MIEJSKA BIBLIOTEKA PUBLICZNA
ul. Fałata 4a
05-230 KOBYŁKA
tel. 22 763-42-42

Kobyłka dn., 11.04.2019r.

Zarządzenie Nr 2/2019

Dyrektora M.B.P. w Kobyłce z dnia 11.04.2019 r.
w sprawie wprowadzenia
Polityki Bezpieczeństwa Danych Osobowych
w Miejskiej Bibliotece Publicznej w Kobyłce

p.o. DYREKTOR
Miejskiej Biblioteki Publicznej
Sylwia Carzyńska

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 zarządzenia.

§2

Zobowiązuję pracowników Miejskiej Biblioteki Publicznej w Kobyłce 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 **5/2018** Dyrektora Miejskiej Biblioteki Publicznej w Kobyłce z dnia: 25.05.2018 roku dotyczące wprowadzenia Polityki Ochrony Danych traci moc.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

p.o. DYREKTOR
Miejskiej Biblioteki Publicznej
Sylwia Carzyńska
11.04.2019 r. .....

(data i podpis dyrektora)

SPIS TREŚCI

DEFINICJE I SKRÓTY

Administrator Danych/ Administrator Danych Osobowych/ ADO – Administratorem danych osobowych jest Miejska Biblioteka Publiczna w Kobyłce przy ul. Fałata 4a, 05-230 Kobyłka, (dalej: Biblioteka lub 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").

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

Dyrektor – Dyrektor Miejska Biblioteka Publiczna w Kobyłce.

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.

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 celom biblioteki jest zaspokajanie potrzeb oświatowych, kulturalnych i informacyjnych ogółu społeczeństwa. Biblioteka gromadzi, opracowuję, przechowuje i chroni materiały biblioteczną. Obsługuje czytelników prowadzi dokumentacje biblioteczną i upowszechnia czytelnictwo.

Biblioteka zlokalizowane jest w budynkach:

- 05-230 Kobyłka, ul. ul. Fałata 4a - budynek Biblioteki.

Główne systemy informatyczne używane w Bibliotece to:

- Strona http://bibliotekakobylka.stronakultury.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 **Infosystem „Groszek"-** służący 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);
4. Firmy obsługujące Bibliotekę w zakresie niszczenia dokumentów;

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 Gmina Kobyłka.

Gmina ma dostęp (a bibliotekę mu ten dostęp zapewnia) do danych osobowych przetwarzanych w bibliotece w związku z realizacją swoich obowiązków wynikających z przepisów prawa.

Dostęp Gminy 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 Gminie, jeżeli takie działanie ma odpowiednią podstawę prawną oraz spełnione zostały wymogi bezpieczeństwa danych osobowych. Gmina jest obowiązany 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 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 (Bibliotekę występuje, jako podmiot przetwarzający).

Ilekroć w Polityce Bezpieczeństwa jest mowa o przetwarzaniu Danych Osobowych, dotyczy to przetwarzania danych osobowych przez Bibliotekę, pracowników i współpracowników Bibliotekę oraz inne osoby i podmioty na podstawie umów zawartych ze 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, Pracownik IT, 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);

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 ryzyku
        - 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 10]**.

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 antywirusowego 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 Bibliotece 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 kart bibliotecznych 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 wyznaczona 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 funkcję 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 przy ul. Fałata 4a, 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 ZABEZPIECZENIADANYCH 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 powinny 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.). Oprogramowanie musi być aktualizowane oraz umożliwiać

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.

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 kopi 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 emailową 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 oddziałowym, 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 (list mailingowych, arkuszy Excel; 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 emailową).

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 Dyrektor.
- 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

Bibliotek 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 on 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.

5.1. ZGŁASZANIE NARUSZEŃ PRZEZ PRACOWNIKÓW BIBLIOTEKI

W celu ustalenia czy doszło do naruszenia pracownik ma obowiązek skonsultowania potencjalnego naruszenia z Inspektorem Ochrony danych (za wyjątkiem, gdy naruszenie znajduje się na referencyjnej liście naruszeń ochrony danych osobowych)

W ramach ustaleń ze zgłaszającym podejmowane są następujące czynności:

1. Weryfikacja czy doszło do naruszenia
2. Ustalenie charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
3. Możliwe konsekwencje naruszenia ochrony danych osobowych;
4. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5.2. DOKUMANTOWANIE NARUSZEŃ

Po otrzymaniu informacji o zgłoszeniu IOD, pracownik wyznaczony przez Dyrektora lub Dyrektor analizuje zgłoszenie i wydaje rekomendację w sprawie jego zgłoszenia do organu nadzorczego.

Przy ocenie zasadności zgłoszenia naruszenia do organu nadzorczego bierze się pod uwagę to, czy jest prawdopodobne, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności biorąc pod uwagę czy skutki naruszenia mogą być następujące:

- Naruszenie prawa do prywatności,
- Dyskryminacja osób,
- Kradzież tożsamości, lub oszustwo związane z użyciem cudzej tożsamości;
- Strata finansowa osoby, której dane dotyczą,
- Naruszenie dobrego imienia (dobra osobiste);

- Naruszenie poufności danych objętych tajemnicą ustawową;
- Pozbawienie praw i wolności i możliwości sprawowania kontroli nad swoimi danymi;
- Możliwość dokonania nieuprawnionej oceny czynników osobowych (np. dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji/zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się (w wyniku profilowania);
- Wpływ naruszenia na dużą liczbę osób jednocześnie (np. wyciek danych bazy liczącej kilkadziesiąt tysięcy użytkowników);

Jeżeli IOD/pracownik wyznaczony przez Dyrektora/Dyrektor ocenił, że istnieje małe prawdopodobieństwo, by naruszenie to skutkowało wysokim ryzykiem naruszenia praw lub wolności osób fizycznych rekomenduje niezgłaszanie naruszenia do organu nadzorczego.

Jeżeli IOD/pracownik wyznaczony przez Dyrektora/Dyrektor ocenił, że istnieje wysokie prawdopodobieństwo naruszenia praw lub wolności osób, których dane dotyczą w wyniku stwierdzonego naruszenia rekomenduje zgłoszenie naruszenia do organu nadzorczego.

W przypadku, gdy zgłoszone naruszenie zostanie zakwalifikowane, jako naruszenie wymagające zgłoszenia do organu nadzorczego podejmowane są następujące czynności.

1. Sporządza się zgłoszenie naruszenia uwzględniające następujące informacje.
    a) Opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    b) Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c) Opis możliwych konsekwencji naruszenia ochrony danych osobowych;
    d) Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
2. Przesyła się zgłoszenie do urzędu ochrony danych osobowych
3. Informuje się osoby, których dane dotyczą o naruszeniu (pkt 3.5)

Wzór zgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego stanowi załącznik do niniejszej polityki bezpieczeństwa danych osobowych – „Wzór zgłoszenia naruszenia ochrony danych" [Załącznik nr 9 do Polityki bezpieczeństwa"].

Zgłoszenie naruszenia ochrony danych do organu nadzorczego następuje nie później niż w ciągu 72 godzin od jego stwierdzenia z wyłączeniem szczególnych przypadków (np. ze względu na czasochłonność analizy naruszenia i jego skalę), kiedy to administrator zgłasza naruszenie w ciągu 72 godzin w niepełnej formie (bez przesłania niektórych informacji). Dodatkowe informacje o naruszeniu przesyła do organu nadzorczego niezwłocznie, gdy tylko uda mu się poczynić dodatkowe ustalenia.

Naruszenia, dla których zachodzi małe prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób, których dane dotyczą rejestrowane są wyłącznie u administratora danych w wewnętrznej ewidencji naruszeń.

Wzór ewidencji naruszeń stanowi załącznik do niniejszej polityki bezpieczeństwa danych osobowych – „Wzór ewidencji naruszeń ochrony danych osobowych" [Załącznik nr 9 do Polityki bezpieczeństwa"].

5.3. INFORMOWANIE O NARUSZENIACH OSOBY, KTÓREJ DANE DOTYCZĄ

W przypadku ustalenia, że naruszenie może spowodować wysokie ryzyko naruszenia praw lub wolności administrator danych zawiadamia osoby, których dane dotyczą o takim naruszeniu.

Formę i sposób zawiadomienia dobiera się w ramach bieżących potrzeb np. poprzez wysłanie komunikatów o naruszeniu emailem, pocztą, sms, bezpośrednio do osoby, której dane dotyczą.

Zawiadomienie nie jest konieczne, jeżeli administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

W przypadku, gdy poinformowanie wymagałoby nadmiernie dużego wysiłku możliwe jest również poinformowanie poprzez:

- Publikację ogłoszenia w prasie
- Wyświetlanie komunikatów o naruszeniu na stronie www administratora

Zawiadomienie zawiera:

a) Dane Inspektora Ochrony Danych (imię, nazwisko, dane kontaktowe), jeśli został wyznaczony,
b) Opis konsekwencji naruszenia ochrony danych,
c) Opis środków zastosowanych lub zaplanowanych do zastosowania w celu zaradzenia naruszeniu i zniwelowania ich negatywnych skutków.

Wyniki analizy naruszeń brane są pod uwagę przy analizie ryzyka, decyzjach dotyczących wdrażania zabezpieczeń i przygotowywaniu programu dotyczącego podnoszenia świadomości pracowników.

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 Bibliotek.

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 SŁUŻACE 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 kontrolą 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**.

MIEJSKA BIBLIOTEKA PUBLICZNA
ul. Fałata 4a
05-230 KOBYŁKA
tel. 22 763-42-42

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Miejskiej Biblioteki Publicznej w Kobyłce

Zatwierdził: 11 kwietnia 2019

p.o. DYREKTOR
Miejskiej Biblioteki Publicznej
Sylwia Czerwińska