MIEJSKA BIBLIOTEKA PUBLICZNA W KOBYŁCE
im. Stanisława Ryszarda Szpotańskiego
ul. Leśna 8 lokal 0.3
05-230 KOBYŁKA
tel. 22 763-42-42
REGON 000939289, NIP 1250559111

Kobyłka, dnia: 02.04.2024 roku

Zarządzenie Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego
nr 08/2024
z 02 kwietnia 2024 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Na podstawie Art. 24 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 (Dziennik Urzędowy Unii Europejskiej L 119/1) dalej RODO, zarządzam co następuje:

§1

Wprowadzam Politykę Bezpieczeństwa Ochrony Danych Osobowych, której treść stanowi Załącznik nr 1 do niniejszego zarządzenia.

§2

Zobowiązuję pracowników Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego do zapoznania się z treścią Załącznika nr 1 do niniejszego Zarządzenia

§3

Zobowiązuję wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa pod groźbą sankcji przewidzianych przepisami prawa.

§4

Zarządzenie nr **17/2022** Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce z dnia: 30.11.2022 roku dotyczące wprowadzenia Polityki Bezpieczeństwa Danych Osobowych Miejskiej Biblioteki Publicznej w Kobyłce traci moc.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Miejskiej Biblioteki Publicznej w Kobyłce
im. Stanisława Ryszarda Szpotańskiego
Sylwia Carzyńska

Załącznik nr 1

do Zarządzenia nr 08/2024

Dyrektora MBP w Kobyłce im. Stanisława Ryszarda Szpotańskiego

z dnia 02.04.2024 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Zatwierdzona 02 kwietnia 2024 rok

SPIS TREŚCI

PAGE

DEFINICJE I SKRÓTY

Administrator Danych/ Administrator Danych Osobowych/ ADO – Administratorem danych osobowych jest Miejska Biblioteka Publiczna w Kobyłce im. Stanisława Ryszarda Szpotańskiego przy ul. Leśna 8 lokal 0.3 05-230 Kobyłka, (dalej: Biblioteka lub MBP), ADO reprezentowany jest przez Dyrektora Biblioteki (dalej: Dyrektor).

Administrator Systemu (AS) - dedykowana osoba lub zespół osób do obsługi informatycznej Miejska Biblioteka Publiczna w Kobyłce. Może to być osoba z firmy zewnętrznej, z którą MBP zawarł umowę na świadczenie takich usług, lub pracownik IT w MBP

Dane Osobowe – dane osobowe w rozumieniu art. 4 RODO, przetwarzane przez Bibliotekę tj. wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą").

Dane wrażliwe/szczególnie chronione - dane o szczególnym charakterze opisane w art. 9 i 10 RODO.

Dyrektor – Dyrektor Miejska Biblioteka Publiczna w Kobyłce.

Incydent ciągłości działania – zdarzenie, które może wystąpić i prowadzić do zakłócenia zdolność organizacji do kontynuacji świadczenia przez nią usług na akceptowalnych, zdefiniowanych poziomach.

Inspektor Ochrony Danych (IOD) lub Osoba nadzorująca – Osoba wyznaczona przez Administratora danych zgodnie z Art. 37 RODO lub osoba wyznaczona przez Administratora danych mająca w obowiązkach nadzorowanie systemu ochrony danych osobowych w Bibliotece, którego zasady zostały opisane w niniejszej polityce.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Organ nadzorczy – Urząd Ochrony Danych Osobowych, niezależny organ publiczny ustanowiony w celu kontroli realizacji przepisów o ochronie danych osobowych, na czele, którego stoi Prezes Urzędu Ochrony Danych Osobowych.

Podmiot przetwarzający – Podmiot, któremu Biblioteka powierzyła dane osobowe, których jest administratorem do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych.

Polityka bezpieczeństwa – niniejsza polityka bezpieczeństwa danych osobowych;

Powierzenie przetwarzania danych osobowych – przekazanie danych osobowych przez Bibliotekę, dla realizacji celów własnych spółki na podstawie umowy powierzenia przetwarzania danych osobowych.

Pracownik – osoba wykonująca prace pod nadzorem Administratora danych na podstawie formalnych ustaleń (osoba pracująca (na podstawie stosunku pracy) oraz współpracująca (na podstawie zlecenia, umowy o dzieło, lub innego rodzaju umowy cywilnoprawnej (UCP)).

Informatyk, Pracownik IT, ASI - dedykowana osoba do obsługi informatycznej Biblioteki. Może to być dedykowana osoba z firmy zewnętrznej, z którą Biblioteka zawarło umowę na świadczenie takich usług.

Przetwarzanie danych osobowych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

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

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Użytkownik – osoba fizyczna korzystająca z systemów teleinformatycznych służących do przetwarzania danych osobowych, których administratorem jest Biblioteka.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem a w szczególności:

- **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Dostępność** – właściwość polegającą na tym, że dane są dostępne dla osoby upoważnionej we właściwym momencie.

Zasada rozliczalności, Rozliczalność - obowiązek przestrzegania zasad ochrony danych i zdolność do wykazania tego poprzez wdrożenie wewnętrznych mechanizmów i procedur.

Zastępca Inspektora Ochrony Danych – Osoba wyznaczona przez Administratora danych do zastąpienie inspektora Ochronny Danych w przypadku absencji lub nieobecności.

Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści a także łączona z innymi oświadczeniami woli.

1. WPROWADZENIE

1.1. CHARAKTERYSTYKA INSTYTUCJI

Biblioteka jest samorządową instytucją kultury posiadającą osobowość prawną, działająca na podstawię statutu. Podstawowym celem Biblioteki jest zaspokajanie potrzeb oświatowych, kulturalnych i informacyjnych ogółu społeczeństwa. Biblioteka gromadzi, opracowuję, przechowuje i chroni materiały biblioteczne. Obsługuje czytelników prowadzi dokumentacje biblioteczną i upowszechnia czytelnictwo.

Biblioteka zlokalizowana jest w budynku :

- 05-230 Kobyłka, ul. Leśna 8 lokal 0.3 05-230 Kobyłka - budynek Biblioteki.

Główne systemy informatyczne używane w Bibliotece to:

- Strona http://biblioteka.kobylka.pl/ gdzie są publikowane informacje o bieżącej pracy biblioteki w tym wizerunek osób które wyraziły zgodę;
- Biuletyn informacji publicznej;
- Oficjalna strona na Facebooku https://www.facebook.com/BibliotekawKobylce/, gdzie są publikowane informacje o bieżącej pracy biblioteki, w tym wizerunek osób które wyraziły zgodę;
- Oprogramowanie **Mateusz** – opracowywanie, wprowadzanie i wypożyczanie księgozbioru;
- Oprogramowanie firmy Vulcan sp. z o.o.- służące do obsługi w zakresie kadr i księgowości;

Dostęp do systemów informatycznych i przetwarzanych tam danych osobowych mają wyłącznie osoby upoważnione przez Administratora danych.

Dostęp do danych powierzonych do przetwarzania mają w szczególności:

1. Inspektor Ochrony Danych w zakresie pełnionej funkcji;
2. Firma hostingowa (hosting i administracja kontami pocztowymi);
3. Urząd miasta Kobyłka (umowy, zamówienia publiczne);

Pełen wykaz podmiotów, którym powierzono dane osobowe do przetwarzania prowadzi IOD **[wzór w załączniku nr 7 do Polityki bezpieczeństwa]**.

Niniejsza dokumentacja obowiązuje w całej Bibliotece i dotyczy wszystkich pracowników i podmiotów współpracujących, bez względu na miejsce wykonywanej pracy.

1.2. ORGAN PROWADZĄCY

Organizatorem Biblioteki jest Miasto Kobyłka.

Miasto Kobyłka ma dostęp (a Biblioteka mu ten dostęp zapewnia) do danych osobowych przetwarzanych w Bibliotece, w związku z realizacją swoich obowiązków wynikających z przepisów prawa.

Dostęp Miasta Kobyłka do danych osobowych jest adekwatny do celu przetwarzania danych, co oznacza, że zakres udostępnianych danych przez Bibliotekę musi być odpowiedni (bez nadmiaru) do celu przetwarzania (zasada minimalizacji danych).

Biblioteka może przekazywać gromadzone przez siebie dane osobowe w postaci papierowej lub elektronicznej Miastu Kobyłka, jeżeli takie działanie ma odpowiednią podstawę prawną oraz spełnione zostały wymogi bezpieczeństwa danych osobowych. Miasto Kobyłka jest obowiązane przetwarzać pozyskane od biblioteki dane w sposób zapewniający ich bezpieczeństwo.

1.3. CEL I ZAKRES POLITYKI

Polityka Bezpieczeństwa została ustanowiona w celu zapewnienia zgodności z wymaganiami a w szczególności zapewnienia zgodności z zasadami podstawowymi RODO tj.:

1) **Zasadą zgodności z prawem, która stanowi, że:**
   - dane przetwarzane są wyłącznie na podstawie przesłanek legalności (art. 6, 9 lub 8 RODO).
2) **Zasadą celowości, która stanowi, że:**
   - dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
3) **Zasadą minimalizacji danych, celowości, która stanowi, że:**
   - dane przetwarza się wyłącznie w zakresie niezbędnym do realizacji celu przetwarzania określonym przy ich zbieraniu.
4) **Zasadą prawidłowości przetwarzania, która stanowi, że:**
   - wdraża się mechanizmy aktualizacji i weryfikacji poprawności przetwarzanych danych osobowych umożliwiające korygowanie nieprawidłowych lub nieaktualnych danych.
5) **Zasadą ograniczania przetwarzania, która stanowi, że:**
   - usuwa się dane, których nie może przetwarzać (gdzie zidentyfikowano brak podstawy prawnej ich przetwarzania).
6) **Zasadą integralności i poufności danych osobowych,**
   - zapewnia się bezpieczeństwo przetwarzanym danym osobowym stosując podejście oparte na ryzyku.

W tym celu wprowadza się obowiązek bezpośredniego stosowania powyższych zasad przetwarzania danych osobowych poprzez określenie stosownych procedur opisanych w niniejszej Polityce bezpieczeństwa danych osobowych.

Polityka bezpieczeństwa dotyczy wszystkich Danych osobowych przetwarzanych w bibliotece, niezależnie od formy ich przetwarzania oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.

Polityka bezpieczeństwa jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora danych.

Wszelkie dowody na zgodność przetwarzania danych osobowych w postaci wypełnionych załączników do niniejszej polityki przechowywane mogą być zarówno w wersji papierowej, jak również elektronicznej.

Polityka bezpieczeństwa może być udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wiosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią. „Wzór upoważnienia do przetwarzania danych osobowych" stanowi **Załącznik nr 3 do Polityki bezpieczeństwa.**

Odpowiedzialny za wdrożenie i utrzymanie Polityki bezpieczeństwa jest Dyrektor.

Za nadzór i monitorowanie przestrzegania Polityki bezpieczeństwa odpowiada **Inspektor Ochrony Danych**.

Za stosowanie niniejszej Polityki bezpieczeństwa odpowiedzialni są:

a) Biblioteka za pośrednictwem Dyrektora;
b) Wszyscy członkowie personelu biblioteki, w tym pracownicy i osoby/podmioty współpracujące z Biblioteką na umowach cywilnoprawnych.

Biblioteka przetwarza dane osobowe zgodnie z RODO i aktualnie obowiązującymi przepisami prawa krajowego regulującymi kwestie przetwarzania danych osobowych.

Niniejsza Polityka Bezpieczeństwa dotyczy przetwarzania Danych Osobowych, na które składają się:

a) Dane osobowe, których administratorem w rozumieniu RODO jest Biblioteka, przetwarzane przez Bibliotekę osobiście;
b) Dane osobowe, których administratorem w rozumieniu RODO jest Biblioteka, powierzane przez Bibliotekę podmiotom współpracującym (kontrahentom, partnerom, zleceniobiorcom itp.);
c) Dane osobowe przetwarzane przez Bibliotekę na podstawie umów o powierzenie przetwarzania danych osobowych (Biblioteka występuje, jako podmiot przetwarzający).

Ilekroć w Polityce Bezpieczeństwa jest mowa o przetwarzaniu Danych Osobowych, dotyczy to przetwarzania danych osobowych przez Bibliotekę, pracowników i współpracowników Biblioteki oraz inne osoby i podmioty na podstawie umów zawartych z Biblioteką, w związku z realizacją celów przetwarzania Danych Osobowych, o których mowa w Polityce Bezpieczeństwa.

Wszelkie zestawienia uzupełniające treść dokumentu zebrano w postaci załączników. Wykaz załączników i dokumentów związanych znajduje się na końcu niniejszego dokumentu.

1.4. Struktura ochrony danych osobowych

Struktura ochrony danych osobowych zapewnia kompleksowe i spójne zarządzanie bezpieczeństwem danych osobowych. W zakresie struktury występują następujące role:

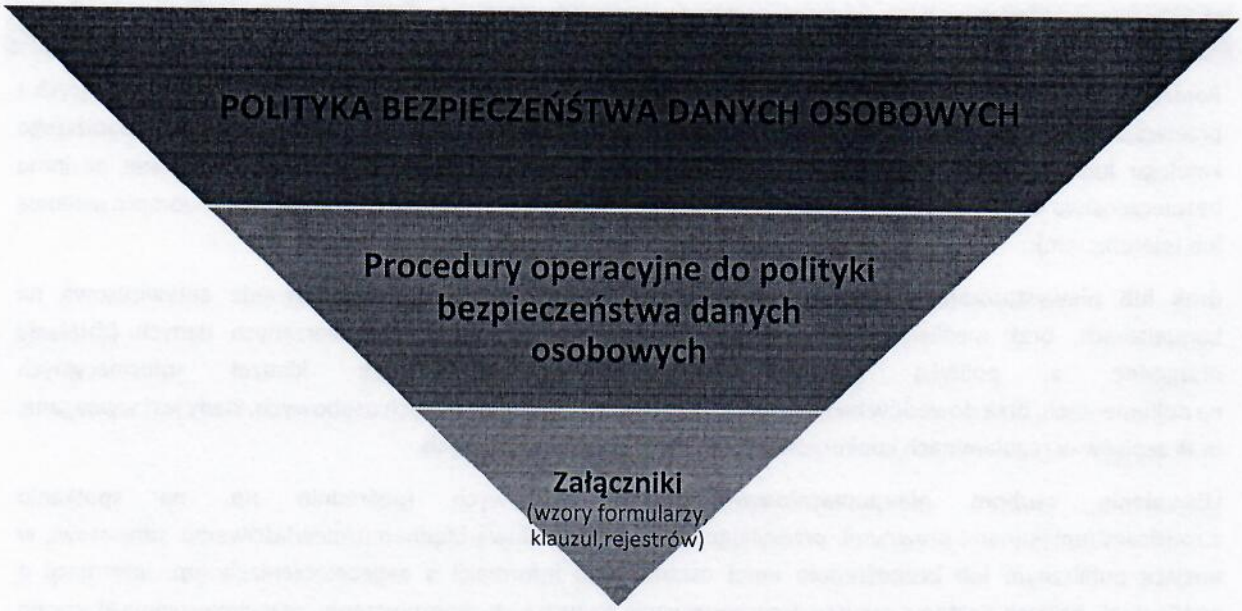
- **Administrator danych** w imieniu, którego występuje Dyrektor;
- **Inspektor Ochrony Danych** – osoba wyznaczona przez Dyrektora w celu nadzorowania przepisów o ochronie danych osobowych;
- **Informatyk, Administrator Systemu (ASI)** – Pracownik Urzędu Miasta Kobyłka, pracownik Biblioteki posiadający odpowiednie kompetencje w obszarze IT lub podmiot zewnętrzny świadczący usługi IT (bieżące zarządzanie i obsługa infrastruktury IT, nadzór nad wdrożonymi zabezpieczeniami, utrzymywanie systemów Informatycznych);
- **Koordynator** – Osoba wyznaczona przez Dyrektora lub sam Dyrektor w celu nadzorowania planu na wypadek wystąpienia incydentu ciągłości działania.

1.5. Struktura polityki bezpieczeństwa danych osobowych

Na strukturę dokumentacji składają się:

- Regulacje zewnętrzne, a w szczególności przepisy prawa powszechnie obowiązującego w zakresie ochrony danych osobowych. Wykaz tych przepisów, jak również dokumentów zewnętrznych (wytyczne, opinie w zakresie przetwarzania danych osobowych itp.) jest prowadzony i aktualizowany przez IOD oraz udostępniany pracownikom i współpracownikom w razie potrzeby.
- Regulacje wewnętrzne, w tym:
    - Polityka bezpieczeństwa danych osobowych
    - Procedury wykonawcze do polityki bezpieczeństwa danych osobowych
        - Procedura podejścia opartego na ryzy
        - Procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
        - Procedury ciągłości działania
    - Formularze, załączniki, wzory dokumentów, klauzul, rejestrów.

Struktura dokumentacji polityki bezpieczeństwa opisana jest na poniższym rysunku:



Polityka bezpieczeństwa danych osobowych jest nadrzędnym dokumentem regulującym podstawowe zasady przetwarzania danych osobowych w Bibliotece.

Za przegląd i aktualizację Polityki bezpieczeństwa danych osobowych odpowiedzialny jest IOD.

Za zatwierdzenie niniejszego dokumentu oraz dokumentów niższego rzędu odpowiedzialny jest Dyrektor.

Zmiana załączników do niniejszej polityki bezpieczeństwa nie wymaga zmiany samej polityki.

Wzory formularzy określone w niniejszej polityce mogą być prowadzone w wersji elektronicznej z użyciem aplikacji dedykowanej obsłudze systemu ochrony danych osobowych pod warunkiem, że systemy te odzwierciedlają minimalny zakres informacji ustalony w załącznikach.

2 PODSTAWY PRAWNE

2.1. OTOCZENIE PRAWNE

Podstawowe przepisy prawa w zakresie ochrony danych osobowych, mające wpływ na kształt niniejszej dokumentacji to:

- 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: **RODO, Rozporządzenie 2016/679**.
- Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. 2018 r. poz. 1000), dalej **Ustawa**.
- Ustawa o bibliotekach z dnia 27 czerwca 1997 r.
- Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego w sprawie sposobu i trybu zaliczania bibliotek do niektórych bibliotek naukowych oraz ustalenia ich wykazu z dnia 2 kwietnia 2012 r.

Kompletny wykaz aktów prawnych, jak również dokumentów zewnętrznych (wytyczne, opinie w zakresie przetwarzania danych osobowych itp.) jest prowadzony i aktualizowany przez IOD oraz udostępniany pracownikom i współpracownikom w razie potrzeby **[załącznik nr 8]**.

3 PODEJŚCIE OPARTE NA RYZYKU

3.1. Identyfikacja zagrożeń

Poniżej przytoczone przykłady zdarzeń stanowią wynik analizy najistotniejszych zagrożeń i ryzyk wynikających z przetwarzania danych osobowych w Bibliotece. W przypadku stwierdzenia zaistnienia zdarzenia z poniższego katalogu lub stwierdzenia prawdopodobieństwa zdarzenia mogącego mieć wpływ na obniżenie poziomu bezpieczeństwa przetwarzanych danych, należy poinformować o tym fakcie **IOD** (wysyłając wiadomość mailową lub telefonicznie):

Brak lub niewystarczające zabezpieczenia – brak lub nieaktualne oprogramowanie antywirusowe na komputerach, brak możliwości zapewnienia poufności / dostępności przetwarzanych danych (działania niezgodne z polityką czystego biurka i ekranu), brak klauzul informacyjnych na dokumentach, brak dowodów na wyrażenie zgody na przetwarzanie danych osobowych, kiedy jest wymagana, brak zapisów w regulaminach konkursów dot. ochrony danych osobowych.

Ujawnienie osobom nieupoważnionym danych osobowych (pośrednio np. na spotkaniu z rodzicami/opiekunami prawnymi, przesyłając wiadomość mailową błędnemu/niewłaściwemu adresatowi, w miejscu publicznym lub bezpośrednio innej osobie) albo informacji o zabezpieczeniach (np. informacji o konfiguracji, hasłach dostępu, miejscu przechowywania danych i ich zabezpieczeniu, przechowywania kluczy do pomieszczeń itp.).

Rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, kopiowanie dokumentów w celu ich wyniesienia poza Bibliotekę bez zgody Dyrektora, wynoszenie dokumentów (oryginały) poza Bibliotekę bez zgody Dyrektora, nie zamknięcie biura (pozostawienie sprzętu komputerowego (serwer, urządzenia mobilne), przesyłanie na swoją prywatną skrzyknę mailową dokumentów służbowych bez zgody Dyrektora, wykorzystanie danych ze zbiorów Biblioteki do celów prywatnych, celowe lub omyłkowe przekazanie danych osobowych podmiotom nieuprawnionym do ich przetwarzania, zbieranie danych osobowych bez podstawy prawnej, pozostawienie danych osobowych bez nadzoru (umożliwienie dostępu osobom trzecim poprzez zaniechania ustanowionych zabezpieczeń), itp.).

Przełamanie zabezpieczeń tradycyjnych – pozostawienie klucza w szafie/drzwiach/miejscu widocznym, dostępnym dla osób nieupoważnionych.

Niewłaściwe przechowywanie dokumentów zawierających dane osobowe (np. zagubione dokumenty, pozostawione karty biblioteczne z danymi, wywieszone informacje zawierające dane osobowe, z którymi mogą się zapoznać osoby nieupoważnione).

Zgłoszone przez rodziców/opiekunów skargi dotyczące przetwarzania danych osobowych

Brak upoważnienia do przetwarzania danych osobowych lub jego niewłaściwy zakres

Żądanie udostepnienia danych osobowych składane bezpośrednio do pracownika Biblioteki z pominięciem IOD

Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność pomieszczenia lub jego wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych, nagłe zaniki prądu, niestabilność napięcia w sieci.

Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, pozostawienie niezabezpieczonego sprzętu/oprogramowania np. przy pracach serwisowych, itp.

Pojawienie się komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów (np. komunikat o błędach lub awarii sprzętu, wykrytym wirusie) lub inny komunikat o podobnym znaczeniu.

Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie (niezgadzanie się danych źródłowych (np. wprowadzanych z dokumentu) z danymi z systemu jeżeli mają wpływ na zbiory danych osobowych przetwarzanych przez Bibliotekę (np. informacji wprowadzonych do Mateusza).

Próba modyfikacji lub modyfikacja danych bez odpowiedniego upoważnienia np. poprzez pracę na wspólnym koncie użytkownika lub włamanie na konto użytkownika bez jego wiedzy.

Ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub ich podglądu w nieautoryzowany sposób.

Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowanie lub kopiowanie danych.

Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

Wykaz zagrożeń referencyjnych prowadzony jest przez IOD w **[załączniku nr 1 do Procedury podejścia opartego na ryzyku]** tj. Kwestionariusza oceny ryzyka.

3.2. Podejście oparte na ryzyku

Wdrażanie zabezpieczeń pozwalających osiągnąć określony poziom ochrony danych osobowych odbywa się na podstawie:

- Oceny ryzyka, zgodnie z wymaganiami określonymi w Art. 24 RODO
- Wdrożenia zasad ochrony prywatności w fazie projektowania i domyślnej ochrony danych (PIA/Privacy by design/Privacy by default), zgodnie z wymaganiami określonymi w art. 25 RODO
- Wdrożeniu zasad przeprowadzania oceny skutków przetwarzania danych osobowych (DPIA), zgodnie z wymaganiami określonymi w art. 35 i 36 RODO

Ocena ryzyka wykonywana jest nie rzadziej niż raz w roku lub doraźnie, w przypadku zmian w otoczeniu lub działaniu Biblioteki mającym znaczący wpływ na przetwarzanie danych osobowych. O podejmowaniu działań związanych z oceną ryzyka decyduje osoba merytoryczna, realizująca działanie. Ocena ryzyka może zostać przeprowadzona również na wniosek IOD/pracownika wyznaczonego przez Dyrektora/Dyrektora.

Szczegółowe działania związane z podejściem opartym na ryzyku określa załącznik do niniejszej polityki – „Procedura podejścia opartego ryzyku" [Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych"].

Kluczowe procedury dotyczące ochrony danych osobowych

3.3. Rejestrowanie czynności przetwarzania

W Bibliotece wprowadza się obowiązek rejestrowania czynności przetwarzania.

Każdy pracownik Biblioteki ma obowiązek zgłoszenia czynności przetwarzania jakie realizuje do IOD lub Dyrektora w celu ich opisania w rejestrze czynności przetwarzania.

Rejestr czynności przetwarzania określa załącznik do niniejszej polityki bezpieczeństwa danych osobowych – „Rejestr czynności przetwarzania" [Załącznik nr 5 do Polityki bezpieczeństwa].

Rejestr czynności zawiera przynajmniej następujące informacje:

- Dane administratora danych osobowych (Nazwa oraz dane kontaktowe)
- Dane współadministratorów, (jeśli dotyczy) (Nazwa oraz dane kontaktowe)

- Dane Inspektora Ochrony Danych (Imię, Nazwisko i dane kontaktowe)
- Dane przedstawiciela administratora, (jeśli dotyczy) (Imię, Nazwisko lub nazwa i dane kontaktowe)
- Opis celów przetwarzania danych osobowych
- Opis kategorii osób, których dane dotyczą
- Opis kategorii danych, jakie będą przetwarzane
- Opis kategorii odbiorców danych, do których Biblioteka planuje dane przekazywać lub już przekazuje
- Informację czy dane będą przetwarzane w Państwach trzecich (poza Europejskim Obszarem Gospodarczym)
- Informacje o planowanych terminach usunięcia danych
- Ogólne informacje o zabezpieczeniach chroniących przetwarzanie danych w ramach wykonywanych czynności.

Informacje o czynnościach przetwarzania przekazują do IOD osoby merytoryczne, wskazane przez Dyrektora (np. członkowie stałych zespołów zadaniowych powoływanych Zarządzeniem Dyrektora).

W przypadku wątpliwości **IOD** udziela rekomendacji w zakresie wpisów w rejestrze czynności przetwarzania.

Rejestr jest aktualizowany przynajmniej raz na rok lub przy każdej zmianie w ramach realizowanych czynności przetwarzania. Za wprowadzenie zmian odpowiedzialne są osoby wyznaczone do prowadzenia rejestru.

IOD nadzoruje prawidłowość procesu rejestrowania czynności przetwarzania poprzez:

- Prowadzenie audytów;
- Udzielanie rekomendacji (w przypadku zidentyfikowania potencjalnych niezgodności lub obszarów, które wymagają regulacji);
- Udzielanie konsultacji (na wniosek).

Czynności przetwarzania nie ma obowiązku opisywania w rejestrze w przypadku, gdy łącznie spełniono następujące przesłanki:

- Przetwarzanie, nie powoduje ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- Przetwarzanie ma charakter sporadyczny;
- Przetwarzanie nie obejmuje szczególnych kategorii danych osobowych;
- Przetwarzanie nie obejmuje danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

W przypadku podjęcia decyzji o nieopisywaniu czynności przetwarzania w rejestrze należy ją skonsultować z **IOD**.

3.4. Nadawanie, zmiana, odbieranie Upoważnień do przetwarzania danych osobowych

W bibliotece zabrania się:

- Przetwarzać danych osobowych, do których nie posiada się uprawnień (zgodnie z art. 29 RODO dane osobowe można przetwarzać wyłącznie na polecenie Administratora danych);
- Ujawniać danych osobowych stronom trzecim, jeżeli te nie są uprawnione (na podstawie umowy powierzenia, przepisu prawa lub stosownych upoważnień) do ich otrzymania.

W celu zapewnienia nadzoru nad przetwarzaniem danych osobowych w Bibliotece, każda osoba dopuszczona do przetwarzania danych osobowych ma obowiązek posiadania upoważnienia do przetwarzania danych osobowych o odpowiednim zakresie oraz obowiązek zachowania danych osobowych w poufności co potwierdza złożeniem stosownego oświadczenia o zachowaniu poufności.

Wzór upoważnienia określa załącznik do niniejszej polityki bezpieczeństwa danych osobowych – „Upoważnienie do przetwarzania danych osobowych" [Załącznik nr 3 do Polityki bezpieczeństwa].

Upoważnienia nadawane są przez Administratora danych. Administrator danych może scedować nadawanie upoważnień na wyznaczoną osobę, która będzie nadawała upoważnienia w jego imieniu na podstawie pisemnego upoważnienia lub pełnomocnictwa szczególnego wystawionego przez Dyrektora.

IOD nadzoruje proces nadawania upoważnień do przetwarzania danych osobowych poprzez:

- Audyty,
- Doraźne kontrole aktualności.

Informacje dotyczące zatrudnienia nowego pracownika, zmian na stanowisku pracy czy też rozwiązania stosunku pracy przekazuje **IOD** niezwłocznie **Pracownik kadr** lub inna osoba wyznaczona przez **Dyrektora**.

W tym celu **IOD** jest uprawniony do otrzymania z kadr oraz od innych osób merytorycznych niezbędnych do przeprowadzenia audytu informacji.

IOD prowadzi rejestr osób upoważnionych, w którym odnotowuje:

- Imię i Nazwisko osoby upoważnionej
- Zakres upoważnienia
- Datę nadania upoważnienia
- Datę zmiany upoważnienia
- Datę odebrania upoważnienia
- Inne informacje istotne dla nadzorowania procesu nadawania upoważnień.

Upoważnienia przechowywane są przez **IOD** (wersja elektroniczna) oraz w aktach osobowych pracowników (wersja papierowa, przechowywana przez Pracownika Kadr).

Dyrektor w każdej chwili może podjąć decyzję o cofnięciu lub zmianie upoważnienia, w tym celu przekazuje dyspozycję mailową do **IOD lub innej osoby przez siebie wyznaczonej w celu przygotowania stosownego dokumentu.**

3.5. Powierzenie przetwarzania danych

W przypadku konieczności przetwarzania danych przez odrębne podmioty świadczące usługi dla **Administratora danych** może on powierzyć ich przetwarzanie, w drodze umowy zawartej na piśmie, pod następującymi warunkami:

Każda osoba odpowiedzialna za zawieranie umów ma obowiązek zweryfikować, czy w ramach zawartej umowy będą powierzane dane osobowe przez Bibliotekę. W przypadku weryfikacji pozytywnej (zachodzi powierzenie przetwarzania danych osobowych) osoba odpowiedzialna za zawarcie umowy ma obowiązek sporządzenia umowy powierzenia przetwarzania danych osobowych lub zawnioskowania o sporządzenie takiej umowy przez **IOD**.

Sporządzona jest umowa powierzenia przetwarzania danych osobowych w formie pisemnej. Dopuszcza się, aby funkcje uregulowań dotyczących powierzenia przetwarzania danych stanowiły zapisy w umowie właściwej (np. w formie wyodrębnionego rozdziału/sekcji regulującej przetwarzanie powierzonych danych osobowych) lub w formie aneksu do umowy **[wzór umowy w załączniku nr 6]**.

Podmiot, któremu powierzono przetwarzanie danych, może przetwarzać je wyłącznie w zakresie, celu i na warunkach przewidzianych w umowie.

Administrator danych może skorzystać z prawa do kontroli przetwarzania powierzonych danych. W tym celu może żądać udzielenia informacji od podmiotu przetwarzającego lub przeprowadzić u niego kontrolę.

Podmiot przetwarzający ma obowiązek realizować zadania określone w art. 28 RODO a w szczególności:

- ✔ Informować o zidentyfikowanych naruszeniach ochrony danych osobowych;
- ✔ Upoważnić swoich pracowników do przetwarzania danych powierzonych przez Bibliotekę oraz zobowiązać ich do zachowania poufności;
- ✔ Przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające, o których mowa w art. 24 i 32 RODO. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak Administrator danych;
- ✔ Poinformować Administratora danych o podpowierzaniu danych;

IOD gromadzi informacje o podmiotach, z którymi Administrator danych zawarł umowy powierzenia przetwarzania danych w celu ich ewidencjonowania i zapewnienia bezpieczeństwa powierzanych danych **[wzór rejestru w załączniku nr 7]**.

3.6. KLAUZULE ZGODY I OBOWIĄZEK INFORMACYJNY

Biblioteka zbiera dane osobowe bezpośrednio od osób, których dane dotyczą, w związku z tym jak każdy administrator danych ma obowiązek zapewnić dostęp do informacji, o których mowa w Art. 13 RODO. W tym celu wszędzie tam, gdzie ADO uzna to za konieczne zamieszczona jest treść klauzuli informacyjnej.

Treść klauzuli musi być zgodna z wymaganiami art. 13 RODO lub Art. 14 RODO.

Dopuszczalne sposoby informowania to:

- Strona www
- Tablica informacyjna
- Klauzule na dokumentach

W przypadku, gdy Biblioteka otrzymuje dane z innego źródła niż od osoby, której dane dotyczą na podstawie i w celu realizacji zadania publicznego, podlega wyłączeniu od obowiązku informacyjnego na mocy art. 14 ust 5 RODO.

Biblioteka zbiera zgody na przetwarzanie danych osobowych.

Treść klauzuli zgody brzmi następująco:

> *„Wyrażam zgodę na przetwarzanie moich danych osobowych podanych w **[powyższym formularzu /oświadczeniu]** w celach **[należy wpisać, w jakim celu]** przez Miejską Bibliotekę Publiczną w Kobyłce im. Stanisława Ryszarda Szpotańskiego przy ul. Leśna 8 lokal 0.3 05-230 Kobyłka .*

Elementem obowiązkowym klauzuli zgody na przetwarzanie danych osobowych jest klauzula informacyjna zgodna z wymaganiami art. 13 RODO, w tym w szczególności informacja o możliwości odwołania zgody w każdym czasie.

Informacje nt. wyrażonych zgód przechowują pracownicy Biblioteki w segregatorach.

IOD na podstawie informacji udzielonych przez pracowników Biblioteki identyfikuje dokumenty i formularze, w których niezbędne jest umieszczenie klauzuli informacyjnej oraz zgody.

3.7. PRZEGLĄDY I KONSERWACJE ZABEZPIECZENIA DANYCH W SYSTEMACH INFORMATYCZNYCH

Za przeglądy i konserwacje urządzeń służących do przetwarzania danych osobowych odpowiedzialny jest ASI. ASI w na bieżąco zapewnia poprawność działania urządzeń służących do przetwarzania danych. Każde urządzenie, na którym przetwarzane są dane osobowe powinno być zabezpieczone z użyciem co najmniej poniższych standardów.

Do każdego urządzenia i aplikacji służących do przetwarzania danych osobowych należy ustanowić obowiązkowe uwierzytelnianie (z zastosowaniem unikalnego identyfikatora i hasła dostępu o długości co najmniej 8 znaków (małe i wielkie litery, cyfry lub znaki specjalne).

Każde urządzenie i/lub aplikacja służące do przetwarzania danych osobowych muszą być chronione przez licencjonowane (legalne) oprogramowanie zapewniające ochronę przed oprogramowaniem szkodliwym (wirusy, trojany, malware, spyware itp.).

Urządzenia i aplikacje służące do przetwarzania danych osobowych wynoszone poza siedzibę Biblioteki, powinny być zabezpieczone hasłem dostępu a nośniki danych zaszyfrowane.

Dla każdej bazy danych zawierającej dane osobowe, należy sporządzać kopie zapasowe lub zapewnić inną możliwość odtworzenia danych na wypadek awarii.

Użytkownicy przetwarzający dane lokalnie mają obowiązek wykonywania kopii zapasowych we własnym zakresie.

3.8. Przeglądy i aktualizacja polityki bezpieczeństwa danych osobowych

Polityka bezpieczeństwa danych osobowych podlega corocznemu przeglądowi pod kątem aktualności. Okresowy przegląd polityki bezpieczeństwa powinien mieć na celu stwierdzenie, czy postanowienia dokumentu odpowiadają aktualnej i planowanej działalności Biblioteki.

Polityka bezpieczeństwa danych osobowych powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami w funkcjonowaniu Biblioteki, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

Zmiany niniejszej polityki bezpieczeństwa wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w Bibliotece.

Projekt aktualizacji polityki bezpieczeństwa przygotowuje Inspektor Ochrony Danych.

4 Prawa osób, których dane dotyczą

4.1. Prawa osób, których dane dotyczą

Biblioteka, jako Administrator danych osobowych uwzględnia w prowadzonej działalności prawa osób, których dane dotyczą.

Realizacja praw odbywa się zgodnie z zasadami opisanymi w niniejszej polityce.

Dla celów obsługi żądań osób, których dane dotyczą lub kontrahentów podaje się na stronie www i w innych materiałach (np. papierowa wersja klauzuli informacyjnej lub umowa powierzenia) **kontakt do Inspektora Ochrony Danych**, jeśli został wyznaczony lub informację, pod jakim adresem email i/lub numerem telefony można składać wnioski w zakresie praw osób, których dane dotyczą.

W przypadku, gdy pracownik Biblioteki otrzymał wniosek/zapytanie od osoby, której dane dotyczą w zakresie realizacji jego praw i jest w stanie samodzielnie go obsłużyć (np. usunąć dane; wycofać zgodę na przetwarzanie danych itp.), ma obowiązek poinformować o tym zdarzeniu Inspektora Ochrony Danych poprzez przesłanie takiej informacji na emaila (lub inny wskazany przez Dyrektora) lub załączenie go do korespondencji w kopii wiadomości, (jeśli przesłano odpowiedź poprzez email).

W przypadku, gdy zgłoszenie realizacji praw osoby, której dane dotyczą złożone zostało przez telefon, pracownik przyjmujący zgłoszenie ma obowiązek sporządzić z niego notatkę i przesłać na skrzynkę e-mail iod@biblioteka.kobylka.pl lub inny wskazany przez Dyrektora.

W przypadku, gdy pracownik sam nie jest w stanie zrealizować żądania, przekazuje on sprawę na skrzynkę mailową lub inny wskazany przez Dyrektora. Na podstawie takiego zlecenia Dyrektor, przy wsparciu Inspektora Ochrony danych udziela odpowiedzi na wniosek/żądanie.

Odpowiedź jest archiwizowana na skrzynce pocztowej lub segregatorze, jako dowód na realizacje wniosku z uwzględnieniem okresów retencji danych.

4.2. Prawo do wycofania zgody na przetwarzanie danych osobowych w każdym czasie

Osoba, która wyraziła zgodę na przetwarzanie danych osobowych może ją odwołać w każdym czasie. W związku z tym, wprowadza się następujące zasady odwoływania zgód na przetwarzanie danych osobowych.

Pracownik Biblioteki, który otrzymał dyspozycję odwołania zgody (wycofania zgody) na przetwarzanie danych osobowych przez osobę, która ją wyraziła lub jej pełnomocnika ma obowiązek poinformowania o wpłynięciu dyspozycji osoby współpracujące tak, aby wiedza o wycofaniu zgody była powszechna.

Pracownik Biblioteki lub Informatyk odpowiedzialny za zarządzanie bazą danych ma obowiązek usunąć dane z systemów i aplikacji (programu Mateusz do obsługi czytelników i wypożyczalni; bazy danych).

Od momentu odwołania zgody na przetwarzanie danych osobowych nie można już przetwarzać ich w celu, na który była wyrażona zgoda.

Biblioteka może dalej przechowywać dane po odwołaniu zgody na ich przetwarzanie, wyłącznie w celu zabezpieczenia przyszłych roszczeń lub gdy ma obowiązek ich przechowywania dla innych prawnie usprawiedliwionych celów (np. podatkowych; sprawozdawczych; kontrolnych itp.).

4.3. Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora danych niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

W przypadku złożenia dyspozycji uzupełnienia niekompletnych danych osobowych, pracownik przyjmujący dyspozycję aktualizuje dane lub gdy nie ma takiej możliwości przekazuje sprawę do realizacji do Informatyka lub pracownika Biblioteki, który realizuje wniosek w imieniu Administratora danych.

Pracownik ma prawo zażądać od osoby, której dane dotyczą dowodów na potwierdzenie tożsamości osoby, która składa dyspozycję.

4.4. Prawo do usunięcia danych

Każda osoba, której dane dotyczą ma prawo złożenia dyspozycji ich usunięcia.

Z prawa do usunięcia danych może skorzystać osoba:

- Której dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- Która wycofała zgodę na przetwarzanie danych osobowych;
- Której dane osobowe były przetwarzane niezgodnie z prawem;
- Której dane przetwarzane są na podstawie umowy i umowa ta wygasła lub została rozwiązana;
- Której dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator;
- Której dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w Artykuł 8 ust. 1. bez zachowania warunków w nim określonych.

W przypadku spełnienia powyższych warunków, pracownik przyjmujący dyspozycję usuwa dane w imieniu Administratora danych.

O usunięciu danych każdorazowo informowany jest IOD (drogą e-mailową).

4.5. Prawo do przeniesienia danych

Każda osoba, której dane przetwarzane są na podstawie przesłanki umowy lub zgody na przetwarzanie danych osobowych w sposób zautomatyzowany ma prawo zwrócić się do Dyrektora z dyspozycją:

- Wydania kopii danych, które przetwarza Administrator;
- Przeniesienia określonych danych do innego Administratora .

W tym celu pracownik Biblioteki przekazuje wniosek (po konsultacjach z IOD, jeśli został wyznaczony) bezpośrednio do Dyrektora, który realizuje wniosek w imieniu Administratora danych.

W Bibliotece Prawo do przeniesienia danych nie może być zrealizowane odnośnie przeniesienia danych, przetwarzanych na podstawie przepisów prawa.

4.6. Prawo do ograniczania przetwarzania danych osobowych

Biblioteka ogranicza przetwarzanie danych osobowych w przypadkach i na zasadach określonych poniżej:

- Osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych;
- Przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- Osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Dane osobowe podlegające ograniczonemu przetwarzaniu są wyraźnie oznaczone, tak, aby pracownicy wiedzieli, że można je przetwarzać wyłącznie na zasadach określonych w niniejszej polityce bezpieczeństwa.

4.7. Prawo do sprzeciwu wobec przetwarzania danych osobowych

Biblioteka umożliwia realizację prawa do sprzeciwu wobec przetwarzania danych osobowych:

- W zakresie marketingu bezpośredniego usług i produktów administratora danych świadczonych na podstawie przesłanki prawnie usprawiedliwionego celu, Art. 6 ust 1 lit f) RODO.
- W zakresie podejmowania automatycznych decyzji wywołujących skutki prawne (w tym oceny ryzyka kredytowego i profilowania), Art. 22 RODO.
- W zakresie prowadzenia badań naukowych lub historycznych lub do celów statystycznych na mocy Artykuł 89 ust. 1 RODO.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania danych osobowych nie wolno już przetwarzać do takich celów. Zostają one oznaczone, jako dane, których przetwarzanie zostało ograniczone.

Biblioteka po wniesieniu sprzeciwu przez osobę, której dane dotyczą, zaprzestaje przetwarzania takich danych, chyba, że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

W przypadku, gdy został wniesiony sprzeciw a Administrator danych wyraża wolę przetwarzania danych osoby, która złożyła sprzeciw należy ten fakt skonsultować z Inspektorem Ochrony Danych, jeśli został wyznaczony, który wydaje rekomendację w tej sprawie.

5. NARUSZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Dyrektor zarządza naruszeniami ochrony danych osobowych zgodnie z wymaganiami Art. 37 RODO.

Każdy pracownik Biblioteki ma obowiązek zgłaszania naruszeń przetwarzania danych osobowych do IOD lub na adres mailowy iod@biblioteka.kobylka.pl lub inny wskazany przez Dyrektora.

Wszelkie szczegółowe informacje dot. postępowania w przypadku wystąpienia naruszenia przetwarzania danych znajdują się w „Procedurze zarządzanie naruszeniami danych osobowych".

6. RETENCJA DANYCH

Biblioteka, zgodnie z zasadą ograniczania przetwarzania danych osobowych określa okresy retencji danych.

Okresy retencji danych osobowych ustalone są w zależności od celów ich przetwarzania zgodnie z poniższym standardem:

- **Dla celów realizacji umowy** – przez okres trwania umowy
- **Dla celów realizacji przepisu prawa** – przez okres wymagalności przepisu prawa lub przez okres podany w przepisie prawa
- **Dla celów rozpatrywania skarg i zgłoszonych roszczeń** – do momentu przedawnienia potencjalnych roszczeń z tytułu naruszenia przetwarzania danych
- **Dla celów windykacji i dochodzenia roszczeń**– do momentu przedawnienia potencjalnych roszczeń osoby, której dane dotyczą
- **Dla celów związanych z prowadzeniem postępowań sądowych** – dane mogą być przetwarzane do 10 lat od dnia wydania prawomocnego orzeczenia kończącego postepowanie;
- **Dla celów tworzenia zestawień, analiz i statystyk**– przez czas trwania umowy, a następnie nie dłużej niż przez okres, po którym przedawnią się roszczenia wynikające z umowy;
- **Dla celów archiwalnych** – okresy przechowywania danych opisano szczegółowo w Jednolitym Rzeczowym Wykazie Akt, które prowadzi Biblioteka.

7. ZAPEWNIENIE ŚWIADOMOŚCI I KOMPETENCJI PRACOWNIKÓW W ZAKRESIE ZGODNEGO Z PRAWEM PRZETWARZANIA DANYCH OSOBOWYCH

W ramach zapewnienia niezbędnej świadomości i kompetencji pracowników w zakresie ochrony danych osobowych realizuje się następujące działania:

- Zapoznaje się pracownika z dokumentacją ochrony danych osobowych
- Przeprowadza się szkolenia dla nowoprzyjętych pracowników
- Prowadzi się szkolenia okresowe
- Zapewnia się dostępność Inspektora Ochrony Danych, który udziela konsultacji i rekomendacji w zakresie związanym z ochroną danych osobowych na życzenie pracowników
- Komunikuje się wszystkim pracownikom zagrożenia i ważne zdarzenia w zakresie ochrony danych osobowych (dobre praktyki, zmiany przepisów, głośne medialnie naruszenia mogące mieć znaczenie na działanie administratora danych).

Każdy nowy pracownik przed przystąpieniem do pracy, zobowiązany jest do ukończenia szkolenia związanego z ochroną danych osobowych, zapoznania się z wymogami stanowiskowymi w zakresie bezpiecznego przetwarzania danych osobowych,

Szkolenia okresowe przeprowadzane są nie rzadziej niż raz na 2 lata.

Szkolenia może prowadzić:

- **Inspektor Ochrony Danych** – szkolenia okresowe i wstępne.
- **Osoba wyznaczona przez Dyrektora**– szkolenia doraźne w zakresie przekazania wiedzy o rekomendacjach udzielonych przez IOD
- **Firma zewnętrzna** – szkolenia okresowe i specjalistyczne.

8. MONITOROWANIE SYSTEMU OCHRONY DANYCH OSOBOWYCH

W celu zapewnienia aktualności z bieżącymi standardami ochrony danych oraz obowiązującymi przepisami prawa wprowadza się obowiązek monitorowania systemu ochrony danych osobowych.

Monitorowanie polega na:

- Monitorowaniu przez pracowników Biblioteki w zakresie realizacji swoich obowiązków służbowych
- Monitorowaniu przez Informatyka/firmę IT w zakresie związanym z bezpieczeństwem technicznym infrastruktury i bazy danych.
- Nadzorowaniu procesów przetwarzania danych osobowych przez Inspektora Ochrony Danych lub inną osobę wyznaczoną przez Dyrektora
- Prowadzeniu okresowych audytów ochrony danych
- Prowadzeniu doraźnych audytów ochrony danych lub u podmiotu przetwarzającego.

Inspektor Ochrony Danych lub inna osoba wyznaczona przez Dyrektora prowadzi audyty w celu potwierdzenia zgodności przetwarzania danych osobowych w Bibliotece z obowiązującymi przepisami prawa i regulacjami wewnętrznymi.

O zamiarze przeprowadzenia audytu IOD informuje osoby zainteresowane w terminie minimum 7 dni przed przeprowadzeniem audytu.

Z przeprowadzonego audytu IOD sporządza raport, w którym opisuje minimum:

- Cel przeprowadzenia audytu
- Zakres podlegający audytowaniu
- Opis
- Dowody na zgodność lub niezgodność z przepisami prawa/wewnętrznymi procedurami.
- Rekomendacje dla systemu ochrony danych osobowych
- Opis działań doskonalących uzgodnionych w celu zaradzenia niezgodnościom.

Raport przesyłany jest do Dyrektora lub osoby przez niego wyznaczonej w celu uzgodnienia działań doskonalących.

9. ZABEZPIECZENIA (ŚRODKI TECHNICZNE I ORGANIZACYJNE SŁUŻĄCE DO OCHRONY DANYCH OSOBOWYCH)

9.1. ŚRODKI ORGANIZACYJNE OCHRONY DANYCH OSOBOWYCH

W Bibliotece stosuje się następujące środki organizacyjne w celu zabezpieczenia przetwarzanych danych osobowych.:

- ✔ Przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań („zakresów obowiązkowi czynności pracowniczych"). Każde odstępstwo od tej reguły wymaga zgody **Dyrektora lub osoby przez Dyrektora upoważnionej**.
- ✔ Zgodnie z art. 37 RODO, Administrator danych **powołuje Inspektora Ochrony Danych (IOD).**

- ✔ **IOD** nadzoruje przetwarzanie danych osobowych w Bibliotece, ma możliwość wydawania rekomendacji w zakresie zabezpieczeń dotyczących danych osobowych.
- ✔ **IOD** jest bezpośrednio podległy **Dyrektorowi.**
- ✔ **Administrator danych (Dyrektor)** zgłasza **IOD** do UODO w celu zarejestrowania na formularzu https://www.biznes.gov.pl/opisy-procedur/-/proc/871-zawiadomienie-o-wyznaczeniu-nowego-iod/45 lub listownie.
- ✔ **IOD** prowadzi **Rejestr osób upoważnionych do przetwarzania danych osobowych**.
- ✔ **IOD** prowadzi **Rejestr czynności przetwarzania.**
- ✔ **IOD** prowadzi **Rejestr umów powierzenia przetwarzania danych osobowych**
- ✔ **IOD** prowadzi planowe audyty ochrony danych osobowych. **Audytom mogą podlegać m.in.**
    - dokumentacja opisująca sposób przetwarzania oraz ochrony zbiorów danych
    - podstawy prawne przetwarzania danych przez pracowników (m.in. aktualność i zakres upoważnień do przetwarzania danych osobowych oraz rejestru osób upoważnionych)
    - prawidłowość informowania o przetwarzanych zbiorach danych (obowiązek informacyjny)
    - podstawy prawne przetwarzania danych osobowych przez Administratora danych
    - realizowanie przez pracowników wymagań opisanych w niniejszej dokumentacji, przepisach prawa dotyczących ochrony danych osobowych i innych procedur wewnętrznych
    - fizyczne zabezpieczenia pomieszczeń, w których przetwarzane są informacje
    - poprawność zabezpieczeń danych przetwarzanych metodami tradycyjnymi (dokumentacja papierowa)
    - sposób pracy serwisu IT (wykonywania napraw, konserwacji, aktualizacji, zabezpieczania oraz likwidacji urządzeń i programów komputerowych)
    - sposób działania oprogramowania antywirusowego (legalność, aktualizacje)
    - wykonywanie kopii zapasowych
    - mechanizmy uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych
    - zawieranie umów powierzania przetwarzania danych osobowych (prawidłowość zawierania umów, zakres i celowość zawierania umów, sposób zabezpieczania powierzonych danych)
    - inne działania pracowników Biblioteki związane bezpośrednio z przetwarzaniem danych osobowych.
- ✔ Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie.**
- ✔ Każdy pracownik Biblioteki, zapoznaje się z niniejszą polityką bezpieczeństwa i zasadami w niej opisanymi. Nowo przyjęty pracownik odbywa instruktaż lub zostaje przeszkolony przed przystąpieniem do przetwarzania danych z podstawowych obowiązków wynikających z niniejszej dokumentacji i przepisów dotyczących ochrony danych osobowych
- ✔ Każdy upoważniony do przetwarzania danych **potwierdza pisemnie** fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument jest dołączany do akt osobowych (Oświadczenie o zapoznaniu się z dokumentacją i zasadami bezpieczeństwa)
- ✔ Określony obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych
- ✔ Przebywanie osób, nieuprawnionych w w/w obszarze jest dopuszczalne wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych
- ✔ Pomieszczenia stanowiące obszar przetwarzania danych są zamykane na klucz. Klucze przechowywane są:
    - w szafce na klucze w pomieszczeniu socjalnym (klucze do pomieszczenia mają wskazane osoby)
    - zapasowe klucze znajdują się w szyfrowanym sejfie na klucze w gabinecie dyrektora
    - Księgowa i Specjalista ds. płac pobierają klucz do pokoju księgowość od pracownika obecnego na zmianie

- ✔ Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym
- ✔ Przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna, drzwi oraz usunąć z biurka wszystkie dokumenty i nośniki z danymi osobowymi tak, aby nie było możliwości dostępu do nich dla osób nieupoważnionych (np. sprzątających pomieszczenia)
- ✔ Numery telefonów/kontakty mailowe (informatyk, firma hostingowa, księgowa, straż pożarna, pogotowie energetyczne, policja, ochrona, IOD) są dostępne dla wszystkich pracowników. W razie zidentyfikowania zagrożeń przy przetwarzaniu danych w pierwszej kolejności zgłaszane są one do Dyrektora lub do IOD
- ✔ Pracownicy mają obowiązek usuwania plików roboczych zawierających dane osobowe (np. listy dzieci (wersje elektroniczne))
- ✔ Pracownicy Biblioteki mający dostęp do systemów informatycznych mają obowiązek okresowej zmiany haseł dostępu do systemów, w których przetwarzają dane osobowe zgodnie z procedurami określonymi w Procedurach Zarządzania Systemem Informatycznym.

9.2. Środki techniczne ochrony danych osobowych

Zbiory danych przetwarzane w Bibliotece zabezpiecza się poprzez:

1. **Środki ochrony fizycznej:**
   - ✔ Przechowywanie danych osobowych w pomieszczeniach zamykanych na klucz, do których dostęp mają tylko osoby upoważnione przez **Administratora danych**
   - ✔ Zbiory danych osobowych w formie papierowej przechowywane są w zamykanych szafach w gabinecie dyrektora oraz pokoju księgowości
   - ✔ Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarki do dokumentów.

2. **Środki sprzętowe, infrastruktury informatycznej i telekomunikacyjnej:**
   - ✔ Zastosowano środki ochrony przed szkodliwym oprogramowaniem (Program Antywirusowy , firewall programowy)
   - ✔ Zainstalowano wygaszacze ekranów na urządzeniach, na których przetwarzane są dane osobowe.
   - ✔ Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej (serwer)
   - ✔ Dostęp do stacji roboczych możliwy jest po uprzednim uwierzytelnieniu
   - ✔ Użyto system Firewall do ochrony dostępu do sieci komputerowej.

3. **Środki ochrony w ramach systemowych narzędzi programowych i baz danych:**
   - ✔ Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbiorów danych osobowych
   - ✔ Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanych zbiorów danych osobowych (Mateusz)
   - ✔ Dostęp do zbiorów danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
   - ✔ Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych
   - ✔ Zainstalowano wygaszacze ekranów na urządzeniach, na których przetwarzane są dane osobowe
   - ✔ Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (wylogowanie po 1 minutach nieaktywności).

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określają **Procedury zarządzania systemem informatycznym** służącym do przetwarzania danych osobowych.

10. CIĄGŁOŚĆ DZIAŁANIA

Plan ciągłości działania jest opisaniem czynności zapewniających przywrócenie dostępności działań i usług realizowanych przez Bibliotekę w przypadkach wystąpienia incydentu ciągłości działania. Realizacja planu ciągłości działania ma za zadanie zapewnić skrócenie okresu niedostępności oraz jak najszybsze przywrócenie pełnej dostępności usług.

W Bibliotece podjęto środki organizacyjne na wypadek utraty ciągłości działania, na które składa się:

- opracowanie oceny ryzyka uwzgledniającej czynniki mogące wpływać na zaburzenie ciągłości działania (utrata danych, pożar, zalanie, utrata zasiania, itd.)
- zastosowanie zabezpieczeń np.: system zasilania gwarantowanego UPS-y podtrzymujące zasilanie serwera i pozostałych kluczowych elementów systemu IT do czasu bezpiecznego wyłączenia, listwy przeciwprzepięciowe
- opracowanie planu ciągłości działania na wypadek incydentu ciągłości działania wpływających na ochronę danych osobowych dla zdarzeń z wysokim poziomem ryzyka albo takich, które zostały wskazane przez Administratora Danych.

Bibliotece w przypadku niedostępności Inspektora Ochronny Danych Osobowych spowodowaną absencją lub niedostępnością wyznaczono Zastępcę Inspektora Ochronny Danych Osobowych jako osobę kontaktową z podmiotami danych, organem nadzorczym.

10.1. POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA INCYDENTU CIĄGŁOŚCI DZIAŁANIA MAJĄCEGO WPŁYW NA OCHRONĘ DANYCH OSOBOWYCH

Plan postępowania na wypadek wystąpienie incydentu ciągłości działania mającego wpływ na ochronę danych osobowych został opracowany na podstawie oceny ryzyka, w której wskazano zdarzenia mające wpływ na ciągłość działania, które są na nieakceptowalnym przez organizację poziomie ryzyka i dla których Administrator Danych podjął taką decyzję.

Wzór planu ciągłości działania na wypadek wystąpienie incydentu ciągłości działania mającego wpływ na ochronę danych osobowych określa załącznik do niniejszej polityki bezpieczeństwa – „Plan postępowania na wypadek wystąpienie incydentu ciągłości działania mającego wpływ na ochronę danych osobowych" [Załącznik nr 9 do Polityki bezpieczeństwa].

ZAŁĄCZNIKI

1. Załącznik nr 1 - Procedura podejścia opartego na ryzyku.
2. Załącznik nr 2 - Procedury Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Bibliotece.
3. Załącznik nr 3 – Upoważnienie do przetwarzania danych osobowych.
4. Załącznik nr 4 - Rejestr osób upoważnionych do przetwarzania danych osobowych
5. Załącznik nr 5 – Rejestr czynności przetwarzania
6. Załącznik nr 6 – Wzór umowy powierzenia przetwarzania danych osobowych.
7. Załącznik nr 7 - Wzór Rejestr umów powierzenia przetwarzania danych osobowych.
8. Załącznik nr 8 – Wykaz aktów prawnych.
9. Załącznik nr 9 – Plan postępowania na wypadek wystąpienie incydentu ciągłości działania mającego wpływ na ochronę danych osobowych

Załącznik nr 1 do Polityki bezpieczeństwa danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

PROCEDURA PODEJŚCIA OPARTEGO NA RYZYKU

Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Spis treści

DEFINICJE

Administrator Danych/ Administrator Danych Osobowych/ ADO – Administratorem danych osobowych jest Miejska Biblioteka Publiczna w Kobyłce im. Stanisława Ryszarda Szpotańskiego przy ul. Leśna 8 lokal 0.3 05-230 Kobyłka. (dalej: MBP), ADO reprezentowany jest przez Dyrektora Biblioteki (dalej: Dyrektor).

Dane Osobowe – dane osobowe w rozumieniu art. 4 RODO, przetwarzane przez Bibliotekę tj. wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą").

DPIA – Ocena Skutków dla Ochrony Danych. Proces oceny niezbędności, proporcjonalności stopnia naruszenia praw i wolności osób, których dane dotyczą realizowany dla nowych operacji przetwarzania z użyciem danych osobowych

Dyrektor – Dyrektor Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego.

Inspektor Ochrony Danych (IOD) – Osoba wyznaczona przez Administratora danych zgodnie z Art. 37 RODO mająca w obowiązkach nadzorowanie systemu ochrony danych osobowych w MBP, którego zasady zostały opisane w niniejszej polityce.

Następstwo - konsekwencje, jakie może wywołać zdarzenie.

Organ nadzorczy – Urząd Ochrony Danych Osobowych, niezależny organ publiczny ustanowiony w celu kontroli realizacji przepisów o ochronie danych osobowych, na czele którego stoi Prezes Urzędu Ochrony Danych Osobowych.

Osoba odpowiedzialna za obszar - osoba odpowiedzialna za dany zakres działania organizacji: w przypadku procesu – właściciel procesu, w przypadku działań realizowanych przez komórkę organizacyjną kierownik tej komórki, w przypadku wybranych zagadnień osoba wyznaczona przez kierującego organizacją np. pełnomocnik, w przypadku projektu – kierownik projektu.

PIA – Ocena Skutków dla Prywatności. Proces oceny niezbędności, proporcjonalności identyfikacji ryzyk naruszenia praw i wolności osób, których dane dotyczą realizowany dla wszystkich nowych operacji przetwarzania z użyciem danych osobowych w ramach wdrożenia w organizacji zasad ochrony prywatności w fazie projektowania w celu zapewnienia zgodności z wymaganiami przepisów o ochronie danych osobowych.

Podatność - słabość lub wrażliwość, która tworzy pozytywne środowisko do wystąpienia zdarzenia/ zagrożenia.

Poziom ryzyka - wielkość ryzyka lub kombinacji ryzyk, wyrażona w postaci iloczynu następstw oraz ich prawdopodobieństwa.

Polityka Bezpieczeństwa – Polityka bezpieczeństwa danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

Pracownik – osoba wykonująca prace pod nadzorem Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego na podstawie formalnych ustaleń (osoba pracująca (na podstawie stosunku pracy) oraz współpracująca (na podstawie zlecenia, umowy o dzieło, lub innego rodzaju umowy cywilnoprawnej (UCP)). Osobą taką jest pracownik (nauczyciel/pracownik administracyjny) związany umową o pracę, jak również inne osoby np.: praktykanci, wykonujące prace na podstawie umów cywilnych.

Informatyk, Pracownik IT, ASI- dedykowana osoba do obsługi informatycznej Biblioteki. Może to być dedykowana osoba z firmy zewnętrznej, z którą MBP posiada umowę na świadczenie takich usług lub osoba wyznaczona przez Dyrektora posiadająca odpowiednie kompetencje.

Prawdopodobieństwo - możliwość, szanse wystąpienia zdarzenia/ zagrożenia.

Przetwarzanie danych osobowych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

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

Ryzyko - wpływ niepewności na cele. Ryzyko jest wyrażane, jako kombinacja następstw zdarzenia/ zagrożenia i związanego z nim prawdopodobieństwa jego wystąpienia.

Ryzyko nieodłączne - ryzyko bez uwzględnienia stosowanych środków kontrolnych.

Ryzyko rezydualne (szczątkowe) - ryzyko pozostające po zastosowaniu środków kontrolnych.

System informatyczny – każdy program/aplikacja używana w Bibliotece, służący do przetwarzania danych osobowych.

Środek kontroli - wszystko, co modyfikuje ryzyko.

Użytkownik – osoba fizyczna korzystająca z systemów teleinformatycznych służących do przetwarzania danych osobowych których administratorem jest Biblioteka.

Zdarzenie - wystąpienie lub zmiana konkretnego zestawu okoliczności.

Zagrożenie - potencjalną przyczyna niepożądanego zdarzenia.

1. CEL PROCEDURY

Celem niniejszego dokumentu jest określenie zasad stosowanych w zakresie podejścia opartego na ocenie ryzyka wynikających z Art. 24,25,35 i 36 RODO.

Wdrażanie zabezpieczeń pozwalających osiągnąć określony poziom ochrony danych osobowych odbywa się na podstawie:

- oceny ryzyka, zgodnie z wymaganiami określonymi w Art. 24 RODO
- wdrożeniu zasad ochrony prywatności w fazie projektowania i domyślnej ochrony danych (PIA/Privacy by design/Privacy by default), zgodnie z wymaganiami określonymi w art. 25 RODO
- wdrożeniu zasad przeprowadzania oceny skutków przetwarzania danych osobowych (DPIA), zgodnie z wymaganiami określonymi w art. 35 i 36 RODO

W związku z powyższym wprowadza się zasady określające wymagania w zakresie podejścia opartego na ryzyku określone w niniejszej procedurze i zobowiązuje do ich stosowania.

2. UCZESTNICY PROCEDURY I ICH OBOWIĄZKI I UPRAWNIENIA

2.1. PRACOWNIK/WSPÓŁPRACOWNIK

2.1.1. Uczestniczy w ocenie ryzyka/ocenie PIA/Ocenie DPIA
2.1.2. Udziela niezbędnych informacji dotyczących zidentyfikowanych zagrożeń
2.1.3. Zgłasza zidentyfikowane zagrożenia do bezpośredniego przełożonego lub Inspektora Ochrony Danych.

2.2. INSPEKTOR OCHRONY DANYCH (INSPEKTOR, IOD)

2.2.1. Nadzoruje proces podejścia opartego na ryzyku
2.2.2. Udziela rekomendacji Administratorowi danych w zakresie planu postępowania z ryzykiem oraz wdrażania zabezpieczeń.

2.3. ADMINISTRATOR DANYCH

2.3.1. Podejmuje decyzje o wdrożeniu planu postępowania z ryzykiem
2.3.2. Podejmuje decyzje o przeprowadzeniu oceny skutków dla ochrony danych (DPIA)
2.3.3. Podejmuje decyzje o konsultacjach z organem nadzorczym w zakresie DPIA o wysokim ryzyku naruszenia praw i wolności osób, których dane dotyczą.

3. SPOSÓB DZIAŁANIA

3.1. OCENA RYZYKA

W MBP wdraża się obowiązek przeprowadzenia oceny ryzyka.

Proces oceny ryzyka prowadzony jest zgodnie z przyjętym sposobem postępowania:

3.1.1. Ocena ryzyka przeprowadzana jest wspólnie dla całego zakresu działania organizacji
3.1.2. Ocenę ryzyka przeprowadza IOD / osoba odpowiedzialna w organizacji za ochronę danych osobowych

3.1.3. IOD / osoba odpowiedzialna w organizacji za ochronę danych osobowych dokonując oceny ryzyka może powołać zespół ds. oceny ryzyka lub współpracować z osobami odpowiedzialnymi za obszar. Osoby odpowiedzialne za obszar są zobligowane do aktywnego wsparcia IOD/ osoby odpowiedzialna w organizacji za ochronę danych osobowych w przeprowadzeniu oceny ryzyka i jeżeli ma to zastosowanie w opracowanie planu postępowania z ryzykiem

3.1.4. Ocena ryzyka przeprowadzana jest, co najmniej raz w roku oraz w przypadkach, gdy wystąpią istotne zmiany kontekstu działania organizacji, tak zdecyduje Administrator Danych albo zmaterializują się istotne ryzyka

3.1.5. Na zarządzanie ryzykiem składa się:

- Ocena ryzyka: identyfikacja ryzyka, analiza ryzyka, ewaluacja ryzyka
- Postępowanie z ryzykiem w tym modyfikacja ryzyka

3.1.6. Przez identyfikację ryzyka rozumie się wyspecyfikowanie zagrożeń /zdarzeń ich następstw i prawdopodobieństwa

3.1.7. Przez analizę ryzyka rozumie się ocenę następstw i prawdopodobieństwa wystąpienia zagrożeń/ zdarzeń oraz wyznaczenie poziomu ryzyka

3.1.8. Przez ewaluację ryzyka rozumie się dokonanie przeglądu wyników analizy ryzyka z kryteriami w celu stwierdzenia czy ryzyko jest akceptowalne

3.1.9. Odpowiedzialnymi za ryzyka są ich właściciele – osoby odpowiedzialne za obszar

3.1.10. Ocena ryzyka prowadzona jest dwu etapowa:

- Identyfikacja, ocena oraz selekcja zagrożeń/zdarzeń
- Pogłębiona oceny ryzyka

3.1.11. Pogłębiona ocena ryzyka jest prowadzona obligatoryjnie w odniesieniu do ryzyka rezydualnego.

3.1.12. Ocena ryzyka jest dokumentowana z zastosowaniem arkusza oceny ryzyka

3.1.13. Ocena ryzyka jest zatwierdzane przez Administratora Danych

3.1.14. Tolerowanie ryzyka dużego i bardzo dużego jest wyłącznym uprawnieniem Administratora Danych

3.1.15. W przypadku podjęcia decyzji o postępowaniu z ryzykiem działania planowane są z zastosowaniem Planu postępowania z ryzykiem

3.1.16. Kolejne okresowe oceny ryzyka są kontynuacją ocen poprzednich (przegląd ryzyka i jeżeli to niezbędne ponowna ocena)

3.1.17. Okresowa ocena ryzyka dokonywana jest z zastosowaniem skali 1-5 a poziom ryzyka jest obliczany, jako iloczyn oceny prawdopodobieństwa i następstw według zasad określonych w niniejszej procedurze (patrz załącznik nr 1 do niniejszej procedury)

3.1.18. Postępowanie z ryzykiem może obejmować:

- Zapobieganie, czyli działania polegające na zmniejszeniu poziomu ryzyka (zmniejszenie prawdopodobieństwa np. eliminacja podatności lub następstw)
- Przeniesienie ryzyka na inny podmiot zewnętrzny, w tym ubezpieczyciela
- Unikanie, czyli zaprzestanie działań wywołujących ryzyko przekraczające akceptowany poziom ryzyka
- Tolerowanie (akceptowanie) ryzyka w przypadku, gdy: ryzyko jest na poziomie akceptowalnym; istnieją określone trudności w przeciwdziałaniu ryzyku lub gdy koszty planowanych działań modyfikujących ryzyko mogą przekroczyć przewidywane korzyści

3.1.19. W ramach postępowania z ryzykiem można zastosować więcej niż jedną metodę postępowania z ryzykiem

3.1.20. Każdy pracownik zobowiązany jest do monitorowania działalności (podczas wykonywania obowiązków służbowych), którą nadzoruje lub którą realizuje oraz

identyfikowania związanych z tym zagrożeń/ zdarzeń i stosowania właściwych środków kontroli/ zabezpieczeń

3.1.21. Proces oceny ryzyka jest udokumentowany. Do oceny ryzyka stosuje się Kwestionariusze oceny ryzyka lub rozwiązania informatyczne umożliwiające ocenę ryzyka i sporządzenie zapisu z takiej oceny.

Wzór kwestionariusza stanowi załącznik nr 1 do niniejszej procedury.

3.2. OCHRONA PRYWATNOŚCI W FAZIE PROJEKTOWANIA I DOMYŚLNA OCHRONA DANYCH (PIA/PRIVACY BY DESIGN/PRIVACY BY DEFAULT),

Osoba odpowiedzialna za nowe operacje przetwarzania (np. czynność przetwarzania/zbiór danych/oprogramowanie), ma obowiązek przeprowadzenia zapewnienia ochrony prywatności danych, które będą przetwarzane w ramach nowych operacji przetwarzania.

Do operacji przetwarzania, które wymagają przeprowadzenia oceny zalicza się:

- Wdrożenie nowego oprogramowania służącego do przetwarzania danych osobowych
- Podpisanie umowy na nowy produkt/usługę, gdzie zachodzić będzie przetwarzanie danych osobowych
- Rozwój istniejącego oprogramowania o nowe moduły/funkcjonalności, z pomocą których będzie zachodzić przetwarzanie danych osobowych

Ocenę zgodności przetwarzania z wymaganiami przepisów o ochronie danych osobowych (Privacy by design) przeprowadza się z użyciem kwestionariusza PIA lub z użyciem narzędzia informatycznego służącego do takiej oceny (np. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment) lub w inny sposób wg wytycznych IOD.

W przypadku, gdy któreś z zagadnień opisanych w kwestionariuszu nie jest realizowane, należy niezwłocznie doprowadzić do stanu, w którym wdroży się odpowiednie zabezpieczenia w celu zapewnienia zgodności przetwarzania z przepisami prawa.

W przypadku wątpliwości, osoba dokonująca oceny może zwrócić się do Inspektora Ochrony Danych z wnioskiem o rekomendacje.

Ostateczną decyzję odnośnie przetwarzania podejmuje Administrator Danych.

3.3. OCENA SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH (DPIA)

Osoba odpowiedzialna za nowe operacje przetwarzania (np. czynność przetwarzania/zbiór danych/oprogramowanie). Ma obowiązek przeprowadzenia oceny skutków dla ochrony danych w przypadku gdy:

- w kwestionariuszu oceny potrzeby przeprowadzenia DPIA dla nowych operacji przetwarzania/aplikacji spełnione zostały 2 lub więcej kryteriów lub
- gdy organ nadzorczy zamieścił daną czynność przetwarzania w publikowanym przez siebie wykazie (wykaz rodzajów przetwarzania, dla których obowiązkowe jest przeprowadzenie oceny skutków).
- gdy taką decyzję podjął Administrator Danych

W przypadku podjęcia decyzji o przeprowadzeniu DPIA należy włączyć w proces oceny skutków przetwarzania Inspektora Ochrony Danych, który przygotowuje rekomendacje w zakresie ryzyk związanych z przetwarzaniem danych.

Wzór kwestionariusza oceny potrzeby przeprowadzenia DPIA stanowi załącznik nr 2 do niniejszej procedury.

Ocenę skutków przetwarzania przeprowadza się z użyciem kwestionariusza DPIA lub z użyciem narzędzia informatycznego służącego do takiej oceny (np. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment) lub w inny sposób wg wytycznych IOD.

Wzór kwestionariusza DPIA stanowi załącznik nr 3 do niniejszej procedury.

W przypadku gdy wynikiem oceny będzie konkluzja, iż oceniane operacje przetwarzania, pomimo zaproponowanych i zaakceptowanych do wdrożenia zabezpieczeń stanowić będą wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, należy zgłosić potrzebę konsultacji z organem nadzorczym (Urząd Ochrony Danych Osobowych). W wyniku konsultacji organ nadzorczy wyda decyzję, na podstawie której:

- Administrator danych będzie mógł przetwarzać dane bez ograniczeń
- Administrator danych będzie mógł przetwarzać dane pod warunkiem wdrożenia dodatkowych zabezpieczeń rekomendowanych przez organ nadzorczy
- Administrator będzie musiał zaprzestać przetwarzania danych osobowych w ramach podlegającej ocenie operacji przetwarzania

Każdorazowo Administrator danych ma obowiązek zastosowania się do decyzji podjętej przez organ nadzorczy i poinformować o niej swoich pracowników i współpracowników celem uniknięcia sytuacji,że dochodzić będzie do przetwarzania niezgodnego z prawem.

4. ZAŁĄCZNIKI:

1. **Załącznik nr 1** - Kwestionariusz oceny ryzyka
2. **Załącznik nr 2** - Kwestionariusz PIA (Privacy Impact Assesment).
3. **Załącznik nr 3** - Kwestionariusz oceny potrzeby przeprowadzenia DPIA dla nowych operacji przetwarzania/aplikacji.
4. **Załącznik nr 4** - Kwestionariusz DPIA

Załącznik nr 1 Kwestionariusz oceny ryzyka – znajduje się w osobnym pliku

Załącznik nr 2 – Kwestionariusz PIA (Privacy Impact Assessment)

Nazwa operacji przetwarzania	Opis operacji przetwarzania
Kliknij tutaj, aby wprowadzić tekst.	Kliknij tutaj, aby wprowadzić tekst.

Lp.	Pytanie	status	Dodatkowe informacje
1.	**[zasada legalności]** Czy dane przetwarzane są z użyciem podstawy prawnej ?	Wybierz element.	
2.	**[zasada legalności]** Podstawa prawna przetwarzania danych	Wybierz element.	
3.	**[zasada celowości]** Czy dane będą przetwarzane wyłącznie w celu określonym przy ich zbieraniu?	Wybierz element.	
4.	**[zasada celowości]** Jaki jest cel/cele przetwarzania danych w zbiorze	Kliknij tutaj, aby wprowadzić tekst.	
6.	**[kategorie danych]** Jakie kategorie danych będą przetwarzane **?**	Wybierz element.	
		Wybierz element.	
		Wybierz element.	
7.	**[zasada adekwatności]** Czy wszystkie dane wymienione w pkt. 6 są niezbędne do realizacji celu przetwarzania?	Wybierz element.	
8.	**[ryzyko naruszenia praw i wolności osób, których dane dotyczą]** Ryzyko jakich z wymienionych szkód w stosunku do osób których dane dotyczą może spowodować planowane przetwarzanie danych?		
	a) Dyskryminacja osób	Wybierz element.	
	b) Kradzież tożsamości	Wybierz element.	
	c) Oszustwo	Wybierz element.	
	d) Strata finansowa	Wybierz element.	
	e) Szkody dla reputacji	Wybierz element.	
	f) Utrata poufności danych	Wybierz element.	
	g) Nieautoryzowane odwrócenie pseudonimizacji	Wybierz element.	
	h) Pozbawienie praw i wolności	Wybierz element.	
	i) Utrata kontroli nad danymi osób, których dane dotyczą	Wybierz element.	
9.	**[zasada ograniczenia przechowywania]** Czy wyznaczono czas usunięcia danych?	Kliknij tutaj, aby wprowadzić tekst.	
10.	**[realizacja obowiązku informacyjnego]** Czy potrzebne przygotowanie klauzul informacyjnych?	**Wybierz element.**	
11.	**[powierzanie przetwarzania]** Czy potrzebne będzie zawarcie umowy/umów powierzenia przetwarzania danych osobowych?	Wybierz element.	
12.	**[ocena ryzyka]** Czy dane są odpowiednio zabezpieczone?	Wybierz element.	
13.	**[ocena ryzyka]** Opisz proponowane zabezpieczenia przetwarzanych danych	Wybierz element.	
14.	**[konsultacje z ekspertami]** Czy potrzebne konsultacje z ekspertami ?	Wybierz element.	
15.	**[konsultacje z osobami, których dane dotyczą]** Czy potrzebne konsultacje z osobami, których dane dotyczą ?	Wybierz element.	

16.	**[konsultacje z IOD]** Czy omówiono planowane działania z Inspektorem Ochrony Danych ?	Wybierz element.	
17.	**[rejestr czynności przetwarzania]** Czy operacje przetwarzania mieszczą się w zakresie zidentyfikowanych już i opisanych czynności przetwarzania?	Wybierz element.	
18.	**[prawa osób, których dane dotyczą]** Czy uwzględniono środki niezbędne w celu realizacji praw osób, których dane dotyczą (prawo do sprzeciwu, ograniczenia przetwarzania danych, sprostowania, usunięcia danych, przenoszenia danych)?	Wybierz element.	

Załącznik nr 3 – Kwestionariusz oceny potrzeby przeprowadzenia DPIA dla nowych operacji przetwarzania/aplikacji

Lp.	Opis kryterium	Spełnia/Nie spełnia	Uwagi / Wyjaśnienia
1.	Operacje będą służyły do Ewaluacji lub oceny z użyciem danych w tym profilowania i przewidywania, szczególnie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą".	Wybierz element.	
2.	Operacje będą polegały na zautomatyzowanym podejmowaniu decyzji wywołujących skutki prawne lub podobne istotne skutki.	Wybierz element.	
3.	Operacje będą polegały na systematycznym monitorowaniu, tj. przetwarzaniu wykorzystywanym do obserwacji, monitorowania i kontroli osób, których dane dotyczą, w tym zbieraniu danych poprzez „systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie".	Wybierz element.	
4.	Operacje będą polegały na przetwarzaniu danych obejmujących szczególne kategorie danych określonych w artykule 9 i 10 RODO.	Wybierz element.	
5.	Operacje będą polegały na przetwarzaniu danych na dużą skalę	Wybierz element.	
6.	Operacje będą polegały na dokonywaniu porównań lub połączeń zestawów danych: na przykład pochodzących z dwóch lub większej liczby operacji przetwarzania prowadzonych w różnych celach i/lub przez różnych administratorów danych w sposób, który wykracza poza racjonalne oczekiwania osoby, której dane dotyczą.	Wybierz element.	
7.	Przetwarzane będą dane osób wymagających szczególnego traktowania ze względu na brak równowagi sił pomiędzy Administratorem danych a tymi osobami (pracownicy; dzieci; osoby niepełnosprawne; osoby psychicznie chore).	Wybierz element.	
8.	Zastosowane będą innowacyjne rozwiązania technologiczne lub organizacyjne.	Wybierz element.	
9.	Przetwarzanie samo w sobie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy". Dotyczy to przetwarzania prowadzonego w miejscu publicznym, którego przechodzący ludzie nie mogą uniknąć, lub przetwarzania, którego celem jest umożliwienie, zmiana lub odmowa dostępu osób, których dane dotyczą, do usługi lub zawarcia umowy.	Wybierz element.	
10.	**Wynik (suma odpowiedzi)**	Wybierz element.	
11.	**Decyzja o przeprowadzeniu DPIA (w przypadku oceny negatywnej –**	**Wybierz element.**	Wybierz

	należy uzasadnić)		element.

Załącznik nr 4 – Kwestionariusz DPIA

Lp.	Nazwa operacji przetwarzania/aplikacji dla której przeprowadza się DPIA Uwagi		
1.	**Opis planowanych operacji przetwarzania i celów przetwarzania**		
	Kliknij tutaj, aby wprowadzić tekst.		Aby stwierdzić, że operacje przetwarzania są systematycznie opisane należy: • uwzględnić charakter, zakres, kontekst i cele przetwarzania (motyw 90); • zapewnić że opisano operacje przetwarzania w rejestrze czynności przetwarzania; • przedstawić funkcjonalny opis operacji przetwarzania; • zidentyfikować zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań); • uwzględnić przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8); - jeżeli zostały opracowane;
2.	**Ocena niezbędności i proporcjonalności przetwarzania**		
	Wynik oceny niezbędności i proporcjonalności przetwarzania	Wybierz element. Kliknij tutaj, aby wprowadzić tekst.	Aby stwierdzić że operacje przetwarzania są niezbędne i proporcjonalne należy zapewnić że: Uwzględniono środki przyczyniające się do niezbędności i proporcjonalności przetwarzania • Przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach (art. 5 ust. 1 lit. b)); • Przetwarzane zgodnie z prawem (art. 6); • adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c)); • określono czas przechowywania danych (art. 5 ust. 1 lit. e)); Uwzględniono środki przyczyniające się do zachowania praw osób, których dane dotyczą: • poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14); • prawo dostępu i prawo do przenoszenia danych (art. 15 i 20); • prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19); • prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21); • relacje z podmiotem przetwarzającym (art. 28); • zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V); • uprzednie konsultacje (art. 36);
3.	**Ocena ryzyka naruszenia praw i wolności osób, których dane dotyczą**		
	Wynik oceny ryzyka naruszenia praw i wolności osób, których dane dotyczą	Wybierz element.	Wynik uwzględnia wyniki przeprowadzonej oceny ryzyka. Można dołączyć arkusze oceny lub link do wyników oceny ryzyka.
	Środki jakie planuje się	Kliknij tutaj, aby	Opis planowanych lub podjętych zabezpieczeń.

	podjąć lub podjęto w celu zaradzenia ryzyku	wprowadzić tekst.	
4.	**Ocena stron zainteresowanych**		
	Wynik konsultacji z Inspektorem Ochrony Danych	Kliknij tutaj, aby wprowadzić tekst.	Opis rekomendacji IOD
	Wynik konsultacji z osobami, których dane dotyczą lub ich przedstawicielami (jeśli uznano za niezbędne)	Kliknij tutaj, aby wprowadzić tekst.	Opis i wyniki konsultacji

Załącznik nr 2 do Polityki bezpieczeństwa danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

PROCEDURA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego

SPIS TREŚCI

DEFINICJE I SKRÓTY

Administrator Danych/ Administrator Danych Osobowych/ ADO – Administratorem danych osobowych Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego (dalej: MBP), ADO reprezentowany jest przez Dyrektora Biblioteki (dalej: Dyrektor)

Administrator systemu – Informatyk, osoba wyznaczona przez Dyrektora posiadająca odpowiednie kompetencje lub firma zewnętrzna nadzorująca prawidłowe funkcjonowanie urządzeń i aplikacji służących do przetwarzania danych osobowych.

Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, np. dane dotyczące dzieci ich rodziców i opiekunów prawnych, dane pracowników, dane kontrahentów przetwarzane w zbiorach danych osobowych w Bibliotece.

Dyrektor – Dyrektor Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Inspektor Ochrony Danych (IOD) – osoba nadzorująca przetwarzanie danych osobowych w Bibliotece, zgłoszona do UODO.

Przetwarzanie danych - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

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

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych opisanych w Procedurach Zarządzania Systemem Informatycznym Bibliotece.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem a w szczególności:

- **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Dostępność** – właściwość polegającą na tym, że dane są dostępne dla osoby upoważnionej we właściwym momencie.

1. PROCEDURY ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1.1. OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

Inspektor Ochrony Danych odpowiada za aktualizowanie niniejszej instrukcji w przypadku zmian wymuszonych przepisami prawa, jak również zmian organizacyjno-funkcjonalnych, które mogą zajść w MBP.

Za realizację postanowień niniejszej Instrukcji odpowiedzialne są osoby wymienione jako realizatorzy czynności:

a. **Administrator Systemu** – Informatyk, osoba wyznaczona przez Dyrektora posiadająca odpowiednie kompetencje w zakresie obsługi systemów informatycznych lub zewnętrzna firma obsługująca MBP w zakresie konfiguracji, zabezpieczania i utrzymania systemów informatycznych.

b. **Administrator danych** – Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego.

c. **Inspektor Ochrony Danych** – osoba wyznaczona przez Dyrektora nadzorująca system ochrony danych osobowych w MBP.

d. **Użytkownicy** - pracownicy MBP (Bibliotekarze, pracownicy administracyjni, pracownicy obsługi).

Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie z użyciem:

a. Licencjonowanego oprogramowania (oprogramowania, do którego MBP posiada licencję na jego użytkowanie w zakresie zgodnym z jego przeznaczeniem). Dopuszczalne jest używanie aplikacji zarówno komercyjnych jak również innych (freeware; oprogramowanie opensourcoe).

b. Oprogramowania, które posiada wsparcie techniczne producenta (np. niedopuszczalne jest przetwarzanie danych osobowych na komputerach z systemami operacyjnymi Windows XP).

Wszędzie tam, gdzie na urządzeniach przetwarzane są dane osobowe lub inne istotne dla MBP informacje do eksploatacji dopuszcza się systemy informatyczne wyposażone w:

a. Mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika (uwierzytelnianie), z pominięciem narzędzi do edycji tekstu i arkuszy kalkulacyjnych (przy używaniu do gromadzenia danych ww. programów zaleca się stosowanie zabezpieczenia w postaci hasła dostępu do pliku),

b. Mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej (w przypadku korzystania z programów typu Word i Excel integralność danych można zapewnić poprzez włączenie opcji „ograniczenia edycji" i ustawienie hasła dostępu do pliku i jego edycji lub publikowanie i przekazywanie osobom uprawnionym plików nieedytowalnych (np. w formacie pdf)),

c. Oprogramowanie antywirusowe z najnowszą aktualizacją bazy dot. wirusów i innych zagrożeń,

d. Mechanizmy umożliwiające szyfrowanie danych,

e. Mechanizmy umożliwiające bezpieczne przechowywanie haseł,

f. Mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,

g. Urządzenia niwelujące zakłócenia i podtrzymujące zasilanie (tam gdzie są niezbędne, o czym decyduje **Administrator danych**),

Użytkownikom zabrania się:

a. Udostępniania stacji roboczych osobom nieuprawnionym,

b. Wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez **Administratora danych**,

c. Korzystania ze stanowisk komputerowych w celach prywatnych bez zgody **Administratora danych**,

d. Uruchamiania witryn internetowych o treściach niestosownych i nielegalnych (strony zawierające przemoc, pornografię, treści nawołujące do nienawiści),

e. Samowolnego instalowania i używania programów komputerowych o nieustalonym pochodzeniu,

f. Korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich oraz warunkami użytkowania określonymi w licencji na oprogramowanie,

g. Umożliwiania dostępu do sieci internetowej osobom nieuprawnionym,

h. Używania komputera bez zainstalowanego oprogramowania antywirusowego,

i. Odchodzenia od urządzeń, na których przetwarzane są dane osobowe bez uprzedniego wylogowania się z systemu/aplikacji za pomocą którego przetwarzano dane osobowe lub aktywowanie wygaszacza ekranu chronionego hasłem dostępu.

j. Przekazywania własnych danych dostępowych innym użytkownikom.

Administrator systemu informuje Inspektora Ochrony danych o wszelkich zidentyfikowanych naruszeniach ochrony danych a w szczególności:

a. Próbach nieuprawnionego dostępu do danych,

b. Wyciekach danych (udostepnieniach osobom nieuprawnionym),

c. Przypadkach instalowania nielegalnego oprogramowania,

d. Przypadkach przechowywania na urządzeniach bez zabezpieczenia,

e. Przypadkach przechowywania haseł w miejscach do tego nieprzeznaczonych,

f. Innych przypadkach naruszeń zidentyfikowanych przez **Administratora systemu**.

1.2. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Konta użytkowników systemu informatycznego tworzy/modyfikuje oraz usuwa **Administrator systemu** (ASI) na podstawie zgody Administratora danych (np. konto użytkownika na stacji roboczej), Administrator danych lub inna osoba przez niego wyznaczona posiadająca odpowiednie kompetencje.

Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym, jak również w rejestrach tradycyjnych wymagane jest upoważnienie do przetwarzania danych osobowych nadane przez **Administratora danych lub osobę przez niego wyznaczoną, która nadaje upoważnienia w imieniu Administratora danych**.

O ile ma to zastosowanie, uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta i zawieszenie dostępu w przypadku nieobecności pracownika w pracy trwającej dłużej niż 6 miesięcy (pracownik ma obowiązek zdać przypisany mu komputer, który użytkuje, poczta pracownika jeżeli pracodawca uzna to za stosowne przekierowywana jest na czas jego nieobecności na inne aktywne konto pocztowe).

Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy lub wygaśnięcia umowy cywilno-prawnej, na podstawie której je nadano. Pracownik zobowiązany jest do zdania przypisanego mu urządzenia, odbiera się również dostęp do poczty i aplikacji.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

1.3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

W MBP stosuje się następujące środki:

- ✓ Główny komputer dostępowy zlokalizowany jest w odrębnym pomieszczeniu MBP, do którego dostęp osób trzecich jest ograniczony
- ✓ Do stacji roboczych wykorzystywane są dane uwierzytelniające w postaci loginu i hasła
- ✓ W identyfikatorze pomija się polskie znaki
- ✓ Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny
- ✓ Zmianę hasła należy dokonywać nie rzadziej niż co 90 dni lub w przypadkach, gdy zewnętrzne procedury wskazują na inne postepowanie – zgodnie z nimi
- ✓ Hasła użytkowników, w zależności od systemu informatycznego generuje **Administrator systemu lub Administrator Danych** i przekazuje użytkownikowi. Użytkownik, po otrzymania hasła ustawia spersonalizowane hasło
- ✓ Hasło nie może być zapisywane i przechowywane bez użycia specjalistycznego oprogramowania (np. manager haseł typu Keypass: http://keepass.info/)
- ✓ Użytkownik nie może udostępniać haseł osobom nieupoważnionym
- ✓ Możliwe jest użycie innej metody uwierzytelniania (np. token, metody biometryczne) z zachowaniem zasad ogólnych określonych w RODO
- ✓ W wykorzystywanym programie Mateusz, utworzono 3 konta z uprawnieniami administratora. Pozostałe przeznaczone zostały dla innych pracowników i posiadają niższy poziom uprawnień. Poszczególne konta użytkowników zabezpieczone są indywidualnym loginem i hasłem. Możliwość pracy na programie Mateusz jest możliwa po zalogowaniu do głównego komputera.

1.4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Użytkownik rozpoczynający pracę w systemie informatycznym, wprowadzając identyfikator i hasło ma obowiązek upewnić się, że nie ma ryzyka podejrzenia hasła przez osoby nieupoważnione.

Użytkownik systemu jest odpowiedzialny za ochronę danych wyświetlanych na ekranie urządzenia przed osobami nie mającymi uprawnień.

Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.

Każde urządzenie, na którym przetwarza się dane osobowe posiada funkcję autowylogowywania, który uaktywnia się automatycznie po 5 minutach bezczynności. Użytkownik po tym czasie odzyskuje dostęp poprzez podanie hasła.

Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem w pozostania w pomieszczeniu

Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera. Po zakończonej pracy należy upewnić się czy w urządzeniach drukujących nie pozostały żadne wydruki zawierające dane osobowe.

Stanowisko pracy, po jej zakończeniu powinno uniemożliwiać dostęp do danych osobowych osobom nieupoważnionym.

1.5. PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.

Kopie zapasowe mogą być sporządzane automatycznie lub manualnie.

Kopie zapasowe mogą być wykonywane tylko na nośnikach będących własnością MBP.

Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych (aby zapewnić ciągłość działania właściciel przechowuje zakupione nośniki i licencje na oprogramowanie). Kopie potrzebnych programów i ustawień konfiguracyjnych znajdują się u **Administratora systemu** lub przechowywane są na dysku lokalnym Dyrektora.

Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego (hasła dostępu, klucze aktywacyjne, ustawienia połączeń sieciowych, ustawienia poszczególnych aplikacji) przetwarzającego dane osobowe.

Za proces tworzenia kopii awaryjnych na serwerze odpowiada **Administrator systemu**.

Kopie zapasowe mogą być wykonywane również przez dostawców rozwiązań informatycznych w ramach wykupionej licencji na oprogramowanie (np. dla oprogramowania przetwarzanego w chmurze obliczeniowej), w takim przypadku Administrator danych powinien zadbać o odpowiednie uregulowanie zapisów dotyczących wykonywania kopii zapasowych w umowie głównej lub innym dokumencie (regulamin, licencja, warunki użytkowania).

1.6. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje **Dyrektor.**

Zabrania się wykonywania kopii danych z systemów informatycznych w sposób inny niż dopuszczony przez **Administratora danych** a w szczególności przez nieautoryzowanie kopiowanie na prywatny nośnik, wykonywanie nieautoryzowanych wydruków, wykonywanie zdjęć itp.

Przenośne nośniki danych jeżeli przechowywane na nich są dane osobowe powinny być zabezpieczone ochroną kryptograficzną (szyfrowanie nośnika lub dostęp poprzez podanie hasła).

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, 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 (np. formatując nośnik i nadpisując dane),
3. **naprawy** — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem pracownika.

1.7. SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA SZKODLIWEGO

MBP używa licencjonowanego oprogramowania Antywirusowego (AV) dla zabezpieczenia danych przed oprogramowaniem szkodliwym.

Administrator systemu zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne programy (spyware, malware etc.). System antywirusowy jest skonfigurowany zapewniając:

a. skanowanie poczty elektronicznej
b. skanowanie nośników
c. skanowanie witryn internetowych przeglądanych przez użytkownika
d. kontrolkę ruchu sieciowego (programowa zapora)
e. automatyczną aktualizację bazy wirusów (w przypadku gdy urządzenie nie jest podłączone do sieci publicznej, **użytkownik** ma obowiązek okresowej aktualizacji manualnej).

W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie **Administratora systemu**.

Administrator systemu monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system poprzez przeglądanie logów systemu i zainstalowanych aplikacji.

1.8. PRZESYŁANIE DANYCH POZA DOZWOLONY OBSZAR PRZETWARZANIA

Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, a w szczególności poprzez zastosowanie ochrony kryptograficznej a jeżeli dane przesyłane są w pliku do edycji dla podmiotu z zewnątrz, należy włączyć opcję dostępu po wpisaniu hasła lub skompresować plik programem typu „winrar" z opcją dostępu poprzez hasło.

Hasło do odbiorcy nie może być przesyłane w tej samej wiadomości co dane/plik (sugerowany sposób przekazania: sms do odbiorcy).

Dodatkowo w wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy, jeśli jest to konieczne zastosować szczególne środki bezpieczeństwa, które obejmują:

a) zatwierdzenie przez **Administratora danych** zakresu danych osobowych przeznaczonych do wysłania,
b) zastosowanie mechanizmów szyfrowania danych osobowych,.

1.9. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez **Administratora systemu lub za jego zgodą i uprzednimi konsultacjami**.

Przeglądy i konserwacje przeprowadzane są doraźnie, na wniosek użytkowników przy okazji prowadzonych interwencji i dokonywanych napraw.

Każdy użytkownik ma możliwość zgłoszenia problemu z działaniem (awaria, nieaktualne oprogramowanie itp.) bezpośrednio do **Administratora systemu**. Każdorazowo o awarii informowany jest również Administrator danych (np. poprzez opcję DW w wiadomości e-mail).

W przypadku uszkodzenia urządzenia, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez użytkownika do czasu naprawy.

W przypadku konieczności przeprowadzenia prac serwisowych poza MBP, należy upewnić się czy firma serwisująca ma podpisaną z MBP umowę powierzenia przetwarzania danych osobowych, w innym przypadku nośnik z danymi jest wymontowywany na czas naprawy.

Upoważnienie do przetwarzania danych osobowych nr .....

Kobyłka, Kliknij tutaj, aby wprowadzić datę.
miejscowość i data

[Podstawa prawna upoważnienia] Na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

upoważniam

Panią/Pana:

zatrudnioną/ego/świadczącą/ego usługi (stanowisko)*

na rzecz **Miejskiej Biblioteki Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego**

do przetwarzania danych osobowych w ramach następujących czynności przetwarzania

- .
- .
- .

[szczegóły zakresu przetwarzania] Przetwarzanie danych osobowych dopuszczalne jest wyłącznie w zakresie jaki niezbędny jest do realizacji obowiązków służbowych/obowiązków wynikających ze świadczonej usługi osoby upoważnionej, w ramach opisanych u Administratora danych czynności przetwarzania.

[klauzula poufności] Równocześnie zobowiązuję Pana/Panią do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia w trakcie i po ustaniu zatrudnienia/świadczenia usług* na rzecz Administratora danych.

[Informacja o ważności upoważnienia] Upoważnienie ważne jest do dnia, w którym upływa data zatrudnienia/świadczenia usług* na rzecz Administratora danych lub do odwołania.

.....

(Podpis Administratora Danych

lub osoby upoważnionej w imieniu Administratora danych)

* *niewłaściwe skreślić*

[oświadczenie o zapoznaniu się z zasadami ochrony danych osobowych]

Ja [Imię i Nazwisko] oświadczam, że zapoznałam/em, się z przepisami o ochronie danych osobowych oraz zasadami ochrony danych osobowych obowiązującymi wewnątrz organizacji a w szczególności zakazowi udostępniania danych osobowych osobom nieuprawnionym i obowiązkowi ochrony danych osobowych przed zabraniem, zniszczeniem, zagubieniem wynikające z Polityki bezpieczeństwa danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego.

Przyjęłam/Przyjąłem do wiadomości i do stosowania:

.....

(data i czytelny podpis)

Rejestr osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko	Data nadania	Data odebrania

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa, zawarta w dniu Kliknij tutaj, aby wprowadzić datę.. roku, w Kliknij tutaj, aby wprowadzić tekst. pomiędzy:

.....
Reprezentowanym przez:

.....

zwanym dalej „Administratorem danych"

a

.....

zwanym dalej „Podmiotem przetwarzającym"

Zważywszy, iż:

a) od dnia 25 maja 2018 r. w zakresie ochrony danych osobowych zastosowanie mają przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego dalej "Rozporządzeniem 2016/679"

b) Administrator danych i Podmiot przetwarzający zawarli Umowę o współpracy w zakresie Kliknij tutaj, aby wprowadzić tekst., zwaną dalej "Umową główną", w związku z którą Administrator danych powierza Podmiotowi przetwarzającemu, w rozumieniu art. 28 ust. 3 RODO, przetwarzanie danych osobowych, a Podmiot przetwarzający to powierzenie przyjmuje

Strony postanowiły zawrzeć Umowę powierzenia przetwarzania danych osobowych o treści następującej:

§1

Przedmiot umowy

1. Zleceniodawca oświadcza, że jest Administratorem danych osobowych w stosunku do danych powierzonych Podmiotowi przetwarzającemu, w rozumieniu art. 4 pkt. 7 Rozporządzenia 2016/679.
2. Powierzone Podmiotowi przetwarzającemu dane osobowe obejmują wszystkie niezbędne dane przetwarzane w szczególności w umowach, dokumentach i systemach informatycznych, do których w związku z umową główną ma dostęp Podmiot przetwarzający lub, które są powierzane Podmiotowi przetwarzającemu przez Administratora danych.
3. Podmiot przetwarzający oświadcza, że będzie przetwarzał powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem 2016/679 i innymi przepisami prawa regulującymi kwestie ochrony danych osobowych.

§2

Zakres i cel przetwarzania danych

1. **[Przedmiot i cel]** Przedmiot przetwarzania danych obejmuje dokonywanie przetwarzania danych osobowych w celach niezbędnych do prawidłowej realizacji Umowy głównej. Operacje przetwarzania wykonywane przez Podmiot przetwarzający mają charakter subsydiarny do wykonywania usług objętych Umową główną.
2. **[Zakres przetwarzania]** Powierzone przez Administratora danych, dane osobowe będą przetwarzane przez podmiot przetwarzający wyłącznie w zakresie niezbędnym do prawidłowej realizacji Umowy Głównej a w szczególności obejmuje dane określone w załączniku nr 1 do niniejszej umowy.
3. **[Zmiana zakresu przetwarzania]** Zakres powierzenia, może zostać w każdym momencie rozszerzony albo ograniczony przez Administratora danych. Ograniczenie albo rozszerzenie może być dokonane poprzez przesłanie przez Administratora danych do podmiotu przetwarzającego nowej wersji Załącznika nr 1 w formie elektronicznej (na adres e-mail wskazany w Załączniku nr 1). W przypadku braku reakcji podmiotu przetwarzającego w ciągu 5 Dni Roboczych (na potrzeby Umowy „Dni Robocze" należy rozumieć dni od poniedziałku do piątku, poza dniami ustawowymi wolnymi od pracy) od daty wysłania wiadomości przez Administratora danych przyjmuje się, że podmiot przetwarzający zaakceptował zmianę zakresu powierzenia.
4. **[Czas przetwarzania]** Podmiot przetwarzający będzie przetwarzał powierzone mu dane osobowe przez czas obowiązywania umowy głównej.

§3

Podpowierzenie przetwarzania danych

1. **[Podpowierzenie]** Strony ustaliły że dane osobowe nie będą podpowierzono innym podmiotom niż określone w załączniku nr 1 do niniejszej umowy (niewypełnienie załącznika oznacza, że dane osobowe nie będą podpowierzane).
2. **[Podpowierzenie]** Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy, po uzyskaniu uprzedniej pisemnej zgody Administratora danych. Zgoda administratora nie wymaga aneksu do niniejszej umowy a jedynie aktualizacji załącznika nr 1.
3. **[Obowiązki podpowierzającego]** Podmiot podpowierzający musi spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. **[Odpowiedzialność podpowierzającego]** Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§4

Państwa trzecie i organizacje międzynarodowe

1. **[Przetwarzanie w państwach trzecich]** Przekazanie powierzonych danych do państwa trzeciego (państwa nie będącego członkiem Europejskiego Obszaru Gospodarczego) może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym w postaci zmiany załącznika nr 1 do niniejszej umowy, o ile prawo to

nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny. Zgoda administratora nie wymaga aneksu do niniejszej umowy.

2. **[Wykaz państw trzecich i organizacji międzynarodowych]** Strony ustaliły, że przetwarzanie nie będzie odbywać się na terytorium Państw trzecich lub przez organizacje międzynarodowe inne niż określone w załączniku nr 1 do niniejszej umowy (niewypełnienie załącznika oznacza, że dane osobowe nie będą podpowierzane).

§5

Obowiązki podmiotu przetwarzającego

1. **[Należyta staranność]** Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
2. **[Zabezpieczenie danych]** Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia 2016/679. Szczegółowe wymagania w zakresie zabezpieczeń powierzonych danych osobowych określone zostały w załączniku nr 1 do niniejszej umowy (niewypełnienie załącznika oznacza, że powierzone dane osobowe powinny być zabezpieczone na zasadach ogólnych określonych w rozporządzeniu 2016/679).
3. **[Upoważnienie do przetwarzania danych]** Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. **[Zapewnienie poufności]** Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia 2016/679) 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. **[Zwrot/usunięcie danych]** 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. **[Zgłaszanie naruszeń]** Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin. W szczególności zgłaszane są przypadki gdy:
   - w trakcie przetwarzania powierzonych danych wystąpiło zdarzenie mające wpływ na ich bezpieczeństwo,
   - toczy się wobec podmiotu przetwarzającego lub podmiotu któremu podpowierzono dane postępowanie przed organem ochrony danych osobowych,
   - do podmiotu powierzającego lub podmiotu któremu podpowierzono dane osobowe wpłynęła zasadna skarga na przetwarzanie danych osobowych od osoby, której dane dotyczą.
   - Organ nadzorczy wydał decyzję administracyjną lub orzeczenie dotyczące przetwarzania powierzonych danych, skierowaną do Podmiotu przetwarzającego

§6

Kontrola danych przez administratora

1. **[Prawo do kontroli]** Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. **[Terminy kontroli]** Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7 dniowym wyprzedzeniem za wyjątkiem spraw związanych z naruszeniami przetwarzania (w takim przypadku obowiązuje 1 dniowy termin na poinformowanie).
3. **[Działania pokontrolne]** Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. **[Dostęp do informacji o powierzonych danych]** Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. **[Wsparcie dla administratora]** 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, poprzez udzielanie pisemnych informacji na pytania administratora w zakresie związanym z powierzonymi danymi osobowymi.
6. **[Usunięcie lub zwrot danych]** O ile Administrator danych lub przepis prawa nie stanowi inaczej, Podmiot przetwarzający po zakończeniu usług związanych z przetwarzaniem zobowiązuje się do usunięcia wszelkich powierzonych mu danych osobowych na mocy niniejszej umowy niezwłocznie po jej wygaśnięciu. Na dowód podjęcia czynności usunięcia danych podmiot przetwarzający prześle Administratorowi dokument lub jego kopię potwierdzający przeprowadzenie czynności (np. protokół zniszczenia, notatkę, wiadomość email) na adres wskazany w załączniku nr 1 do niniejszej umowy.
7. **[Sposób zabezpieczenia danych]** W ramach zapewnienia prawa do kontroli przetwarzania powierzonych zgodnie z przepisami prawa Podmiot przetwarzający na wniosek Administratora danych przedstawia pisemną informację na temat sposobu zabezpieczenia powierzonych danych oraz wyniku przeprowadzonych kontroli wewnętrznych.

§7

Odpowiedzialność

1. Podmiot przetwarzający może przetwarzać dane osobowe powierzone przez Administratora danych wyłącznie w zakresie i w celu określonych w niniejszej umowie.
2. Podmiot przetwarzający odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez Podmiot przetwarzający powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do pokrycia administracyjnych kar pieniężnych nałożonych na Administratora danych wskutek lub w związku z niewykonaniem lub nienależytym wykonaniem przez Podmiot przetwarzający zobowiązań określonych w niniejszej Umowie.

§8

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia do czasu obowiązywania Umowy Głównej.

§9

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
b) przetwarza dane osobowe w sposób niezgodny z umową;
c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§10
Poufność

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§11
Postanowienia końcowe

1. Umowa wchodzi w życie od dnia 25 maja 2018r. i zastępuje wszelkie wcześniejsze ustalenia dotyczące powierzenia przetwarzania danych osobowych przez Administratora danych, jeżeli takie były.
2. Zmiany informacji określonych w załączniku nr 1 do niniejszej umowy wymagają formy pisemnej. Informacja o zmianach przekazywana jest na dane kontaktowe stron i wymaga zmiany załącznika nr 1.
3. Zmiany załącznika nr 1 do niniejszej umowy nie wymagają zawarcia aneksu.
4. W sprawach nieuregulowanych niniejszą umową zastosowanie znajdują przepisy dotyczące ochrony danych osobowych, Kodeksu Cywilnego oraz innych przepisów.
5. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora danych.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Administrator danych

.....

Podmiot przetwarzający

.....

ZAŁĄCZNIK NR 1 DO
UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH
- „SZCZEGÓŁOWY OPIS POWIERZENIA"

Część A
WYPEŁNIA ADMINISTRATOR DANYCH

1) **Cele przetwarzania:**
   a.

2) **Kategorie osób, których dane dotyczą: dane pracowników;**
   a.

3) **Powierzenie danych szczególnie chronionych (Art. 9 i 10 Rozporządzenia 2016/679):**
   (w przypadku, gdy wpisano „nie dotyczy" lub pola pozostają nieuzupełnione uznaje się, że podmiot przetwarzający nie przetwarza danych szczególnie chronionych)
   a.

4) **Rodzaje danych osobowych:**
   a.

5) **Korespondencja w sprawach związanych z Umową będzie kierowana do Administratora danych na następujące dane kontaktowe:**
   a. Dane do korespondencji tradycyjnej, Nr telefonu, Adres email:

6) **Dane Inspektora Ochrony Danych u Administratora danych**
   (w przypadku, gdy dane nie zostaną podane, uznaje się, że IOD nie został wyznaczony)
   a. **[jeśli dotyczy]** Imię i nazwisko, Nr telefonu, Adres Email

7) **Wymagania w zakresie zabezpieczeń:**
   a. Standardowe zabezpieczenia, zgodnie z przepisami Rozporządzenia 2016/679

Część B
WYPEŁNIA PODMIOT PRZETWARZAJĄCY

1) **Przetwarzanie w państwach trzecich: TAK/NIE**
   (w przypadku gdy wpisano „nie dotyczy" lub pola pozostaną nieuzupełnione uznaje się, że podmiot przetwarzający nie będzie przetwarzał powierzonych danych w państwach trzecich ani przekazywał organizacjom międzynarodowym)
   a. **[jeśli dotyczy]** Nazwa państwa trzeciego,
   b. **[jeśli przetwarzanie w państwie trzecim]** Informacje o gwarancjach wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia 2016/679.

2) **Podmioty, którym podmiot przetwarzający podpowierza przetwarzanie danych osobowych:**
   (w przypadku gdy wpisano „nie dotyczy" lub pola pozostają nieuzupełnione uznaje się że podmiot przetwarzający nie zadeklarował podpowierzenia przetwarzania danych osobowych):
   a. **[jeśli dotyczy]** Nazwa podmiotu podpowierzającego; Dane adresowe; Dane kontaktowe (email, telefon); Cel podpowierzenia (np. rodzaj świadczonej usługi przez podmiot podpowierzający) :

3) **Korespondencja w sprawach związanych z Umową będzie kierowana do podmiotu przetwarzającego na następujące dane kontaktowe:**
   a. Dane do korespondencji tradycyjnej, Nr telefonu, Adres email:

4) **Dane Inspektora Ochrony Danych Podmiotu przetwarzającego**
   (w przypadku, gdy dane nie zostaną podane, uznaje się, że IOD nie został wyznaczony)

Z komentarzem [RR1]: a realizacja umowy głównej (umowy na świadczenie usług .....
Należy wpisać identyfikator umowy np. umowy z dnia ..... lub umowy nr.....

Z komentarzem [RR2]: Należy podać kategorie osób, których dane będą przetwarzane np. dane pracowników, dane klientów, itp.

Z komentarzem [RR3]: Możemy posłużyć się kategoriami (np. dane identyfikacyjne, dane adresowe, dane o stanie zdrowia, dane finansowe) lub określić szczegółowy zakres np. :Dane z formularza, dane z wniosku, lub precyzyjnie wskazać że to będą np.: Imię, nazwisko, wiek, nr konta bankowego, itp.,

Z komentarzem [RR4]: Podanie tych danych jest obowiązkowe

Z komentarzem [RR5]: Wypełniane wyłącznie wtedy, gdy IOD został powołany

Z komentarzem [RR6]: Państwa poza Europejskim obszarem gospodarczym. Liczy się również np. korzystanie z usługi chmurowej.

Z komentarzem [RR7]: Np. dostawca usługi hostingowej; Dostawca środowiska aplikacji (np. chmury obliczeniowej); Developer; Inne zewnętrzne podmioty działający jako podwykonawcy podmiotu przetwarzającego.

Z komentarzem [RR8]: Do uzgodnienia, na jakie dane chcemy otrzymywać korespondencję

Z komentarzem [RR9]: Wypełniane wyłącznie wtedy, gdy IOD został powołany

a. **[jeśli dotyczy]** Imię i nazwisko, Nr telefonu, Adres Email

Załącznik nr 8 do polityki bezpieczeństwa danych osobowych

Wykaz aktów prawnych związanych z ochroną danych osobowych w Miejskiej Bibliotece Publicznej w Kobyłce im. Stanisława Ryszarda Szpotańskiego przy ul. Leśna 8 lokal 0.3, 05-230 Kobyłka.

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)

   https://www.privacy-regulation.eu/pl/index.htm

2. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.

   http://www.dziennikustaw.gov.pl/DU/2018/1000

3. Ustawa o bibliotekach z dnia 27 czerwca 1997 r.

   http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180000574

4. Ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej

   https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19911140493

5. Ustawa o zmianie ustaw regulujących wykonywanie niektórych zawodów z dnia 13 czerwca 2013 r.

   http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20130000829

6. Rozporządzenie Ministra Kultury I Dziedzictwa Narodowego w sprawie narodowego zasobu bibliotecznego z dnia 4 lipca 2012 r.

   http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001308

7. Ustawa o restytucji narodowych dóbr kultury z dnia 25 maja 2017 r.

   http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20170001695

8. Rozporządzenie Ministra Kultury I Dziedzictwa Narodowego w sprawie sposobu ewidencji materiałów bibliotecznych z dnia 29 października 2008 r.

   http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20082051283

9. Rozporządzenie Ministra Kultury I Dziedzictwa Narodowego w sprawie organizacji i trybu działania Krajowej Rady Bibliotecznej z dnia 14 lutego 2012 r.

   http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20120000198

10. Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy.

    http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19740240141

11. Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie.

    http://www.dziennikustaw.gov.pl/du/2016/1817

12. Rozporządzenie Rady Ministrów z dnia 15 października 2021 r. zmieniające rozporządzenie w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii

    https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001878

..._ICDz		Data utworzenia
Opis wymagania:		
Koordynator - osoba odpowiedzialne za realizację planu:		

Opis realizacji planu: