POLITYKA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

Lubartowskiego Ośrodka Kultury
w Lubartowie

ZATWIERDZIŁ

SPIS TREŚCI

I. Definicje

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

Polityka bezpieczeństwa danych osobowych – dokument określający zasady przetwarzania danych osobowych przez Administratora oraz środki techniczne i organizacyjne wdrożone, aby to przetwarzanie odbywało się zgodnie z prawem.

Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").

Szczególne kategorie danych osobowych – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Zbiór danych – każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów.

Przetwarzanie danych – oznacza jakiekolwiek operacje wykonywane na danych osobowych, takie 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, wykonywane zarówno w formie tradycyjnej jak i w systemach informatycznych.

Organ Nadzorczy – Prezes Urzędu Ochrony Danych Osobowych.

Administrator Danych Osobowych (ADO) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez administratora do wykonywania zadań informacyjno – doradczych oraz monitorowania przestrzegania przepisów i polityk w zakresie ochrony danych osobowych, w tym podziałów obowiązków, szkoleń oraz audytów, a także współpracy z organem nadzorczym i kontaktów z osobami, których dane dotyczą – zgodnie z art. 38 i 39 RODO.

Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Obszar przetwarzania – wszelkie pomieszczenia w budynkach stanowiących siedzibę Administratora, w których odbywa się przetwarzanie Danych osobowych w jakiejkolwiek formie oraz komputery przenośne i inne nośniki danych jeżeli znajdują się poza obszarem wskazanym powyżej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe (nie dotyczy organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania).

Zgoda – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

System informatyczny (SI) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Administrator systemu informatycznego (ASI) – osoba fizyczna lub prawna wyznaczona przez Administratora Danych Osobowych do administrowania systemem informatycznym.

Osoba upoważniona – osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona do przetwarzania danych osobowych w zakresie i formach wskazanych w upoważnieniu.

Użytkownik systemu – osoba posiadająca nadane uprawnienia do pracy w systemie informatycznym.

II. Cel i zakres polityki bezpieczeństwa danych osobowych

1. Zgodnie z art. 24 RODO obowiązkiem Administratora danych jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z prawem i aby móc to wykazać. Wdrażając ww. środki Administrator musi uwzględnić charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw i wolności osób, których dane dotyczą. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Polityka bezpieczeństwa określa zasady i reguły ochrony wszystkich danych osobowych w **Lubartowskim Ośrodku Kultury w Lubartowie**, zarówno w przypadku gdy jest ona administratorem danych jak i podmiotem przetwarzającym. Dotyczy ona zarówno danych osobowych przetwarzanych w formie tradycyjnej – papierowej, jak i przetwarzanych
   w systemach informatycznych. Przestrzeganie tych zasad ma na celu zapewnienie zgodnego z prawem przetwarzania danych oraz ograniczenie ryzyka wystąpienia naruszeń ochrony danych osobowych.
3. Polityka bezpieczeństwa obowiązuje wszystkie osoby dopuszczone do przetwarzania danych w **Lubartowskim Ośrodku Kultury w Lubartowie** tj.: pracowników, osoby zatrudnione na podstawie umów cywilnoprawnych, a także praktykantów i stażystów. Każda taka osoba powinna zostać zapoznana z dokumentacją ochrony danych, o której mowa w ust. 4.
4. Polityka bezpieczeństwa stanowi integralną całość jako dokumentacja ochrony danych osobowych w **Lubartowskim Ośrodku Kultury w Lubartowie** wraz z załącznikami wymienionymi w Rozdziale XII.

III. Organizacja ochrony danych osobowych

1. **Administratorem Danych Osobowych (ADO)** w Lubartowskim Ośrodku Kultury w Lubartowie jest **Lubartowski Ośrodek Kultury** (dalej **Ośrodek** lub **LOK**)**, 21-100 Lubartów, ul. Rynek II 1, tel. 81 8552242, e-mail: lok@loklubartow.pl,** który reprezentuje **Dyrektor Lubartowskiego Ośrodka Kultury.**
2. Do obowiązków ADO należy:
   1) zapewnienie aby przetwarzanie danych osobowych odbywało się zgodnie z prawem poprzez:

a) oparcie przetwarzania o aktualne podstawy prawne,
b) zbieranie danych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzanie dalej w sposób niezgodny z tymi celami,
c) przetwarzanie danych jedynie w takim zakresie jaki jest niezbędny do celów, w których są przetwarzane (minimalizacja danych),
d) zapewnienie prawidłowości i aktualności przetwarzanych danych;

2) zapewnienie realizacji praw osób, których dane dotyczą poprzez realizację:
a) obowiązku informacyjnego,
b) prawa do:
- dostępu do danych,
- do sprostowania danych,
- do usunięcia danych (prawo do bycia zapomnianym),
- do ograniczenia przetwarzania,
- do przenoszenia danych,
- do sprzeciwu wobec przetwarzania danych;

3) zastosowanie środków technicznych i organizacyjnych aby przetwarzanie danych odbywało się zgodnie z prawem z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw i wolności osób, których dane dotyczą;
4) uwzględnienie ochrony danych w fazie projektowania – wdrażanie odpowiednich zabezpieczeń już na etapie określania sposobów przetwarzania;
5) uwzględnienie domyślnej ochrony danych przez zapewnienie, aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania;
6) prowadzenie polityki bezpieczeństwa danych osobowych wraz z załącznikami;
7) prowadzenie rejestru czynności przetwarzania danych osobowych;
8) prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów – gdy ma to zastosowanie;
9) przeprowadzanie analizy ryzyka dla przetwarzanych zasobów danych osobowych;
10) przeprowadzenie oceny skutków dla ochrony danych – w przypadku wystąpienia takiej konieczności;
11) zapewnienie by każda osoba mająca dostęp do danych posiadała upoważnienie do przetwarzania danych oraz prowadzenie ewidencji osób upoważnionych;
12) wyznaczenie Inspektora Ochrony Danych – w przypadku wystąpienia takiej konieczności;
13) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu – w przypadku wystąpienia takiej konieczności;
14) zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych - w przypadku wystąpienia takiej konieczności;
15) zawieranie umów powierzenia przetwarzania danych osobowych (innych instrumentów prawnych) z podmiotami przetwarzającymi;
16) wykonywanie innych obowiązków Administratora określonych w RODO, a nie wymienionych w niniejszej Polityce – w przypadku wystąpienia takiej konieczności.

3. Obowiązki ADO realizowane są według następujących zasad:
1) Dyrektor Lubartowskiego Ośrodka Kultury w Lubartowie, który reprezentuje Administratora, jest uprawniony do podejmowania wszelkich ostatecznych decyzji w zakresie ochrony danych osobowych;
2) Pracownicy na stanowiskach samodzielnych wykonują obowiązki określone w ust. 2 w odniesieniu do swoich merytorycznych zakresów czynności;

3) Dyrektor Lubartowskiego Ośrodka Kultury w Lubartowie, który reprezentuje Administratora może wyznaczyć określone osoby do wykonywania poszczególnych czynności określonych w ust. 2 w odniesieniu do całego Ośrodka;
4) osoby, o których mowa w pkt. 2) i 3) powinny mieć wydane upoważnienia do przetwarzania danych osobowych w zakresie zgodnym z pełnioną funkcją lub zajmowanym stanowiskiem.

4. Inspektor Ochrony Danych (IOD) to osoba fizyczna, lub prawna, która jest wyznaczana przez Administratora lub Podmiot przetwarzający gdy:
   1) Administrator lub Podmiot przetwarzający jest organem, albo podmiotem publicznym;
   2) główna działalność Administratora lub Podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres oraz cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą;
   3) główna działalność Administratora lub Podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych dotyczących wyroków skazujących i naruszeń prawa.

Inspektor Ochrony Danych (IOD) realizuje zadania wynikające z art. 39 ust. 1 oraz art 38 ust. 4 RODO, do których w szczególności należą:
1) informowanie Administratora, Podmiotu przetwarzającego oraz pracowników o obowiązkach wynikających z przepisów o ochronie danych osobowych;
2) monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz Polityki Administratora lub Podmiotu przetwarzającego w tym: podział obowiązków, szkolenia i audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego i osób, których dane dotyczą.

Lubartowski Ośrodek Kultury w Lubartowie, jako Administrator jest zobowiązana do wyznaczenia Inspektora Ochrony Danych ponieważ zachodzi przesłanka wymieniona w ust. 4 pkt. 1.

5. **Administrator Systemu Informatycznego (ASI)** to osoba fizyczna lub prawna odpowiedzialna za prawidłowe funkcjonowanie, zarządzanie i nadzór nad systemem informatycznym służącym do przetwarzania danych osobowych.

6. Obowiązki ASI określa Instrukcja Zarządzania Systemem Informatycznym, stanowiąca dokument Załącznik Nr 2, do niniejszej Polityki bezpieczeństwa lub umowa na świadczenie usługi outsourcingu ASI (jeżeli nie ma etatowego ASI). Należą do nich m.in.:
   1) wdrożenie i nadzór nad funkcjonowaniem środków technicznych i programowych chroniących bezpieczeństwo danych osobowych, określonych w Instrukcji Zarządzania Systemem Informatycznym;
   2) sprawowanie nadzoru nad bezpieczeństwem sieci i systemów informatycznych Administratora;
   3) zarządzanie kontami użytkowników systemu poprzez: nadawanie identyfikatorów, zakładanie, blokowanie lub usuwanie kont, a także zmianę haseł dostępu – jeżeli są wdrożone takie rozwiązania;
   4) sprawowanie nadzoru nad wykonywaniem napraw i konserwacji systemu, a także nad wykonywaniem kopii zapasowych i ich okresowym sprawdzaniem pod kontem

przydatności do użycia oraz nad brakowaniem i niszczeniem wycofanych z użytku urządzeń i nośników zawierających dane osobowe;
5) informowanie Administratora i Inspektora Ochrony Danych o wszystkich naruszeniach ochrony danych osobowych oraz wszelkich zauważonych nieprawidłowościach mogących mieć wpływ na bezpieczeństwo danych, współdziałanie z nimi przy usuwaniu skutków tych naruszeń i nieprawidłowości oraz wyjaśnianiu ich przyczyn.

7. **Osoba upoważniona** to każda osoba, której Administrator nadał upoważnienie do przetwarzania danych. Osoba taka może przetwarzać dane osobowe jedynie w zakresie i celu określonym w upoważnieniu.

8. Do obowiązków Osoby upoważnionej należy m.in.:
   1) zapoznanie się z przepisami o ochronie danych osobowych oraz z Polityką bezpieczeństwa danych osobowych;
   2) przetwarzanie danych jedynie w celu realizacji obowiązków służbowych, zgodnie z zakresem czynności na zajmowanym stanowisku oraz przepisami prawa i postanowieniami Polityki bezpieczeństwa;
   3) stosowanie się do poleceń i zaleceń ADO i ASI dotyczących przetwarzania i ochrony danych osobowych;
   4) zachowanie w tajemnicy danych osobowych, do których uzyskała dostęp oraz sposobów ich zabezpieczenia, także po ustaniu stosunku pracy, umowy o świadczeniu usług lub sprawowania pełnionej funkcji;
   5) niezwłoczne informowanie ASI o wszystkich naruszeniach ochrony danych osobowych oraz wszelkich zauważonych nieprawidłowościach mogących mieć wpływ na ich bezpieczeństwo;
   6) zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym, a także utratą, uszkodzeniem lub zniszczeniem poprzez:
      a) nie pozostawianie bez nadzoru dokumentów zawierających dane osobowe i zabezpieczanie ich po zakończeniu pracy – zasady czystego biurka i czystego ekranu;
      b) stosowanie się do zasad określonych w dokumentach stanowiących załączniki do Polityki bezpieczeństwa dotyczących korzystania z systemów informatycznych, Internetu i poczty służbowej.

IV. Zasady i podstawy prawne przetwarzania danych osobowych

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach gdy spełniony jest co najmniej jeden z poniższych warunków (Art. 6 RODO):
   1) osoba, której dane dotyczą wyraziła na to zgodę w jednym lub większej liczbie określonych celów;
   2) jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie tej osoby przed zawarciem umowy;
   3) jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO (np. w przypadku zatrudnienia lub wypłaty wynagrodzeń);
   4) jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
   5) jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
   6) jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez Stronę trzecią (np. w przypadku prowadzenia marketingu produktów i usług, dochodzenia roszczeń z tytułu

prowadzonej działalności, obsługi korespondencji, obsługa reklamacji, organizacja szkoleń).

2. Dane muszą być przetwarzane zgodnie z poniższymi zasadami (Art. 5 RODO):
   1) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami;
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
   4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania zostały niezwłocznie usunięte lub sprostowane;
   5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
   6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

3. Przetwarzanie szczególnych kategorii danych osobowych jest zabronione chyba, że spełniony jest jeden z warunków określonych w Art. 9 ust. 2 RODO, a w szczególności:
   1) osoba, której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie tych danych;
   2) jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
   3) jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
   4) jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, lub zabezpieczenia społecznego;
   5) jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi, transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej.

4. Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa jest możliwe wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem.

5. Realizacja obowiązku informacyjnego oraz praw osób, których dane dotyczą:
   1) w przypadku zbierania danych od osoby, której dane dotyczą Administrator lub osoba przez niego upoważniona podczas pozyskiwania tych danych podaje jej informacje określone w Art. 13 RODO w postaci przedstawienia odpowiedniej klauzuli informacyjnej;
   2) w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą Administrator lub osoba przez niego upoważniona podczas pozyskiwania tych danych podaje jej informacje określone w Art. 14 RODO w postaci przedstawienia odpowiedniej klauzuli informacyjnej;
   3) w przypadku gdy osoba, której dane dotyczą zwróci się do Administratora w celu realizacji swoich praw:
      a) dostępu do danych – Art. 15 RODO;
      b) do sprostowania danych – Art. 16 RODO;

c) do usunięcia danych – Art. 17 RODO;
d) do ograniczenia przetwarzania – Art. 18 RODO;
e) do przenoszenia danych – Art. 20 RODO;
f) do sprzeciwu – Art. 21 RODO;

Administrator ma obowiązek podjąć odpowiednie działania określone w ww. przepisach RODO, aby zapewnić realizację praw osób, których dane dotyczą. Realizacja tych praw może być oparta o procedurę określającą szczegóły i zasady ich realizacji przez danego ADO. W **Lubartowskim Ośrodku Kultury w Lubartowie**, realizacja praw osób, których dane są przetwarzane jest oparta o taką procedurę, która stanowi Załącznik Nr 11, do niniejszej Polityki bezpieczeństwa. Lubartowski Ośrodek Kultury w Lubartowie jako (ADO) prowadzi Rejestr realizacji praw osób, których dane dotyczą stanowiący Załącznik Nr 12 do niniejszej Polityki bezpieczeństwa. Natomiast realizacja obowiązków informacyjnych następuję za pomocą klauzul informacyjnych opisujących podstawy realizacji poszczególnych czynności przetwarzania danych osobowych. Zbiór klauzul informacyjnych stanowi Załącznik Nr 17 do niniejszej Polityki bezpieczeństwa.

V. Obszar przetwarzania danych osobowych

Siedziba Lubartowskiego Ośrodka kultury w Lubartowie zlokalizowana jest pod adresem: **ul. Rynek II 1, 21-100 Lubartów**. Pomieszczenia Ośrodka stanowiące obszar przetwarzania danych osobowych w siedzibie LOK są zlokalizowane **na parterze i piętrze budynku**. Są to: gabinet Dyrektora, pomieszczenia biurowe i techniczne, pomieszczenia użytkowe – sale do zajęć oraz pomieszczenia kina LEWART.

Dodatkowe pomieszczenie biurowe zajmuje gazeta „LUBARTOWIAK” w budynku przy **ul. Farnej 4, 21-100 Lubartów**, zlokalizowane we wschodniej części budynku parterowego.

Obszar, w którym przetwarzane są dane osobowe, obejmuje zarówno miejsca, w których wykonuje się operacje na nich (wpisuje, modyfikuje, kopiuje itp.), jak również te, gdzie dane są jedynie przechowywane w jakiejkolwiek formie (szafy z dokumentacją papierową bądź komputerowymi nośnikami informacji zawierającymi dane, stacje komputerowe, serwery i inne urządzenia komputerowe, na których dane osobowe są przetwarzane na bieżąco). W przypadku komputerów przenośnych oraz nośników danych obszar przetwarzania stanowi każdorazowa lokalizacja tych urządzeń lub nośników.

Wszystkie pomieszczenia obejmujące obszar przetwarzania danych osobowych są zabezpieczone standardowymi drzwiami wejściowymi zamykanymi zamkami mechanicznymi. Dodatkowo pomieszczenie przy ul. Farnej 4 jest zabezpieczone kratami w oknach i drzwiach wejściowych. Kwestie związane z nadzorem nad kluczami do pomieszczeń obejmujących obszar przetwarzania danych osobowych w Ośrodku zostały uregulowane w dokumentach stanowiących Załączniki Nr 9, 9.1, 9.2 oraz 9.3 do niniejszej Polityki bezpieczeństwa.

VI. Dokumentowanie czynności przetwarzania - rejestr czynności przetwarzania danych osobowych i rejestr wszystkich kategorii przetwarzań w imieniu innego administratora

1. Każdy Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za który odpowiada.

2. Rejestr czynności przetwarzania danych osobowych jest elementem dokumentacji ochrony danych, powinien być prowadzony odrębnie dla każdego procesu przetwarzania danych i zawierać następujące informacje:
   1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
   2) cele przetwarzania;
   3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   5) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
   6) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   7) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
3. Rejestr czynności nie musi być prowadzony przez przedsiębiorców zatrudniających mniej niż 250 osób, chyba, że:
   1) przetwarzanie może naruszać prawa lub wolności osób, których dane dotyczą;
   2) przetwarzanie obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących;
   3) przetwarzanie nie ma charakteru sporadycznego.

   Dyrektor Lubartowskiego Ośrodka Kultury w Lubartowie, prowadzi Rejestr czynności przetwarzania danych osobowych, zgodnie z zasadami określonymi w Art. 30 ust. 1 RODO, który jest na bieżąco aktualizowany przez upoważnioną osobę. Rejestr ten stanowi Załącznik Nr 4, do niniejszej Polityki bezpieczeństwa.
4. Gdy ma to zastosowanie, każdy Podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów, który na bieżąco aktualizuje.
5. Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów, jest elementem dokumentacji ochrony danych, powinien być prowadzony odrębnie dla każdej kategorii przetwarzań w odniesieniu do każdego z administratorów i zawierać następujące informacje:
   1) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a także gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
   2) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
   3) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w Art. 49 ust.1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń;
   4) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
6. Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów nie musi być prowadzony przez przedsiębiorców zatrudniających mniej niż 250 osób, chyba, że:
   1) przetwarzanie może naruszać prawa lub wolności osób, których dane dotyczą;
   2) przetwarzanie obejmuje szczególne kategorie danych lub dane dotyczące wyroków skazujących;

3) przetwarzanie nie ma charakteru sporadycznego.

Dyrektor Lubartowskiego Ośrodka Kultury w Lubartowie aktualnie nie prowadzi Rejestru wszystkich kategorii czynności przetwarzania danych osobowych, zgodnie z zasadami określonymi w Art. 30 ust. 2 RODO, natomiast może go prowadzić jeżeli pojawi się taka konieczność. Wzór tego rejestru stanowi Załącznik Nr 7, do niniejszej Polityki bezpieczeństwa.

VII. Powierzenie przetwarzania danych innym podmiotom oraz przetwarzanie danych w imieniu innych administratorów

1. Lubartowski Ośrodek Kultury w Lubartowie, jako Administrator może powierzać przetwarzanie danych osobowych innym podmiotom jedynie w formie umowy (lub innego instrumentu prawnego) zawartej/go na piśmie, zgodnie z wymogami określonymi w art. 28 RODO;
2. Administrator zamieszcza informacje o zawartych umowach powierzenia przetwarzania danych (innych instrumentach prawnych) w Rejestrze umów (innych instrumentów prawnych) powierzenia przetwarzania danych osobowych stanowiącym Załącznik Nr 10, do niniejszej Polityki bezpieczeństwa;
3. Administrator podejmuje wszelkie rozsądne starania, aby wybierać podmioty przetwarzające dane, zapewniające wystarczające gwarancje zgodnego z prawem przetwarzania danych osobowych;
4. Lubartowski Ośrodek Kultury w Lubartowie jako podmiot przetwarzający może przetwarzać dane w imieniu innych Administratorów;
5. Dane osobowe, o których mowa w ust. 4 przetwarzają tylko upoważnieni pracownicy, a szczegółowy zakres i formę przetwarzania tych danych regulują umowy powierzenia przetwarzania danych (inne instrumenty prawne) zawarte z ich Administratorami;
6. Lubartowski Ośrodek Kultury w Lubartowie jako podmiot przetwarzający dokumentuje czynności przetwarzania w rejestrze wszystkich kategorii czynności przetwarzania danych dokonywanych w imieniu innych administratorów.

VIII. Analiza ryzyka oraz ocena skutków dla ochrony danych

1. Analizę ryzyka naruszenia praw lub wolności osób fizycznych wynikającego z przetwarzania ich danych osobowych, przeprowadza się w celu identyfikacji zagrożeń, prawdopodobieństwa ich wystąpienia, a także oceny skutków. Analizę wykonuje się nie rzadziej niż co 2 lata w całości, lub po wystąpieniu naruszenia ochrony danych osobowych w zakresie związanym z tym naruszeniem.
2. Dla Lubartowskiego Ośrodka Kultury w Lubartowie taka analiza została wykonana w ramach aktualizacji dokumentacji z zakresu ochrony danych osobowych i stanowi Załącznik Nr 1 do niniejszej Polityki bezpieczeństwa.
3. W przypadkach określonych w Art. 35 RODO tj. jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Aktualnie w Lubartowskim Ośrodku Kultury w Lubartowie nie ma konieczności przeprowadzania takiej oceny skutków.

4. Wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych ustanawia i podaje do publicznej wiadomości organ nadzorczy.
5. Gdy będzie to mieć zastosowanie Administrator może przeprowadzić stosowną ocenę skutków dla ochrony danych, która będzie stanowić załącznik do niniejszej Polityki bezpieczeństwa.

IX. Określenie środków organizacyjnych i technicznych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator wdraża i stosuje środki techniczne i organizacyjne niezbędne dla zapewnienia:
   1) **poufności**, czyli zapewnienia, że informacja nie jest udostępniana lub ujawniana nieuprawnionym osobom;
   2) **integralności**, czyli zapewnienia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **rozliczalności**, czyli zapewnienia, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   4) **dostępności**, czyli zapewnienia upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami.
2. Zastosowane środki organizacyjne i techniczne powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów i kategorii przetwarzanych danych określonych w analizie ryzyka, lub ocenie skutków dla przetwarzania danych (gdy ma to zastosowanie), o których mowa w Rozdziale VIII.
3. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa znajduje się w załącznikach do niniejszej Polityki bezpieczeństwa.

X. Zasady wprowadzania do użytku, modyfikacji i likwidacji procesów przetwarzania danych osobowych oraz kategorii przetwarzań dokonywanych w imieniu administratora – stosowanie zasad ochrony danych w fazie projektowania i domyślnej ochrony danych

1. Wprowadzanie, modyfikacja lub likwidacja procesów przetwarzania danych osobowych oraz kategorii przetwarzań dokonywanych w imieniu administratora może nastąpić wyłącznie w drodze decyzji Administratora.
2. Aby wprowadzić do użytku nowy proces przetwarzania danych, system informatyczny lub program służący do przetwarzania danych osobowych, albo zmodyfikować go w zakresie zmieniającym cel lub zakres przetwarzania danych osobowych Administrator sprawdza następujące kwestie:
   1) kto jest administratorem (*czy administrator działa sam czy występują współadministratorzy*);
   2) cel przetwarzania danych (*należy określić*);
   3) zakres kategorii osób, których dane dotyczą (*należy określić jakich kategorii osób dane zamierza przetwarzać*);
   4) zakres kategorii danych *(należy określić jakie konkretne dane mają być przetwarzane i czy ten zakres jest adekwatny do celu przetwarzania – czy dane nie mają być zbierane w zbyt szerokim zakresie)*;

5) kategorie odbiorców, którym dane zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych (*należy określić komu dane mogą być ujawnione)*;
6) czy będzie miało miejsce przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej (*należy określić jakie to państwa lub organizacje*);
7) planowane terminy usunięcia poszczególnych kategorii danych;
8) sposób realizacji obowiązku informacyjnego oraz praw osób, których dane dotyczą – określonych w rozdziale III RODO.

3. Aby wprowadzić do użytku, zmodyfikować lub zlikwidować kategorię przetwarzań dokonywanych w imieniu administratora, albo rozpocząć korzystanie z usług innego podmiotu przetwarzającego, konieczna jest uprzednia, szczegółowa lub ogólna, pisemna zgoda administratora.

4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie pisemnej umowy z administratorem (innego instrumentu prawnego) określającej/ego przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą obowiązki i prawa administratora, a w szczególności powinna/ien stanowić, że podmiot przetwarzający:
   1) przetwarza dane wyłącznie na udokumentowane polecenie administratora, co dotyczy też przekazywania danych do państwa trzeciego, lub organizacji międzynarodowej;
   2) zapewnia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy;
   3) podejmuje wszelkie możliwe środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

5. Przeprowadza analizę ryzyka lub w przypadku, gdy jest to przewidziane prawem (art. 35 RODO) ocenę skutków dla ochrony danych i na jej podstawie określa środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku – zgodnie z art. 32 RODO.

6. Na podstawie powyższych informacji Administrator ustala, czy wprowadzenie lub modyfikacja nowego procesu przetwarzania danych/systemu/programu, albo kategorii przetwarzań dokonywanych w imieniu innego administratora jest zgodne z prawem.

7. W przypadku, gdy przetwarzanie danych jest dopuszczalne Administrator nadaje wdrożeniu dalszy bieg oraz uzgadnia z Administratorem systemu informatycznego kwestie dotyczące możliwości technicznych wprowadzenia systemu/programu (*w przypadku procesów przetwarzanych w formie elektronicznej*).

8. Przed rozpoczęciem przetwarzania danych Administrator uzupełnia niniejszą dokumentację o wprowadzone zmiany oraz aktualizuje prowadzony przez siebie rejestr czynności przetwarzania danych osobowych.

9. Jeżeli zmiana dotyczy zakresu przetwarzania danych jako podmiotu przetwarzającego, aktualizuje się rejestr wszystkich kategorii czynności przetwarzania w imieniu administratora danych.

10. Administrator systemu informatycznego, w razie konieczności aktualizuje procedury dotyczące nadawania/odbierania uprawnień w systemie informatycznym.

11. Jeżeli Administrator uzna, że dany zakres danych nie jest mu już potrzebny, w przypadku ustania podstaw prawnych przetwarzania danych lub osiągnięcia celu dla którego dane zostały zebrane, a obowiązek ich przechowywania nie wynika z odrębnych przepisów prawa, usuwa te dane ze wszystkimi wykonanymi kopiami,

trwale je niszcząc w sposób uniemożliwiający ich odtworzenie. Usunięcie danych dokumentuje się przez podanie daty usunięcia, zakresu usuniętych danych oraz powód usunięcia zgromadzonych danych. Administrator sporządza protokół z likwidacji danych.

XI. Procedury postępowania w przypadku wystąpienia naruszeń ochrony danych osobowych, prowadzenia rejestru naruszeń oraz informowania o naruszeniach Organu nadzorczego i osób, których dane dotyczą

1. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   1) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe;
   2) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
   3) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia ochrony danym osobowym;
   4) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
   5) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem, w którym zostały zebrane;
   6) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
   7) naruszenie praw osób, których dane dotyczą.
2. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych podejmuje się następujące działania:
   1) Osoba upoważniona zobowiązana jest do podjęcia wszystkich niezbędnych działań, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora, a w przypadku, gdy naruszenie dotyczy bezpieczeństwa systemu informatycznego także Administratora systemu informatycznego;
   2) Administrator systemu informatycznego ustala charakter incydentu oraz podejmuje odpowiednie działania mające na celu wyeliminowanie zagrożenia i przywrócenia poprawnego działania systemu, a także dokumentuje te działania;
   3) Administrator przy pomocy Administratora systemu informatycznego dokonuje analizy naruszenia pod kątem przyczyn, przebiegu i skutków oraz weryfikuje zastosowane zabezpieczenia i ich skuteczność;
   4) Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych;
   5) W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych Organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia;
   6) Wzór zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu określa PUODO pod adresem: **https://uodo.gov.pl/pl/134/233**;
   7) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, Administrator bez zbędnej zwłoki

zawiadamia o incydencie także osobę, której dane dotyczą, Wzór zawiadomienia osoby fizycznej stanowi Załącznik Nr 13 do niniejszej Polityki bezpieczeństwa.

3. Zawiadomienie, o którym mowa w ust. 2 pkt. 7), nie jest wymagane, w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych w Rejestrze naruszeń stanowiącym Załącznik Nr 8 do niniejszej Polityki bezpieczeństwa.

XII. Wykaz załączników do Polityki bezpieczeństwa

1. **Załącznik Nr 1** – Analiza ryzyka (do wiadomości Dyrektora i ASI).
2. **Załącznik Nr 2** – Instrukcja zarządzania systemem informatycznym (do wiadomości Dyrektora i ASI).
3. **Załącznik Nr 3** – Regulamin Użytkownika Systemów Informatycznych (do wiadomości wszystkich osób upoważnionych).
4. **Załącznik Nr 4** – Rejestr czynności przetwarzania danych osobowych (do wiadomości wszystkich upoważnionych do przetwarzania danych osobowych).
5. **Załącznik Nr 5** – Wzór upoważnienia do przetwarzania danych osobowych (do wiadomości wszystkich osób upoważnionych).
6. **Załącznik Nr 6** – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych (do wiadomości Dyrektora i innej osoby upoważnionej do jej prowadzenia).
7. **Załącznik Nr 7** – Wzór Rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych Administratorów (do wiadomości wszystkich upoważnionych do przetwarzania danych osobowych).
8. **Załącznik Nr 8** - Rejestr naruszeń ochrony danych osobowych (do wiadomości Dyrektora, ASI i IOD).
9. **Załącznik Nr 9** – Procedura nadzoru nad kluczami do pomieszczeń Gminnej Biblioteki Publicznej w Kamionce (do wiadomości wszystkich pracowników).
10. **Załącznik Nr 9.1 -** Wzór upoważnienia do dysponowania kluczami do pomieszczeń Biblioteki (do wiadomości wszystkich pracowników) .
11. **Załącznik Nr 9.2** – Wzór ewidencji upoważnień do dysponowania kluczami do pomieszczeń Biblioteki (do wiadomości Dyrektora, ASI i IOD).
12. **Załącznik Nr 9.3** - Wzór Rejestru użycia kluczy zapasowych (do wiadomości wszystkich pracowników).
13. **Załącznik Nr 10 –** Rejestr umów powierzenia przetwarzania danych osobowych (do wiadomości Dyrektora, ASI i IOD).

14. **Załącznik Nr 11 –** Procedura realizacji praw osób, których dane dotyczą (do wiadomości wszystkich osób upoważnionych).
15. **Załącznik Nr 12** - Rejestr realizacji praw osób, których dane dotyczą (do wiadomości Dyrektora, ASI i IOD).
16. **Załącznik nr 13** – Wzór zgłoszenia naruszenia ochrony danych osobowych (do wiadomości Dyrektora, ASI i IOD).
17. **Załącznik Nr 14** – Wykaz innej dokumentacji dotyczącej ochrony danych osobowych (do wiadomości Dyrektora, ASI i IOD).
18. **Załącznik Nr 15** - Rejestr zmian dokumentacji ochrony danych osobowych (do wiadomości Dyrektora, ASI i IOD).
19. **Załącznik Nr 16 –** Ewidencja udostępnień danych osobowych.
20. **Załącznik Nr 17 -** Zbiór klauzul informacyjnych (pracownik, kandydat, uczestnik zajęć, kontrahent i innych…) (do wiadomości wszystkich osób upoważnionych).