

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych**

1. Termin przekazania sprawozdania: 04.03.2022

2. Rodzaj sprawdzenia:

Sprawozdanie dla: Administratora

Sprawdzenie przeprowadzili: Karolina Nęga oraz Paweł Jasiołek.

Sprawozdanie opracował: Paweł Jasiołek

3. Przedmiot i zakres sprawdzenia:

MJO: Młodzieżowy Dom Kultury im. Andrzeja Bursy

Dyrektor: Joanna Słomka

Przedmiot i zakres sprawdzenia:

- 1) **Organizacyjne środki ochrony – wprowadzenie Polityki Bezpieczeństwa Danych Osobowych**
 - Przegląd zarządzeń wprowadzających PBDO.
- 2) **Organizacyjne środki ochrony - Zasady dopuszczania do przetwarzania danych osobowych**
 - Przegląd zobowiązań do zachowania w poufności informacji.
 - Przegląd upoważnień do przetwarzania danych osobowych w oparciu o rejestr czynności przetwarzania oraz weryfikacja zasadności.
 - Przegląd potwierdzeń zapoznania się PBDO.
- 3) **Monitoring wizyjny (jeśli dotyczy):**
 - Sprawdzenie wybranych wymagań z art. 108a PO, art. 22² KP oraz art. 13 RODO.
- 4) **Techniczne środki ochrony - Wymagania bezpieczeństwa oraz zasady zarządzania systemami informatycznymi zgodnie z instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych:**
 - Sprawdzenie metod zabezpieczeń stanowisk komputerowych oraz sposobów uwierzytelnienia (typ konta: użytkownik/administrator, uwierzytelnianie za pomocą hasła oraz jego długość, zgodność identyfikatorów z załącznikiem „Rejestr identyfikatorów systemowych”,)
- 5) **Fizyczne środki ochrony:**
 - Strefy bezpieczeństwa - weryfikacja załącznika.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów
o ochronie danych osobowych**

Ryzyka do sprawdzenia:

1. Brak wprowadzenia PBDO,
2. Brak potwierdzenia zapoznania się z PBDO,
3. Brak zastosowania się do obowiązujących przepisów prawa,
4. Niezastosowanie się do art. 13 RODO oraz do wytycznych określonych w procedurze monitoringu,
5. Brak lub niezgodny z PBDO podział na strefy bezpieczeństwa,
6. Brak lub wadliwość zobowiązania o zachowaniu w poufności informacji,
7. Brak lub wadliwość upoważnienia do przetwarzania danych osobowych,
8. Niezastosowanie się do PBDO w tym w szczególności do przyjętych procedur wewnętrznych.

4. Data rozpoczęcia i zakończenia sprawdzenia:

Data rozpoczęcia: 04.03.2021

Data zakończenia: 04.03.2021

5. Wykaz czynności podjętych w sprawdzeniu oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:

Przebieg audytu:

A: Sprawdzenie przeprowadzone zostało w siedzibie placówki w dniu 04.03.2022r. Przed przystąpieniem do audytu zorganizowano krótkie spotkanie otwierające w trakcie którego omówiono zagadnienia związane z celem, zakresem, ryzykami do zbadania w trakcie sprawdzenia oraz omówiono kwestie organizacyjne przeprowadzania czynności audytowych. Spotkanie zamykające odbyło się po przeprowadzeniu badania.

B: Czynności audytowe objęły analizę przesłanych materiałów dowodowych:

- a) arkusz sprawdzenia pn. „Arkusz sprawdzenia_MDK im A_Bursy”
- b) zał. 5 do PBDO wykaz stref bezpieczeństwa pn. „zał 5”
- c) zarządzenie wprowadzające PBDO pn. „zarządzenie PBDO 2018”
- d) Zobowiązania do zachowania w poufności informacji 5 pracowników pn. „zobowiazania”
- e) Upoważnienia do przetwarzania danych osobowych 5 pracowników pn. „upowaznienia”
- f) Uzgodnienie dotyczące monitoringu wizyjnego z organem prowadzącym pn. „uzgodnienie OC”

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych**

- g) Konsultacje dotyczące monitoring wizyjnego z radą rodziców pn. „uzgo rr i rp 20e”
- h) Konsultacje dotyczące monitoring wizyjnego z radą pedagogiczną pn. „uzgo rr i rp 2019, rada z 2018”
- i) Skan zapisu w regulaminie pracy odnośnie zapisów dotyczących monitoringu wizyjnego pn. „regulamin pracy”
- j) Potwierdzenie poinformowania pracownika o funkcjonowaniu monitoringu wizyjnego w placówce pn. „PBDO”
- k) Potwierdzenie zapoznania się pracowników z PBDO pn. „PBDO”
- l) Wykaz kamer, piktogramy, obowiązki informacyjne pn. „obowiązek informacyjny, obowiązek informacyjny 2, piktogram”

6. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zdarzenia:

PRZEBIEG BADANIA I OPIS STANU FAKTYCZNEGO:

Młodzieżowy Dom Kultury im. Andrzej Bursy zostało poproszone o wylosowanie próbki 5 pracowników na podstawie których będzie przeprowadzana badanie – tzw. próbki losowej.

1. Brak wprowadzenia PBDO.

Młodzieżowy Dom Kultury im. Andrzej Bursy został poproszony o przedstawienie dowodów na potwierdzenie wprowadzenia przedstawionej w formie papierowej dokumentacji pn. Polityka Bezpieczeństwa Danych Osobowych. Wyniki zostały odnotowane w arkuszu sprawdzenia – dowód a) oraz c). Stwierdzono, iż PBDO zostało wprowadzone zarządzeniem Dyrektora placówki.

RYZYKO SIĘ NIE ZMATERIALIZOWAŁO**2. Brak potwierdzenia zapoznania się z PBDO.**

Młodzieżowy Dom Kultury im. Andrzej Bursy został poproszony o przedstawienie dowodów na potwierdzenie zapoznania się z PBDO pracowników z wylosowanej próbki losowej, a następnie wyniki zostały odnotowane w arkuszu sprawdzenia – dowody a) oraz k). Stwierdzono, iż wszyscy badani pracownicy zostali poinformowani o istnieniu PBDO, potwierdzając swoim podpisem w protokole zapoznania się z PBDO.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów
o ochronie danych osobowych****RYZYO SIĘ NIE ZMATERIALIZOWAŁO****3. Brak zastosowania się do obowiązujących przepisów prawa**

Młodzieżowy Dom Kultury im. Andrzej Bursy został poproszony o przedstawienie dowodów na potwierdzenie zastosowania się do obowiązujących przepisów prawa w zakresie monitoringu wizyjnego w obszarze wskazanym w arkuszu sprawdzenia, dowody a), f), g), h), i), j) oraz l). Zgodnie z deklaracją oraz wizją lokalną, zakres monitoringu nie obejmuje pomieszczeń niezgodnych z prawem, przetwarza tylko wizję, nagrania przetwarzane są tylko dla celów w jakim zostały zebrane i nie są przechowywane dłużej niż 3 miesiące – dowód a) i i). Pracownicy stanowiący próbkę losową, zostali pisemnie poinformowani o stosowaniu monitoringu wizyjnego w placówce dowód a) i k). Młodzieżowy Dom Kultury im. Andrzej Bursy posiada: wystąpiło o uzgodnienie do organu prowadzącego – dowód a) i f); posiadają uzgodnienie monitoringu z radą pedagogiczną dowód a) i h); uzgodnienie monitoringu z radą rodziców – dowód a) i g). Zapisy określające zakres, sposób monitorowania oraz cel zastosowania monitoringu w regulaminie pracy znajdują się w regulaminie pracy dowód a) i i). Z załączonych dowodów wynika, że brak jest niezgodności w badanym obszarze.

RYZYO SIĘ NIE ZMATERIALIZOWAŁO

UWAGI: Rekomenduje się coroczne przeprowadzenie konsultacji z radą pedagogiczną oraz radą rodziców.

4. Niezastosowanie się do art. 13 RODO oraz do wytycznych określonych w procedurze monitoringu

Młodzieżowy Dom Kultury im. Andrzej Bursy został poproszony o przedstawienie dowodów na potwierdzenie zastosowania się do art. 13 RODO oraz do wytycznych określonych w procedurze monitoringu. Deklaracja Dyrektora placówki została odnotowana w arkuszu sprawdzenia, dowód a), z której wynika, że piktogramy informujące o monitoringu wizyjnym na terenie jednostki są zgodne z ZMMW, a obowiązki informacyjne umieszczone w sposób czytelny i dostępny dla osób – dowód a) i i).

RYZYO SIĘ NIE ZMATERIALIZOWAŁO**5. Brak lub niezgodny z PBDO podział na strefy bezpieczeństwa.**

Młodzieżowy Dom Kultury im. Andrzej Bursy posiada wypełniony zał. nr 5 do PBDO Wykaz stref

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów
o ochronie danych osobowych**

bezpieczeństwa. Pomieszczenia takie jak: kancelaria dyrektora, archiwum (składnica akt), sekretariat, księgowość znajdują się w strefie bezpiecznej – dowód a) i d).

RYZYO SIĘ NIE ZMATERIALIZOWAŁO

6. Brak lub wadliwość zobowiązania o zachowaniu w poufności informacji.

W oparciu o próbkę losową poproszono o przedstawienie zobowiązań do zachowania w poufności informacji wylosowanych osób, na których zostało przeprowadzone badanie, a wyniki zostały odnotowane w arkuszu sprawdzenia – dowody a) oraz d). Stwierdzono, iż wszyscy pracownicy posiadają zobowiązanie oraz że są one podpisane przez pracowników.

RYZYO SIĘ NIE ZMATERIALIZOWAŁO

7. Brak lub wadliwość upoważnienia do przetwarzania danych osobowych

Badanie zostało przeprowadzone w oparciu o 5 przesłanych skanów upoważnień z wylosowanej próbki losowej, a następnie wyniki zostały odnotowane w arkuszu sprawdzenia – dowody e) oraz a). Stwierdzono, iż pracownicy przetwarzający dane osobowe posiadają wystawione upoważnienia do przetwarzania danych osobowych.

RYZYO SIĘ NIE ZMATERIALIZOWAŁO

8. Niezastosowanie się do PBDO w tym w szczególności do przyjętych procedur wewnętrznych

Zgodnie z deklaracją z pośród wylosowanej próbki dwóch pracowników posiada konta w systemie informatycznym. Pracownicy pracują na kontach z uprawnieniami administrator, długość hasła nie jest zgodna z przyjętymi zasadami, identyfikatory nie są zinwentaryzowane w załączniku nr 1 do Instrukcji Zarządzania Systemem Informatycznym - dowód a). W toku wyjaśnień ustalono, iż Pan Michał Piosek nie posiadają indywidualnego konta w systemie informatycznym Młodzieżowego Domu Kultury - korzystają stanowiska komputerowego służącego dla celów edukacyjno-dydaktycznych - dowód a).

RYZYO SIĘ ZMATERIALIZOWAŁO

7. Stwierdzone przypadki naruszenia w zakresie objętym sprawdzeniem.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych**

Stwierdzono przypadki naruszenia:

☒

Tak

☐

Nie

8. Rodzaj naruszenia☒

a) Incydent bezpieczeństwa „zwykły” naruszający zasady PBDO

☐

b) Incydent bezpieczeństwa naruszający prawa i wolności osób fizycznych skutkujący zgłoszeniem do Prezesa Urzędu Ochrony Danych Osobowych,

☐

c) Incydent w podmiocie publicznym, związany z krajowym systemem cyberbezpieczeństwa,

9. Planowane lub podjęte działania przywracające stan zgodny z prawem (w tym rekomendacje):**UWAGI:**

Zgodnie z przyjętymi ustaleniami, upoważnienia do przetwarzania danych osobowych powinny bezpośrednio odnosić do rejestru czynności przetwarzania, który stanowi ewidencję procesów związanych z przetwarzaniem danych osobowych. Należy uzupełnić formę przetwarzanych danych: papierowo, elektronicznie lub papierowo i elektronicznie.

REKOMENDACJE:

Zmienić uprawnienia pracowników z administrator/admin na użytkownik/user oraz zmodyfikować hasła tak, aby były zgodne z założeniami zapisanymi w dokumentacji PBDO. Zweryfikować uprawnienia wszystkich pracowników pod kątem nadanych uprawnień oraz mocy zastosowanych haseł. W przypadku występowania kont z uprawnieniami administrator/admin dokonać zmian jak powyżej.

W związku z pracami nad aplikacją do zarządzania bezpieczeństwem w Gminie Miejskiej Kraków pn. BIGMK, w której będzie m.in. ewidencja upoważnień – przed przeniesieniem ich do aplikacji należy dokonać przeglądu i inwentaryzacji upoważnień do przetwarzania danych osobowych.

Coroczne przeprowadzanie konsultacji z radą pedagogiczną oraz radą rodziców.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów
o ochronie danych osobowych****10. Załączniki stanowiące składową część sprawozdania:**

- a) arkusz sprawdzenia pn. „Arkusz sprawdzenia_MDK im A_Bursy”
- b) zał. 5 do PBDO wykaz stref bezpieczeństwa pn. „zał 5”
- c) zarządzenie wprowadzające PBDO pn. „zarządzenie PBDO 2018”
- d) Zobowiązania do zachowania w poufności informacji 5 pracowników pn. „zobowiązania”
- e) Upoważnienia do przetwarzania danych osobowych 5 pracowników pn. „upoważnienia”
- f) Uzgodnienie dotyczące monitoringu wizyjnego z organem prowadzącym pn. „uzgodnienie OC”
- g) Konsultacje dotyczące monitoringu wizyjnego z radą rodziców pn. „uzgo rr i rp 20e”
- h) Konsultacje dotyczące monitoringu wizyjnego z radą pedagogiczną pn. „uzgo rr i rp 2019, rada z 2018”
- i) Skan zapisu w regulaminie pracy odnośnie zapisów dotyczących monitoringu wizyjnego pn. „regulamin pracy”
- j) Potwierdzenie poinformowania pracownika o funkcjonowaniu monitoringu wizyjnego w placówce pn. „PBDO”
- k) Potwierdzenie zapoznania się pracowników z PBDO pn. „PBDO”
- l) Wykaz kamer, piktogramy, obowiązki informacyjne pn. „obowiązek informacyjny, obowiązek informacyjny 2, piktogram”

Sprawozdanie opracował/a:

.....

(data i podpis)