

Zarządzenie Nr 72/2019
Dyrektora Gminnego Centrum Kultury w Cewicach
z dnia 18 stycznia 2019r.
w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych
w Gminnym Centrum Kultury w Cewicach

Na podstawie 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), dalej zwane również „RODO”, ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000), ustawy o organizowaniu i prowadzeniu działalności kulturalnej z dnia 3 października 2018 r. (Dz. U. z 2018 poz. 1983), ustawy o samorządzie gminnym z dnia 9 maja 2018 r. (Dz. U. z 2018 r., poz. 994), Kodeksu Pracy z dnia 13 kwietnia 2018 r. (Dz. U. z 2018 r., poz. 917) oraz ustawy o systemie ubezpieczeń społecznych z dnia 15 września 2017 r. (Dz. U. z 2017 r., poz. 1778).

Zarządzam, co następuje:

§1

Ustalam i wprowadzam do stosowania w Gminnym Centrum Kultury w Cewicach:
Politykę Bezpieczeństwa Danych Osobowych w Gminnym Centrum Kultury w Cewicach,
stanowiącą załącznik Nr 1 do niniejszego zarządzenia.

§2

Zarządzenie wchodzi w życie z dniem 18 stycznia 2019r.

DYREKTOR
Gminnego Centrum Kultury w Cewicach
Dominiła Bardowska

Załącznik nr 1

do Zarządzenia Nr 72/2019

Dyrektora Gminnego Centrum Kultury w Cewicach

z dnia 18.01.2019r.

**Polityka bezpieczeństwa (ochrony) danych osobowych
w Gminnym Centrum Kultury w Cewicach**

Spis treści

Rozdział 1.	Postanowienia ogólne	2
Rozdział 2.	Prawa osoby, której dane osobowe dotyczą.....	8
Rozdział 3.	Obowiązek informacyjny	9
Rozdział 4.	Prawo dostępu do danych osoby, której dane dotyczą i do ich sprostowania	10
Rozdział 5.	Prawo do usunięcia danych lub ograniczenia ich przetwarzania	11
Rozdział 6.	Prawo do przenoszenia danych.....	12
Rozdział 7.	Prawo sprzeciwu.....	12
Rozdział 8.	Zadania i obowiązki administratora danych osobowych.....	13
Rozdział 9.	Zadania i obowiązki IODO wyznaczonego przez administratora danych osobowych...	16
Rozdział 10.	Szacowanie ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych	21
Rozdział 11.	Zadania i obowiązki osób zatrudnionych w Gminnym Centrum Kultury w Cewicach ..	24
Rozdział 12.	Podstawowe sposoby zabezpieczenia danych osobowych	26
Rozdział 13.	Przetwarzanie danych w systemie tradycyjnym.....	26
Rozdział 14.	Przetwarzanie danych w systemie informatycznym	27
Rozdział 15.	Postępowanie z nośnikami danych osobowych	28
Rozdział 16.	Zdarzenia naruszające lub grożące naruszeniem bezpieczeństwa (ochrony) danych osobowych	29
Rozdział 17.	Powiadomienia o naruszeniu bezpieczeństwa (ochrony) danych osobowych	30
Rozdział 18.	Wykaz załączników do polityki bezpieczeństwa (ochrony) danych osobowych	31

Rozdział 1. Postanowienia ogólne

§ 1.

1. Celem polityki bezpieczeństwa (ochrony) danych osobowych w Gminnym Centrum Kultury w Cewicach jest określenie zasad przetwarzania, ochrony i udostępniania gromadzonych i przetwarzanych danych osobowych, oraz nadzoru nad procesem przetwarzania tych danych, w szczególności zasad
 - 1) zbierania oraz rzetelnego i przejrzystego przetwarzania,
 - 2) uzasadnionych interesów realizowanych przez administratora danych osobowych,
 - 3) pseudonimizacji danych osobowych,
 - 4) informowania
 - a) opinii publicznej,
 - b) osób, których dane dotyczą,
 - c) Prezesa Urzędu ochrony Danych Osobowych,
 - 5) wykonywania przez osoby, których dane dotyczą, przysługujących im praw,
 - 6) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem,
 - 7) powoływania i zasad działania inspektora ochrony danych osobowych,
 - 8) zapewniania bezpieczeństwa przetwarzania,
 - 9) postępowania w sprawach skarg i wniosków dotyczących przetwarzania danych osobowych,
 - 10) postępowania w sprawach naruszeń bezpieczeństwa (ochrony) danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;
 - 11) zgłaszania naruszeń bezpieczeństwa (ochrony) danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych,
 - 12) zawiadamiania o naruszeniach bezpieczeństwa (ochrony) danych osobowych osób, których dane dotyczą,
 - 13) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych;
 - 14) postępowań sądowych, pozasądowych oraz innych trybów rozstrzygania sporów dotyczących przetwarzania oraz bezpieczeństwa (ochrony) danych osobowych.
2. Polityka bezpieczeństwa (ochrony) danych osobowych została opracowana w oparciu o przepisy:
 - 1) 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), dalej zwane również „RODO”,
 - 2) ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000),
 - 3) ustawa o organizowaniu i prowadzeniu działalności kulturalnej tj. z dnia 3 października 2018 r. (Dz. U. z 2018 poz. 1983),
 - 4) ustawa o samorządzie gminnym, tj. Z dnia 9 maja 2018 r. (Dz. U. z 2018 r., poz. 994),
 - 5) Kodeks pracy, tj. z dnia 13 kwietnia 2018 r. (Dz. U. z 2018 r., poz. 917),

- 6) ustawa o systemie ubezpieczeń społecznych, tj. z dnia 15 września 2017 r. (Dz. U. z 2017 r., poz. 1778).
3. Polityka bezpieczeństwa (ochrony) danych osobowych obowiązuje wszystkie osoby realizujące jakiegokolwiek zadania Gminnego Centrum Kultury w Cewicach, niezależnie od podstawy wykonywania tych zadań.

§ 2.

1. Użyte w niniejszej Polityce określenia oznaczają:

- 1) administrator danych osobowych – Gminne Centrum Kultury w Cewicach,
- 2) dane osobowe - 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, a także wizerunek,
- 3) hasło - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
- 4) identyfikowanie ryzyka –czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować naruszenie lub zagrożenie naruszeniem bezpieczeństwa (ochrony) danych osobowych,
- 5) integralność i poufność danych osobowych – dane przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo (ochronę) danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem, uszkodzeniem lub ujawnieniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,
- 6) IODO – inspektor ochrony danych osobowych w rozumieniu art. 37 – 39 RODO, wyznaczony przez administratora danych osobowych,
- 7) klient - osoba uczestnicząca w przedsięwzięciu lub osoba, której dane osobowe Gminne Centrum Kultury w Cewicach przetwarza w związku z prowadzeniem działalności oraz w związku z realizacją obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do Gminnego Centrum Kultury w Cewicach, a także w aktach prawnych i innych aktach Gminy Cewice,
- 8) kryteria akceptacji ryzyka – kryteria, które określają dopuszczalność danego ryzyka, zdefiniowaną poprzez wartość progową,
- 9) kryteria oceny ryzyka –kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka,
- 10) login - identyfikator użytkownika, stanowiący ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- 11) minimalny zakres danych osobowych – dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane,
- 12) naruszenie bezpieczeństwa (ochrony) danych osobowych - 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,

- 13) nośnik danych osobowych – wydruk, formularz lub inne pismo, dysk twardy, dyskietka, płyta CD lub DVD, pendrive, pamięć flash, taśma magnetyczna oraz inny materiał lub urządzenie służące do przechowywania danych osobowych,
- 14) obszar przetwarzania danych osobowych - budynki, obiekty, pomieszczenia oraz meble i urządzenia, w których przetwarzane są dane osobowe,
- 15) ograniczenie celu przetwarzania danych osobowych – dane, zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- 16) ograniczenie przechowywania danych osobowych – dane przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane,
- 17) operacja przetwarzania danych osobowych – każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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,
- 18) osoba zatrudniona – pracownik lub inna osoba, zatrudniona w Gminnym Centrum Kultury w Cewicach, bez względu na podstawę prawną zatrudnienia, posiadająca upoważnienie do przetwarzania danych osobowych,
- 19) polityka bezpieczeństwa lub polityka – niniejszy dokument opisujący stosowane w Gminnym Centrum Kultury w Cewicach zasady bezpieczeństwa (ochrony) danych osobowych,
- 20) poufności danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
- 21) prawidłowość przetwarzania danych osobowych – dane prawidłowe i w razie potrzeby uaktualniane; w zakresie celów ich przetwarzania, przy jednoczesnym podejmowaniu wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,
- 22) proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania,
- 23) przedsięwzięcie – impreza, usługa, zajęcia lub inna forma organizacyjna, realizowana w imieniu lub na rzecz Gminnego Centrum Kultury w Cewicach oraz na zlecenie innego podmiotu,
- 24) przetwarzający – podmiot, któremu administrator danych osobowych powierzył przetwarzanie danych osobowych w zakresie określonym umową o powierzeniu przetwarzania danych osobowych,
- 25) pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
- 26) rozliczalność danych osobowych – wdrożenie odpowiednich zasad i procedur, pozwalających na wykazanie przestrzegania przepisów prawa, ze szczególnym uwzględnieniem udziału w tych działaniach IODO,

- 27) ryzyko – wpływ niepewności na cele przetwarzania oraz bezpieczeństwo (ochronę) danych osobowych; w przypadku ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych w zakresie praw i wolności osób, których dane dotyczą, celem jest bezpieczeństwo (ochrona) tych praw i wolności,
 - 28) szacowanie ryzyka – całościowy proces identyfikacji ryzyka, ustalania prawdopodobieństwa i oceny skutków, analizy ryzyka oraz oceny ryzyka,
 - 29) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
 - 30) użytkownik – osoba zatrudniona przetwarzająca dane osobowe w systemie przetwarzania danych,
 - 31) zgoda – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie danych osobowych dotyczących tej osoby,
 - 32) zgodność z prawem, rzetelność i przejrzystość przetwarzania danych osobowych – przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty, poprzez zapewnienie podstaw prawnych przetwarzania oraz realizację praw klientów obejmujących w szczególności informowanie klientów o przetwarzaniu ich danych zgodnie z wymogami prawa i polityki.
2. Ilekcio w polityce uŹywa się sformułowania „osoba, której dane dotyczą” dotyczy to także osoby uprawnionej do składania oświadczenia woli w imieniu lub na rzecz osoby, której dane dotyczą.
3. W przypadkach, w których administrator danych osobowych – na podstawie przepisów RODO – nie jest do tego zobowiązany i nie powoła lub nie wyznaczy IODO, zadania, które są przewidziane dla IODO w polityce oraz w RODO, realizuje administrator danych osobowych lub inna osoba przez niego wyznaczona.

§ 3.

Administrator danych osobowych przetwarza dane osobowe, jeśli spełniony jest co najmniej jeden z poniŹszych warunków:

- 1) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych w jednym lub w większej liczbie określonych celów,
- 2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na Źądanie osoby, której dane dotyczą, przed zawarciem umowy,
- 3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych osobowych,
- 4) przetwarzanie jest niezbędne do ochrony Źywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
- 5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi danych osobowych,
- 6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora danych osobowych lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

§ 4.

1. Administrator danych osobowych może przetwarzać dane osobowe, powierzone do przetwarzania przez inny podmiot.
2. Tryb i zasady przetwarzania powierzonych danych osobowych określa umowa o powierzeniu przetwarzania danych zawarta pomiędzy podmiotem powierzającym a Gminnym Centrum Kultury w Cewicach, pełniącym funkcję przetwarzającego.
3. W przypadku przetwarzania danych osobowych na podstawie umowy o powierzeniu przetwarzania danych osobowych Gminnemu Centrum Kultury w Cewicach, postanowienia polityki stosuje się odpowiednio, w zakresie nieuregulowanym umową o powierzeniu przetwarzania danych.

§ 5.

1. Postanowienia ust. 2 – 12 stosuje się w przypadku, gdy zgoda osoby, której dane mają być przetwarzane, ma stanowić wyłączną podstawę prawną przetwarzania danych w określonym celu lub celach.
2. Przez zgodę osoby, której dane dotyczą, należy rozumieć 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.
3. Wyrażenie zgody przez osobę powinno nastąpić przed faktycznym rozpoczęciem przetwarzania w tym celu lub celach.
4. Zapytanie o zgodę musi być wyrażone w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem, a dodatkowo w przypadku zapytań elektronicznych – w zwięzłej formie i nie może niepotrzebnie zakłócać korzystania z przedsięwzięcia, którego dotyczy.
5. Zgoda w formie oświadczenia woli powinna być wyrażona w zrozumiałej i łatwo dostępnej formie oraz sformułowana jasnym i prostym językiem, a także stanowić odrębną deklarację. Dopuszcza się włączenie klauzuli zgody do umowy lub wniosku o zawarcie umowy, z zastrzeżeniem umożliwienia osobie złożenia odrębnego podpisu lub zaznaczenia okienek wyboru na umowie.
6. Oświadczenie woli może być wyrażone w dowolnej formie (ustnej, dokumentowej, pisemnej lub elektronicznej), w tym np. poprzez zaznaczenie okienek wyboru na formularzu lub w systemie informatycznym, przy których wskazane są klauzule zgód, złożenie przez osobę podpisu na dokumencie tradycyjnym pod oświadczeniem woli, złożenie podpisu elektronicznego na dokumencie elektronicznym z oświadczeniem woli, oświadczenie o wyrażeniu zgody przesłane drogą elektroniczną.
7. Do wyraźnych działań wskazujących na wyrażenie zgody przez klienta zaliczyć można w szczególności wybór przez klienta ustawień technicznych systemu informatycznego, przekazanie przez klienta ustnie, pisemnie lub za pomocą elektronicznych środków komunikacji stosowanych przez administratora danych osobowych swoich danych osobowych, wrzucenie przez klienta wizytówki do pojemnika w celu udziału w przedsięwzięciu organizowanym lub realizowanym przez Gminne Centrum Kultury w Cewicach, pod warunkiem, że wcześniej osoba ta zostanie poinformowana o konieczności przekazania danych (np. wizytówki) w przypadku chęci wzięcia udziału w przedsięwzięciu. Informacja o konieczności przekazania danych może zostać zawarta w regulaminie lub w innym akcie określającym prawa i obowiązki uczestników przedsięwzięcia.
8. Jedna zgoda klienta obejmuje jeden cel przetwarzania danych osobowych. Na jednym dokumencie lub w jednym formularzu klient może wyrazić wiele zgód na przetwarzanie danych

osobowych dla różnych celów.

9. Za wyrażenie zgody nie uznaje się milczenia osoby, braku sprzeciwu, niepodjęcia przez nią działań oraz nie zaznaczenia domyślnych okienek wyboru w systemie informatycznym.
10. Zgody nie uważa się za wyrażoną świadomie lub dobrowolnie, jeśli:
 - 1) od wyrażenia przez osobę zgody uzależnione jest wykonanie umowy, w tym świadczenie przedsięwzięcia, a do wykonania tej umowy zgoda nie jest niezbędna,
 - 2) osoba, której dane dotyczą nie ma możliwości udzielenia osobnej zgody na różne cele przetwarzania danych w przypadkach, kiedy jest to stosowne, np. osobna zgoda na przetwarzanie danych w celach marketingowych a osobna na udostępnienie danych innemu podmiotowi,
 - 3) zapytanie o zgodę nie zostało przedstawione w sposób pozwalający wyraźnie odróżnić go od pozostałych kwestii, w przypadku gdy treść zgody na przetwarzanie danych zawarta jest w pisemnym oświadczeniu, które zawiera również inne treści, np. klauzula zgody na przetwarzanie danych osobowych zawarta w treści umowy pomiędzy Gminnym Centrum Kultury w Cewicach a klientem.
11. Administrator danych osobowych umożliwia osobie, która wyraziła zgodę na przetwarzanie danych osobowych, wycofanie tej zgody w dowolnym momencie oraz w sposób równie łatwy, jak jej wyrażenie. Odwołanie zgody może nastąpić w dowolnej formie.
12. Wzór zgody na przetwarzania danych osobowych określa załącznik nr 1 do polityki.

§ 6.

1. Osoba zatrudniona, odpowiadająca za organizację lub prowadzenie przedsięwzięcia jest zobowiązana do ustalenia, czy w związku z przedsięwzięciem:
 - 1) są, będą lub mogą być przetwarzane dane osobowe klienta,
 - 2) jaki jest, będzie lub może być zakres przetwarzanych danych,
 - 3) na jakiej podstawie dane są, będą lub mają być przetwarzane,
 - 4) w jakim okresie dane są, będą lub mogą być przetwarzane,
 - 5) w jaki sposób dane są, będą lub mają być zabezpieczone (chronione),
 - 6) jaki jest, będzie lub może być tryb i zasady postępowania z danymi osobowymi po zakończeniu przedsięwzięcia.
2. W przypadku, gdy organizację i przeprowadzenie przedsięwzięcia reguluje regulamin przedsięwzięcia lub inny akt określający prawa i obowiązki uczestników przedsięwzięcia, w regulaminie lub innym akcie wskazuje się w szczególności:
 - 1) zakres i cele przetwarzanych danych osobowych,
 - 2) podstawę prawną przetwarzania danych osobowych,
 - 3) jeżeli dane osobowe mają być przetwarzane wyłącznie na podstawie zgody uczestnika przedsięwzięcia – formę i sposób wyrażenia zgody,
 - 4) prawa osoby, której dane mają być przetwarzane,
 - 5) warunki i zasady, określające możliwość zapoznania się uczestnika przedsięwzięcia z zasadami bezpieczeństwa (ochrony) danych osobowych.
3. Ustalenie, o którym mowa w ust. 1 dokonywane jest w uzgodnieniu z IODO.
4. Ustalenie, o którym mowa w ust. 1 dokonywane jest w uzgodnieniu z inną komórką

organizacyjną lub stanowiskiem pracy, jeżeli tak wynika z zakresu zadań i obowiązków komórek organizacyjnych lub stanowisk pracy.

5. Ustalenie, o którym mowa w ust. 1 dokonywane jest na formularzu, którego wzór określa załącznik nr 2 do polityki.

Rozdział 2. Prawa osoby, której dane osobowe dotyczą

§ 7.

1. Administrator danych osobowych realizuje prawa osób, których dane dotyczą, w tym:
 - 1) prawo do informacji (obowiązek informacyjny)'
 - 2) prawo dostępu do danych lub otrzymania kopii danych,
 - 3) prawo do sprostowania danych,
 - 4) prawo do usunięcia danych,
 - 5) prawo do ograniczenia przetwarzania,
 - 6) prawo do przenoszenia danych,
 - 7) prawo do sprzeciwu.
2. Klient jest uprawniony do zgłoszenia żądania dotyczącego jego praw w formie pisemnej lub w innej formie możliwej do udokumentowania przez administratora danych osobowych.
3. Żądanie klienta powinno wskazywać, jakich danych osobowych i czynności dotyczy.
4. W przypadku braku sprecyzowania przez klienta jakich danych i jakich czynności żądanie dotyczy, administrator danych osobowych jest uprawniony do wstrzymania realizacji żądania do momentu uzyskania wystarczających informacji od klienta.
5. Gminne Centrum Kultury w Cewicach realizuje żądanie klienta zgodnie ze swoimi wewnętrznymi procedurami.
6. Realizacja praw osoby, której dane dotyczą, następuje w rozsądnym terminie uwzględniającym koszty, stopień trudności realizacji żądania oraz w oparciu o wewnętrzne procesy.
7. W zakresie realizacji praw osoby, której dane dotyczą, komunikacja z tą osobą, które dane dotyczą, powinna odbywać się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, oraz:
 - 1) bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania osoby, której dane dotyczą,
 - 2) w przypadku konieczności wydłużenia terminu realizacji żądania osoby, której dane dotyczą, najpóźniej w terminie miesiąca od otrzymania żądania administrator danych osobowych udziela informacji o przedłużeniu terminu rozpatrzenia żądania oraz podaje przyczyny opóźnienia; wydłużenie terminu może nastąpić z uwagi na skomplikowany charakter żądań lub liczbę żądań, lecz nie więcej niż o dwa miesiące,
 - 3) w przypadku nieuwzględnienia żądania osoby, której dane dotyczą, najpóźniej w ciągu miesiąca od otrzymania żądania osoby, której dane dotyczą, administrator danych osobowych udziela informacji o odmowie podjęcia działań w związku z żądaniem osoby, powodach niepodjęcia działań, możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skorzystania ze środków ochrony prawnej przed sądem oraz o ustaniu podstawy do ograniczenia przetwarzania danych klienta.
8. Administrator danych osobowych komunikuje się z klientem w języku polskim.

9. Realizacja wniosku o wydanie kopii danych lub przeniesienie danych następuje w języku, w jakim są one przetwarzane.
10. Informacje mogą zostać udzielone w sposób pisemny, w formie tradycyjnej lub elektronicznej.
11. Administrator danych osobowych jest uprawniony do odmowy podjęcia działań w związku z żądaniem klienta w sytuacji, gdy:
 - 1) żądanie ma zostać zrealizowane w formacie lub na nośniku nieznanym lub niestosowanym przez administratora danych osobowych,
 - 2) wniosek jest niejasny i klient składający wniosek, mimo prośby, nie wyjaśnił niejasności związanych z wnioskiem,
 - 3) tożsamość wnioskodawcy jest nieustalona i pomimo prób, nie udało się potwierdzić tożsamości wnioskodawcy,
 - 4) realizacja żądania mogłaby spowodować ujawnienie tajemnicy państwowej, tajemnicy służbowej lub tajemnicy przedsiębiorstwa administratora danych osobowych lub innej tajemnicy prawnie chronionej,
 - 5) klient zażąda wydania kopii danych lub przeniesienia danych w języku innym niż język, w jakim dane są przetwarzane.
12. Termin na realizację żądania klienta biegnie od dnia ustalenia tożsamości klienta lub złożenia przez klienta wyjaśnień lub uzupełnienia żądania.

Rozdział 3. Obowiązek informacyjny

§ 8.

1. W przypadku zbierania danych osobowych, jak również w przypadku zmiany celów przetwarzania danych osobowych w stosunku do celu, dla których dane osobowe zostały zebrane, administrator danych osobowych dopełnia obowiązku informacyjnego.
2. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, informacja jest przekazywana podczas pozyskiwania danych.
3. Zakres informacji o przetwarzaniu danych osobowych zbieranych bezpośrednio od osoby, której dane dotyczą, określa załącznik nr 3 do polityki.
4. W przypadku zbierania danych osobowych nie od osoby, której dane dotyczą:
 - 1) w rozsądnym terminie, nie później jednak niż w ciągu miesiąca od pozyskania danych,
 - 2) najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą,
 - 3) najpóźniej przy pierwszym ujawnieniu danych, jeżeli planuje się ujawnić dane osobowe innemu odbiorcy danych.
5. Zakres informacji o przetwarzaniu danych osobowych zbieranych nie od osoby, której dane dotyczą, określa załącznik nr 4 do polityki.
6. Odstępstwo od wypełnienia obowiązku informacyjnego w stosunku do osoby, której dane dotyczą, są możliwe, jeśli:
 - 1) klient posiada stosowne informacje,
 - 2) udzielenie informacji osobie, której dane zostały zebrane nie bezpośrednio od niej, jest niemożliwe lub wymagałoby niewspółmiernego dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych,
 - 3) pozyskanie lub ujawnienie danych osoby, której dane są zebrane nie bezpośrednio od niej,

uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów osoby, której dane dotyczą,

- 4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy państwowej, tajemnicy służbowej lub tajemnicy przedsiębiorstwa administratora lub innej tajemnicy prawnie chronionej.

Rozdział 4. Prawo dostępu do danych osoby, której dane dotyczą i do ich sprostowania

§ 9.

1. Osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy administrator danych osobowych przetwarza jego dane osobowe, a jeżeli ma to miejsce, osoba ta jest uprawniona do uzyskania dostępu do danych oraz następujących informacji o:
 - 1) celu przetwarzania, który powinien być konkretny, wyraźnie określony i prawnie uzasadniony,
 - 2) kategorii odnośnych danych osobowych,
 - 3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub mogą zostać ujawnione,
 - 4) w miarę możliwości planowany okres przetwarzania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu, przy założeniu, iż zapewnione zostanie ograniczenie okresu przechowywania danych do ścisłego minimum,
 - 5) prawie do żądania sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
 - 6) prawie wniesienia skargi do Prezesa Urzędu ochrony Danych Osobowych, jeżeli osoba, której dane dotyczą uważa, że przetwarzanie jego danych osobowych narusza jego prawa,
 - 7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – ich źródle,
 - 8) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, jeżeli jest realizowane, oraz o zasadach ich podejmowania, a także znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, związanych z przekazaniem.
3. Administrator danych osobowych może udostępnić klientom kanał, w którym klient będzie mógł samodzielnie pobrać dane w przypadku żądania klienta dostępu do danych. W przypadku złożenia przez klienta wniosku o uzyskanie dostępu do danych lub ich otrzymania, administrator danych osobowych jest uprawniony w pierwszej kolejności do skierowania klienta do skorzystania z takiego kanału.
4. Administrator danych osobowych dostarcza klientowi kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się klient, administrator danych osobowych może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów jej wytworzenia.
5. Jeżeli osoba, której dane dotyczą zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacja może zostać udzielona powszechnie stosowaną drogą elektroniczną.
6. Spełnienie obowiązku informacyjnego może nastąpić również przez wskazanie kategorii odbiorców uprawnionych do żądania dostępu do danych osobowych na podstawie przepisów prawa.

§ 10.

1. Osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących go danych osobowych, które są nieprawidłowe.
2. Osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Rozdział 5. Prawo do usunięcia danych lub ograniczenia ich przetwarzania

§ 11.

1. W przypadku, gdy osoba, której dane dotyczą, chce zrealizować uprawnienie do żądania usunięcia danych osobowych jej dotyczących, żądanie takie powinno być wyrażone w formie pisemnego, wyraźnego oświadczenia wskazującego przedmiotowy zakres żądania.
2. Administrator danych osobowych ustali okresy przechowywania danych, uwzględniając okres nie dłuższy, niż jest to niezbędne dla celów, w których dane są przetwarzane oraz okres dla przechowywania danych w celach archiwalnych lub statystycznych.
3. Administrator danych osobowych może nie uwzględnić żądania usunięcia danych wynikającego z cofnięcia zgody przez osobę, której dane dotyczą na przetwarzanie jej danych, w przypadku gdy zgoda osoby, której dane dotyczą nie była jedyną przesłanką przetwarzania jej danych, w szczególności, gdy celem przetwarzania danych klienta jest nadal realizacja umowy wiążącej osobę, której dane dotyczą i administratora danych osobowych albo gdy przetwarzanie danych osoby, której dane dotyczą jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze danych osobowych.
4. Przetwarzanie danych osobowych osoby, której dane dotyczą, pomimo jej żądania usunięcia danych, jest zgodne z prawem, jeżeli jest niezbędne w szczególności do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym, do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.
5. Po usunięciu danych zgodnie z żądaniem osoby, której dane dotyczą, administrator danych osobowych jest uprawniony do zachowania informacji o tym, czy i jaki wniosek wykonał. W tym celu może przetwarzać w szczególności imię i nazwisko, PESEL, adres do doręczeń wnioskującego, adres poczty elektronicznej, numer telefonu oraz informację o zakresie usuniętych danych i terminie ich usunięcia.

§ 12.

1. Żądanie ograniczenia przetwarzania danych powinno być złożone w formie wyraźnego oświadczenia osoby, której dane dotyczą, wskazującego przedmiotowy zakres swojego żądania.
2. Ograniczenie przetwarzania danych można realizować w szczególności poprzez oznaczenie w systemie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.
3. Administrator danych osobowych może dodatkowo, w celu ograniczenia przetwarzania danych osobowych, w szczególności:
 - 1) czasowo przenieść wybrane dane osobowe do innego systemu przetwarzania,
 - 2) uniemożliwić osobom zatrudnionym dostęp do wybranych danych,
 - 3) czasowo usunąć ze strony internetowej opublikowane dane,
 - 4) ograniczyć środkami technicznymi przetwarzanie w zautomatyzowanych zbiorach danych w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.

4. Administrator danych osobowych dokłada należytej staranności w celu wykonania ciążących na nim obowiązków związanych z ograniczeniem przetwarzania danych osobowych osoby, której dane dotyczą, a w szczególności dokonuje niezwłocznej weryfikacji prawidłowości przetwarzania danych w przypadku, złożenia żądania.
5. Administrator danych osobowych może przechowywać dane osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.
6. Realizacja żądania ograniczenia przetwarzania danych nie powoduje zaprzestania przetwarzania, które jest niezbędne do wykonania obowiązków wynikających z przepisów prawa, zaleceń lub rekomendacji Prezesa Urzędu ochrony Danych Osobowych oraz innych organów nadzorujących Gminne Centrum Kultury w Cewicach.

Rozdział 6. Prawo do przenoszenia danych

§ 13.

1. Osobie, której dane dotyczą przysługuje prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych go dotyczących oraz prawo do żądania przestania tych danych innemu administratorowi.
2. Osobie, której dane dotyczą przysługuje prawo do żądania przenoszenia danych go dotyczących, które dostarczył administratorowi danych osobowych, jeżeli dane te są przetwarzane na podstawie zgody osoby, której dane dotyczą lub na podstawie umowy, której klient jest stroną.
3. Dane podlegające przenoszeniu to dane przetwarzane w sposób zautomatyzowany. Przenoszeniu nie podlegają dane znajdujące się w zbiorach papierowych.
4. Dane podlegające przenoszeniu to dane, które zostały przekazane przez osobę, której dane dotyczą świadomie i aktywnie oraz dane wygenerowane przez działanie osoby, której dane dotyczą.
5. Dane niepodlegające przenoszeniu to dane wywnioskowane i/lub dane wywiedzione przez administratora danych osobowych na podstawie danych przekazanych przez osobę, której dane dotyczą, jak również dane pochodzące od osób trzecich.
6. W przypadku, gdy administrator danych osobowych nie ma możliwości oddzielenia danych, o których przeniesienie wnosi wnioskodawca, od innych danych znajdujących się w systemach informatycznych, administrator może się powstrzymać z wykonaniem żądania osoby do czasu uzgodnienia z nią ostatecznego zakresu jej żądania i złożenia przez nią odpowiednich oświadczeń (zgód) niezbędnych do umożliwienia przekazania danych w innym zakresie niż pierwotnie wnioskowany.
7. Osoba, której dane dotyczą może złożyć wniosek w celu skorzystania z przysługującego mu prawa do przenoszenia danych osobiście lub przez osobę upoważnioną. We wniosku osoba, której dane dotyczą obowiązana jest wskazać, jakie konkretnie dane osobowe objęte są żądaniem przeniesienia.

Rozdział 7. Prawo sprzeciwu

§ 14.

1. W przypadku wniesienia przez osobę, której dane dotyczą sprzeciwu, osoba, której dane dotyczą powinna wskazać, wobec jakiego konkretnego celu przetwarzania wnosi sprzeciw i wykazać, na czym polega jej szczególna sytuacja.
2. Administrator danych osobowych uwzględnia sprzeciw bądź odmawia jego uwzględnienia, po dokonaniu analizy, czy szczególna sytuacja osoby, której dane dotyczą, ma charakter nadrzędny wobec prawnie uzasadnionych podstaw do dokonywanego przetwarzania.

3. Odmawiając uwzględnienia sprzeciwu, administrator danych osobowych w przystępny sposób wyjaśnia osobie, której dane dotyczą przyczyny, dla których uważa, że interesy, prawa i wolności tej osoby, nie mają charakteru nadrzędnego.
4. Administrator danych osobowych może przetwarzać dane osobowe dla celów statystycznych, w przypadku złożenia przez osobę sprzeciwu wobec przetwarzania danych osobowych. W tym celu, osoba, której dane dotyczą powinna wykazać, na czym polega szczególny charakter jej sytuacji i jakie prawa osoby są zagrożone.
5. Po dokonaniu analizy szczególnej sytuacji tej osoby, administrator danych osobowych w zakresie dotyczącym osób, których dane dotyczą odmawia uwzględnienia sprzeciwu, w przypadku gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, w jasny i przystępny sposób wyjaśniając przyczyny odmowy.
6. W ramach realizacji prawa do sprzeciwu, administrator danych osobowych w zakresie dotyczącym osób, których dane dotyczą umożliwia złożenie sprzeciwu drogą elektroniczną, przy zachowaniu procedur bezpieczeństwa i identyfikacji osoby składającej żądanie.
7. Za złożenie sprzeciwu nie pobiera się opłat.

Rozdział 8. Zadania i obowiązki administratora danych osobowych

§ 15.

1. Przetwarzanie danych osobowych przez administratora danych osobowych odbywa się w systemie tradycyjnym, prowadzonym w formie papierowej lub w systemie informatycznym.
2. System tradycyjny tworzą zbiory danych zawarte w kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych oraz w innych dokumentach papierowych.
3. System informatyczny tworzą zbiory danych zawarte na nośnikach informatycznych takich jak dyski twarde, dyskietki, płyty CD lub DVD, pendrive, pamięć flash, taśmy magnetyczne lub inne urządzenia elektroniczne lub informatyczne.
4. Wykaz budynków, obiektów, pomieszczeń lub ich części oraz urządzeń, w których przetwarzane są dane osobowe, a także zabezpieczeń fizycznych, określa załącznik nr 5 do polityki.
5. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych (w przypadku zbiorów danych prowadzonych w systemie informatycznym), stanowi załącznik nr 6 do polityki.

§ 16.

1. Dane osobowe osób, których dane dotyczą nie mogą być przechowywane w formie umożliwiającej ich identyfikację przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
2. Po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, o których mowa w ust. 1, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba, że ich dalsze przechowywanie znajduje podstawę prawną.
3. Dalsze przetwarzanie danych osobowych jest dopuszczalne w przypadku ich przetwarzania dla prawnie uzasadnionego interesu, w celu
 - 1) realizacji działań zmierzających do zapewnienia ochrony i odporności systemów informatycznych,
 - 2) ciągłego i niezakłóconego prowadzenia działalności poprzez zapewnienie integralności kopii zarchiwizowanych/ zapasowych/ awaryjnych od momentu ich utworzenia aż do likwidacji,
 - 3) archiwizacyjnym (dowodowym) dla zabezpieczenia się przed różnymi rodzajami twierdzeń

i roszczeń (zarzutów), dotyczy to zwłaszcza danych osobowych znajdujących się we wnioskach niezakończonych zawarciem umowy,

- 4) realizacji zadań związanych z zapobieganiem przestępstwom dokonywanym na szkodę administratora danych osobowych, w tym w szczególności w celu zapobiegania oszustwom, a także zarządzania ryzykiem,
 - 5) wypełnienia zaleceń i rekomendacji Prezesa Urzędu ochrony Danych Osobowych,
 - 6) analityki działalności kulturalnej, celów naukowych lub do celów wewnętrznych analiz statystycznych,
 - 7) marketingu bezpośredniego.
4. Usunięcie danych osobowych osób, których dane dotyczą następuje np. poprzez ich zniszczenie lub anonimizację.

§ 17.

1. Administrator danych osobowych informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe osoby, której dane dotyczą.
2. Obowiązek o którym mowa w ust. 1 jest wyłączony, gdy zawiadomienie okaże się niemożliwe lub wymagać będzie niewspółmiernie dużego wysiłku, w szczególności gdy:
 - 1) zmiana, sprostowanie, ograniczenie lub usunięcie nie jest widoczne dla odbiorcy, w tym podmiotów przetwarzających, lecz wymaga ustanowienia odrębnego kanału komunikacji;
 - 2) odbiorca dalej nie funkcjonuje, został zlikwidowany lub wykreślony z rejestru (zakończył działalność),
 - 3) z okoliczności wynika, że dane nie będą dalej przetwarzane.
3. Administrator danych osobowych na żądanie osoby, której dane dotyczą, przekazuje informacje o odbiorcach, którym przekazano jego dane.
4. Jeśli obowiązek, o którym mowa w ust. 3, okaże się niewykonalny lub wymaga niewspółmiernie dużego wysiłku, administrator danych osobowych powinien udokumentować podjęcie racjonalnych działań, z uwzględnieniem dostępnych mu technologii i dostępnych mu środków, w tym technicznych, w celu wypełnienia tego obowiązku.

§ 18.

1. Administrator danych osobowych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Opis środków technicznych i organizacyjnych zawiera załącznik nr 7 do polityki.
3. Administrator danych osobowych zapewnia, aby przetwarzanie danych osobowych odbywało się:
 - 1) zgodnie z prawem, rzetelnie i w sposób przejrzysty,
 - 2) dla wyraźnych i prawnie uzasadnionych celów,
 - 3) w minimalnym zakresie,
 - 4) prawidłowo,
 - 5) z ograniczeniem przechowywania,

- 6) w sposób zapewniający integralność i poufność.
4. Administrator danych osobowych wyznacza IODO oraz wyznacza osobę, która zastępuje IODO w razie takiej konieczności. Osoba, która zastępuje IODO wykonuje zadania i obowiązki oraz uprawnienia IODO podczas wykonywania zastępstwa.
5. Administrator danych osobowych udostępnia treść polityki w trybie i na zasadach przyjętych dla publikowania regulaminu pracy.

§ 19.

1. Czynności związane z przetwarzaniem danych osobowych mogą wykonywać osoby upoważnione przez administratora danych osobowych, w okresie wskazanym w upoważnieniu.
2. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 8 do polityki.
3. Upoważnienie do przetwarzania danych osobowych podlega włączeniu do akt pracownika lub dokumentów związanych z inną podstawą zatrudnienia.
4. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do:
 - 1) zapoznania się z zasadami i przepisami określającymi obowiązki w zakresie prawidłowego przetwarzania danych osobowych i zapewniania bezpieczeństwa (ochrony) przetwarzanym danym, w tym z polityką,
 - 2) przetwarzania danych osobowych zgodnie z przepisami prawa i poszanowaniami polityki,
 - 3) zapewniania bezpieczeństwa (ochrony) przetwarzania danych osobowych,
 - 4) zgłaszania IODO wszelkich zdarzeń naruszających lub mogących naruszyć bezpieczeństwo (ochronę) danych osobowych.
5. Administrator danych osobowych może cofnąć upoważnienie do przetwarzania danych osobowych w każdym czasie.
6. Administrator danych osobowych cofa upoważnienie do przetwarzania danych osobowych w przypadku ustania podstawy do przetwarzania danych osobowych.
7. Zabrania się przetwarzania danych osobowych przez osobę, której administrator danych osobowych cofnął upoważnienie.
8. Administrator danych osobowych sprawuje kontrolę nad prawidłowością przetwarzania danych osobowych przez osoby upoważnione.

§ 20.

1. Administrator danych osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi („przetwarzający”).
2. Powierzenie przetwarzania danych osobowych następuje na podstawie zawartej umowy pomiędzy administratorem danych osobowych a przetwarzającym, w formie pisemnej pod rygorem nieważności. Wzór umowy określa załącznik nr 9 do polityki.
3. Przetwarzający jest zobowiązany do zapewnienia bezpieczeństwa (ochrony) przetwarzanych danych osobowych zgodnie z przepisami prawa oraz zgodnie z polityką, obowiązującą u administratora danych osobowych.
4. Przetwarzający może powierzyć czynności związane z przetwarzaniem danych osobowych osobom upoważnionym przez siebie, w okresie wskazanym w upoważnieniu.
5. Wzór upoważnienia do przetwarzania danych osobowych, stosowany przez przetwarzającego wymaga zatwierdzenia przez administratora danych osobowych, w formie pisemnej pod rygorem nieważności.

6. Osoby upoważnione do przetwarzania danych osobowych przez przetwarzającego są zobowiązane do:
 - 1) zapoznania się z zasadami i przepisami określającymi obowiązki w zakresie prawidłowego przetwarzania danych osobowych i zapewniania bezpieczeństwa (ochrony) przetwarzanym danym, w tym z polityką,
 - 2) przetwarzania danych osobowych zgodnie z przepisami prawa i poszanowaniami polityki,
 - 3) zapewniania bezpieczeństwa (ochrony) przetwarzania danych,
 - 4) zgłaszania IODO wyznaczonemu przez administratora danych osobowych wszelkich zdarzeń naruszających lub mogących naruszyć bezpieczeństwo (ochronę) danych osobowych ,
 - 5) wykonywania poleceń IODO wyznaczonemu przez administratora danych osobowych dotyczących zapewniania bezpieczeństwa (ochrony) danych osobowych ,
 - 6) udzielania IODO wyznaczonemu przez administratora danych osobowych informacji i udostępniania dokumentów lub innych dowodów w razie prowadzenia przez IODO postępowania w sprawie naruszenia bezpieczeństwa (ochrony) danych osobowych.
7. Przetwarzający może cofnąć upoważnienie do przetwarzania danych osobowych w każdym czasie.
8. Przetwarzający cofa upoważnienie do przetwarzania danych osobowych w przypadku ustania podstawy do przetwarzania danych osobowych.
9. Zabrania się przetwarzania danych osobowych przez osobę, której przetwarzający cofnął upoważnienie.
10. Administrator danych osobowych może żądać cofnięcia upoważnienia do przetwarzania danych osobowych wskazanej osobie, bez podania przyczyn, a przetwarzający jest zobowiązany do cofnięcia upoważnienia niezwłocznie i do powiadomienia administratora danych osobowych o dacie cofnięcia upoważnienia.
11. Administrator danych osobowych sprawuje kontrolę nad prawidłowością przetwarzania danych osobowych przez przetwarzającego.

Rozdział 9. Zadania i obowiązki IODO wyznaczonego przez administratora danych osobowych

§ 21.

1. IODO odpowiada za bezpieczeństwo (ochronę) danych osobowych przetwarzanych przez administratora danych osobowych oraz przez przetwarzającego.
2. IODO prowadzi postępowanie w sprawie praw osoby, której dane osobowe są przetwarzane przez administratora danych osobowych lub przetwarzającego.
3. Do zadań IODO należy:
 - 1) informowanie administratora, podmiotu przetwarzającego oraz osób zatrudnionych, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa i polityki, o trybach i zasadach zapewniania bezpieczeństwa (ochrony) danych osobowych i doradzanie im w tej sprawie, w szczególności w formie:
 - a) szkoleń,
 - b) instruktarzy,
 - c) wytycznych,

- 2) monitorowanie przestrzegania przepisów prawa i polityki w dziedzinie bezpieczeństwa (ochrony) danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia osób zatrudnionych uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty, w szczególności:
 - a) zbieranie informacji w celu identyfikacji procesów przetwarzania,
 - b) analizowanie i sprawdzanie zgodności przetwarzania,
 - c) informowanie, doradzanie i rekomendowanie określonych działań,
 - 3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, w szczególności
 - a) czy należy przeprowadzić ocenę skutków dla ochrony danych,
 - b) co do metodyki przeprowadzenia oceny skutków dla ochrony danych,
 - c) czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu,
 - d) co do zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą,
 - e) prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO
 - czy należy kontynuować przetwarzanie,
 - czy nie należy kontynuować przetwarzania,
 - jakie zabezpieczenia należy zastosować,
 - 4) współpraca z Prezesem Urzędu Ochrony Danych Osobowych,
 - 5) pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach, w szczególności w zakresie:
 - a) naruszeń bezpieczeństwa (ochrony) danych osobowych ,
 - b) konsultacji,
 - 6) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw, w szczególności w zakresie:
 - a) charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych,
 - b) ryzyka naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych, w tym naruszenia praw lub wolności o różnym prawdopodobieństwie i wadze zagrożenia,
 - c) doboru i wdrażania środków technicznych i organizacyjnych, służących bezpieczeństwu (ochronie) danych osobowych.
4. Do zadań IODO należy także prowadzenie:
- 1) rejestru upoważnień wydanych osobom zatrudnionym
 - 2) rejestru podmiotów, którym powierzono przetwarzanie danych osobowych,
 - 3) rejestru czynności przetwarzania danych osobowych, obejmującego w szczególności informacje:

- a) oznaczenie i dane kontaktowe
 - administratora danych osobowych,
 - IODO,
- b) cele przetwarzania danych osobowych,
- c) kategorie
 - osób, których dane dotyczą,
 - przetwarzanych danych, w odniesieniu do zidentyfikowanych celów,
- d) miejsce
 - zlokalizowania danych osobowych,
 - przekazywania danych osobowych, w tym kategorie odbiorców w odniesieniu do zidentyfikowanych celów,
- e) okres przetwarzania danych osobowych, ze wskazaniem przewidywanego terminu usunięcia poszczególnych kategorii danych,
- f) sposób zapewniania bezpieczeństwa (ochrony) danych osobowych, w formie ogólnego opisu środków technicznych i organizacyjnych.

wzór rejestru czynności określa załącznik nr 10 do polityki,

- 4) rejestru kategorii czynności, którego wzór określa załącznik nr 11 do polityki,
- 5) rejestru naruszeń, którego wzór określa załącznik nr 12 do polityki,
- 6) wykazu zbiorów danych osobowych,
- 7) wykazu budynków i zabezpieczeń fizycznych,
- 8) rejestru przypadków udostępniania danych osobowych, którego wzór określa załącznik nr 13 do polityki.

5. Do obowiązków IODO należy:

- 1) należyte wykonywanie zadań IODO,
- 2) nadzór nad przestrzeganiem bezpieczeństwa (ochrony) danych osobowych przetwarzanych w systemach informatycznych,
- 3) nadzór i kontrola nad prawidłowością działania systemów, w których przetwarzane są dane osobowe oraz nad prawidłowością postępowania osób przy nich zatrudnionych,
- 4) nadzór nad właściwym zabezpieczeniem budynków, obiektów, pomieszczeń oraz mebli i urządzeń, w których przetwarzane są dane osobowe,
- 5) nadzór nad wykorzystanym oprogramowaniem oraz jego legalnością,
- 6) dopuszczanie nośników danych do użytkowania,
- 7) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,
- 8) podejmowanie odpowiednich działań w celu właściwego zabezpieczania danych,
- 9) badanie naruszeń w systemie bezpieczeństwa (ochrony) danych osobowych,
- 10) podejmowanie decyzji w sprawie instalowania nowych mebli i urządzeń oraz oprogramowania wykorzystanego do przetwarzania danych osobowych lub wydawanie poleceń w tym zakresie,

- 11) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń, zawierających dane osobowe, w tym urządzeń informatycznych,
 - 12) definiowanie haseł dostępu lub wydawanie poleceń w tym zakresie,
 - 13) aktualizowanie oprogramowania antywirusowego i innego, chyba, że aktualizacje te wykonywane są automatycznie,
 - 14) wykonywanie kopii zapasowych danych osobowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności lub wydawanie poleceń w tym zakresie,
 - 15) wdrożenie wewnętrznych szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz stosowanych środków technicznych i organizacyjnych przy przetwarzaniu danych osobowych,
 - 16) sporządzanie raportów z naruszenia bezpieczeństwa (ochrony) danych osobowych oraz systemów przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w formie elektronicznej oraz w innej formie, niż elektroniczna,
 - 17) zapewnienie ochrony i bezpieczeństwa (ochrony) danych osobowych znajdujących się w systemach przetwarzania danych oraz w zbiorach danych, ze szczególnym uwzględnieniem dokumentacji działalności statutowej,
 - 18) niezwłoczne informowanie administratora danych osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych oraz naruszenia przepisów prawa i polityki,
 - 19) podejmowanie, stosownych działań w przypadku wykrycia nieuprawnionego dostępu do danych osobowych lub bazy danych albo naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych zgromadzonych i utrwalonych w formie elektronicznej oraz w innej formie, niż elektroniczna,
 - 20) zapewnienie fizycznego bezpieczeństwa (ochrony) systemów, w których przetwarzane są dane osobowe lub wydawanie poleceń w tym zakresie,
 - 21) zapewnienie bezpieczeństwa funkcjonowania wszystkich urządzeń pracujących w systemach, w których przetwarzane są dane osobowe lub wydawanie poleceń w tym zakresie,
 - 22) zapewnienie dostępu do systemu, w którym przetwarzane są dane osobowe wyłącznie osobom uprawnionym lub wydawanie poleceń w tym zakresie,
 - 23) ustalanie podmiotów, z którymi komunikacja elektroniczna została uznana za niebezpieczną.
6. IODO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:
- 1) imię i nazwisko osoby upoważnionej,
 - 2) datę nadania i ustania upoważnienia,
 - 3) zakres przedmioty upoważnienia,
 - 4) potwierdzenie zapoznania się z zasadami i przepisami określającymi obowiązki w zakresie prawidłowego przetwarzania danych osobowych i zapewniania bezpieczeństwa przetwarzanym danym, w tym z polityką.
7. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych określa załącznik nr 14 do polityki.

§ 22.

1. W razie stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa (ochrony) danych osobowych oraz w razie powzięcia wiadomości o naruszeniu lub o podejrzeniu naruszenia bezpieczeństwa (ochrony) danych osobowych IODO:
 - 1) dokonuje zabezpieczenia danych osobowych lub wydaje polecenia w sprawie ich zabezpieczenia,
 - 2) ustala przyczyny, okoliczności oraz skutki naruszenia lub zagrożenia naruszeniem,
 - 3) rejestruje naruszenie bezpieczeństwa (ochrony) danych osobowych w rejestrze naruszeń.
2. IODO jest uprawniony do pozyskiwania informacji od:
 - 1) osoby, która zgłosiła naruszenie lub zagrożenie naruszeniem bezpieczeństwa (ochrony) danych osobowych ,
 - 2) osoby, która była upoważniona do przetwarzania danych osobowych, których bezpieczeństwo zostało naruszone lub wystąpiło zagrożenie naruszeniem,
 - 3) osoby nadzorującej pracę osoby, która zgłosiła naruszenie lub zagrożenie naruszeniem bezpieczeństwa (ochrony) danych osobowych lub osoby, która była upoważniona do przetwarzania danych osobowych, których bezpieczeństwo zostało naruszone lub wystąpiło zagrożenie naruszeniem
 - 4) osoby podlegającej osobie, która zgłosiła naruszenie lub zagrożenie naruszeniem bezpieczeństwa (ochrony) danych osobowych lub osoby, która była upoważniona do przetwarzania danych osobowych, których bezpieczeństwo zostało naruszone lub wystąpiło zagrożenie naruszeniem
 - 5) osoby, której dane osobowe podlegały naruszeniu lub zagrożeniu naruszeniem bezpieczeństwa,
 - 6) osoby, która posiada wiedzę o naruszeniu lub zagrożeniu naruszeniem bezpieczeństwa (ochrony) danych osobowych.
3. IODO jest uprawniony do pozyskiwania dowodów co do naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych :
 - 1) z dokumentów,
 - 2) z wystuchań/ zeznań/ wyjaśnień,
 - 3) z monitoringu wizyjnego,
 - 4) z monitoringu poczty elektronicznej,
 - 5) z oględzin,
 - 6) z innych źródeł.
4. IODO jest uprawniony do pozyskiwania, za zgodą administratora danych osobowych, opinii ekspertów.
5. IODO sporządza i przedkłada administratorowi danych osobowych do zatwierdzenia sprawozdanie z postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych .
6. Sprawozdanie z postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych zawiera ocenę charakteru naruszenia lub zagrożenia naruszeniem oraz wnioski co do zgłoszenia naruszenia bezpieczeństwa (ochrony) danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych.

7. Instrukcję postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych określa załącznik nr 15 do polityki.
8. Wzór sprawozdania z postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych określa załącznik nr 16 do polityki.

§ 23.

1. IODO przeprowadza kontrole oraz dokonuje ocen stanu bezpieczeństwa (ochrony) danych osobowych.
2. IODO dokonuje, nie rzadziej niż raz na pół roku:
 - 1) kontroli prawidłowości
 - a) konfiguracji sprzętu komputerowego,
 - b) instalacji i użytkowania oprogramowania i aplikacji, wykorzystywanych do przetwarzania danych osobowych,
 - c) instalacji i użytkowania oprogramowania chroniącego dane osobowe przez nieuprawnionym dostępem,
 - d) instalacji i użytkowania oprogramowania antywirusowego,
 - 2) kontroli bezpieczeństwa (ochrony) systemów, w których przetwarzane są dane osobowe,
 - 3) kontroli bezpieczeństwa (ochrony) programów i aplikacji, wykorzystywanych do przetwarzania danych osobowych,
 - 4) kontroli bezpieczeństwa (ochrony) nośników danych osobowych,
 - 5) kontroli bezpieczeństwa (ochrony) kopii zapasowych danych osobowych i ich przydatności do odtwarzania,
 - 6) kontroli systemu bezpieczeństwa (ochrony) danych osobowych, w tym kontroli prawidłowości postępowania w zakresie nadawania i cofania upoważnień, loginów i haseł uprawniających do przetwarzania danych osobowych i dostępu do systemów, w których są przetwarzane,
 - 7) kontroli prawidłowości postępowania przy usuwaniu danych osobowych,
 - 8) kontroli prawidłowości postępowania przy przekazywaniu urządzeń lub nośników danych osobowych innym podmiotom, w szczególności do przeglądu lub naprawy,
 - 9) analizy zagrożeń bezpieczeństwa (ochrony) danych osobowych.
3. IODO przedstawia administratorowi danych osobowych raport ze stanu bezpieczeństwa (ochrony) danych osobowych, w terminie 30 dni od zakończenia półrocza, zawierający sprawozdanie z dokonanych w poprzednim kwartale czynności kontrolnych i analiz oraz wnioski dotyczące działania i poprawy systemu bezpieczeństwa (ochrony) danych osobowych. Wzór raportu określa załącznik nr 17 do polityki.

Rozdział 10. Szacowanie ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych

§ 24.

IODO szacuje ryzyko naruszenia bezpieczeństwa (ochrony) danych osobowych poprzez dokonywanie:

- 1) identyfikacji ryzyka,
- 2) analizy ryzyka,
- 3) oceny skutków ryzyka.

§ 25.

1. IODO przeprowadza ocenę skutków dla bezpieczeństwa (ochrony) danych osobowych, w szczególności:
 - 1) w przypadku przetwarzania danych osobowych na podstawie przepisów prawa,
 - 2) w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych,
 - 3) przed wdrożeniem lub użyciem nowych rozwiązań technologicznych lub organizacyjnych (technologii, systemów, procesów, funkcjonalności lub zmian),
 - 4) przed rozpoczęciem profilowania danych osobowych Klientów niezależnie od celu, dla którego będzie to robione, które jest podstawą do decyzji wywołującej skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływające na osobę fizyczną,
 - 5) w przypadku nabycia zbiorów danych od innego administratora danych,
 - 6) w przypadku naruszenia ochrony danych osobowych,
 - 7) przed przetwarzaniem danych biometrycznych lub innych szczególnych kategorii danych osoby, której dane dotyczą, w celu podjęcia decyzji wobec tej osoby,
 - 8) przed wprowadzeniem nowego przedsięwzięcia,
 - 9) w przypadku stwierdzenia wysokiego poziomu ryzyka naruszenia bezpieczeństwa (ochrony) danych..
2. IODO przeprowadza ocenę skutków dla bezpieczeństwa (ochrony) danych osobowych dla następujących rodzajów operacji przetwarzania danych osobowych, nie obejmujących czynności przetwarzania związanych z oferowanymi przedsięwzięciami osobom, których dane dotyczą lub z monitorowaniem ich zachowania:
 - 1) ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych,
 - 2) zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki,
 - 3) systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie, wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni; do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa,
 - 4) przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych),
 - 5) dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy:
 - a) liczby osób, których dane są przetwarzane,
 - b) zakresu przetwarzania,
 - c) okresu przechowywania danych,
 - d) geograficznego zakresu przetwarzania,
 - 6) przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł,
 - 7) przetwarzanie danych dotyczących osób, których ocena i świadczone im przedsięwzięcia są uzależnione od podmiotów lub osób, które dysponują uprawnieniami władczymi i / lub

oceniającymi,

- 8) innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych,
 - 9) gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z przedsięwzięcia lub umowy.
3. Ocena skutków dla bezpieczeństwa (ochrony) danych osobowych, powinna obejmować w szczególności:
- 1) ocenę zgodności z RODO wszystkich procesów przetwarzania danych osobowych u administratora danych osobowych lub przetwarzającego,
 - 2) niezbędność operacji przetwarzania danych osobowych,
 - 3) ocenę proporcjonalności ingerencji w prywatność związanej z przetwarzaniem danych osobowych do celów przetwarzania.

§ 26.

1. Na podstawie oceny prawdopodobieństwa wystąpienia ryzyka i oceny skutków ryzyka IODO dokonuje oceny ryzyka.
2. Do ustalenia poziomu prawdopodobieństwa wystąpienia ryzyka naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych dotyczą oraz poziomu skutków naruszenia stosuje się postanowienia Polityki Zarządzania Ryzykiem W Gminnym Centrum Kultury W Cewicach, z zastrzeżeniem ust. 3 i 4.
3. Poziom skutków ryzyka naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych ustala się odrębnie dla:
 - 1) dostępności informacji,
 - 2) integralności,
 - 3) poufności.
4. Poziom ryzyka ustala się jako iloczyn poziomu prawdopodobieństwa jego wystąpienia oraz sumy poziomów skutków naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych.

§ 27.

1. Ryzyko naruszenia praw i wolności osób fizycznych jest obecne, kiedy naruszenie bezpieczeństwa (ochrony) ochrony danych osobowych może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. w szczególności:
 - 1) dyskryminacja,
 - 2) kradzież tożsamości lub oszustwo dotyczące tożsamości,
 - 3) nadużycia finansowe,
 - 4) straty finansowe,
 - 5) nieuprawnione cofnięcie pseudonimizacji,
 - 6) utrata poufności danych osobowych chronionych tajemnicą zawodową,
 - 7) naruszenie dobrego imienia.
 - 8) inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

2. Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić przez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej i rzeczowej analizy, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.
3. Jeżeli naruszenie bezpieczeństwa (ochrony) danych osobowych dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, uznaje się, że występuje duże prawdopodobieństwo szkody, o której mowa w ust. 1.

§ 28.

1. IODO ustala kryteria akceptacji ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych i przedkłada administratorowi danych osobowych do zatwierdzenia.
2. IODO ustala i wdraża procedury postępowania ukierunkowane na unikanie ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych oraz obniżanie jego poziomu.
3. IODO przedkłada administratorowi danych osobowych propozycje zabezpieczenia się przed wystąpieniem ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych poprzez ubezpieczenie.

Rozdział 11. Zadania i obowiązki osób zatrudnionych w Gminnym Centrum Kultury w Cewicach

§ 29.

1. Wszystkie osoby zatrudnione w Gminnym Centrum Kultury w Cewicach, bez względu na podstawę prawną zatrudnienia, łącznie zwane „osobami zatrudnionymi” mają obowiązek przestrzegać postanowień zawartych w polityce.
2. Każda osoba jest zobowiązana do zapoznania się z przepisami dotyczącymi ochrony danych osobowych, w tym z polityką, przed podjęciem czynności obejmujących przetwarzanie danych osobowych.
3. Fakt zapoznania się zostaje potwierdzony poprzez złożenie podpisu pod oświadczeniem o zapoznaniu się i zobowiązaniu do przestrzegania.
4. Oświadczenie o zapoznaniu się i zobowiązaniu do przestrzegania bezpieczeństwa przetwarzania danych osobowych podlega włączeniu do akt pracownika lub dokumentów związanych z inną podstawą zatrudnienia.

§ 30.

1. Osoby zatrudnione zobowiązane są dbać o bezpieczeństwo (ochronę) danych osobowych powierzonych im do przetwarzania, archiwizowania lub przechowywania, zgodnie z obowiązującą w polityką, w tym w szczególności:
 - 1) chronić dane osobowe przed dostępem osób nieupoważnionych,
 - 2) chronić dane osobowe przed przypadkowym zniszczeniem, utratą lub modyfikacją,
 - 3) chronić nośniki zawierające dane osobowe, w szczególności nośniki magnetyczne, optyczne, nośniki pamięci oraz wszelkiego rodzaju druki i wydruki, przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
 - 4) utrzymywać w tajemnicy login i hasła, częstotliwość ich zmiany oraz szczegóły technologiczne, także po ustaniu zatrudnienia w Gminnym Centrum Kultury w Cewicach,
 - 5) archiwizować dane osobowe zgodnie z przepisami i zasadami archiwizowania.

2. Osoba zatrudniona, ma obowiązek sprawdzić przed rozpoczęciem wykonywania czynności, czy stan budynku, pomieszczenia, mebla, urządzenia lub nośnika danych nie wskazuje na naruszenie lub próbę naruszenia bezpieczeństwa (ochrony) danych osobowych .
3. Każde zakończenie wykonywania czynności, w ramach których przetwarzane są dane osobowe, wymaga zabezpieczenia danych osobowych.

§ 31.

Osoba zatrudniona zobowiązana jest do współdziałania z IODO w zakresie identyfikacji, analizy i oceny ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych.

§ 32.

1. Osoba, która stwierdziła naruszenie bezpieczeństwa (ochrony) danych osobowych lub przypuszcza, że do naruszenia bezpieczeństwa (ochrony) danych osobowych mogło lub może dojść, jest zobowiązana do niezwłocznego powiadomienia IODO.
2. Osoba zatrudniona zobowiązana jest do udzielania pomocy IODO oraz do realizowania jego zaleceń dotyczących bezpieczeństwa (ochrony) danych osobowych .
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z polityki mogą być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych lub rażące nienależyte wykonanie zobowiązania, w szczególności przez osobę, która nie powiadomiła IODO o przypadku naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych .

§ 33.

1. Zabrania się:
 - 1) ujawniać dane osobowe, w tym dane zawarte w obsługiwanych systemach,
 - 2) kopiować dane osobowe , bazy danych lub ich części bez wyraźnego upoważnienia,
 - 3) kopiować
 - a) oprogramowanie i aplikacje wykorzystywane do przetwarzania danych osobowych,
 - b) oprogramowanie uniemożliwiające nieuprawniony dostęp do danych osobowych,
 - c) oprogramowanie antywirusowe,
 - 4) instalować bez upoważnienia:
 - a) oprogramowanie i aplikacje wykorzystywane do przetwarzania danych osobowych,
 - b) oprogramowanie uniemożliwiające nieuprawniony dostęp do danych osobowych,
 - c) oprogramowanie antywirusowe,
 - 5) przetwarzać dane w sposób inny, niż wynikający z obowiązujących przepisów prawa i polityki,
 - 6) udostępniać dane osobowe w formie transmisji elektronicznej bez uprzedniego zabezpieczenia danych przed nieuprawnionym dostępem,
 - 7) używać nośniki danych niedopuszczone do użytkowania przez IODO,
 - 8) udostępniać innej osobie, przypisany sobie login, hasło lub inny regulator dostępu, określający zakres upoważnień do przetwarzania danych osobowych,
 - 9) otwierać wiadomości poczty elektronicznej oraz załącznik do wiadomości pochodzący od podmiotu nieznanego lub podmiotu, z którym komunikacja została uznana za niebezpieczną,

- 10) wyłączać lub blokować oprogramowanie uniemożliwiające nieuprawniony dostęp do danych osobowych lub oprogramowanie antywirusowe,
 - 11) usuwać lub odinstalowywać oprogramowanie uniemożliwiające nieuprawniony dostęp do danych osobowych lub oprogramowanie antywirusowe,
 - 12) pozostawiać budynki, obiekty, pomieszczenia, meble, urządzenia lub nośniki danych bez zabezpieczenia ich przed nieuprawnionym dostępem.
2. Naruszenie zakazu, o którym mowa w ust. 1 stanowi ciężkie naruszenie podstawowego obowiązku pracowniczego lub rażące naruszenie obowiązku należytego wykonywania zobowiązania.

Rozdział 12. Podstawowe sposoby zabezpieczenia danych osobowych

§ 34.

Administrator danych osobowych stosuje następujące kategorie zabezpieczeń przed ryzykiem naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych:

- 1) organizacja bezpieczeństwa (ochrony) danych osobowych i bezpieczeństwa (ochrony) informacji,
- 2) bezpieczeństwo osób zatrudnionych,
- 3) zarządzanie aktywami,
- 4) kontrola dostępu,
- 5) kryptografia,
- 6) bezpieczeństwo fizyczne i środowiskowe,
- 7) bezpieczna eksploatacja,
- 8) bezpieczeństwo komunikacji,
- 9) pozyskiwanie, rozwój i utrzymanie systemów,
- 10) relacje z dostawcami, odbiorcami i innymi podmiotami,
- 11) zarządzanie incydentami związanymi z bezpieczeństwem(ochroną) danych osobowych i bezpieczeństwem (ochroną) informacji,
- 12) aspekty bezpieczeństwa (ochrony) danych osobowych i bezpieczeństwa (ochrony) informacji w zarządzaniu ciągłością działania.

Rozdział 13. Przetwarzanie danych w systemie tradycyjnym

§ 35.

1. Podstawowym sposobem zabezpieczenia danych przetwarzanych w systemie tradycyjnym, jest ograniczenie dostępu do danych za pomocą elementów:
 - 1) zabezpieczeń fizycznych, w szczególności poprzez składowanie nośników danych w urządzeniach, meblach lub pomieszczeniach do tego przeznaczonych oraz dokonywanie zamknięć tych urządzeń, mebli lub pomieszczeń,
 - 2) zabezpieczeń organizacyjnych, w szczególności poprzez stosowanie wydanych upoważnień dostępu do danych.
2. Przetwarzanie danych osobowych w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy wykonywać w taki sposób, aby uniemożliwić osobom nieuprawnionym wgląd w dane.

3. Zbiory danych osobowych w systemie tradycyjnym są zabezpieczane przed utratą, uszkodzeniem lub ujawnieniem albo innym zagrożeniem, w szczególności za pomocą:
 - 1) urządzeń zabezpieczających przed zalaniem, pożarem, zniszczeniem przez gryzonie lub inne istoty żywe albo innym zdarzeniem losowym o ile jest to możliwe,
 - 2) zabezpieczenia fizycznego uniemożliwiającego nieuprawniony dostęp do danych,
4. Niedopuszczalne jest zakończenie pracy w systemie tradycyjnym bez zabezpieczenia danych osobowych przed utratą, zniszczeniem, uszkodzeniem lub innym zagrożeniem.

Rozdział 14. Przetwarzanie danych w systemie informatycznym

§ 36.

1. Podstawowym sposobem zabezpieczenia danych przetwarzanych w systemie informatycznym jest stosowanie zdefiniowanych loginów i haseł, określających zakres upoważnień do przetwarzania danych osobowych.
2. Przetwarzanie danych osobowych w systemie informatycznym wymaga uprzedniego zalogowania się do tego systemu przy użyciu imiennie przypisanego loginu i hasła.
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po :
 - 1) podaniu loginu użytkownika i właściwego hasła w przypadku obsługi programu BIP,
 - 2) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi programów RADIX- Kadry, RADIX-Płace, PŁATNIK lub innych programów aplikacji, w których przetwarzane są dane osobowe.
4. IODO przypisuje loginy i hasła poszczególnym osobom zgodnie z ich zakresem upoważnienia.
5. Login użytkownika nie podlega zmianie.
6. Login użytkownika nie może być przypisany innemu użytkownikowi.
7. Hasło przypisane danej osobie podlega zmianie nie rzadziej, niż co kwartał od dnia jego ustanowienia.
8. W przypadku cofnięcia upoważnienia do przetwarzania danych osobowych, IODO powoduje wygaśnięcie loginu i hasła użytkownika.

§ 37.

1. Rozpoczęcie pracy w programie komputerowym lub aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji programu lub aplikacji.
2. Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji.
3. Niedopuszczalne jest zakończenie pracy w systemie informatycznym bez wykonania pełnej i poprawnej operacji wylogowania i poprawnego zamknięcia systemu lub programu albo aplikacji.
4. Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe, należy ustawić w taki sposób, aby uniemożliwić osobom nieuprawnionym wgląd w dane.

§ 38.

1. Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą, zniszczeniem, uszkodzeniem lub innym zagrożeniem za pomocą:
 - 1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej, o ile jest to możliwe,
 - 2) sporządzanie kopii zapasowych (kopie pełne),
 - 3) oprogramowania uniemożliwiającego nieuprawniony dostęp do danych,
 - 4) oprogramowania antywirusowego.
2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku, z zastrzeżeniem ust. 3.
3. W uzasadnionych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu.

§ 39.

1. Zmiana:
 - 1) konfiguracji sprzętu komputerowego,
 - 2) oprogramowania i aplikacji, wykorzystywanych do przetwarzania danych osobowych,
 - 3) oprogramowania chroniącego dane osobowe przez nieuprawnionym dostępem,
 - 4) oprogramowania antywirusowego,dokonywana jest przez lub za zgodą IODO.
2. Zgoda IODO, o której mowa w ust. 1 umieszczana jest w dokumentacji komputera, oprogramowania lub aplikacji.

Rozdział 15. Postępowanie z nośnikami danych osobowych

§ 40.

1. Kopie danych osobowych przetwarzanych w systemie tradycyjnym lub informatycznym umieszcza się na nośnikach danych osobowych.
2. Dostęp do nośników danych osobowych ma wyłącznie osoba upoważniona.
3. Okres przechowywania nośników zawierających dane osobowe ustala się w instrukcji kancelaryjnej Gminnego Centrum Kultury w Cewicach.
4. Nośniki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom nieupoważnionym.
5. Przemieszczanie nośników danych osobowych wymaga upoważnienia.

§ 41.

1. Urządzenia lub nośniki danych osobowych, przeznaczone do:
 - 1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
 - 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
 - 3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich

odzyskanie, albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych osobowych lub w inny sposób gwarantujący zachowanie poufności tych danych.

2. Nośniki zawierające dane osobowe po ich wykorzystaniu są niszczone w sposób uniemożliwiający odczytanie znajdujących się na nich danych.
3. Do postępowania z nośnikami danych osobowych stosuje się odpowiednio postanowienia obowiązujące w Gminnym Centrum Kultury w Cewicach:
 - 1) regulamin pracy,
 - 2) instrukcja kancelaryjna,
 - 3) instrukcja archiwalna,
 - 4) zarządzanie ryzykiem,
 - 5) kontrola zarządcza.

Rozdział 16. Zdarzenia naruszające lub grożące naruszeniem bezpieczeństwa (ochrony) danych osobowych

§ 42.

1. Do zdarzeń naruszających bezpieczeństwo (ochrona) danych osobowych lub grożących takim naruszeniem należą w szczególności:
 - 1) zagrożenia losowe zewnętrzne (np. pożar, powódź, zniszczenie przez gryzonie, brak zasilania itp.), które mogą prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, w którym przetwarzane są dane osobowe oraz zakłócenia ciągłości jego pracy,
 - 2) zagrożenia losowe wewnętrzne (np. pomyłki, błędy i inne naruszenia obowiązków, awarie urządzeń, awarie oprogramowania itp.), które mogą prowadzić do zniszczenia danych, zakłócić ciągłość pracy systemu w którym przetwarzane są dane osobowe, powodować naruszenie poufności danych, integralności danych oraz ich prawidłowości,
 - 3) zagrożenia zamierzone, świadome i celowe, które polegać mogą na nieuprawnionym dostępie do systemu, w którym przetwarzane są dane osobowe, nieuprawnionym przekazaniu danych osobowych, pogorszeniu jakości pracy urządzenia lub oprogramowania, bezpośrednim zagrożeniu materialnych składników systemu, w którym przetwarzane są dane osobowe.
2. Do przypadków kwalifikowanych jako naruszenie lub uzasadnione podejrzenie naruszenia bezpieczeństwa (ochrony) danych osobowych, w tym zabezpieczenia systemu, w którym przetwarzane są dane osobowe, należą w szczególności:
 - 1) sytuacje losowe, nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. pożar, zalanie pomieszczeń, katastrofa budowlana, itp.),
 - 2) naruszenie obowiązków w zakresie przestrzegania przepisów i zasad bezpieczeństwa (ochrony) danych osobowych (np. prace na danych osobowych w celach prywatnych, nie zabezpieczenie pomieszczenia, w którym znajduje się urządzenie albo element wyposażenia do przechowywania danych osobowych, itp.),
 - 3) niewłaściwe parametry środowiska, w którym pracuje urządzenie (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od innych urządzeń itp.),
 - 4) awaria urządzenia lub oprogramowania lub elementu wyposażenia do przechowywania danych osobowych, a także niewłaściwe działanie serwisu,

- 5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
 - 6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
 - 7) próba modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia,
 - 8) niedopuszczalna manipulacja danymi osobowymi w systemie,
 - 9) ujawnienie osobom nieupoważnionym danych osobowych lub sposobów zabezpieczenia danych osobowych albo innych strzeżonych elementów systemu bezpieczeństwa (ochrony) danych osobowych,
 - 10) odstępstwa od założonego rytmu pracy wskazujące na złamanie lub zaniechanie ochrony danych osobowych, w tym praca przy komputerze lub w sieci osoby, która nie jest upoważniona do jego obsługi, sygnał o uporczywych nieautoryzowanych próbach logowania, itp.,
 - 11) istnienie nieautoryzowanych kont dostępu do danych,
 - 12) nieuprawnione otwarcie budynku, obiektu, pomieszczenia lub mebla,
 - 13) nieuprawnione uruchomienie urządzenia,
 - 14) nieuprawnione przemieszczenie nośnika danych,
 - 15) sygnalizacje z oprogramowania uniemożliwiającego nieuprawniony dostęp do danych osobowych,
 - 16) sygnalizacje z oprogramowania antywirusowego.
3. W szczególności do naruszenia mogą prowadzić następujące sytuacje:
- 1) utrata danych osobowych uniemożliwiająca wykonanie zobowiązania,
 - 2) naruszenie integralności danych osobowych niosące ryzyko błędnego wykonania zobowiązania,
 - 3) utrata poufności danych osobowych,
- a będące następstwem:
- 4) skompromitowania lub błędnego działania systemu informatycznego,
 - 5) zdarzeń losowych/ środowiskowych,
 - 6) niepożądanych (sabotażowych/ dezorganizacyjnych) działań osób, w tym osób trzecich (kradzież, zniszczenie, uniemożliwienie dostępu, modyfikacja, ujawnienie danych itp.),
 - 7) błędu ludzkiego, w tym w ramach niewłaściwego postępowania osoby zatrudnionej, w zakresie zabezpieczenia danych osobowych.
4. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc, mebli (szaf, regałów i sejfów) oraz urządzeń służących do przechowywania danych osobowych na papierowych nośnikach, wydrukach, lub elektronicznych nośnikach zewnętrznych tych danych.

Rozdział 17. Powiadomienia o naruszeniu bezpieczeństwa (ochrony) danych osobowych

§ 43.

1. Naruszenie bezpieczeństwa (ochrony) danych osobowych rozpatrywane jest jako zdarzenie występujące w ramach ryzyka, które należy rozumieć jako możliwość wystąpienia straty

wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych.

2. Naruszeniem bezpieczeństwa (ochrony) danych osobowych jest naruszenie 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 w ramach działalności prowadzonej przez administratora danych osobowych.
3. Za naruszenie bezpieczeństwa (ochrony) danych osobowych podlegające obowiązkowi zgłoszenia:
 - 1) Prezesowi Urzędu ochrony Danych Osobowych – uznaje się sytuację, w której ryzyko naruszenia praw lub wolności osób fizycznych zostało oszacowane na poziomie wyższym niż niski,
 - 2) osobie, której dane dotyczą - uznaje się sytuację, w której ryzyko naruszenia praw lub wolności osób fizycznych zostało oszacowane na poziomie wysokim, w szczególności poprzez:
 - a) niekontrolowane ujawnienie danych,
 - b) niekontrolowane ujawnienie uprawnień, w tym loginów lub haseł dostępu do systemu przetwarzania danych osobowych,
 - c) niekontrolowane wtargnięcie do obszaru przetwarzania danych osobowych.
4. Obowiązek notyfikacji powinien zostać wykonany bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Przez stwierdzenie naruszenia uznaje się godzinę, w której IODO przedstawił administratorowi danych osobowych sprawozdanie z postępowania w sprawie naruszenia bezpieczeństwa (ochrony) danych osobowych.
5. W przypadku niedotrzymania powyższego terminu do zgłoszenia należy dołączyć wyjaśnienie przyczyny opóźnienia.
6. Zawiadomienie o naruszeniu bezpieczeństwa (ochrony) danych osobowych nie jest konieczne, jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W takim przypadku IODO dokonuje adnotacji w rejestrze naruszeń, z podaniem przyczyny, z powodu której administrator danych osobowych uznał, że naruszenie bezpieczeństwa (ochrony) danych osobowych nie wymaga zawiadomienia.
7. Zawiadomienie osoby fizycznej nie jest konieczne, jeśli wdrożono adekwatne środki ochrony obejmując nimi dane osobowe, których dotyczy naruszenie oraz zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
8. Wzór zawiadomienia osoby fizycznej o naruszeniu bezpieczeństwa (ochrony) danych osobowych określa załącznik nr 18 do polityki.
9. W przypadku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych stosuje się formularze udostępnione przez Urząd Ochrony Danych Osobowych.

Rozdział 18. Wykaz załączników do polityki bezpieczeństwa (ochrony) danych osobowych

1. Załącznik nr 1 Wzór zgody na przetwarzania danych osobowych
2. Załącznik nr 2 Formularz ustalenia przetwarzania danych osobowych w związku z przedsięwzięciem

3. Załącznik nr 3 Zakres informacji o przetwarzaniu danych osobowych zbieranych bezpośrednio od osoby, której dane dotyczą
4. Załącznik nr 4 Zakres informacji o przetwarzaniu danych osobowych zbieranych nie od osoby, której dane dotyczą
5. Załącznik nr 5 Wykaz budynków, obiektów, pomieszczeń lub ich części oraz urządzeń, w których przetwarzane są dane osobowe, a także zabezpieczeń fizycznych
6. Załącznik nr 6 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych (w przypadku zbiorów danych prowadzonych w systemie informatycznym)
7. Załącznik nr 7 Opis środków technicznych i organizacyjnych
8. Załącznik nr 8 Wzór upoważnienia do przetwarzania danych osobowych
9. Załącznik nr 9 Wzór umowy o powierzenie przetwarzania danych osobowych
10. Załącznik nr 10 Wzór rejestru czynności
11. Załącznik nr 11 Wzór rejestru kategorii czynności
12. Załącznik nr 12 Wzór rejestru naruszeń
13. Załącznik nr 13 Wzór rejestru przypadków udostępniania danych osobowych
14. Załącznik nr 14 Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
15. Załącznik nr 15 Instrukcja postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych
16. Załącznik nr 16 Wzór sprawozdania z postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych
17. Załącznik nr 17 Wzór raportu ze stanu bezpieczeństwa (ochrony) danych osobowych
18. Załącznik nr 18 Wzór zawiadomienia osoby fizycznej o naruszeniu bezpieczeństwa (ochrony) danych osobowych

Załącznik nr 1 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór zgody na przetwarzanie danych osobowych

.....
Miejscowość, data

.....
Imię i nazwisko

.....
PESEL

.....
Adres do doręczeń

ZGODA

Wyrażam zgodę na przetwarzania moich danych osobowych przez Gminne Centrum Kultury w Cewicach w następujących celach i odpowiadających tym celom zakresach moich danych osobowych:

Lp.	Cel przetwarzania danych osobowych	Zakres danych osobowych

.....
czytelny podpis osoby składającej oświadczenie

Załącznik nr 2 do polityki bezpieczeństwa (ochrony) danych osobowych
Formularz ustalenia przetwarzania danych osobowych w związku z przedsięwzięciem

.....
Miejscowość, data

.....
Imię i nazwisko

.....
stanowisko

INFORMACJA o PRZETWARZANIU DANYCH OSOBOWYCH w ZWIĄZKU z REALIZACJĄ PRZEDSIĘWZIĘCIA

1. Oznaczenie przedsięwzięcia
2. Osoba odpowiedzialna za
 - 1) Organizację przedsięwzięcia
 - 2) Prowadzenie przedsięwzięcia
 - 3) Rozliczenie przedsięwzięcia
3. Organizacja i przeprowadzenie przedsięwzięcia jest/ nie jest* regulowane regulaminem/ innym aktem*
.....
(oznaczenie regulaminu/ innego aktu*)

4. Przetwarzanie danych osobowych w związku z przedsięwzięciem:

Lp.	Cel przetwarzania danych	Zakres przetwarzanych danych	Kategoria osób, których dane mają być przetwarzane	Podstawa przetwarzania danych	Okres przetwarzania danych	Sposób zabezpieczenia (ochrony) danych	Tryb i zasady postępowania z danymi po zakończeniu przedsięwzięcia

5. Uzgodnienie IODO:

- 1) Wyrażam zgodę/ nie wyrażam zgody* na przedstawione zasady i tryb przetwarzania danych osobowych w związku z organizacją i prowadzeniem przedsięwzięcia.

.....
(data i podpis IODO)

6. Uzgodnienia innych komórek lub stanowisk

- 1) Wyrażam zgodę/ nie wyrażam zgody* na przedstawione zasady i tryb przetwarzania danych osobowych w związku z organizacją i prowadzeniem przedsięwzięcia.

.....
(data i podpis upoważnionej osoby)

7. Wniosek o zatwierdzenie

- 1) Wnoszę o zatwierdzenie przedstawionych zasad i trybu przetwarzania danych osobowych w związku z organizacją i prowadzeniem przedsięwzięcia.

.....
(data i podpis osoby wnioskującej)

8. Zatwierdzenie

- 1) Zatwierdzam/ nie zatwierdzam*

.....
(data i podpis administratora)

Załącznik nr 3 do polityki bezpieczeństwa (ochrony) danych osobowych

Zakres informacji o przetwarzaniu danych osobowych zbieranych bezpośrednio od osoby, której dane dotyczą

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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

- administratorem Pani/Pana danych osobowych jest **Gminne Centrum Kultury w Cewicach** dane kontaktowe /;
- inspektorem ochrony danych osobowych w **Gminnym Centrum Kultury w Cewicach** jest Pani/Pani /imię i nazwisko, kontakt: adres e-mail, telefon/ *;
- Pani/Pana dane osobowe przetwarzane będą w celu
- odbiorcami Pani/Pana danych osobowych będą
- Pani/Pana dane osobowe będą przechowywane przez okres
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany,
- posiada Pani/Pan:
 - prawo dostępu do danych osobowych Pani/Pana dotyczących,
 - prawo do sprostowania Pani/Pana danych osobowych,
 - prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
- W przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie przepisów prawa, nie przysługuje Pani/Panu:
 - prawo do usunięcia danych osobowych;
 - prawo do przenoszenia danych osobowych,
 - prawo sprzeciwu, wobec przetwarzania danych osobowych.

Załącznik nr 4 do polityki bezpieczeństwa (ochrony) danych osobowych

Zakres informacji o przetwarzaniu danych osobowych zbieranych nie od osoby, której dane dotyczą

Zgodnie z art. 14 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, informuję, że:

1. Administratorem Pani/ Pana danych jest Gminne Centrum Kultury w Cewicach
2. Inspektorem Ochrony Danych Osobowych jest, dane kontaktowe
3. Pani/Pana dane osobowe przetwarzane są/ będą w celu, a także w celach archiwalnych oraz statystycznych.
4. Przetwarzanie Pani/Pana danych osobowych jest zgodne z prawem i spełnia warunki, o których mowa w RODO.
5. Zakres przetwarzanych danych osobowych obejmuje:(kategorie-rodzaj przetwarzanych danych osobowych).
6. Odbiorcami Pani/ Pana danych osobowych będą:
7. Pani/Pana dane osobowe będą przechowywane przez okres niezbędny na potrzeby oraz do czasu zakończenia archiwizowania dokumentacji.
8. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, ograniczenia przetwarzania, prawo wniesienia sprzeciwu, prawo do usunięcia danych, z wyjątkiem przypadków, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii oraz prawa polskiego, któremu podlega administrator danych osobowych.
9. Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

Załącznik nr 5 do polityki bezpieczeństwa (ochrony) danych osobowych

Wykaz budynków, obiektów, pomieszczeń lub ich części oraz urządzeń, w których przetwarzane są dane osobowe, a także zabezpieczeń fizycznych

1. Obszarem przetwarzania danych osobowych są pomieszczenia:
 - 1) zlokalizowane w Gminnym Centrum Kultury w Cewicach przy ul. J. Węgrzynowicza 16,
 - 2) zlokalizowane w Domu Kultury w Maszewie Lęborskim ul. Drewniana 35,
 - 3) zlokalizowane w obiekcie siłowni w Łebuni przy ul. Pomorskiej (działka nr 117/1)
 - 4) zlokalizowane w budynku na Osiedlu Na Wzgórzu 35
2. Zabezpieczenie pomieszczeń wskazanych w ust. 1:
 - 1) w odniesieniu do pomieszczeń wskazanych w pkt 1 zastosowano zabezpieczenia w postaci
 - a) drzwi antywłamaniowych,
 - b) krat w oknach,
 - c) systemu alarmowego połączonego z dozorem i ochroną wyspecjalizowanej firmy ochroniarskiej,
 - 2) w odniesieniu do pomieszczeń wskazanych w pkt 2 zastosowano zabezpieczenia w postaci
 - a) drzwi antywłamaniowych,
 - b) krat w oknach
 - 3) w odniesieniu do pomieszczeń wskazanych w pkt 3 zastosowano zabezpieczenia w postaci
 - a) drzwi antywłamaniowych,
 - b) krat w oknach.
 - 4) w odniesieniu do pomieszczeń wskazanych w pkt 4 zastosowano zabezpieczenia w postaci
 - a) drzwi antywłamaniowych,
 - b) krat w oknach.
3. Fizyczny dostęp do pomieszczeń, w których przetwarzane są dane osobowe, blokują drzwi zaopatrzone w zamki:
 - a) do których klucze zostały powierzone osobom odpowiedzialnym za realizację zadań statutowych pod w/w adresem tzw. opiekunom siłowni,
 - b) zamykane zawsze, gdy pomieszczenie opuszczają osoby upoważnione do przetwarzania danych,
4. Fizyczny dostęp do mebli tj. szaf i biurka, w których przechowywane są dokumenty zawierające dane osobowe, zlokalizowane w pomieszczeniach, o których mowa w ust. 1, blokują drzwi zaopatrzone w zamki:
 - a) do których klucze są powierzone osobom odpowiedzialnym za realizację zadań statutowych pod w/w adresem tzw. opiekunom siłowni
 - b) zamykane zawsze, gdy pomieszczenie opuszczają osoby upoważnione do przetwarzania danych,
5. Dostęp do pomieszczeń oraz mebli zlokalizowanych w pomieszczenia posiadają osoby upoważnione.
6. Dokumenty zawierające dane osobowe przekazywane są przez upoważnione osoby do Gminnego Centrum Kultury w Cewicach każdorazowo po zakończonym miesiącu- najpóźniej do 10 dnia miesiąca następnego.
7. Transport dokumentów zawierających dane osobowe odbywa się z zamkniętych, nieprzeźroczystych teczkach, możliwie najkrótszą i najbezpieczniejszą drogą w sposób uniemożliwiający wgląd osobom nieupoważnionym.

Załącznik nr 6 do polityki bezpieczeństwa (ochrony) danych osobowych

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych (w przypadku zbiorów danych prowadzonych w systemie informatycznym)

1. W Gminnym Centrum Kultury w Cewicach prowadzone są następujące zbiory danych osobowych:

- 1) rejestr klientów,
- 2) rejestr dokumentacji prowadzonej w wersji papierowej,
- 3) rejestr pracowników
- 4) rejestr osób zatrudnionych na innej podstawie niż stosunek pracy

2. Do przetwarzania danych w formie elektronicznej stosuje się następujące oprogramowanie:

Oznaczenie programu	Licencja lub inna podstawa stosowania	Cel przetwarzania	Zakres danych osobowych

Załącznik nr 7 do polityki bezpieczeństwa (ochrony) danych osobowych
Opis środków technicznych i organizacyjnych

1. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
2. Środki ochrony, zastosowane dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
 - 1) środki ochrony fizycznej,
 - 2) środki techniczne,
 - 3) środki organizacyjne,
3. Środki ochrony fizycznej danych:
 - 1) zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmocnionymi, nie przeciwpożarowymi),
 - 2) pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy,
 - 3) dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników objęty jest dozorem wyspecjalizowanej firmy ochroniarskiej,
 - 4) zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej szafie niemetalowej lub metalowej,
 - 5) kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie niemetalowej lub metalowej, sejfie, lub kasie pancernej,
 - 6) pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
 - 7) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
4. Środki ochrony technicznej danych:
 - 1) zastosowano urządzenia typu UPS chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
 - 2) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
 - 3) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,
 - 4) zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł,
 - 5) zastosowano system rejestracji dostępu do systemu/ zbioru danych osobowych,
 - 6) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,
 - 7) użyto system Firewall do ochrony dostępu do sieci komputerowej,
 - 8) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
 - 9) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego,
 - 10) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych,
 - 11) zastosowano kryptograficzne środki ochrony danych osobowych,
 - 12) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

- 13) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.
5. Środki organizacyjne:
- 1) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
 - 2) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
 - 3) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
 - 4) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
 - 5) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Załącznik nr 8 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE nr
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem upoważniam Pana/Panią*

.....
(Imię i nazwisko, PESEL)

do przetwarzania danych osobowych:

Kategoria danych osobowych	Oznaczenie zbioru danych

Niniejsze upoważnienie nie upoważnia do udzielania dalszych upoważnień.
Niniejsze upoważnienie wygasa z chwilą jego cofnięcia (odwołania).

.....
Miejscowość, data, czytelny podpis, osoby upoważnionej do wydawania i odwoływania upoważnień

- Oświadczam, że zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych, w tym z
- 1) 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 zwane również „RODO”,
 - 2) ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000),
 - 3) polityką bezpieczeństwa (ochrony) danych osobowych, obowiązującą w Gminnym Centrum Kultury w Cewicach

Zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia, jak też po jego ustaniu.

.....
Miejscowość, data, czytelny podpis osoby składającej oświadczenie

Upoważnienie otrzymałem/am

.....
Miejscowość, data, czytelny podpis osoby składającej oświadczenie

Załącznik nr 9 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór umowy o powierzenie przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

(zwana dalej „Umową”)

zawarta w w dniu pomiędzy:

Gminne Centrum Kultury z siedzibą, NIP, REGON,
....., reprezentowany przez,
zwanym w dalszej części umowy „**Administratorem**”

a

....., z siedzibą NIP, REGON:,
....., reprezentowana przez,
zwanym w dalszej części umowy „**Podmiotem przetwarzającym**”.

§ 1. Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego 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 2016 nr 119, str. 1) (zwanego w dalszej części „Rozporządzeniem”) oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000), 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 z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z obowiązującą u Administratora polityką bezpieczeństwa (ochrony) danych osobowych. Administrator udostępnia aktualny tekst polityki bezpieczeństwa (ochrony) danych bezzwłocznie.
4. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.
5. Podmiot przetwarzający oświadcza, iż wdroży środki bezpieczeństwa spełniające wymogi polityki bezpieczeństwa (ochrony) danych obowiązującej u Administratora bezzwłocznie. Podmiot przetwarzający powiadamia Administratora o wdrożeniu środków bezpieczeństwa spełniających wymogi polityki bezpieczeństwa (ochrony) danych.
6. Podmiot przetwarzający podejmuje przetwarzanie danych osobowych począwszy od dnia wdrożenia środków bezpieczeństwa, o których mowa w ust. 4 i 5.

§2. Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane:
a)
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy

§3. Obowiązki podmiotu przetwarzającego

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.
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, 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 wszelkie dane osobowe 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 48 godzin.

§4. Prawo kontroli

1. Administrator ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 24 godzinnym jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 72 godziny.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków.

§5. Dalsze powierzenie danych do przetwarzania

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.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora 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 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 nie wywiązanie 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 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 Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§7. Czas obowiązywania umowy

Strony oświadczają, że niniejsza umowa obowiązuje i jest realizowana przez strony od dnia, do dnia

§8. Rozwiązanie umowy

Administrator 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.

§9. Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora 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 w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10. Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora.

Administrator

Podmiot przetwarzający

Załącznik nr 10 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór rejestru czynności

Rejestr czynności przetwarzania danych osobowych			
	Administrator danych osobowych	Przedstawiciel administratora danych osobowych (jeśli wyznaczono)	Inspektor ochrony danych osobowych
Oznaczenie			
Adres			
Email			
Telefon			

LP.	
	Nazwa czynności przetwarzania
	Komórka organizacyjna/ stanowisko
Art.. 30. 1 pkt b RODO	Cel przetwarzania
Art.. 30 ust. 1	Kategorie osób
Art.. 30 ust. 1 pkt c RODO	Kategorie danych
	Podstawa prawna
	Źródło danych
Art.. 30 ust. 1 pkt f RODO	Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)
Art.. 30 ust. 1 pkt d RODO	Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)
Art.. 30 ust. 1	Kategorie odbiorców (innych niż podmiot przetwarzający)
	Nazwa systemu lub oprogramowania
Art.. 30 ust. 1	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)
	Ocena skutków dla bezpieczeństwa (ochrony) danych osobowych -DPIA (lokalizacja raportu)
Art. 30 ust. 1	Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)
Art. 30 ust. 1 pkt e RODO	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń

[illegible]

[illegible]

Załącznik nr 11 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór rejestru kategorii czynności

Rejestr kategorii czynności przetwarzania danych osobowych			
	Administrator danych osobowych	Przedstawiciel administratora danych osobowych (jeśli wyznaczono)	Inspektor ochrony danych osobowych
Oznaczenie			
Adres			
Email			
Telefon			

LP	Kategorie przetwarzania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Czas trwania przetwarzania	Miejsce zlokalizowania danych osobowych	Miejsce przekazywania danych osobowych, w tym kategorie odbiorców w odniesieniu do zidentyfikowanych celów	Nazwy państw lub organizacji trzecich lub międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiedzialności za bezpieczeństwo danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Okres przetwarzania danych osobowych, ze wskazaniem przewidywanego terminu usunięcia poszczególnych kategorii danych	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
									Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie powierzonych przetwarzania
Art. 30 ust. 2 lit. b RODO	Art. 30 ust. 2 lit. d, art. 32 ust. 1 RODO					Art. 30 ust. 2 lit. c RODO	Art. 30 ust. 2 lit. c RODO			

Załącznik nr 12 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór rejestru naruszeń

[illegible]

Załącznik nr 13 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór rejestru przypadków udostępniania danych osobowych

Rejestr przypadków udostępniania danych osobowych								
Lp	Podmiot, który wystąpił z wnioskiem o udostępnienie danych osobowych (nazwa, adres)	Data wpływu wniosku	Data udostępnienia danych	Podmiot, któremu dane udostępniono (nazwa, adres)	Nazwa zbioru z którego udostępniono dane	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych	Imię i nazwisko pracownika dokonującego udostępnienia

Załącznik nr 14 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych						
Lp.	Nazwisko i Imię upoważnionego	Zakres upoważnienia		Identyfikator użytkownika	Data nadania upoważnienia	Data ustania upoważnienia
		Nazwa zbioru danych	Rodzaj uprawnień			

Załącznik nr 15 do polityki bezpieczeństwa (ochrony) danych osobowych
Instrukcja postępowania w sprawie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych

1. Stwierdzenie naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych podlega niezwłocznemu zgłoszeniu.
2. Zgłoszenie, o którym mowa w ust. 1 dokonywane jest w formie pisemnej.
3. Zgłaszający kieruje zgłoszenie, o którym mowa w ust. 1 do bezpośredniego przełożonego albo do IODO.
4. Przełożony, do którego skierowano zgłoszenie, o którym mowa w ust. 1 niezwłocznie kieruje otrzymane zgłoszenie do IODO
5. IODO podejmuje postępowania bezpośrednio po otrzymaniu zawiadomienia, o którym mowa w ust. 1.
6. Postępowanie wyjaśniające obejmuje czynności zmierzające do ustalenia okoliczności faktycznych zdarzenia wskazanego w zgłoszeniu, o którym mowa w ust. 1, a w szczególności:
 - 1) ustalenie podejrzanego lub obwinionego naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych,
 - 2) sformułowania zarzutu wobec podejrzanego lub obwinionego, ze wskazaniem przepisu regulaminu pracy oraz postanowienia polityki bezpieczeństwa (ochrony) danych osobowych, jako podstawy prawnej zarzutu,
 - 3) przesłuchania podejrzanego lub obwinionego na okoliczność zarzutu,
 - 4) przesłuchania świadków lub biegłych na okoliczność zarzutu,
 - 5) przegląd monitoringu wizyjnego i monitoringu poczty elektronicznej,
 - 6) oględziny budynków, pomieszczeń, mebli, urządzeń, innych obiektów,
 - 7) ustalenia i zebrania innych materiałów dowodowych na okoliczność zarzutu.
7. Przesłuchanie świadka lub biegłego dokonywane jest po pouczeniu świadka lub biegłego o odpowiedzialności karnej a składanie fałszywych zeznań lub poświadczanie nieprawdy.
8. Materiały dowodowe, o których mowa w ust. 6 pkt 5 obejmują w szczególności:
 - 1) dokumenty ze stosunku pracy lub ich potwierdzone odpisy (kopie),
 - 2) odpisy (kopie) z ksiąg, rejestrów, ewidencji i innych dokumentów administratora danych osobowych,
 - 3) protokoły oględzin,
 - 4) inne dokumenty pisemne,
 - 5) przedmioty.
9. Materiały dowodowe podlegają zabezpieczeniu przed zniekształceniem, zniszczeniem lub zagubieniem.
10. Zabezpieczenia materiałów dowodowych dokonuje IODO.
11. Postępowanie wyjaśniające podlega zamknięciu, jeżeli wszystkie elementy sprawy na okoliczność zarzutu zostały wyjaśnione.
12. Zamknięcie postępowania wyjaśniającego dokonywane jest poprzez sporządzenie sprawozdania z posterowania wyjaśniającego.

Załącznik nr 16 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór sprawozdania z postępowania w sprawie naruszenia lub zagrożenia naruszeniem
bezpieczeństwa (ochrony) danych osobowych

**SPRAWOZDANIE z POSTĘPOWANIA w SPRAWIE NARUSZENIA LUB ZAGROŻENIA NARUSZENIEM
BEZPIECZEŃSTWA (OCHRONY) DANYCH OSOBOWYCH**

1. Osoba prowadząca postępowanie
 2. Data sporządzenia sprawozdania
 3. Podstawa podjęcia postępowania
.....
 4. Osoba podejrzanego lub obwinionego
 5. Zarzut i jego podstawa prawna
 6. Opis przebiegu postępowania :
.....
 7. Opis i ocena dowodów uwzględnionych oraz odrzuconych w toku postępowania wraz z uzasadnieniem:
.....
 8. Wnioski z postępowania
 - 1) Wnioski ogólne, wraz z uzasadnieniem
.....
 - 2) Wskazanie czy doszło do naruszenia praw i wolności osoby, której dane zostały naruszone, wraz z uzasadnieniem
.....
 - 3) Wskazanie poziomu ryzyka ziszczonego wskutek naruszenia bezpieczeństwa (ochrony) danych osobowych, wraz z uzasadnieniem
.....
 - 4) Wskazanie, czy naruszenie bezpieczeństwa (ochrony) danych osobowych polegające na naruszeniu praw i wolności osoby fizycznej podlega obowiązkowi zgłoszenia, wraz z uzasadnieniem
 - a) Prezesowi Urzędu ochrony Danych Osobowych
.....
 - b) osobie, której dane dotyczą
.....
 - 5) Wskazanie, czy w toku postępowania ustalono okoliczności uzasadniające podejrzenie popełnienia przestępstwa, wraz z uzasadnieniem
.....
 - 6) Wnioski dotyczące ustalenia winy podejrzanego lub obwinionego, wraz z uzasadnieniem
.....
 - 7) Wnioski dotyczące systemu bezpieczeństwa (ochrony) danych osobowych, wraz z uzasadnieniem
.....
 9. Propozycja umorzenia postępowania w przypadku, gdy w postępowaniu nie potwierdzono naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych, wraz z uzasadnieniem
.....
 10. Przedłożenie sprawozdania administratorowi danych osobowych
.....
- (data, podpis IODO)
11. Decyzja administratora danych osobowych
 - 1) Odmawiam zatwierdzenia sprawozdania i zwracam sprawozdanie w celu uzupełnienia o następujące elementy
.....

-
.....
.....
(data, podpis)
- 2) Zatwierdzam sprawozdanie
.....
(data, podpis)
- 3) Stwierdzam, że sprawozdanie stanowi podstawę zgłoszenia naruszenia bezpieczeństwa (ochrony) danych osobowych polegające na naruszeniu praw i wolności osoby fizycznej
- a) Prezesowi Urzędu ochrony Danych Osobowych
.....
(data, podpis)
- b) osobie, której dane dotyczą
.....
(data, podpis)
- 4) Stwierdzam, że sprawozdanie stanowi podstawę
- a) pociągnięcia do odpowiedzialności osoby zatrudnionej, winnej dopuszczenia się naruszenia lub zagrożenia naruszeniem bezpieczeństwa (ochrony) danych osobowych
.....
(data, podpis)
- b) powiadomienia organów ścigania o podejrzeniu popełnienia przestępstwa
.....
(data, podpis)

Załącznik nr 17 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór raportu ze stanu bezpieczeństwa (ochrony) danych osobowych

RAPORT ZE STANU BEZPIECZEŃSTWA (OCHRONY) DANYCH OSOBOWYCH

1. Osoba prowadząca badanie stanu bezpieczeństwa (ochrony) danych osobowych
 2. Data sporządzenia raportu
 3. Okres objęty raportem
 4. Opis przebiegu badania stanu bezpieczeństwa (ochrony) danych osobowych:
 - 1) Polityka bezpieczeństwa:
 - 2) Podstawy prawne przetwarzania danych osobowych:
 - 3) Prawa osób, których dane przetwarzano:
 - 4) Obowiązek informacyjny:
 - 5) Zadania i obowiązki administratora danych osobowych:
 - 6) Zadania i obowiązki IODO:
 - 7) Ryzyko naruszenia bezpieczeństwa (ochrony) danych osobowych i ocena skutków:
 - 8) Zadania i obowiązki osób zatrudnionych:
 - 9) Upoważnienia do przetwarzania danych osobowych:
 - 10) Środki techniczne i organizacyjne:
 - 11) Zdarzenia naruszające bezpieczeństwo (ochronę) danych osobowych:
 - 12) Powiadomienia o naruszeniu bezpieczeństwa (ochrony) danych osobowych:
 1. Opis i ocena dowodów uwzględnionych oraz odrzuconych w toku badania, wraz z uzasadnieniem:
 2. Wnioski z badania
 - 1) Wnioski ogólne, wraz z uzasadnieniem
 - 2) Wnioski w zakresie ryzyka naruszenia bezpieczeństwa (ochrony) danych osobowych ziszczonego w okresie badanym, wraz z uzasadnieniem
 - 3) Wnioski w zakresie środków technicznych i organizacyjnych
 - 5) Wnioski dotyczące systemu bezpieczeństwa (ochrony) danych osobowych, wraz z uzasadnieniem
 3. Przedłożenie raportu administratorowi danych osobowych
- (data, podpis IODO)
4. Decyzja administratora danych osobowych

- 1) Odmawiam zatwierdzenia raportu i zwracam raport w celu uzupełnienia o następujące elementy

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

(data, podpis)

- 2) Zatwierdzam raport

.....

(data, podpis)

- 3) Polecam wdrożyć wnioski z raportu w terminie

.....

(data, podpis)

- 4) Polecam przedłożyć sprawozdanie z wdrożenia wniosków z raportu w terminie

.....

(data, podpis)

Załącznik nr 18 do polityki bezpieczeństwa (ochrony) danych osobowych
Wzór zawiadomienia osoby fizycznej o naruszeniu bezpieczeństwa (ochrony) danych osobowych

Cewice,

Gminne Centrum Kultury w Cewicach
Cewice, ul.

Szanowny Panie/Szanowna Pani,

.....

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ o NARUSZENIU OCHRONY DANYCH OSOBOWYCH

W związku z art. 34 ust. 1 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), informuję o stwierdzeniu naruszenia ochrony Pana/Pani danych osobowych przetwarzanych w związku z[opisać w związku z jakim celem przetwarzane są dane osobowe].

Naruszenie ochrony danych osobowych polega na[wskazać charakter naruszenia] i może mieć następujące skutki dla Pana/Pani

Niezwłocznie po stwierdzeniu naruszenia, administrator danych osobowych podjął następujące środki w celu usunięcia/ zminimalizowania ewentualnych skutków.....[opisać zastosowane lub proponowane środki bezpieczeństwa].

Administrator danych osobowych zapewnia, że podjął niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości.

W razie dodatkowych pytań lub wątpliwości proszę o podjęcie kontaktu z[wskazać dane kontaktowe inspektora danych osobowych – imię, nazwisko, adres email / nr telefoniczny].

Z poważaniem,

.....

podpis