ZARZĄDZENIE NR 10/2018
DYREKTORA GMINNEJ BIBLIOTEKI PUBLICZNEJ
W DĘBOWEJ KŁODZIE
Z DNIA 02 grudnia 2018 R.

w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych"
w Gminnej Bibliotece Publicznej w Dębowej Kłodzie

Na podstawie art. 36 ust.2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych oraz na podstawie art. 17 ustawy z dnia 25 października 1991r. o organizowaniu i prowadzeniu działalności kulturalnej (Dz. U. z 2013 r. poz. 406) wprowadzam:

§ 1

Politykę bezpieczeństwa danych osobowych w Gminnej Bibliotece Publicznej w Dębowej Kłodzie, która stanowi załącznik nr 1 do zarządzenia

§ 2

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w GBP w Dębowej Kłodzie stanowi załącznik nr 2

§ 2

Administratorem danych jest Dyrektor GBP w Dębowej Kłodzie.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania

DYREKTOR
Gminnej Biblioteki Publicznej
w Dębowej Kłodzie
mgr Katarzyna Kowalczyk

Załącznik Nr 1
do Zarządzenia nr 10/2018
Dyrektora Gminnej Biblioteki Publicznej
w Dębowej Kłodzie
z dnia 02 grudnia 2018 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Gminnej Bibliotece Publicznej w Dębowej Kłodzie

Polityka bezpieczeństwa danych osobowych, zwana dalej Polityką bezpieczeństwa, dotyczy procesu zarządzania danymi osobowymi zawartymi w dokumentacji pracowników Gminnej Biblioteki Publicznej w Dębowej Kłodzie

1. Podstawa prawna.

Zawarte w Polityce bezpieczeństwa metody ochrony danych osobowych są zgodne z Ustawą z dn. 29 sierpnia 1997 r. o ochronie danych osobowych.

2. Słownik pojęć:

1) **ośrodek**- należy przez to rozumieć Gminną Bibliotekę Publiczną w Dębowej Kłodzie oraz podległe jej filie

2) **administrator danych**- Dyrektor Gminnej Biblioteki Publicznej w Dębowej Kłodzie,

3) **użytkownik systemu**- to osoba upoważniona do przetwarzania danych osobowych

4) **uwierzytelnianie**- działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

5) **integralność danych**- właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

6) **poufność danych**- właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom.

3. Zastosowanie.

Polityka bezpieczeństwa dotyczy ochrony danych osobowych w procesie pobierania, przetwarzania i zabezpieczania danych osobowych w:

Gminna Biblioteka Publiczna w Dębowej Kłodzie
Dębowa Kłoda 116 A
21-211 Dębowa Kłoda
oraz filie biblioteczne

4. Cele.

Politykę bezpieczeństwa wprowadza się w celu ochrony danych gromadzonych przetwarzanych w GBP. Polityka bezpieczeństwa reguluje określone w niniejszym dokumencie zasady bezpieczeństwa danych osobowych.

5. Wykaz zbiorów danych osobowych.

Za zbiór danych osobowych przetwarzanych w GBP uważa się dokumentację papierową, tj. akta osobowe zatrudnionych tam pracowników oraz inne dane osób współpracujących z ośrodkiem.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności zbioru danych osobowych.

Dane osobowe tworzone przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach i przechowywane w zamykanych szafach. Dyrektor, na potrzeby niniejszej Polityki bezpieczeństwa zwany administratorem danych, nadzoruje przestrzeganie zasady ochrony

danych określonych w Polityce bezpieczeństwa danymi osobowymi z uwzględnieniem spraw dotyczących ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach.

8. Środki ochrony fizycznej danych osobowych.

Dostęp do zbioru danych osobowych posiadają pracownicy GBP (dyrektor i księgowa), którzy oświadczają, iż zapoznali się z obowiązującymi przepisami prawa w zakresie zarządzania danymi osobowymi.

Wejście do budynku zabezpieczone jest drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). Zbiór danych osobowych przechowywany jest w pomieszczeniu którym okna zabezpieczone są za pomocą krat, rolet. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi Dyrektor.

Przebywanie osób nieuprawnionych w pomieszczeniach GOK tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności administratora danych osobowych. Pomieszczenia te zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych w sposób uniemożliwiający dostęp do nich osób trzecich.

Pracownicy przetwarzający dane osobowe zobowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy.

Wszelka korespondencja zabezpieczona jest kopertą, która uniemożliwi wgląd osobom niepowołanym.

11 Jeśli pracownik wykaże, że używane przez niego oprogramowanie jest niezbędne do wykonywanej pracy, a wersja, którą posiada jest wersją do użytku osobistego, istnieje możliwość zakupienia przez placówkę wersji komercyjnej.

12 Nie dopuszcza się modyfikacji konfiguracji systemów operacyjnych zainstalowanych na urządzeniach przekazanych do użytkowania pracownikowi.

13 Korzystanie ze służbowych kont poczty elektronicznej dozwolone jest tylko i wyłącznie w celach służbowych. Zabronione jest przesyłanie informacji skalsyfikowanej jako „limitowana", w tym danych osobowych w formie jawnej (niezaszyfrowanej),

14 Zakazane jest udostępnianie haseł do służbowych kont poczty elektronicznej innym osobom

15 Należy zapewnić bezpieczeństwo fizyczne urządzeniom przekazanym do używania i chronić je przed kradzieżą, zagubieniem, zniszczeniem lub uszkodzeniem. W szczególności należy unikać pozostawiania przekazanych urządzeń bez opieki.

16 Każdy pracownik opuszczający swoje stanowisko pracy jest zobowiązany do zablokowania komputera oraz stosowania zasady czystego biurka i ekranu. Niedopuszczalne jest pozostawianie włączonych komputerów na noc i w czasie dni wolnych od pracy. Wyjątkiem od tej reguły są przypadki w których zgodę na tego typu działania wyraża Administrator Bezpieczeństwa Teleinformatycznego.

17 Wszelkie nieprawidłowości w działaniu, kradzieże, awarie sprzętu komputerowego lub oprogramowania należy bezzwłocznie zgłaszać do Administratora Bezpieczeństwa Teleinformatycznego lub Pełnomocnika ds. Bezpieczeństwa.

18 Zabrania się pracownikom korzystającym z Internetu następujących praktyk:

a przeglądania oraz ściągania materiałów o treściach pornograficznych lub prawnie zakazanych,

b uprawiania hazardu za pomocą Internetu,

c wyrażania osobistych opinii jako opinii placówki,

d wyrażania lub przesyłania nieprzyzwoitych uwag lub propozycji,

e ściągania programów komercyjnych z naruszeniem praw autorskich,

f ściągania programów lub plików elektronicznych bez odpowiedniej ochrony antywirusowej,

g umyślnego zakłócania normalnej pracy urządzeń dostępowych do Internetu,

h uczestniczenia w czynnościach, które powodują zator lub zakłócenia w pracy sieci komputerowej placówki oraz innej działalności naruszającej dobre imię placówki