NOTATKA POUDAYTOWA

Data audytu: 30.10.2024 r.
Przeprowadzający audyt: Mateusz Zarychta
Podmiot audytowany: Muzeum Historyczno-Etnograficzne w Chojnicach
Zakres audytu: Audyt zgodności z przepisami RODO (Rozporządzenie (UE) 2016/679)
Okres objęty audytem: 2024 rok

---

1. Cel audytu:

Celem audytu było sprawdzenie zgodności procesów przetwarzania danych osobowych z wymogami Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz identyfikacja ewentualnych obszarów wymagających poprawy w zakresie ochrony danych osobowych.

2. Zakres audytu:

Audyt obejmował następujące obszary:

- Procedury przetwarzania danych osobowych,
- Zabezpieczenia techniczne i organizacyjne stosowane w organizacji,
- Polityki i procedury związane z ochroną danych osobowych,
- Prawa osób, których dane dotyczą (m.in. prawo do dostępu, sprostowania, usunięcia),
- Zgody na przetwarzanie danych osobowych,
- Przeszkolenie personelu w zakresie ochrony danych osobowych,
- Dokumentacja związana z przetwarzaniem danych osobowych (np. rejestr czynności przetwarzania).

3. Wyniki audytu:

Audyt wykazał, że:

- Zgodność z RODO: Organizacja w większości spełnia wymagania RODO, jednak zauważono pewne niedociągnięcia w zakresie dokumentacji procesów przetwarzania danych osobowych.
- Zabezpieczenia danych: Stosowane są adekwatne środki techniczne i organizacyjne, jednak sugeruje się wzmocnienie procedur ochrony danych osobowych, zwłaszcza w zakresie szyfrowania wrażliwych informacji.
- Polityki wewnętrzne: Polityki ochrony danych osobowych są wdrożone, ale niektóre z nich wymagają aktualizacji, aby w pełni odpowiadały aktualnym przepisom prawa.
- Szkolenia: Personel jest zazwyczaj przeszkolony, ale audyt sugeruje zorganizowanie dodatkowych szkoleń w zakresie zarządzania incydentami związanymi z danymi osobowymi.

4. Zalecenia:

Na podstawie przeprowadzonego audytu, zaleca się:

- Zaktualizować rejestr czynności przetwarzania danych osobowych o tzw. „Ustawę Kamilka”.
- Przeprowadzenie dodatkowych szkoleń dla pracowników w zakresie postępowania w sytuacjach naruszenia ochrony danych osobowych. W tym celu przygotowany został test z tak zwanych ataków „phishing”.

- Zgodnie z nowymi wytycznymi ekspertów CSIRT NASK hasła dostępowe powinny spełniać minimalne wymagania tj. nie mniej niż 14 znaków, najlepiej w postaci znanego tylko nam zdania lub frazy składającej się z co najmniej pięciu słów. Zmiana hasła nie rzadziej niż co 6 miesięcy.

5. Podsumowanie:

Organizacja wykazuje dużą dbałość o przestrzeganie zasad ochrony danych osobowych, jednak istnieją obszary wymagające poprawy, zwłaszcza w zakresie dokumentacji i aktualizacji wewnętrznych polityk ochrony danych. Należy podjąć działania naprawcze zgodnie z przedstawionymi zaleceniami w celu zapewnienia pełnej zgodności z przepisami RODO.

Data sporządzenia notatki: 30.12.2024 r.