

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

1. **Termin przekazania sprawozdania do IOD:** 21.06.2021

2. **Rodzaj sprawdzenia:**

Sprawozdanie dla: Administratora

Sprawozdanie przeprowadzili: Agnieszka Metz - Dyrektor, Anna Dorociak – KODO; Agnieszka Sowa – IOD, Agnieszka Zemla-Mitka - Referent.

Sprawozdanie opracowała: Agnieszka Sowa

3. **Przedmiot i zakres sprawdzenia:**

MJO: Samorządowy Żłobek nr 21

Dyrektor: Agnieszka Metz

Przedmiot i zakres sprawdzenia:

- 1) **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.
- 2) **Monitoring wizyjny (jeśli dotyczy):**
 - Sprawdzenie wybranych wymagań z art. 22² KP oraz art. 13 RODO.
- 3) **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”,)
- 4) **Fizyczne środki ochrony:**
 - Strefy bezpieczeństwa - weryfikacja załącznika.

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

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych****4. Data rozpoczęcia i zakończenia sprawdzenia:**

Data rozpoczęcia: 21.06.2021

Data zakończenia: 21.06.2021

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

A: Sprawdzenie przeprowadzone zostało w formie stacjonarnej, na podstawie przedstawionych materiałów dowodowych. W dniu 26.02.2021 odbyło się spotkanie otwierające przy pomocy aplikacji Microsoft Teams. Omówiono zagadnienia związane z celem, zakresem, ryzykami do zbadania w trakcie sprawdzenia oraz omówiono kwestie organizacyjne przeprowadzania czynności audytowych. Spotkanie zamykające odbyło się w siedzibie Żłobka w dniu 21.06.2021. W spotkaniu uczestniczyła Pani Agnieszka Metz – Dyrektor, Anna Dorociak – KODO, Agnieszka Zemla-Mitka - Referent oraz Agnieszka Sowa – IOD.

B: Czynności audytowe objęły analizę przesłanych materiałów dowodowych:

- 1) Arkusz sprawdzenia
- 2) Zobowiązania do zachowania poufności 5 pracowników
- 3) Upoważnienia do przetwarzania danych 5 pracowników
- 4) Lista pracowników zapoznających się z PBDO 5 pracowników
- 5) Oświadczenia o zapoznaniu się z monitoringiem wizyjnym dla 5 pracowników
- 6) Zarządzenie wprowadzające PBDO
- 7) Rejestr czynności przetwarzania
- 8) Wykaz stref bezpieczeństwa
- 9) Rejestr identyfikatorów systemowych

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

Przebieg badania i opis stanu faktycznego:

I. Brak wprowadzenia PBDO

Zgodnie z dowodem nr 6 ZL21 wprowadził zasady ochrony danych w postaci Polityki Bezpieczeństwa Danych Osobowych, zarządzenie nr 10/2018 Dyrektora Żłobka Samorządowego nr 21 z dnia 25 października 2018 roku.

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

Ryzyko się nie zmaterializowało.

II. Brak potwierdzenia zapoznania się z PBDO

ZL21 został poproszony o wylosowanie 5 pracowników. Zgodnie z przesłaną dokumentacją, wszyscy pracownicy podpisują się na Liście zbiorczej „Lista pracowników Żłobka Samorządowego nr 21 dot. Zapoznania się z Polityką Bezpieczeństwa Danych Osobowych”. Nowo zatrudnieni pracownicy podpisują oświadczenie o zapoznaniu się z dokumentacją. Dowód nr 4.

Dodatkowo każdy nowy pracownik zostaje skierowany na szkolenie z zakresu bezpieczeństwa danych osobowych prowadzonych przez IOD jednostki. Na szkoleniu IOD informuje o PBDO. Ostatnie szkolenie dla pracowników ZL21 zostało przeprowadzone w dniu 17.06.2021 r.

Ryzyko się nie zmaterializowało.

III. Brak zastosowania się do obowiązujących przepisów prawa

Osoba przetwarza dane osobowe niezgodnie z uprawnioną formą, celem i zakresem

ZL21 nie ma wprowadzonych zapisów dotyczących celu, sposobu i zakresu monitoringu wizyjnego do Regulaminu pracy.

Nagrania z monitoringu są przechowywane nie dłużej niż 3 miesiące. Przetwarza tylko wizję. Monitoring nie obejmuje toalet, pomieszczeń socjalnych czy jadali. Dowód nr 1.

Niezgodność: Zgodnie z art. 22² Kodeksu pracy pkt 6, zapisy dotyczące celu, zakresu i sposobu monitorowania powinny być wprowadzone do Regulaminu Pracy jednostki. Zgodnie z powyższym należy uaktualnić Regulamin pracy o zapisy dotyczące funkcjonowania monitoringu na terenie szkoły.

Poinformowanie pracownika o funkcjonowaniu monitoringu wizyjnego w placówce

ZL21 informuje pracownikom o funkcjonowaniu monitoringu wizyjnego w jednostce. Pracownik podpisuje odrębne oświadczenie. Dowód nr 1 i 5.

Ryzyko zmaterializowało się częściowo.

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

ZL21 posiada klauzulę informacyjną, warstwową. Na wejściu, bramkach do żłobka jest umieszczona informacja o administratorze oraz telefon. W ogólnodostępnym miejscu w żłobku umieszczona jest klauzula dotycząca monitoringu.

Ryzyko się nie zmaterializowało.

V. Brak lub niezgodny z PBDO podział na strefy bezpieczeństwa.

ZL21 posiada wypełniony zał. nr 5 do PBDO Wykaz stref bezpieczeństwa. Zgodnie z zapisami wyróżnia się trzy strefy bezpieczeństwa: ogólnodostępną, administracyjną (ograniczonego dostępu) oraz strefę bezpieczną. Pomieszczenia, w których przetwarza się dane osobowe są w strefie bezpiecznej, która jest pod szczególnym nadzorem. Dowód nr 8.

Ryzyko się nie zmaterializowało.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych****VI. Brak lub wadliwość zobowiązania o zachowaniu w poufności informacji.**

ZL21 został poproszony o wylosowanie 5 pracowników. W oparciu o 5 skanów zobowiązań do zachowania poufności dla poszczególnych pracowników zostało przeprowadzone badanie, a następnie wyniki zostały odnotowane w arkuszu sprawdzenia – dowód nr 1 oraz 2. Stwierdzono, iż wszyscy pracownicy posiadają zobowiązanie w poufności informacji. We wszystkich przypadkach zobowiązania były kompletne, czyli zawierały: imię i nazwisko pracownika, datę urodzenia, podpis, miejsce i datę podpisania oraz oznaczenie podmiotu dla którego było wystawione.

Ryzyko się nie zmaterializowało.

VII. Brak lub wadliwość upoważnienia do przetwarzania danych osobowych

ZL21 został poproszony o wylosowanie 5 pracowników. W oparciu o 5 skanów upoważnień zostało przeprowadzone badanie, a następnie wyniki zostały odnotowane w arkuszu sprawdzenia – dowody nr 1 oraz 3. Stwierdzono, iż wszyscy pracownicy posiadają upoważnienia do przetwarzania danych osobowych. Upoważnienia są aktualne, z określoną formą przetwarzania danych. Zawierają imię i nazwisko osoby, numer upoważnienia oraz czynności przetwarzania, termin obowiązywania upoważnienia oraz podpis osoby upoważnionej.

Następnie przebadano upoważnienia pod kątem aktualności z obowiązującym Zał. nr 3 do PBDO Rejestrem czynności przetwarzania. Upoważnienie jest zgodne z czynnościami przetwarzania. Dowód nr 3 i 7.

Ryzyko się nie zmaterializowało.

VIII. Niezastosowanie się do PBDO w tym w szczególności do przyjętych procedur wewnętrznych**Brak lub niezgodne hasło zabezpieczające stację roboczą przed nieautoryzowanym dostępem**

ZL21 został poproszony o wylosowanie 5 pracowników. 4 z wylosowanych pracowników posiada dostęp do systemu informatycznego jednostki, posiadają oni dostęp do konta ogólnego, zabezpieczonego hasłem min. 8 znakowym. 1 z wylosowanych pracowników nie posiada dostępu do komputera. Dowód 1.

Praca na koncie z uprzywilejowanymi uprawnieniami (uprawnienia typu Administrator).

ZL21 został poproszony o wylosowanie 5 pracowników. Żaden z wylosowanych pracowników nie posiada dostępu do konta administratora. Praca wykonywana jest na koncie użytkownika. Jediną osobą posiadającą dostęp do konta uprzywilejowanego jest informatyk. Dowód – 1 i 9.

Niezgodność identyfikatorów z prowadzonym rejestrem

ZL21 został poproszony o wylosowanie 5 pracowników. Konta pracowników, którzy posiadają dostęp do systemu informatycznego ZL21 jest zgodny z załącznikiem nr 1 do zał. 7 do PBDO Instrukcji Zarządzania Systemem Informatycznym - Rejestrem identyfikatorów systemowych. Dowód – 1 i 9.

Ryzyko się nie zmaterializowało.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów
o ochronie danych osobowych****7. Stwierdzone przypadki naruszenia w zakresie objętym sprawdzeniem.**

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):

Zgodnie z art. 22² Kodeksu pracy pkt 6, zapisy dotyczące celu, zakresu i sposobu monitorowania powinny być wprowadzone do Regulaminu Pracy jednostki. Zgodnie z powyższym należy uaktualnić Regulamin pracy o zapisy dotyczące funkcjonowania monitoringu na terenie szkoły

10. Załączniki stanowiące składową część sprawozdania:

brak

Sprawozdanie opracował/a:

**INSPEKTOR
OCHRONY DANYCH**...29.06.2021 r. (data i podpis) **Agnieszka Sowa**