Miejska Biblioteka Publiczna
im. Marii Danilewicz Zielińskiej
w Aleksandrowie Kujawskim
ul. Wojska Polskiego 2
87-700 Aleksandrów Kujawski
NIP 8911496694, tel. 54 4412550

ZARZĄDZENIE Nr 18 /2020
Dyrektor Miejskiej Biblioteki Publicznej w Aleksandrowie Kujawskim
z dnia 30 lipca 2020 r.

w sprawie **wprowadzenia Polityki Ochrony Danych Osobowych w Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim**

Na podstawie Uchwały Nr XXXIII/189/2001 Rady Miejskiej Aleksandrowa Kujawskiego z dnia 27 czerwca 2001 roku w sprawie wyodrębnienia Biblioteki z Miejskiego Centrum Kultury w Aleksandrowie Kujawskim oraz Uchwały Nr XXXVII /197/2001 Rady Miejskiej Aleksandrowa Kujawskiego z dnia 28 listopada 2001 roku w sprawie przyjęcia statutu Miejskiej Biblioteki Publicznej w Aleksandrowie Kujawskim, w szczególności §9 pkt 1 i 4 Statutu Miejskiej Biblioteki Publicznej w Aleksandrowie Kujawskim stanowiącego załącznik do ww. uchwały, oraz w związku z Art 37 ust.1 pkt „a" ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zarządzam co następuje:

§ 1.

Wprowadzam w Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim, Politykę Bezpieczeństwa, której treść stanowi załącznik nr 1 do zarządzenia, oraz Instrukcję zarządzania przetwarzaniem danych osobowych przy użyciu systemu informatycznego i w sposób ręczny, która stanowi załącznik nr 2 do zarządzenia.

§ 2.

Każdy pracownik dopuszczony do przetwarzania danych osobowych jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do zarządzenia lub wybranym zakresem odpowiednim do wydanego upoważnienia.

§ 3.

Oświadczenie o zapoznaniu się z treścią powyższych załączników zaopatrzone w podpis pracownika i datę, dołącza się do akt osobowych.

§ 4.

Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa oraz stosowania w pracy Instrukcji przetwarzania danych osobowych przy użyciu systemów informatycznych i w sposób ręczny, pod sankcją konsekwencji służbowych, przewidzianych prawem.

§ 5.

Zarządzenie wchodzi w życie z dniem ogłoszenia.

DYREKTOR
Miejskiej Biblioteki Publicznej
mgr Weronika Koźmińska

Inspektor
Ochrony Danych Osobowych
Marek Angowski

Załącznik Nr1 do Zarządzenia Nr 18/2020
Dyrektora Miejskiej Biblioteki Publicznej
im. Marii Danilewicz Zielińskiej
w Aleksandrowie Kujawskim

Polityka bezpieczeństwa
w Miejskiej Bibliotece Publicznej im. Marii Danilewicz Zielińskiej w Aleksandrowie Kujawskim

§ 1
Zagadnienia wstępne i definicje

Polityka bezpieczeństwa w Miejskiej Bibliotece Publicznej im. Marii Danilewicz Zielińskiej jest zbiorem zasad przetwarzania danych osobowych, zwanym dalej „Polityką bezpieczeństwa" celem których jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe zgodnie z Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,

- Administratorem danych osobowych przetwarzanych w Miejska Biblioteka Publiczna im. Marii Danilewicz Zielińskiej, ul. Wojska Polskiego 2, 87-700 Aleksandrów Kujawski
- Administrator danych osobowych powołał inspektora ochrony danych, zgodnie art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO oraz w Zarządzeniu 5/2018 Dyrektora MBP z dnia 17 maja 2018r w sprawie powołania IODO.

Polityka ta oraz związane z nią dokumenty zostały opracowane zgodnie z wymaganiami obowiązujących przepisów prawnych, a w szczególności przepisów art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2019 r. poz.1781ze zm.)
Niniejsza polityka dotyczy wszystkich osób biorących udział w przetwarzaniu danych osobowych w bibliotece.
Wszystkie osoby biorące udział w procesie przetwarzania danych osobowych są odpowiedzialne za właściwe zabezpieczenie danych.
Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

- poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych – rozumianą jako właściwość zapewniającą, że dane

osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
- dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
- zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

Przez użyte w polityce określenia należy rozumieć:

a) administrator danych osobowych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
b) inspektor ochrony danych – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
c) ustawa – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2019 r. poz.1781ze zm.ze zm.)
d) 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 /Dz. Urz. UE.L nr 119, str. 1/,
e) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
f) zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
g) przetwarzane danych – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
h) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
i) system tradycyjny – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
j) zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

k) administrator systemu informatycznego – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,

l) odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,

ł) strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,

o) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

p) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

§ 2
Przepisy ogólne

1. W bibliotece przetwarzanie danych osobowych czytelników jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
2. Dostęp do zbioru danych osobowych oraz ich przetwarzania stosownie do zakresu mają tylko osoby upoważnione (wzór upoważnienia – Załącznik Nr 1) i wpisane do ewidencji prowadzonej przez administratora danych (wzór rejestru ewidencji osób upoważnionych - Załącznik Nr 3).
3. Zakres upoważnienia należy rozumieć następująco: przeglądanie, zapisywanie, modyfikacja, pełny dostęp.
4. Osoby przetwarzające dane osobowe są zobowiązane do:
   - Podpisania oświadczenia o zachowaniu w tajemnicy przetwarzania danych osobowych oraz sposobów jego zabezpieczenia (wzór oświadczenia – Załącznik Nr 2);
   - Przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.
5. Zbierane dane osobowe mogą być wykorzystane tylko do celów, w jakich są przetwarzane. Po wykorzystaniu danych osobowych (np. czytelnik zaprzestał korzystania z usług biblioteki), powinny być usuwane. Z czynności usuwania danych należy sporządzić protokół – (wzór Protokołu – Załącznik Nr 4).
6. Osoby przetwarzające dane osobowe w systemie informatycznym są zobowiązane do postępowania zgodnie z „Instrukcję zarządzania przetwarzaniem danych osobowych przy użyciu systemu informatycznego i w sposób ręczny".
7. Osoby przetwarzające dane osobowe są zobowiązane powiadomić Inspektora

Ochrony danych osobowych o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych.

8. W bibliotece zabrania się przetwarzania danych ujawniających:
   - pochodzenie rasowe lub etniczne,
   - poglądy polityczne,
   - przekonania religijne lub filozoficzne,
   - przynależność wyznaniową,
   - przynależność partyjną lub związkową,
   - stan zdrowia, nałogi lub fakty z życia seksualnego oraz danych o karalności.
9. Dane osobowe przetwarzane w bibliotece mogą być uzyskiwane bezpośrednio od osób, których dane dotyczą lub od ich opiekunów prawnych.
10. Pracownicy działów biblioteki zbierających dane osobowe są odpowiedzialni za poinformowanie osób, których dane przetwarzają o:
    a) administratorze danych i jego adresie,
    b) inspektorze ochrony danych osobowych i jego adresie kontaktowym (email)
    c) celu zbierania danych, obowiązku podania danych i podstawie prawnej,
    d) prawie dostępu do treści swoich danych oraz ich poprawiania i usuwania – wzór informacji – Załącznik Nr 5)
11. Kandydaci do pracy w bibliotece winni złożyć pisemną zgodę na przetwarzanie ich danych osobowych w procesie rekrutacji.
12. Pracownicy na samodzielnych stanowiskach są zobowiązani do zgłoszenia Administratorowi Danych Osobowych:
    a) informacji o planowanym lub już istniejącym zbiorze danych osobowych;
    b) propozycji zmian w zbiorach już zarejestrowanych.
13. Osobom, których dane przetwarza się w zbiorze danych przysługuje prawo kontroli danych, które jej dotyczą.
14. Każdej osobie, która wystąpi z wnioskiem o otrzymanie informacji, odpowiedzi na piśmie udziela Administrator Danych Osobowych w terminie nieprzekraczającym 30 dni od daty wpłynięcia wniosku.
15. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa na pisemny umotywowany wniosek, chyba, że odrębne przepisy prawa stanowią inaczej.
16. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
17. Całkowity nadzór i kontrolę przetwarzania danych w bibliotece sprawuje Dyrektor biblioteki osobiście.
18. Inspektor Ochrony Danych Osobowych odpowiada za bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych oraz w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach

ewidencyjnych w zakresie zgodności zasad postępowania przy przetwarzaniu danych z obowiązującymi przepisami o ochronie danych osobowych.

19. Pracownik, który przetwarza w zbiorze danych:
    a) dane osobowe, do których przetwarzania nie jest upoważniony,
    b) dane osobowe, których przetwarzanie jest zabronione,
    c) dane osobowe niezgodne z celem utworzenia zbioru danych,
    d) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
    e) nie zgłasza Administratorowi Danych Osobowych zbiorów danych,
    f) nie dopełnia obowiązku poinformowania osoby, której danej dotyczą, o przysługujących jej prawach,
    g) uniemożliwia osobie, której dane dotyczą, korzystania z przysługujących jej praw

    podlega odpowiedzialności karnej zgodnie z Ustawą oraz przepisami Kodeksu Pracy.

§ 3

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

1. Dane osobowe przetwarzane są w Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim w siedzibie administratora danych osobowych.
2. Pomieszczenia są rozmieszczone na dwóch kondygnacjach (parter, piętro). Obszarem przetwarzania danych osobowych jest:

   a) Na parterze:

   Wypożyczalnia – obszarem przetwarzania danych jest stanowisko bibliotekarskie. Dane zapisywane są w kartotece sposobem tradycyjnym. Na kartotekę składają się deklaracje składane przez czytelników podczas zapisu do biblioteki. Dane zapisywane w kartotece posegregowane są alfabetycznie i przechowywane w drewnianej ladzie bibliotecznej zabezpieczonej zamkami.

   Czytelnia – obszarem przetwarzania danych jest stanowisko bibliotekarskie. Dane osobowe zapisywane są w zeszycie odwiedzin czytelni i zeszycie korzystania z Internetu. Zeszyty przechowywane są w biurku zabezpieczonym zamkiem.

   Gabinet Dyrektora – przetwarzanie danych związanych z pracownikami biblioteki. Dane gromadzone są w teczkach osobowych pracowników i przechowywane w antywłamaniowej metalowej szafie w pomieszczeniu Księgowość.

   Księgowość – przetwarzanie danych pracowników biblioteki związanych z wynagrodzeniami.

   Oddział Dziecięcy – obszarem przetwarzania danych jest stanowisko bibliotekarskie. Dane zapisywane są w kartotece sposobem tradycyjnym. Na kartotekę składają się deklaracje składane przez czytelników podczas zapisu do

biblioteki. Dane zapisywane w kartotece posegregowane są alfabetycznie i przechowywane w drewnianej ladzie zabezpieczonej zamkami. Dane zapisywane są również w zeszycie korzystania ze zbiorów na miejscu i korzystania z Internetu. Zeszyt przechowywany jest w biurku zabezpieczonym zamkiem.

§ 4

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

W Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim zbiory danych osobowych przetwarzane są sposobem tradycyjnym oraz z wykorzystaniem systemu informatycznego.

Dane osobowe przetwarzane są w następujących zbiorach:

„Kartoteka czytelników" - zbiór danych osobowych czytelników biblioteki. Dane osobowe w tym zbiorze przetwarzane są metodą tradycyjną. Na kartotekę składają się deklaracje składane przez czytelników podczas zapisu do biblioteki.

„Czytelnia" - zbiór danych osobowych (imię i nazwisko) czytelników odwiedzających czytelnię. Zbiór sporządzony w celu identyfikacji czytelnika w danej chwili oraz do celów statystycznych. Prowadzony jest sposobem tradycyjnym w zakresie drobnych bieżących spraw życia codziennego.

„Kadry" - zbiór danych osobowych pracowników Miejskiej Biblioteki Publicznej. Dane przetwarzane zgodnie Ustawa z dnia 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją. Dane przetwarzane są w sposób tradycyjny oraz w systemie informatycznym z wykorzystaniem oprogramowania firmy Info-System „Płace. System kadrowo-płacowy".

„Płace" - zbiór danych osobowych związanych z wynagrodzeniami pracowników Miejskiej Biblioteki Publicznej. Dane przetwarzane są w sposób tradycyjny oraz w systemie informatycznym z wykorzystaniem oprogramowania firmy Info-System „Płace. System kadrowo-płacowy" oraz programu Płatnik (ZUS).

§ 5

Opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informatycznych i powiązania między nimi

W zbiorze „Kartoteka czytelników" dane osobowe czytelnika są przetwarzane

tradycyjnie w zakresie:

- imię, nazwisko, data urodzenia, miejsce zamieszkania lub pobytu, nr PESEL, zawód (status społeczno-zawodowy), seria i numer dowodu osobistego, numer telefonu, nazwa szkoły bądź uczelni, adres poczty elektronicznej;
- wszystkich wypożyczeń (nr karty czytelnika, tytuł książki, autor, sygnatura książki, data wypożyczenia.

W zbiorze „Kadry" dane osobowe pracowników są przetwarzane w zakresie:

- nazwisko i imiona, imiona rodziców, nazwisko rodowe, nazwisko rodowe matki, data i miejsce urodzenia, adres stały (miejscowość, ulica, nr domu, nr mieszkania), miejsce zamieszkania, PESEL, NIP, dowód osobisty (seria, numer, wydany przez), obywatelstwo, stan rodzinny (imiona i nazwiska współmałżonka oraz dzieci), telefon, osoba kontaktowa, wykształcenie (nazwa szkoły i rok ukończenia), zawód wyuczony, zawód wykonywany, tytuł zawodowy, staż pracy i przebieg pracy, ukończone kursy, uzyskane kwalifikacje, warunki zatrudnienia, nieobecności w pracy, historia pracy, kary, nagrody, ubezpieczenia ZUS.

W zbiorze „Płace" dane osobowe pracowników są przetwarzane w zakresie:

- imię i nazwisko, dane płacowe, numer konta.

Wykaz zbiorów danych stanowi załącznik Nr 6 do PBOD

§ 6

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych

1. W celu zabezpieczenia danych osobowych przetwarzanych w Miejskiej Bibliotece Publicznej przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne.
2. Środki ochrony fizycznej i technicznej:

a) po zakończeniu pracy dane osobowe przechowywane są w szafach zamykanych na klucz oraz pomieszczeniach zabezpieczonych przed dostępem osób trzecich.
b) pomieszczenia, w których przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
c) pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolno stojących gaśnic.
d) pomieszczenia, w których przetwarzane są dane osobowe są zamykane na klucz na czas nieobecności w nich osób zatrudnionych bądź zabezpiecza się zbiory danych przed wglądem osób postronnych.
e) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
f) pojedyncze komputery zawierające dane osobowe powinny być zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym.
g) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są

dane osobowe.

3. Środki organizacyjne:

a) dostęp do danych osobowych mają osoby upoważnione

b) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,

c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

d) prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 7

Zmiany i udostępnianie tekstu Polityki bezpieczeństwa

1. Dopuszcza się dokonywanie zmian w niniejszym dokumencie przez Administratora Danych Osobowych.

2. Tekst Polityki bezpieczeństwa zostanie udostępniony użytkownikom w celu zapoznania się i wdrożenia w życie jej postanowień.

Inspektor
Ochrony Danych Osobowych
Marek Angowski

Załącznik Nr 1 do PBOD

Aleksandrów Kujawski, dnia .....202...r.

.....
miejscowość, data)

.....
(pieczęć jednostki organizacyjnej)

Nr upoważnienia: 1/2020

Upoważniam i polecam przetwarzanie danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i RE (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 (ogólne rozporządzenie o ochronie danych) upoważniam:

Panią/a .....
(imię i nazwisko)

Miejska Biblioteka Publiczna w Aleksandrowie Kujawskim
(komórka organizacyjna)

do przetwarzania danych osobowych do których dostęp wynika z zakresu czynności, zadań i poleceń służbowych na stanowisku

.....

Jednocześnie zobowiązuję Pana/nią do zachowania w tajemnicy danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz sposobów ich zabezpieczania także po zakończeniu praktyki.

Upoważnienie jest ważne od dnia ..... 202.....r. do czasu zakończenia .....

.....
(podpis upoważnionego)

.....
(podpis Administratora danych osobowych)

Inspektor
Ochrony Danych Osobowych
Marcin Angowski

Załącznik nr 2 do PBOD

OŚWIADCZENIE
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany(a) .....oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczania, do których mam lub będę miał(a) dostęp w związku z wykonywaniem czynności na stanowisku.....w Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim od dnia .....2020 roku:

Rodzaj zadań	*)
zadań i obowiązków służbowych wynikających z umowy o pracę	X
zadań wynikających z umowy zlecenie	
Zadań wynikających z umowy w związku ~~ze stażem~~ (umowa z Urzędem Pracy - praktyka)	

*) właściwe zaznaczyć X

zarówno **w trakcie wykonywania umowy, jak i po jej ustaniu.**

Zobowiązuję się przestrzegać polityki, instrukcji i procedur, obowiązujących w Miejskiej Bibliotece Publicznej w Aleksandrowie Kujawskim – zwanej dalej MBPAK, a dotyczących ochrony danych osobowych.
W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów znajdujących się w MBPAK. Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w MBPAK zasadach, dotyczących przetwarzania danych osobowych.

Oświadczam, że zostałem(am) przeszkolony(a) oraz zapoznany(a) z przepisami jakie wprowadza Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Znana jest mi też treść zarządzenia NR130/2018 z dnia 17 grudnia 2018r. oraz wprowadzonych do stosowania przez zarządzenie procedur, instrukcji i dokumentów.

Oświadczam, że zostałem(am) poinformowany(a) o grożącej, stosownie do przepisów rozdziału 11 w szczególności art. 107 i 108 ustawy o ochronie danych osobowych Dz. U. z dnia 18 maja 2018, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w MBPAK może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.
Zostałam zapoznana z klauzulami informacyjnymi dotyczącymi MBPAK.

Aleksandrów Kujawski, dn ..... 202..... roku
miejsce i data złożenia oświadczenia

.....
czytelny podpis osoby składającej oświadczenie

Inspektor
Ochrony Danych Osobowych
Marek Angowski

Załącznik 4 do PBOD

WZÓR PROTOKOŁU USUNIĘCIA DANYCH OSOBOWYCH ZE ZBIORU DANYCH

Protokółu sunięcia danych osobowych ze zbioru danych
1..... .....
.....
(Rodzaj i nazwa zbioru danych)

2.....
(Podstawa prawna usunięcia danych osobowych)

3..... .....
....
....
....
....
(Opis usuniętych danych osobowych)

4. Skład komisji dokonującej usunięcia danych osobowych:
1. .....
(imię, nazwisko, stanowisko służbowe)
2. .....
(imię, nazwisko, stanowisko służbowe)
3. .....
(imię, nazwisko, stanowisko służbowe)

5. Opis sposobu usunięcia danych osobowych ze zbioru
danych ....
....
....
....
....
.... ,

dnia .... 200.... r. (miejscowość)

1. ..... 2. ..... 3. .....
(podpis członków komisji)

Inspektor
Ochrony Danych Osobowych
Marcin Angowski

Załącznik 5 do PBOD

Obowiązek Informacyjny

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/W – ogólne rozporządzenie o ochronie danych (RODO), informujemy, iż:

1. Administratorem państwa danych osobowych zbieranych przez naszą jednostkę na podstawie Ustawy z dnia 27 czerwca 1997 r. o bibliotekach (Dz.U.2018 poz.574 t.j. z dnia 2018.03.19) oraz Uchwały Nr XXXIII/189/2001 Rady Miejskiej Aleksandrowa Kujawskiego z dnia 27 czerwca 2001 roku w sprawie wyodrębnienia Biblioteki z Miejskiego Centrum Kultury w Aleksandrowie Kujawskim i Uchwały Nr XXXVII /197/2001 Rady Miejskiej Aleksandrowa Kujawskiego z dnia 28 listopada 2001 roku w sprawie przyjęcia statutu Miejskiej Biblioteki Publicznej w Aleksandrowie Kujawskim - jest Miejska Biblioteka Publiczna im. Marii Danilewicz Zielińskiej z siedzibą w Aleksandrowie Kujawskim (MBP), ul. Wojska Polskiego 2; 87-700 Aleksandrów Kujawski.: Tel. 54 441 25 50, email: calbib@poczta.onet.pl
2. Za wyjątkiem sytuacji przewidzianych przepisami prawa z zakresu zadań MBP Państwa dane przetwarzane będą dla celu organizacji i przeprowadzenia konkursów, udziału w zajęciach, imprezach i konsultacjach społecznych, udziału w spotkaniach, wystawach, klubach dyskusyjnych oraz przeprowadzania ankiet i badań społecznych.
3. Do kontaktów w sprawie ochrony Pani/Pana danych osobowych został także powołany inspektor ochrony danych, z którym możesz się kontaktować wysyłając e-mail na adres iodo@aleksandrowkujawski.pl.
4. Pani/Pana dane osobowe na podstawie art. 6 ust. 1 lit a RODO przetwarzane będą w celu obsługi korespondencji z administratorem oraz wypełnienia przez niego zadań określonych w przepisach szczególnych określających zakres jego działania np.: wydania decyzji administracyjnej, postanowienia lub innego działania wynikającego z przepisów prawa, umowy lub Pani/Pana zgody.
5. Pani/Pana dane osobowe możemy przekazywać i udostępniać wyłącznie podmiotom uprawnionym na podstawie obowiązujących przepisów prawa są nimi np.: sądy, organy: ścigania, podatkowe oraz inne podmioty publiczne, gdy wystąpią z takim żądaniem, oczywiście w oparciu o stosowną podstawę prawną. Pani/Pana dane osobowe możemy także przekazywać podmiotom, które przetwarzają je na zlecenie administratora tzw. podmiotom przetwarzającym, są nimi np.: podmioty świadczące usługi informatyczne, telekomunikacyjne, pocztowe i inne. Jednakże przekazanie Pani/Pana danych nastąpić może tylko wtedy, gdy zapewnią one odpowiednią ochronę Pani/Pana praw.
6. Pani/Pana dane osobowe będą przetwarzane przez okres zgodny z obowiązującymi przepisami prawa, następnie zostaną usunięte.
7. Ma Pani/Pan prawo do żądania od administratora dostępu do danych, może je Pani/Pan sprostować, gdy zachodzi taka konieczność. Ma Pani/Pan także prawo żądania usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
8. Przetwarzanie odbywa się na podstawie Pani/Pana zgody informujemy więc, że zgoda może być cofnięta w dowolnym momencie.
9. W przypadku, gdy nie poda nam Pani/Pana swoich danych osobowych nie będziemy mogli rozpatrzyć zgłoszonej przez Pani/Pana sprawy i informować o niej drogą elektroniczną.
10. Przysługuje Pani/Panu także skarga do organu do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie Pani/Pana danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
11. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania.

Inspektor
Ochrony Danych Osobowych
Marek Angowski

Załącznik 6 do PBOD

Wykaz zbiorów danych osobowych w Miejskiej Bibliotece Publicznej
im. Marii Danilewicz Zielińskiej w Aleksandrowie Kujawskim

1. Kartoteka czytelników – zbiór danych osobowych czytelników biblioteki – deklaracje czytelników składane pódczas zapisu do biblioteki. Prowadzony metodą tradycyjną
2. Zeszyt użytkowników czytelni – metoda tradycyjna
3. Zeszyt użytkowników Internetu – metoda tradycyjna
4. Kadry – zbiór danych osobowych pracowników Miejskiej Biblioteki Publicznej – zbiór tradycyjny oraz w systemie informatycznym z wykorzystaniem oprogramowania firmy Info-System „Place. System kadrowo-płacowy"
5. Płace – zbiór danych osobowych związanych z wynagrodzeniami pracowników – dane przetwarzane w sposób tradycyjny oraz w systemie informatycznym z wykorzystaniem oprogramowania firmy Info-System „Płace. System kadrowo-płacowy".
6. Płatnik – zbiór danych osobowych związany z rozliczeniami z ZUS – program Płatnik
7. Rejestr umów o dzieło i zleceń
8. Doraźne zbiory związane z organizacją imprez bibliotecznych np. konkursy, zajęcia dla dzieci, konferencje .

Inspektor
Ochrony Danych Osobowych
Marek Angowski

Załącznik nr 2 do Zarządzenia Nr 18/2020

Instrukcja zarządzania
przetwarzaniem danych osobowych przy użyciu systemu informatycznego i w sposób ręczny

Spis treści:

1. Postanowienia ogólne

1. Instrukcja stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych w MBPAK, zgodnie z RODO.
2. Instrukcja obowiązuje wszystkich pracowników, podmioty przetwarzające dane osobowe na podstawie zawartych umów między przetwarzającym a powierzającym, użytkowników systemów informatycznych z dostępem do danych osobowych upoważnionych przez administratora na piśmie.
3. Każdy z wymienionych podmiotów jest zobowiązany do zapoznania się z dokumentem i bezwzględnego przestrzegania zawartych w nim zasad.
4. Administratorem danych osobowych w MBP jest Dyrektor.
5. Funkcje Inspektora Ochrony Danych sprawuje p. Marek Angowski.

2. Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.
5. Zabrania się w opcjach przeglądarki internetowej włączać opcji auto uzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą. W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

3. Zasady korzystania z poczty elektronicznej

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.
2. W przypadku przesyłania danych osobowych poza MBP należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.
7. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.
8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi lub osobie sprawującej nadzór nad sprzętem IT.
9. Przy wysyłaniu maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
10. Zabrania się rozsyłania maili z tzw. „ łańcuszkami szczęścia". Adres mailowy prywatny służy wyłącznie do korespondencji służbowej.
11. Nakazuje się okresowe czyszczenie poczty z nieaktualnych -e- mali i opróżnianie kosza.
12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
14. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
15. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność.
16. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania operacji bankowych z prywatnego konta.
17. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
18. Wszelkie przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

4. Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 - znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę MBP.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. Administratora Danych lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
1) zaleca się przenoszenie go w specjalnym futerale;

2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru;
3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. W przypadku pozostawiania komputerów przenośnych w MBPAK zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

5. Zasady wynoszenia nośników z danymi osobowymi poza MBPAK

1. Użytkownicy nie mogą wynosić poza szkołę bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.
3. Zabrania się wynoszenia poza szkołę dokumentacji papierowej, zwierającej dane osobowe (np. arkusze ocen). W przypadku innej dokumentacji (prace klasowe, listy uczestników wycieczek, dokumentacja wycieczek) należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.
4. W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

6. Zasady tworzenia kopii zapasowych

1. Zbiory danych osobowych w systemie informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
2) sporządzania kopii zapasowych (kopie pełne).

2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada osoba upoważniona przez Administratora Danych Osobowych.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
6. Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.

7. Zasady zabezpieczania dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach ogólnodostępnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

8. Procedura niszczenia danych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych (pendrive'y) oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
1) za pomocą specjalistycznego oprogramowania;
2) przy użyciu demagnetyzacji;
3) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
2. Wyznaczony przez ADO pracownik dokonuje kontroli prawidłowości usunięcia informacji.
3. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada administrator danych.
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.
7. Czynności kończy protokół ze zniszczenia danych.

9. Procedura niszczenia danych na nośnikach papierowych

1. Dokumentacja papierowa niszczona jest w niszczarkach paskowych.
2. W uzasadnionych przypadkach dokumentacja papierowa może być niszczona za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.
3. Czynności kończy protokół ze zniszczenia danych.

10. Procedura napraw w serwisach zewnętrznych

1. Urządzenia mobilne przeznaczone do naprawy należy wysyłać bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je wpierw trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).

4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku/karcie pamięci. Sprzęt przekazywany jest do serwisu bez podawania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site)

11.Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

DYREKTOR
Miejskiej Biblioteki Publicznej

Aleksandrów Kujawski, 30 lipca 2020roku .....

mgr Weronika Koźmińska

Inspektor
Ochrony Danych Osobowych
Marek Angowski
30.07.2020