Odpowiedź na wniosek o udostępnienie informacji publicznej z 18.03.2026r.

Dotyczy: **Udzielenie odpowiedzi na przesłane pytania oraz udostępnienia formularza audytu bezpieczeństwa informacji (audytu KRI) za rok 2024 oraz 2025.**

a. Czy w placówce w roku 2024 oraz 2025 prowadzony był audyt bezpieczeństwa informacji?

W Szkole prowadzone są cykliczne (coroczne) audyty wewnętrzne obejmujące obszar bezpieczeństwa informacji, realizowane w ramach audytu/systemu ochrony danych osobowych zgodnego z przepisami RODO.

Zakres audytów obejmuje również zagadnienia związane z bezpieczeństwem informacji, w tym zabezpieczenia organizacyjne (w tym procedury), techniczne i fizyczne, co zapewnia realizację wymagań określonych w § 19 ust. 2 pkt 14 Rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

Audyty takie zostały przeprowadzone zarówno w roku 2024, jak i w roku 2025.

---

b. Czy pracownicy zostali przeszkoleni (KRI)?

W placówce realizowane są szkolenia pracowników w zakresie przetwarzania i ochrony danych osobowych oraz bezpieczeństwa informacji. Szkoleniu poddawani są wszyscy nowi pracownicy , następnie szkolenia realizowane i kierowane są w zależności od zmian w przepisach lub przy audycie wewnętrznym (wizyta w poszczególnych działach , odp na pytania pracowników).

Szkolenia obejmują w szczególności zasady bezpiecznego przetwarzania danych, ochrony informacji, korzystania z systemów informatycznych oraz reagowania na incydenty.

Pracownicy dopuszczeni do przetwarzania danych osobowych zapoznawani są również z obowiązującymi regulacjami wewnętrznymi , regulaminami, procedurami oraz zobowiązywani są do zachowania poufności.

Powyższe działania zapewniają realizację wymagań określonych w § 19 ust. 2 pkt 6 Rozporządzenia KRI.

---

c. Czy obowiązują zasady pracy mobilnej?

W szkole obowiązują zasady zapewniające bezpieczeństwo przetwarzania informacji poza siedzibą jednostki, w tym przy wykorzystaniu sprzętu przenośnego - np regulamin użytkowania laptopów czy regulamin pracy zdalnej.

Zasady te obejmują m.in.:

- obowiązek stosowania zabezpieczeń technicznych (w tym haseł oraz szyfrowania),
- zasady ochrony urządzeń mobilnych przed dostępem osób nieuprawnionych,
- obowiązek zgłaszania incydentów związanych z utratą lub naruszeniem bezpieczeństwa danych,
- zasady bezpiecznego korzystania z urządzeń poza terenem placówki.

Zasady te zostały określone w regulacjach wewnętrznych obowiązujących w jednostce, co zapewnia realizację wymagań § 19 ust. 2 pkt 8 Rozporządzenia KRI.

---

d. Kiedy przeprowadzono ostatnią analizę ryzyka?

Ostatnia analiza ryzyka została przeprowadzona w ramach audytu wewnętrznego realizowanego we wrześniu 2025r

Analiza ta obejmowała identyfikację zagrożeń, ocenę ryzyka oraz określenie działań minimalizujących ryzyko, zgodnie z wymaganiami § 19 ust. 2 pkt 3 Rozporządzenia KRI.

---

e. Jakie regulacje wewnętrzne obowiązują w placówce w ramach zarządzania bezpieczeństwem informacji (np. Polityka Bezpieczeństwa Informacji)?

Do kluczowych dokumentów należą w szczególności:

- instrukcja zarządzania systemem informatycznym / wykaz zabezpieczeń,
- polityka ochrony danych
- procedury nadawania i zarządzania uprawnieniami do systemów,
- polityka haseł i kluczy
- procedura tworzenia kopii zapasowych,
- procedura postępowania z nośnikami danych,
- zasady korzystania ze sprzętu komputerowego, w tym urządzeń mobilnych,
- procedury reagowania na incydenty oraz zapewnienia ciągłości działania,
- regulacje dotyczące zabezpieczeń fizycznych (np. polityka kluczy).

2 .Udostępnienie formularza audytu bezpieczeństwa informacji/KRI (Krajowe Ramy Interoperacyjności) przeprowadzonego za rok 2024 oraz 2025, który zastosowany był w Państwa jednostce podczas audytu bezpieczeństwa informacji.

W odpowiedzi na wniosek informuję, że w jednostce audyt bezpieczeństwa informacji realizowany jest w ramach audytów wewnętrznych obejmujących również obszar ochrony danych osobowych.

Audyt prowadzony jest w oparciu o wewnętrzne narzędzia audytowe (formularze/checklisty/procedury), które zawierają szczegółowe informacje dotyczące stosowanych środków bezpieczeństwa organizacyjnego, technicznego i fizycznego.

Z uwagi na fakt, iż dokumenty te zawierają informacje dotyczące zabezpieczeń systemów informatycznych oraz organizacji ochrony danych, ich udostępnienie mogłoby naruszyć

bezpieczeństwo informacji w jednostce. W związku z tym podane do informacji mogą być tylko ogólne zagadnienia zawarte w formularzu:

- audyty bezpieczeństwa informacji były przeprowadzane w latach 2024 i 2025, w ramach audytów wewnętrznych / audytów ochrony danych osobowych a ich zakres obejmował wymagania określone w Krajowych Ramach Interoperacyjności.

1. Zarządzanie bezpieczeństwem informacji

Obszar	Opis
Wymaganie	Wdrożenie systemu zarządzania bezpieczeństwem informacji
Stan	Zrealizowano
Uwagi	System oparty na procedurach wewnętrznych oraz przepisach RODO

---

2. Analiza ryzyka

Obszar	Opis
Wymaganie	Identyfikacja zagrożeń i ocena ryzyka
Stan	Zrealizowano
Uwagi	Analiza prowadzona cyklicznie

---

3. Zarządzanie dostępem

Obszar	Opis
Wymaganie	Kontrola dostępu do danych i systemów
Stan	Zrealizowano
Uwagi	upoważnienia do przetwarzania danych papierowych i w systemach informatycznych. zasada minimalizacji uprawnień/

---

4. Szkolenia pracowników

Obszar	Opis
Wymaganie	Szkolenie osób przetwarzających informacje
Stan	Zrealizowano
Uwagi	Szkolenia realizowane w ramach wdrożonych procedur (nowi pracownicy/ przy zmianie w przepisach/ podczas audytu

---

5. Praca mobilna

Obszar	Opis
Wymaganie	Zasady bezpiecznego przetwarzania poza jednostką
Stan	Zrealizowano
Uwagi	Obowiązują regulacje dotyczące urządzeń mobilnych

---

6. Kopie zapasowe

Obszar	Opis
Wymaganie	Tworzenie i przechowywanie kopii zapasowych
Stan	Zrealizowano
Uwagi	Stosowane procedury backupu danych

---

7. Zarządzanie incydentami

Obszar	Opis
Wymaganie	Reagowanie na incydenty bezpieczeństwa
Stan	Zrealizowano
Uwagi	Wdrożona procedura obsługi incydentów

---

8. Ciągłość działania

Obszar	Opis
Wymaganie	Zapewnienie ciągłości działania
Stan	Zrealizowano
Uwagi	Obowiązuje plan ciągłości działania

---

9. Zabezpieczenia fizyczne i techniczne

Obszar	Opis
Wymaganie	Ochrona infrastruktury i danych
Stan	Zrealizowano
Uwagi	Stosowane środki organizacyjne i techniczne

---

10. Wnioski końcowe

W wyniku przeprowadzonego audytu stwierdzono, że w jednostce funkcjonuje system zapewniający realizację wymagań w zakresie ochrony danych osobowych (RODO) oraz bezpieczeństwa informacji określonych w Krajowych Ramach Interoperacyjności.

Zidentyfikowano obszary wymagające poprawy/doskonalenia - obszary te następnie zostały poprawione.