

KURS

Cyberbezpieczne środowisko w szkole

ATOM 1

Ramy cyberbezpiecznej szkoły

PROWADZĄCY

Artur Rudnicki
Microsoft Innovative Educator Expert



Wprowadzenie

Cyberbezpieczeństwo w szkołach to kluczowy element ochrony danych uczniów, nauczycieli i całej instytucji edukacyjnej. Współczesne zagrożenia cyfrowe wymagają stosowania wytycznych, standardów oraz procedur, które zapewnią bezpieczeństwo systemów informacyjnych.

Unia Europejska reguluje kwestie cyberbezpieczeństwa i ochrony danych w szkołach poprzez kilka kluczowych aktów prawnych i wytycznych. Oto najważniejsze z nich:

1. Ogólne rozporządzenie o ochronie danych (RODO/GDPR)

- **Zakres:** Dotyczy wszystkich podmiotów przetwarzających dane osobowe, w tym szkół.
- **Obowiązki dla szkół:**
 - » Zapewnienie zgodności z zasadami przetwarzania danych, takimi jak: legalność, przejrzystość, celowość i minimalizacja danych.
 - » Wyznaczenie Inspektora Ochrony Danych (IOD), jeśli szkoła przetwarza dane wrażliwe na dużą skalę.
 - » Informowanie uczniów i rodziców o celach i podstawach prawnych przetwarzania ich danych.
 - » Zapewnienie odpowiednich środków technicznych i organizacyjnych, takich jak szyfrowanie, pseudonimizacja i kontrola dostępu.
 - » Obowiązek raportowania incydentów naruszenia ochrony danych w ciągu 72 godzin do odpowiedniego organu (np. krajowego urzędu ochrony danych).

2. Dyrektywa NIS2 (Network and Information Systems Directive)

- **Zakres:** Dotyczy systemów informacyjnych, w tym w sektorze publicznym, który obejmuje szkoły.
- **Obowiązki dla szkół:**
 - » Wprowadzenie mechanizmów identyfikacji i reagowania na cyberzagrożenia.
 - » Stworzenie procedur zarządzania incydentami cyberbezpieczeństwa.
 - » Współpraca z krajowymi jednostkami ds. cyberbezpieczeństwa (CSIRT).

3. Europejska strategia cyberbezpieczeństwa

- **Cele dla instytucji edukacyjnych:**
 - » Podnoszenie świadomości na temat cyberzagrożeń.
 - » Ułatwianie wdrażania najnowszych technologii zabezpieczających.
 - » Promowanie współpracy między instytucjami edukacyjnymi a organami zajmującymi się bezpieczeństwem cyfrowym.

4. Akt o usługach cyfrowych (Digital Services Act - DSA)

- **Zakres:** Reguluje bezpieczeństwo i odpowiedzialność usług cyfrowych, z których mogą korzystać szkoły.
- **Obowiązki dla szkół:** W kontekście korzystania z platform edukacyjnych lub komunikacyjnych:
 - » Zapewnienie bezpieczeństwa danych uczniów i nauczycieli.
 - » Weryfikacja, czy platformy edukacyjne stosują odpowiednie środki ochrony danych.

5. Akt o cyberodporności (Cyber Resilience Act)

- **Zakres:** Dotyczy produktów i usług cyfrowych, w tym tych używanych w szkołach.
- **Wymagania:**
 - » Gwarancja, że sprzęt i oprogramowanie używane w instytucjach edukacyjnych spełniają standardy cyberbezpieczeństwa.
 - » Regularne aktualizacje oprogramowania oraz zarządzanie lukami bezpieczeństwa.

6. Dyrektywa o ochronie dzieci w środowisku cyfrowym

- **Cele:**
 - » Ochrona dzieci przed nadużyciami i cyberprzemocą.
 - » Promowanie bezpiecznych platform edukacyjnych.
 - » Edukacja na temat cyberbezpieczeństwa jako element programu nauczania.

7. Akt o Sztucznej Inteligencji (AI Act, 2024/1689)

AI Act wszedł w życie 1.08.2024, a przepisy stosuje się stopniowo::

- od 2.02.2025 zakazy wybranych praktyk i obowiązki dot. alfabetyzacji AI,
- od 2.08.2025 część obowiązków dla modeli ogólnego przeznaczenia (GPAI),
- od 2.08.2026 zasadniczo systemy wysokiego ryzyka.

8. Krajowe Implementacje

Unijne przepisy są transponowane do prawa krajowego. Przykładowo w Polsce są to m.in.:

- Ustawa o ochronie danych osobowych (implementacja RODO)
- Ustawa o krajowym systemie cyberbezpieczeństwa (wdrożenie dyrektywy NIS)
- Standardy ochrony małoletnich
- Dostępność cyfrowa podmiotów publicznych
- Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej

Wnioski dla szkół

Szkoły w Unii Europejskiej muszą:

- Dostosować swoje polityki i procedury do wymagań RODO oraz innych aktów.
- Inwestować w systemy zabezpieczeń IT zgodne z unijnymi standardami.
- Wdrażać programy edukacyjne, które uczą uczniów i nauczycieli zasad cyberbezpieczeństwa.

Ministerstwo Edukacji Narodowej (MEN) kładzie duży nacisk na bezpieczeństwo cyfrowe w szkołach, publikując wytyczne i ustalając priorytety w polityce oświatowej. Poniżej kluczowe dokumenty i inicjatywy:

1. Poradnik „Bezpieczna szkoła”

Kompendium rozpoznawania zagrożeń i reagowania (obszar fizyczny i cyfrowy) dla dyrektorów, nauczycieli, rodziców i uczniów. Publikacja pozostaje aktualnym punktem odniesienia (ostatnia aktualizacja serwisu ORE z 20.03.2023).

2. „Higiena cyfrowa i cyberbezpieczeństwo”

Poradnik opracowany przez MEN (listopad 2023), zawiera praktyczne wskazówki dla uczniów, nauczycieli i rodziców w zakresie bezpiecznego korzystania z internetu.

3. Podstawowe kierunki realizacji polityki oświatowej państwa 2025/2026

Wśród priorytetów MEN znalazło się m.in. **promowanie higieny cyfrowej i bezpiecznego poruszania się w sieci, rozwijanie krytycznej analizy informacji oraz poprawne metodyczne wykorzystanie nowoczesnych technologii – w szczególności opartych na sztucznej inteligencji.**

4. Cyberlekcje 3.0

18 gotowych scenariuszy (SP i szkoły ponadpodstawowe) z infografikami/animacjami; dostępne na ZPE.

5. SaferInternet

Scenariusze, infolinie (116 111, 800 100 100) i **Dzień Bezpiecznego Internetu** z pakietami dla szkół.

Szkoły są zachęcane do opracowywania własnych planów zapewnienia bezpieczeństwa cyfrowego oraz powoływania szkolnych liderów tej tematyki, wspierających kierownictwo placówki w systemowych działaniach na rzecz cyberbezpieczeństwa.

Podsumowanie

Budowanie ram cyberbezpieczeństwa w szkole wymaga łączenia edukacji, technologii i zgodności z regulacjami prawnymi. Szkoły powinny inwestować w rozwój swoich systemów informatycznych oraz regularnie edukować całą społeczność szkolną w zakresie bezpieczeństwa cyfrowego.