17**.
8. Dodatkowy komplet kluczy jest zdeponowany w pomieszczeniu Dyrektora oraz w pomieszczeniu monitoringu.
9. Pracownicy Centrum Dokumentacji Deportacji Górnoślązaków do ZSRR w 1945 roku przy ul. Św. Wojciecha 118 podpisują oświadczenia o odpowiedzialności za właściwe i odpowiednie zabezpieczenie kluczy przed ich utratą, zgubieniem.
10. W przypadku utraty lub zgubienia kluczy, o których mowa w punkcie 7 i 9, należy o tym fakcie niezwłocznie powiadomić Dyrektora celem podjęcia czynności zabezpieczających w postaci np. wymiany wkładek kluczy na nowe.
11. Każdorazowo przed opuszczeniem pomieszczeń, po zakończeniu godzin pracy, należy sprawdzić prawidłowe zamknięcie okien, szaf, drzwi oraz właściwe wyłączenie sprzętu komputerowego.
12. W dni wolne od pracy lub poza godzinami pracy (dotyczy Centrum Kultury „Karolinka”):
  - 12.1. Przebywanie w budynkach, jest dozwolone tylko i wyłącznie na podstawie zgody Dyrektora.
  - 12.2. Przebywanie w obszarach chronionych, o których mowa w punkcie 1, jest możliwe w towarzystwie osób upoważnionych przez Administratora, chyba że dotyczy to

pracowników i podmiotów zewnętrznych posiadających już stosowane upoważnienia wydane przez Administratora.

### § 3

#### POMIESZCZENIA

1. Każdy pracownik jest zobowiązany do przestrzegania zasad wykonywania pracy wynikającej z zakresu obowiązków służbowych, a w szczególności w pomieszczeniach w których znajdują się obszary chronione o których mowa w **§ 2 pkt.1**.
2. Należy przestrzegać zasady tzw. „czystego biurka” poprzez schowanie i zabezpieczenie, po godzinach pracy, dokumentacji oraz nośników cyfrowych zawierających dane osobowe.
3. W pomieszczeniach, w których występują obszary chronione (**§ 2 pkt.1**), nie należy pozostawiać osób postronnych bez osoby upoważnionej do przetwarzania danych osobowych w tym obszarze.
4. W godzinach pracy, przed czasowym opuszczeniem pomieszczenia, w którym występują obszary chronione (**§ 2 pkt.1**), należy dokonać zabezpieczenia tych obszarów w celu ochrony przed nieuprawnionym dostępem osób trzecich, np. poprzez wylogowanie się z systemu dziedzinowego, wylogowaniu użytkownika systemu operacyjnego, zamknięcie szaf, zabezpieczenie dokumentów, zamknięciu drzwi.

### § 4

#### NOŚNIKI DANYCH

1. Nośniki danych typu pendrive, dyski zewnętrzne, na których są przetwarzane dane osobowe, należy ewidencjonować.
2. Prowadzi się elektroniczną ewidencję wydanych nośników cyfrowych typu pendrive lub przenośnych dysków twardych o których mowa w punkcie 1 wraz z nazwą użytkownika, hasłem lub kodem do mechanizmu szyfrującego - **załącznik nr 7**.
3. W nośnikach cyfrowych na których przechowuje się dane osobowe należy stosować mechanizmy szyfrujące polegające na wgraniu oprogramowania szyfrującego lub na konieczności wprowadzenia klucza dostępu za pomocą którego nastąpi udostępnienie zawartości nośnika cyfrowego.
4. Laptopy, które są przeznaczone m.in. do pracy poza stacjonarnym miejscem pracy użytkownika, a na których dochodzi do przetwarzania danych osobowych, winny posiadać mechanizmy szyfrujące polegające na wgraniu programu szyfrującego. Dopuszcza się szyfrowanie całego dysku twardego lub części jego zawartości np. katalogu.
5. W przypadku stwierdzenia naruszenia ochrony danych osobowych poprzez np. zgubienie, kradzież nośnika cyfrowego lub laptopa, naruszenia zabezpieczeń należy niezwłocznie powiadomić Administratora lub IOD – **załącznik nr 10**.
6. Nie udostępniania się haseł dostępu, kluczy deszyfrujących do nośników cyfrowych na których są przechowywane dane osobowe.
7. W przypadku podejrzenia uszkodzenia dysku twardego lub nośnika cyfrowego należy dokonać zgłoszenia tego faktu do Administratora celem potwierdzenia uszkodzenia. Po stwierdzeniu uszkodzenia, nośnik podlega wykreśleniu z ewidencji oraz trwałej likwidacji.

W przypadku likwidacji dysków twardych należy stosować min. poziom H1 zniszczenia wg normy DIN 66399, tj. uszkodzenie elektroniczne i mechaniczne. W przypadku pendrive wystarczającym będzie uszkodzenie mechaniczne.

8. Likwidację, o której mowa w punkcie 7, może dokonać podmiot posiadający stosowne uprawnienia do realizowania czynności opisanych w pkt.7 i który, po wykonaniu procedury likwidacyjnej, wyda stosowany certyfikat lub protokół potwierdzający zniszczenie wg wskazanej normy H1.
9. W przypadku nośników optycznych lub kompaktowych, na których znajdują się dane osobowe wystarczającym będzie fizyczne uszkodzenie lub zniszczenie w niszczarce, która posiada mechanizm niszczenia płyt. Niszczenie odbywa się w składzie komisyjnym. Z procesu niszczenia tworzy się protokół zniszczenia nośnika – **załącznik nr 11**. Częstotliwość procesu niszczenia ustala się raz w roku.
10. Wszystkie nieużyteczne wydruki lub błędne wydruki, zawierające dane osobowe, winny być niszczone przez pracownika, który je wytworzył, zgodnie z 2 stopniem bezpieczeństwa w klasie 1 DIN 66399, tj. poprzez cięcie na paski o szerokości max. 6mm.

## § 5

### DOKUMENTACJA

1. Należy zwracać szczególną uwagę by dokumentacja w formie papierowej lub elektronicznej służąca do gromadzenia danych osobowych ograniczała się tylko i wyłącznie do danych niezbędnych do osiągnięcia określonego celu. Każde dodatkowe (nadmiarowe) gromadzenie danych, będzie naruszało prawa lub wolności osób, których dane dotyczą (zasada minimalizacji danych).
2. Każdorazowo, przy przetwarzaniu danych osobowych w formie tradycyjnej, należy się kierować zasadą minimalizacji danych, o której mowa w punkcie powyżej
3. Dokumentacja, która stanowi zbiór danych osobowych, winna być przechowywana w szafach zamykanych na klucz, a pomieszczenia w których powyższa dokumentacja się znajduje musi posiadać mechanizm zabezpieczający w postaci możliwości zamknięcia całości na klucz.
4. Po zakończeniu pracy z dokumentacją, która zawiera dane osobowe a przed opuszczeniem biura, należy zachować zasadę tzw. „czystego biurka”.
5. Archiwizacja dokumentacji, która zawiera dane osobowe, winna być realizowana na podstawie odrębnych przepisów dotyczących archiwizacji, tj. zgodnie z kategorią archiwalną.
6. Zabrania się pozostawiać w obszarach chronionych, bez nadzoru osoby upoważnionej, wydruków, próbnych wydruków, błędnych wydruków, kserokopii dokumentów – na których są dane osobowe.
7. W przypadku wykonywania kserokopii z danymi osobowymi należy sprawdzić, czy nie pozostawiono dokumentu głównego w ksero lub dodatkowej kopii ksera.

## § 6

### DZIAŁANIA AKCYJNE, WYSTĘPY ARTYSTYCZNE

1. Każdorazowo, organizując nabór uczestników na zajęcia stałe prowadzone przez Centrum Kultury „Karolinka” należy stosować formularz zgłoszeniowy **opracowany zgodnie z odrębnym regulaminem**.
2. W zakresie prowadzenia naboru osób powyżej 18 roku życia do zespołu „Mały Śląsk” należy stosować formularz **wg załącznika nr 18**. W pozostałych przypadkach, za wyjątkiem punktu 1 i 2, należy stosować ogólny wzór zgody na przetwarzanie danych osobowych **wg załącznika nr 4**.
3. Należy przestrzegać zasady podpisywania karty zgłoszenia przez rodziców lub opiekunów prawnych zgodnie z podawaną ilością, tzn. wypisany na zgłoszeniu jeden rodzic podpisuje zgodę jeden rodzic, wypisani na zgłoszeniu dwoje rodziców podpisuje zgodę dwoje rodziców.
4. Z ostrożności procesowej należy weryfikować, czy dziecko jest odbierane wg zgłoszenia podawanego na karcie zgłoszenia dziecka na zajęcia.
5. Dla działań akcyjnych, gdzie dochodzi do zbierania danych osobowych wraz z utrwaleniem obrazu w celu rozpowszechniania, należy stosować zasady jak dla procesu przetwarzania danych osobowych, które podlegają wytycznym m.in. niniejszej Polityki Ochrony Danych Osobowych.
6. Zabrania się wykonywania zdjęć uczestników celem ich publikacji bez zgody osoby której dane dotyczą, a w przypadku dzieci bez zgody rodzica lub opiekuna prawnego. Zgoda nie może być domniemana i musi umożliwiać potwierdzenie legalności przetwarzania danych osobowych przez Centrum Kultury „Karolinka”. Rygorowi temu nie podlegają imprezy masowe.
7. Należy przedsięwziąć środki legalności związane z ochroną danych osobowych, np. wizerunku, artystów występujących w Centrum Kultury „Karolinka” poprzez stosowne zapisy w umowach (kontraktach) wyrażające lub nie wyrażające zgodę na wykonywanie czynności przetwarzania danych osobowych przez Centrum Kultury „Karolinka”.

## § 7

### SPRZĘT KOMPUTEROWY, SYSTEMY DZIEDZINOWE

1. Należy zwracać szczególną uwagę by systemy informatyczne przetwarzające dane osobowe gromadziły tylko i wyłącznie dane niezbędne do określonego celu. Każde dodatkowe dane, będą naruszały prawa lub wolności osób, których dane dotyczą (zasada minimalizacji danych).
2. Każdorazowo, przy przetwarzaniu danych osobowych w formie elektronicznej należy się kierować zasadą minimalizacji danych, tzn. zbierania danych tylko i wyłącznie niezbędnych do określonego celu o którym mowa w punkcie 1.
3. Każdorazowy dostęp do zestawu komputerowego, laptopa wymaga podania danych autoryzujących do systemu operacyjnego.
4. Podczas czasowego opuszczenia stanowiska pracy należy się wylogować lub ustawić wygaszacz ekranu na hasło (§ 3 pk.4).

5. Ustala się następującą procedurę nadawania haseł:
  - 5.1. Zabrania się przekazywania haseł dostępu do sprzętu komputerowego osobom nieupoważnionym lub współpracownikom.
  - 5.2. Zabrania się przekazywania lub udostępniania haseł do systemów dziedzinowych osobom nieupoważnionym lub współpracownikom.
  - 5.3. Hasła do systemów dziedzinowych należy zmieniać co 30 dni samodzielnie lub poprzez wymuszenie przez system.
  - 5.4. Hasła administratorów do systemów i serwerów powinny składać się przynajmniej z 8 znaków, przy czym wymagane jest, aby występowały w nich przynajmniej wielka litera, 2 cyfry oraz znak specjalny (?><}{[\*&^%\$#@!.,/). Hasła powinny być zmieniane co minimum 90 dni.
  - 5.5. Hasła do laptopów/desktopów powinny składać się przynajmniej z 6 znaków, przy czym wymagane jest, aby występowały w nich przynajmniej wielka litera, 1 cyfra oraz znak specjalny. Hasła należy zmieniać co 30 dni.
  - 5.6. Hasła użytkowników i operatorów danych (do komputerów i usług, np. do poczty elektronicznej, tzw. konta zwykłe) powinny składać się przynajmniej z 6 znaków, przy czym wymagane jest, aby występowała w nich przynajmniej 1 wielka litera, 1 cyfra oraz 1 znak specjalny. Hasła należy zmieniać co 30 dni.
  - 5.7. Hasła do urządzeń mobilnych i nośników danych (telefony, smartfony, terminale blackberry, pamięci flash itp.) powinny być chronione przynajmniej czterocyfrowym kodem PIN. O ile to możliwe, hasła/kody PIN należy okresowo zmieniać.
  - 5.8. Systemy dziedzinowe, przetwarzające dane sensytywne, winny pracować w sieci wydzielonej lub w sposób gwarantujący bezpieczeństwo przetwarzania danych.
6. Każdy użytkownik systemu dziedzinowego winien posiadać określone w systemie uprawnienia.
7. Wszelkiego rodzaju prace związane z przetwarzaniem danych osobowych w systemach dziedzinowych należy wykonywać z zasadą rozliczalności, tj. na własnym koncie użytkownika.
8. Użytkownik przetwarzający dane osobowe na sprzęcie komputerowym zwraca szczególną uwagę na wszelkiego rodzaju wiadomości e-mail niewiadomego pochodzenia lub nakazujące uruchomienie załączonego linka (odnośnika) lub nakazujące uruchomienie załącznika. Wszystkie powyższe wiadomości mogą stanowić potencjalną próbę pozyskiwania danych i próbę nieuprawnionego dostępu do zasobów komputera. Wiadomości takie należy usuwać.
9. Zakazuje się przesyłania danych osobowych za pośrednictwem poczty e-mail bez zastosowania mechanizmów zabezpieczających np. połączenia szyfrowane, archiwizacja z hasłem, przesyłanie z wykorzystaniem metod kryptograficznych.
10. Zabrania się wysyłania wiadomości e-mail na adresy prywatne w sposób hurtowy, tj. jedna wiadomości do wszystkich adresatów prywatnych.
11. Na każdym zestawie komputerowym należy mieć zainstalowane oprogramowanie antywirusowe, które ma być na bieżąco aktualizowane.
12. Systemy operacyjne typu Windows należy systematycznie aktualizować.



13. Wszelkie aktualizacje lub wdrażanie systemów dziedzinowych winny się odbywać w obecności informatyka lub winny być wykonywane przez informatyka lub przez osoby technicznie zdolne zrealizować powyższe czynności przy zachowaniu wszelkich zasad bezpieczeństwa wynikających z Polityki Ochrony Danych Osobowych i przyjętych norm.
14. Podłączony nośnik zewnętrzny do zestawu komputerowego należy w pierwszej kolejności przeskanować programem antywirusowym na obecność wirusów.
15. Administrator musi zmieniać hasło dostępu do serwera co 30 dni.
16. Prowadzi się ewidencję urządzeń Wi-Fi i administruje udostępnianiem łącz internetowych oraz bezpieczeństwem urządzeń dostępowych w tym haseł, prób nieuprawnionego dostępu, prób włamań, itd.
17. Serwisowanie systemów informatycznych (dziedzinowych), które odbywa się drogą on-line, musi być realizowane w sposób bezpieczny np. z wykorzystaniem VPN, tylko w godzinach pracy jednostki i tylko przez upoważnione podmioty zewnętrzne.
18. Systemy dziedzinowe winny być wyposażone w mechanizmy ułatwiające realizację funkcji „bycia zapomnianym” (nie dotyczy danych przetwarzanych na podstawie przepisów prawa) oraz czasu wprowadzenia danych, informacji odnośnie udostępnienia danych i komu, przenoszenia danych.
19. W przypadku awarii sprzętu komputerowego przetwarzającego dane osobowe, użytkownik zgłasza fakt bezzwłocznie do Administratora.
20. Gdy zachodzi konieczność serwisowania sprzętu poza siedzibą, należy wyjąć dysk twardy w przypadku, kiedy są na nim przechowywane dane osobowe.
21. Prowadzi się bieżący nadzór techniczny nad serwerem, sprzętem komputerowym, urządzeniami aktywnymi i pasywnymi, funkcjonowaniem sieci komputerowej w kontekście prawidłowego jej funkcjonowania związanego z przetwarzaniem danych osobowych. Każde wadliwe działanie mogące mieć wpływ na bezpieczeństwo, poufność, integralność i rozliczalność danych musi być usuwane.
22. Prowadzi się na bieżąco elektroniczny wykaz wszystkich systemów informatycznych wraz z loginem i aktualnym hasłem dostępu zgodnie z opisem załącznika nr 8.

## § 8

### BACKUP, ARCHIWIZACJA

1. Należy pamiętać, że z archiwizowane dane osobowe należy przechowywać nie dłużej niż jest to konieczne z punktu widzenia prawa i zawsze z uwzględnieniem celu. Każdy dłuższy okres przechowywania danych zarchiwizowanych, będzie naruszeniem praw lub wolności osób, których dane dotyczą.
2. Dane, które zawierają dane osobowe, można archiwizować na serwerze z wykorzystaniem automatycznych programów do archiwizacji lub urządzeniach zewnętrznych typu QNAP, HDD na USB poprzez narzędzia automatyzujące ich wykonanie.
3. Dane archiwizowane na nośnikach zewnętrznych, dyskach zewnętrznych winny być przechowywane w odrębnym pomieszczeniu, a ich przechowywanie musi być bezpieczne poprzez zamknięcie w sejfie lub w szafie zamykanej na klucz.

4. Archiwizację danych przetwarzanych w systemach informatycznych (dziedzinowych) prowadzi się w trybie 24 godzinnym w okresie 5 dniowym po czym następuje nadpisanie.
5. Archiwizacji podlegają również programy wykonywalne do systemów przetwarzających dane osobowe.
6. Archiwizację należy przeprowadzać zawsze w sposób umożliwiający wskazanie chronologii ich wykonania.
7. Co pół roku należy sprawdzać poprawność tworzonych archiwów pod kątem ich przydatności, odtworzenia, bezpieczeństwa przechowywania.
8. Przed realizacją usługi serwisowej na bazach danych lub na programie wykonywalnym należy zawsze dokonać archiwizacji bieżących danych.
9. Archiwizacja dokumentacji papierowej jest realizowana na podstawie odrębnych przepisów wynikających z Instrukcji Kancelaryjne i jest przechowywana w archiwum.
10. Do archiwalnej dokumentacji zawierającej dane osobowe winni posiadać osoby upoważnione.

## § 9

### PRAWA JEDNOSTKI, ZGODA

1. Poprzez Jednostkę należy rozumieć osobę fizyczną, która posiada:
  - 1.1. Prawo obowiązku informacyjnego.
  - 1.2. Prawo dostępu do danych.
  - 1.3. Prawo poprawiania i aktualizowania danych.
  - 1.4. Prawo do usunięcia (bycia zapomnianym).
  - 1.5. Prawo do ograniczania przetwarzania.
  - 1.6. Prawo do przenoszalności danych.
  - 1.7. Prawo sprzeciwu.
2. Każda osoba, której dane są i będą przetwarzane, musi otrzymać informację odnośnie:
  - 2.1. Sprostowania lub usunięcia danych.
  - 2.2. Przekazania osobie fizycznej informacji o Administratorze.
  - 2.3. Celu przetwarzania.
  - 2.4. Podstawy prawnej.
  - 2.5. Okresie, przez który dane osobowe będą przechowywane.
  - 2.6. Prawa dostępu do danych, sprostowania, usunięcia lub ograniczenia przetwarzania.
  - 2.7. Prawa wniesienia skargi do organu nadzoru.
  - 2.8. Informacji o IOD.
  - 2.9. Cofnięcia zgody.
  - 2.10. W przypadku jeżeli dane będą przekazywane innym odbiorcom, wówczas Administrator musi poinformować osobę, której dane dotyczą, o odbiorcach lub o kategoriach odbiorców.
3. Dokument zawierający wymagane dane informacyjne stanowi – **załącznik nr 3**.
4. Każdorazowa prośba związana z prawem o którym mowa w punkcie 1 należy dokładnie zweryfikować, czy osoba wnioskująca podaje się faktycznie za osobę, której dane dotyczą.

5. Osoby chcące skorzystać z przysługujących im praw winny złożyć do Dyrektora Centrum Kultury „Karolinka” wniosek zgodnie z **załącznikiem nr 13**.
6. W przypadku wniosku osoby trzeciej, podmiotu trzeciego o udostępnienie informacji, która będzie zawierała dane osobowe każdorazowo wniosek taki należy rozeznac pod kątem przysługujących praw, jak i konieczności anonimizacji danych osobowych.

## § 10

### REJESTR CZYNNOŚCI, REJESTR KATEGORII

1. W ramach nadzoru nad właściwą realizacją i funkcjonowaniem RODO, IOD realizuje zadania w zakresie prowadzenia dokumentacji związanej z rejestrem czynności przetwarzania – **załącznik nr 5**.
2. Rejestr czynności winien opisywać poszczególne działania podejmowane względem danych osobowych i być na bieżąco prowadzony.
3. W ramach nadzoru nad właściwą realizacją zadań wynikających z przetwarzaniem danych osobowych powierzonych przez innego Administratora wprowadza się, celem jego prowadzenia, **załącznik nr 19**.

## § 11

### AUDYT (ANALIZA RYZYKA)

1. Administrator odpowiada za monitorowanie procesu audytowego, który określa szacowanie ryzyka i przeciwdziałania tym ryzykom, zgodnie z podsumowaniem audytu, który stanowi – **załącznik nr 6**.
2. Administrator lub IOD każdorazowo bierze udział w planowanych projektach, gdzie będzie zachodziła konieczność przetwarzania danych osobowych lub będą wprowadzane mechanizmy przetwarzania danych osobowych z wykorzystaniem nowoczesnej technologii, celem:
  - 2.1. Bieżącego reagowania w zakresie przetwarzania danych osobowych.
  - 2.2. Przeciwdziałania mającego na celu zmniejszenie ryzyka.
  - 2.3. Opracowania oceny skutków przetwarzania danych osobowych, jeżeli zajdzie taka konieczność. Ocenę skutków należy przeprowadzić z wykorzystaniem **załącznika nr 14**.
3. Określone ryzyka i przeciwdziałania podlegają rocznemu monitorowaniu.
4. Przynajmniej raz w roku należy zweryfikować wywiązywanie się podmiotów zewnętrznych, którym w drodze umowy o powierzeniu danych osobowych, zlecono ich przetwarzanie w imieniu Centrum Kultury „Karolinka”. Z weryfikacji tworzy się protokół.

## § 12

### DANE WRAŻLIWE

1. Co do zasady zakazuje się przetwarzania danych wrażliwych określonych w **art.9 ust.1 RODO**.
2. W szczególnych przypadkach **CK „Karolinka” w Radzionkowie** może przetwarzać dane wrażliwe w postaci zwolnień lekarskich.

3. Zwolnienia lekarskie dostarczane do CK „Karolinka” w Radzionkowie przez winny być przekazane w zaklejonych kopertach i przetwarzane przez osoby posiadające upoważnienie **wg załącznika nr 1A**.
4. Dane wrażliwe przetwarzane w pozostałej dokumentacji należy chronić w sposób szczególnych. Dane te mogą przetwarzać osoby posiadające upoważnienie **wg załącznika nr 1B**.
5. W przypadku złożenia danych wrażliwych np. przez uczestników wyjazdów koniecznym będzie wyrażenie zgody przez składającego **wg załącznika nr 4A**.
6. Dokumentację o której mowa w pkt.3 i 4 przechowuje się miejscu, gdzie dostęp do nich będą miały osoby posiadające upoważnienie do przetwarzania danych wrażliwych.

### § 13

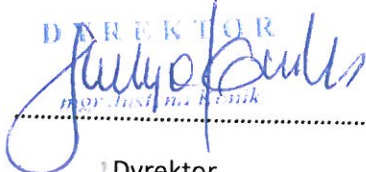
#### ZGŁOSZENIE NARUSZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Każde podejrzenie o naruszeniu przetwarzania danych osobowych należy zgłaszać bezzwłocznie do Administratora lub IOD.
  2. Poprzez naruszenie praw lub wolności osób fizycznych, należy rozumieć m.in.: powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego mienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową.
  3. Naruszenie ochrony danych osobowych dokumentuje się zgodnie z **załącznikiem nr 10**.
  4. Administrator dokonuje zgłoszenia o naruszeniu ochrony danych osobowych do Organu Nadzorczego w terminie do **72 godzin** od podjęcia informacji o tym fakcie – zgodnie z **załącznikiem nr 9**, chyba że jest mało prawdopodobne by naruszenie powodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Należy pamiętać, że ciężar dowodowy w przypadku nie zgłoszenia naruszenia leży po stronie Administratora.
  5. W sytuacji, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko dla naruszenia praw i wolności osób fizycznych należy powiadomić osoby, których dane zostały naruszone, o naruszeniu ochrony danych – zgodnie z **załącznikiem nr 15**.
  6. W sytuacji, kiedy Administrator:
    - 6.1. podejmie odpowiednie kroki w celu wdrożenia odpowiednich środków technicznych i organizacyjnych względem danych, które zostały naruszone,
    - 6.2. zastosuje środki eliminujące prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    - 6.3. poinformowanie wymagałoby niewspółmiernie dużego wysiłku, w takim przypadku wystarczy wydanie ogólnego komunikatu za pomocą którego istnieć będzie prawdopodobieństwo skutecznego powiadomienia
- nie powinno się stosować punktu 5.

§ 14

**POZOSTAŁE INFORMACJE ORGANIZACYJNE**

1. Jednostka winna prowadzić szkolenia, instruktaże pracowników zatrudnionych w Centrum Kultury „Karolinka” w Radzionkowie, osób nowo zatrudnionych, praktykantów, stażystów.
2. Szkolenie z ochrony danych osobowych dla pracowników nowozatrudnionych, stażystów, praktykantów odbywa się w pierwszym dniu pracy.
3. Każda z osób podpisuje stosowne oświadczenie o zapoznaniu się z Procedurą Ochrony Danych Osobowych – **załącznik nr 12**.

DYREKTOR  
  
mgr Justyna Kłęk  
.....  
Dyrektor



Radzionków, dn. ....

Na podstawie art. 29 i 32 ust.4 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) **upoważniam:**

*{Dane identyfikacyjne osoby lub podmiotu upoważnianego}*

**i polecam przetwarzać dane osobowe w:**

*{wskazać zbiór danych, prowadzony w wersji cyfrowej/tradycyjnej}*

**w zakresie:**

*{wskazać zakres czynności przetwarzania danych osobowych}*

**Miejsce przetwarzania danych osobowych:**

*{należy podać miejsce przetwarzania danych osobowych}*

**Data obowiązywania upoważnienia:**

*{należy wskazać czasookres udzielonego upoważnienia}*

**Identyfikator systemu:**

*{należy wskazać login nadany przez Administratora (informatyka)}*

W związku z wydaniem niniejszego upoważnienia traci moc uprzednio wydane upoważnienie na podstawie ustawy o ochronie danych osobowych.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem, o którym mowa powyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....

Data i podpis osoby upoważnionej

.....

Data i podpis Administratora

Radzionków, dn. ....

Na podstawie art. 29 i 32 ust.4 w związku z art. 9 ust.2 lit.b 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) **upoważniam:**

*{Dane identyfikacyjne osoby lub podmiotu upoważnianego}*

**i polecam przetwarzać dane osobowe w:**

*{wskazać zbiór danych, prowadzony w wersji cyfrowej/tradycyjnej}*

**w zakresie:**

*{wskazać zakres czynności przetwarzania danych osobowych}*

**Miejsce przetwarzania danych osobowych:**

*{należy podać miejsce przetwarzania danych osobowych}*

**Data obowiązywania upoważnienia:**

*{należy wskazać czasookres udzielonego upoważnienia}*

**Identyfikator systemu:**

*{należy wskazać login nadany przez Administratora (informatyka)}*

W związku z wydaniem niniejszego upoważnienia traci moc uprzednio wydane upoważnienie na podstawie ustawy o ochronie danych osobowych.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem, o którym mowa powyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....

Data i podpis osoby upoważnionej

.....

Data i podpis Administratora



Radzionków, dn. ....

Na podstawie art. 29 i 32 ust.4 w związku z art. 9 ust.2 lit.a 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) **upoważniam:**

*{Dane identyfikacyjne osoby lub podmiotu upoważnianego}*

**i polecam przetwarzać dane osobowe w:**

*{wskazać zbiór danych, prowadzony w wersji cyfrowej/tradycyjnej}*

**w zakresie:**

*{wskazać zakres czynności przetwarzania danych osobowych}*

**Miejsce przetwarzania danych osobowych:**

*{należy podać miejsce przetwarzania danych osobowych}*

**Data obowiązywania upoważnienia:**

*{należy wskazać czasookres udzielonego upoważnienia}*

**Identyfikator systemu:**

*{należy wskazać login nadany przez Administratora (informatyka)}*

W związku z wydaniem niniejszego upoważnienia traci moc uprzednio wydane upoważnienie na podstawie ustawy o ochronie danych osobowych.

Osoba upoważniona do przetwarzania danych osobowych objętych zakresem, o którym mowa powyżej, jest zobowiązana do zachowania ich w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....  
Data i podpis osoby upoważnionej

.....  
Data i podpis Administratora

**Umowa powierzenia  
przetwarzania danych osobowych**

zawarta dnia ..... (zwana dalej „Umową”) pomiędzy:

.....

(dane podmiotu, który umowę zawiera)

zwany w dalszej części umowy „Podmiotem przetwarzającym”  
reprezentowana przez:

.....

oraz

.....

(dane podmiotu, który umowę zawiera)

zwany w dalszej części umowy „Administratorem danych” lub „Administratorem” reprezentowana  
przez:

.....

**§1**

**Powierzenie przetwarzania danych osobowych**

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art.28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016r. (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

**§2**

**Zakres i cel przetwarzania danych**

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy dane.....(*należy podać rodzaj danych, np. dane zwykłe*) oraz dane szczególnych kategorii.....(*należy podać kategorię osób, których dane dotyczą, itd. pracowników administratora, klientów administratora itd.*) w postaci.....(*np. imion i nazwisk, adresu zamieszkania, nr PESEL, itd.*)

2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu.....(*należy podać cel przetwarzania danych przez podmiot przetwarzający, np. realizacji umowy z dnia.....nr.....w zakresie prowadzenia kadr*).

### §3

#### Sposób wykonania umowy w zakresie przetwarzania danych osobowych

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 lit b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/zwraca Administratorowi wszelkie dane osobowe (należy wybrać, czy podmiot przetwarzający ma usunąć, czy zwrócić dane) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art.32 -36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu..... (*można wskazać, np. w ciągu 24 h*).

### §4

#### Prawo kontroli

1. Administrator danych zgodnie z art.28 ust.3 lit. h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum.....(*należy wpisać, z jakim wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.

3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (*administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

## §5

### Podpowierzenie

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

## §6

### Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

## §7

### Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony/określony od.....do.....
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem..... okresu wypowiedzenia.

## §8

### Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
  - a) Pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
  - b) Przetwarza dane osobowe w sposób niezgodny z umową;
  - c) Powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

## §9

### Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.

## §10

### Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie mają przepisy Kodeksu cywilnego oraz Rozporządzenia.

3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (lub Podmiotu przetwarzającego, w zależności od postanowień stron).

.....

(Administrator danych)

.....

(Podmiot przetwarzający)

## KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust.1 i 2 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 (Dz.Urz.UE L z 2016 r. Nr 119, s.1) informuję, że:

1. Administratorem Pani/Pana danych osobowych jest ..... **{nazwa ADO}** z siedzibą w .....**{adres}**.
2. Inspektorem Ochrony Danych Osobowych w .....**{nazwa ADO}** jest Pani/Pan .....**{imię i nazwisko IDO}**.....**{e-mail lub inne dane kontaktowe}**.
3. Pani/Pana dane osobowe przetwarzane będą w celu .....**{należy podać cel przetwarzania}** na podstawie .....**{należy podać podstawę prawną}**.
4. Odbiorcą Pani/Pana danych będą .....**{kategorie odbiorców}**.
5. Pani/Pana dane osobowe będą przechowywane przez okres .....**{jeżeli nie ma okresu to należy podać kryterium np. do czasu wyłonienia zwycięzcy}**.
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania **{jeżeli przetwarzanie odbywa się na podstawie zgody}**, którego dokonano na podstawie zgody przed jej cofnięciem.
7. Ma Pani/Pan prawo do wniesienia skargi do Prezesa Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. Podanie przez Panią/Pana danych osobowych jest .....**{wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy}**. Jest Pani/Pan zobowiązana do ich podania, a konsekwencją niepodania danych osobowych będzie .....**{jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania, należy wskazać ewentualne konsekwencje niepodania danych}**.
9. Pani/Pana dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach ....., konsekwencją takiego przetwarzania będzie .....**{należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą np. brak potwierdzenia czynności rejestracji do Klubu Książki spowoduje automatycznie usunięcie wniosku o wpisanie na listę klubowiczów}**.

**ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH**

Zgodnie z art. 6 ust.1 lit.a 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 (Dz.Urz.UE L z 2016 r. Nr 119, s.1) wyrażam zgodę na przetwarzanie danych osobowych **{należy wskazać jakich}** w celu **{należy wskazać cel}** przez **{należy wskazać podmiot}**.

.....

Data, czytelnie imię i nazwisko

Oświadczam, że zgodnie z przysługującym mi prawem, jako rodzic/opiekun prawny wyrażam zgodę na przetwarzanie danych dziecka.\*

.....

Data, czytelnie imię i nazwisko rodzica lub opiekuna prawnego

Oświadczam, że zapoznałem/zapoznałam się z Klauzulą Informacyjną o przysługujących mi prawach, której treść stanowi załącznik nr 3 do Polityki Ochrony Danych Osobowych Centrum Kultury „Karolinka” w Radzionkowie.

.....

Data, czytelnie imię i nazwisko

\*) – jeżeli dotyczy



**ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH**

Zgodnie z art. 6 ust.1 lit.a w związku z art.9 ust.2 lit.a 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 (Dz.Urz.UE L z 2016 r. Nr 119, s.1) wyrażam zgodę na przetwarzanie danych osobowych *{należy wskazać jakich}* w celu *{należy wskazać cel}* przez *{należy wskazać podmiot}*.

.....  
Data, czytelnie imię i nazwisko

Oświadczam, że syn/córka jest osobą poniżej 18 roku życia wobec czego, zgodnie z przysługującym mi prawem, jako rodzic/opiekun prawny wyrażam zgodę na przetwarzanie danych dziecka.\*

.....  
Data, czytelnie imię i nazwisko rodzica lub opiekuna prawnego

Oświadczam, że zapoznałem/zapoznałam się z Klauzulą Informacyjną o przysługujących mi prawach, której treść stanowi załącznik nr 3 do Polityki Ochrony Danych Osobowych Centrum Kultury „Karolinka” w Radzionkowie

.....  
Data, czytelnie imię i nazwisko

\*) – jeżeli dotyczy

\*Kolorom czerwonym oznaczono informacje wymagane w rejestrze przez art. 30 ust. 1 RODO

	1	2	3	4	5	6	7
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych
1.			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c		
2.							

8	9	10	11	12
Planowany termin usunięcia kategorii danych <i>(jeżeli jest to możliwe)</i>	Nazwa współadministratora i dane kontaktowe <i>(jeżeli dotyczy)</i>	Nazwa podmiotu przetwarzającego i dane kontaktowe <i>(jeżeli dotyczy)</i>	Kategorie odbiorców <i>(innych niż podmiot przetwarzający)</i>	Nazwa systemu lub oprogramowania
Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d	

13	14	15	16
<p>Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 <i>(jeżeli jest to możliwe)</i></p> <p>Art.. 30 ust. 1 pkt g</p>	<p>DPIA (jeśli tak, lokalizacja raportu)</p>	<p>Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)</p> <p>Art. 30 ust. 1 pkt e</p>	<p>Transfer do kraju trzeciego lub org. międzynarodowej</p> <p>Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń</p> <p>Art. 30 ust. 1 pkt e</p>

Załącznik Nr 7

Lp	Nazwa nośnika	Numer seryjny/model	Użytkownik	Login	Hasło szyfrujące/desyfrujące
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
.....					

Załącznik Nr 8

Lp	Nazwa systemu	Użytkownik	Hasło dostępu
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
.....			

**Organ nadzorczy:**

{adres}

**Administrator Danych:**Centrum Kultury „Karolinka”  
Plac Jana Pawła II  
Radzionków**ZGŁOSZENIE NARUSZENIA DANYCH OSOBOWYCH**

Niniejszym w trybie art.33 ogólnego rozporządzenia o ochronie danych osobowych, zgłaszam naruszenie danych osobowych, które miało miejsce w dniu .....w Centrum Kultury „Karolinka” w Radzionkowie

1	Charakter naruszenia danych:	
2	Kategoria i przybliżona liczba osób, których dane dotyczą:	
3	Liczba rekordów, których dotyczy naruszenie:	
4	Możliwe konsekwencje naruszenia danych:	
5	Środki zastosowane lub proponowane w celu zaradzenia naruszeniom ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:	
6	Dane Inspektora Ochrony Danych lub inny punkt kontaktowy:	

.....  
.....  
..... (\*)

.....  
Dyrektor

\* - w przypadku powiadomienie po 72 godzinach należy wpisać uzasadnienie



**NARUSZENIE OCHRONY DANYCH OSOBOWYCH**

Lp.	Data naruszenia	Rodzaj naruszenia	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

**Czynności dodatkowe:**

1. W przypadku podejrzenia lub naruszenia bezpieczeństwa informacji chronionych zostają podjęte następujące działania:
  - a. W przypadku podejrzenia naruszenia bezpieczeństwa informatycznego systemu natychmiastowa zmiana haseł dostępu, odłączenie sprzętu od Internetu, uruchomienie antywirusa,
  - b. zawiadomienie kierownictwa,
  - c. ewentualne zgłoszenie do innych właściwych służb (np. policji, w przypadku kradzieży sprzętu),
  - d. zabezpieczenie miejsca zdarzenia,
  - e. kontrola danych i stanu ich zabezpieczeń,
  - f. przeprowadzenie przez kierownictwo sprawdzenia doraźnego i przygotowanie sprawozdania w tym zakresie.
2. Jeżeli działania powyższe doprowadzą do stwierdzenia naruszenia ochrony danych osobowych zostają podjęte następujące działania:
  - a. zabezpieczenie danych,
  - b. przeciwdziałanie rozpowszechnianiu danych,
  - c. odtworzenie zniszczonych danych z dostępnych kopii bezpieczeństwa,
  - d. zawiadomienie właściwych organów, w szczególności zgłoszenie incydentu do GIODO wraz z opisem podjętych działań.
  - e. w przypadku naruszenia lub podejrzenia naruszenia prywatności osób, których dane dotyczą, niezwłoczne powiadomienie ich o zaistniałej sytuacji oraz możliwych do podjęcia przez nie środków prewencyjnych,
  - f. podjęcie działań mających na celu zmniejszenie ryzyka wystąpienia naruszenia w przyszłości.
3. W przypadku stwierdzenia wielokrotnego naruszenia ochrony, pomimo podjętych działań określonych w ppkt. 1), 2) należy:
  - a. zablokować uprawnienia dostępu do zagrożonej bazy danych,
  - b. zabezpieczyć kopie bezpieczeństwa i kopie archiwalne,
  - c. zawiadomić GIODO i inne właściwe organy.

**PROTOKÓŁ ZNISZCZENIA NOŚNIKÓW ZAWIERAJĄCYCH DANE OSOBOWE**

W dniu ..... komisja w składzie:

1. Inspektor Ochrony Danych Osobowych
2. ....

dokonała zniszczenia dokumentów/elektronicznych nośników danych osobowych

.....<sup>1</sup>

---

<sup>1</sup> Wskazać o jakie dane chodzi, np. CV kandydatów do pracy

Imię i nazwisko: .....

Stanowisko: .....

Data: .....

**OŚWIADCZENIE**

Oświadczam, że zapoznałem/am się z Polityką Ochrony Danych Osobowych obowiązującą w Centrum Kultury "Karolinka" w Radzionkowie i zobowiązuję się do przestrzegania zasad w nim zawartych oraz zachowania wszelkich informacji chronionych, do których otrzymam dostęp w poufności.

Zostałem/am również zapoznany/a z ogólnymi zasadami zabezpieczenia i przetwarzania danych osobowych wynikającymi z 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 i zobowiązuję się do ich przestrzegania.

Oświadczam, że zachowam w poufności wszelkie informacje chronione, które przetwarzałem/am lub przetwarzam w ramach wykonywanych obowiązków oraz metody ich zabezpieczeń, także po ustaniu wykonywania zlecenia, umowy lub świadczenia pracy.

Czytelny podpis: .....

**Wniosek osoby, której dane osobowe są przetwarzane przez  
Centrum Kultury "Karolinka" w Radzionkowie w związku z \*:**

- 1.1. Prawem obowiązku informacyjnego.
- 1.2. Prawem dostępu do danych.
- 1.3. Prawem poprawiania i aktualizowania danych.
- 1.4. Prawem do usunięcia (bycia zapomnianym).
- 1.5. Prawem do ograniczania przetwarzania.
- 1.6. Prawem do przenoszalności danych.
- 1.7. Prawem sprzeciwu.

**Dane wnioskodawcy:**

Imię i nazwisko lub pełna nazwa: .....

Adres: .....

PESEL/REGON: ..... Telefon: ..... E-mail: .....

**Wnoszę o:**.....  
.....**Uzasadnienie wniosku (wskazanie podstawy prawnej lub faktycznej):**.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

Data i podpis wnioskodawcy .....

Załączniki .....

### Ocena skutków przetwarzania danych osobowych

Lp.	Opis planowanych operacji i celów przetwarzania	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą	Planowane środki w celu zaradzenia ryzyku, w tym zabezpieczenia, oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO z uwzględnieniem praw prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Radzionków, dn.

**Powiadomienie o naruszenie danych osobowych**

1. *Wskazać imię i nazwisko oraz dane kontaktowe IODO lub wskazanie innego punktu kontaktowego, który udzieli informacji.*
2. *Opisać możliwe konsekwencje naruszenia ochrony danych osobowych.*
3. *Opisać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych skutków.*

.....  
Dyrektor

Radzionków, dn. ....

**Z G O D A**

Niniejszym wyrażam zgodę dla ..... na przebywanie w okresie ..... w pomieszczeniu/pomieszczeniach w których znajdują się obszary chronione celem wykonania poniższych czynności:

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

Nadzór nad realizacją powyższych czynności powierzam .....

.....

Dyrektor

## OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałem/-am się z Polityką Ochrony Danych Osobowych w zakresie powierzenia pieczy nad kluczami umożliwiającymi dostęp do pomieszczeń w których są wskazane obszary chronione i w których będę realizować tylko i wyłącznie czynności wynikające z powierzonego mi zakresu obowiązków służbowych.

.....  
Data, czytelnie imię i nazwisko

\*) – dotyczy tylko i wyłącznie osób poniżej 13 roku życia.



## Karta informacyjna

NAZWISKO I IMIĘ UCZESTNIKA ZAJĘĆ

DATA URODZENIA

MIEJSCE ZAMIESZKANIA

IMIĘ I NAZWISKO RODZICÓW/OPIEKUNÓW

TELEFON KONTAKTOWY

TELEFON KONTAKTOWY RODZICÓW/OPIEKUNÓW

ADRES E-MAIL

NR PASZPORTU/NR DOWODU OSOBISTEGO

Oświadczam, że zapoznałem/am się z regulaminem pracy na scenie i uczestnictwem w zajęciach obowiązującym w Centrum Kultury „Karolinka”.

.....  
Podpis

Oświadczam, że jestem świadomy/a ponoszonego ryzyka związanego z wykonywaniem trudnych elementów technicznych podczas prób i występów związanych z opracowywaniem układu choreograficznego oraz, że z tego tytułu nie będę domagał/a się żadnych rekompensat.

.....  
Podpis

Zgodnie z art. 6 ust.1 lit.a 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 (Dz.Urz.UE L z 2016 r. Nr 119, s.1) wyrażam zgodę na przetwarzanie danych osobowych **wskazanych w części pierwszej Karty Informacyjnej i mojego wizerunku** w celu **uczestniczenia w zajęciach zespołu „Mały Śląsk” wraz ze związanymi z tym czynnościami, organizowanych wyjazdach artystycznych oraz promocji** przez Centrum Kultury „Karolinka”

.....  
Podpis

Oświadczam, że zapoznałem/-am się z treścią informacji o przysługujących mi prawach zgodnie z załącznikiem nr 3 Polityki ochrony danych osobowych w Centrum Kultury „Karolinka”, którego treść został mi udostępniona.

.....  
Podpis



inistratora przez CK "Karolinka"

Przekazywanie danych do państwa trzeciego (nazwa organizacji i dane kontaktowe)	Przekazywanie danych do organizacji międzynarodowej (nazwa i dane kontaktowe)	Podstawa prawna transferu danych do państwa trzeciego lub organizacji międzynarodowej (oraz – gdzie ma to zastosowanie – link/odniesienie do dokumentacji odpowiednich zabezpieczeń)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Data utworzenia wpisu	Data ostatniej aktualizacji wpisu
9	10	11	12	13	14



## WYJAŚNIENIE

do

**„POLITYKI OCHRONY DANYCH OSOBOWYCH”** opracowanej dla Centrum Kultury „Karolinka”  
w Radzionkowie:

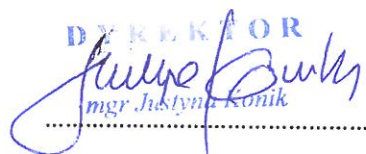
Opracowany dokument pn. POLITYKA **OCHRONY DANYCH OSOBOWYCH** określa obszary chronione oraz zasady w jaki sposób powinny być chronione i przetwarzane dane osobowe pozyskiwane w celu prowadzenia działalności Centrum Kultury „Karolinka” w Radzionkowie.

Wzory dokumentów zawartych w niniejszej Polityce są w razie konieczności odpowiednio modyfikowane i dostosowywane do konkretnego przypadku. Dotyczy to między innymi kart zapisów na zajęcia, kart wynajmu sal, kart wyjazdów na wycieczki, festiwale oraz wszelkich innych sytuacji, kiedy przetwarzanie danych osobowych jest niezbędne do realizacji działań statutowych Centrum Kultury „Karolinka” w Radzionkowie.

Ochrona Danych Osobowych w Centrum Kultury „Karolinka” w Radzionkowie odbywa się 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).

Administrator Danych dokłada wszelkich starań aby pozyskane i przetwarzane dane osobowe były należycie chronione i wykorzystane jedynie do celów, do których zostały zebrane.

Dyrektor

DYREKTOR  
  
mgr Justyna Konik

