ONLINE PRIVACY AND THE GDPR

lesson plan author: John Sudar, American Elementary School in Gdynia

This workshop scenario was created for the educational project DEB@TA. Think.Speak.Act., implemented within the Ministry of National Education program "Young Citizens."

Duration:

2 instructional hours (90 minutes + break + final discussion)

Participants:

Youth aged 13–14

Materials:

- Computer and projector
- Video explaining the GDPR
- Video regarding AI and Ethics/Privacy
- Sets of "Privacy Detective" scenario cards
- Whiteboard / flipchart

General Workshop Objectives:

Participants will:

- Understand the fundamentals of online privacy and its importance.
- Recognize common threats to privacy on social media and online services.
- Identify key aspects, principles, and objectives of the GDPR.
- Recognize Data Subject Rights (informed, access, rectification, erasure).
- Apply knowledge to solve real-world privacy challenges and scenarios.
- Learn best practices to maximize their personal online privacy.

Workshop Flow

1. Introduction and Icebreaker (15 min)

Objective: Assess prior knowledge and visualize the scale of data collection.

Activities:

- **Discussion:** Participants share what they know about online privacy and how laws protect them.
- **Brainstorming:** In small groups, students list all personal data collected in a typical day (emails, social media, shopping, location).
- **Reflection:** A whole-group discussion on why data privacy is important and the dangers of leaving data unprotected.

2. Dive into the GDPR (25 min)

Objective: Understand the core principles and rights within the GDPR.

Activities:

- **Screening:** Watch a short video about the GDPR.
- **Mini-Lecture:** Facilitator explains the **7 Principles** (Lawfulness, Fairness, Transparency, Minimization, Accuracy, Storage Limitation, Integrity, Accountability) and **User Rights** (Right to be informed, access, rectification, erasure).
- **Match-up Activity:** Small groups match real-life scenarios to the correct GDPR principle.
- **Discussion:** Do participants feel adequately protected? What changes would they make to EU regulations?

3. Privacy Detectives Game (25 min)

Objective: Apply GDPR knowledge to identify violations in a business context.

Activities:

- **Scenario Work:** Groups receive a fictional case about a company with poor privacy policies.
- **Investigation:** Teams analyze the case to identify violations and determine which GDPR principles were broken.
- **Problem Solving:** Teams propose solutions and preventative measures for the company.
- **Plenary:** Groups present their findings and solutions to the class.

4. Taking Personal Responsibility (15 min)

Objective: Equip students with practical tools for personal data protection.

Activities:

- **Brainstorming:** The group discusses ways to protect personal data.
- **Instruction:** The facilitator introduces the "10 Steps to Privacy":
    1. Strong, Unique Passwords
    2. Two-Factor Authentication (2FA)
    3. Regular Software Updates
    4. Secure Connections
    5. Limiting Sharing of Information
    6. Avoiding Suspicious Links
    7. Using Privacy Tools (e.g., Firefox, uBlock Origin)
    8. Managing Account Permissions

9. Reading Privacy Policies
10. Continuous Education

5. Wrap-up and Action Plan (10 min)

Objective: Summarize learning and commit to personal changes.

Activities:

- **Review:** Discuss what was learned about online privacy and the GDPR.
- **Future Outlook:** Analyze future challenges to privacy.
- **Personal Action Plan:** Participants list specific steps they will take immediately to improve their own privacy habits.

Learning Outcomes

After the workshop, students:

- Understand the fundamentals of online privacy and its importance.
- Recognize common threats on social media and online services.
- Can identify Key Aspects of the General Data Protection Regulation (GDPR).
- Understand who is affected by GDPR and what constitutes personal data.
- Can analyze case studies to identify non-compliance and risks.
- Can apply knowledge to suggest solutions for everyday privacy challenges.

License

This publication is distributed under the Creative Commons Attribution – NonCommercial (CC BY-NC 4.0) International license.

PRYWATNOŚĆ W SIECI I RODO

autor planu lekcji: John Sudar, Amerykańska Szkoła Podstawowa w Gdyni

Scenariusz powstał na potrzeby projektu DEB@TA. Myślimy.Mówimy.Działamy. realizowanego w ramach programu Ministerstwa Edukacji Narodowej „Młodzi Obywatele".

Czas trwania:

2 godziny dydaktyczne (90 minut + przerwa + dyskusja końcowa)

Uczestnicy:

Młodzież w wieku 13–14 lat

Materiały:

- Komputer i projektor
- Film wyjaśniający RODO (GDPR)
- Film o etyce i prywatności w AI
- Zestaw kart ze scenariuszami „Detektywi Prywatności”
- Tablica / flipchart

Cele ogólne warsztatu:

Uczestnicy:

- Zrozumieją podstawy prywatności w sieci i jej znaczenie.
- Rozpoznają typowe zagrożenia dla prywatności w mediach społecznościowych i usługach online.
- Zidentyfikują kluczowe aspekty i zasady Ogólnego Rozporządzenia o Ochronie Danych (RODO/GDPR).
- Poznają prawa osób, których dane dotyczą (prawo do informacji, dostępu, sprostowania, usunięcia).
- Zastosują wiedzę do rozwiązywania rzeczywistych problemów i scenariuszy.
- Poznają najlepsze praktyki w celu maksymalizacji własnego bezpieczeństwa online.

Przebieg zajęć

1. Wprowadzenie i Icebreaker (15 min)

Cel: Sprawdzenie wiedzy wstępnej i wizualizacja skali zbierania danych.

Działania:

- **Dyskusja:** Uczestnicy dzielą się wiedzą na temat prywatności w sieci i przepisów chroniących użytkowników.
- **Burza mózgów:** W małych grupach uczniowie wypisują wszystkie dane osobiste zbierane podczas typowego dnia (e-maile, media społecznościowe, zakupy, lokalizacja).

- **Refleksja:** Dyskusja na forum o tym, dlaczego prywatność danych jest ważna i jakie są zagrożenia związane z brakiem ochrony.

2. Zanurzenie w RODO (GDPR) (25 min)

Cel: Zrozumienie kluczowych zasad i praw wynikających z RODO.

Działania:

- **Projekcja:** Obejrzenie krótkiego filmu o RODO.
- **Mini-wykład:** Prowadzący omawia **7 Zasad** (Zgodność z prawem, rzetelność, przejrzystość; Minimalizacja danych; Prawidłowość; Ograniczenie przechowywania; Integralność i poufność; Rozliczalność) oraz **Prawa Użytkownika** (Prawo do bycia poinformowanym, dostępu, sprostowania, bycia zapomnianym).
- **Ćwiczenie Dopasuj:** Małe grupy dopasowują opisy sytuacji z życia wziętych do odpowiedniej zasady RODO.
- **Dyskusja:** Czy uczestnicy czują się odpowiednio chronieni? Jakie zmiany wprowadziliby w przepisach UE?

3. Gra: Detektywi Prywatności (25 min)

Cel: Zastosowanie wiedzy o RODO do identyfikacji naruszeń w kontekście biznesowym.

Działania:

- **Analiza scenariusza:** Grupy otrzymują fikcyjny opis firmy, która ma słabe polityki prywatności.
- **Śledztwo:** Zespoły analizują sprawę, aby zidentyfikować naruszenia i określić, które zasady RODO zostały złamane.
- **Rozwiązywanie problemów:** Zespoły proponują rozwiązania i środki zapobiegawcze dla firmy.
- **Prezentacja:** Grupy przedstawiają swoje wnioski i rozwiązania na forum klasy.

4. Odpowiedzialność Osobista (15 min)

Cel: Wyposażenie uczniów w praktyczne narzędzia ochrony danych.

Działania:

- **Burza mózgów:** Grupa omawia sposoby ochrony własnych danych.
- **Instruktaż:** Prowadzący przedstawia „10 kroków do prywatności”:
    1. Silne, unikalne hasła
    2. Uwierzytelnianie dwuskładnikowe (2FA)
    3. Regularne aktualizacje oprogramowania
    4. Bezpieczne połączenia
    5. Ograniczanie udostępniania informacji

6. Unikanie podejrzanych linków
7. Używanie narzędzi chroniących prywatność (np. Firefox, uBlock Origin)
8. Zarządzanie uprawnieniami kont
9. Czytanie polityk prywatności
10. Ciągła edukacja

5. Podsumowanie i Osobisty Plan Działania (10 min)

Cel: Podsumowanie wiedzy i zobowiązanie do zmian nawyków.

Działania:

- **Przegląd:** Dyskusja o tym, czego nauczyliśmy się o prywatności i RODO.
- **Przyszłość:** Analiza przyszłych wyzwań dla prywatności.
- **Osobisty Plan Działania:** Uczestnicy wypisują konkretne kroki, które podejmą natychmiast, aby poprawić swoje nawyki w zakresie prywatności.

Efekty uczenia się

Po warsztacie uczniowie:

- Rozumieją podstawy prywatności w sieci i jej znaczenie.
- Rozpoznają typowe zagrożenia w mediach społecznościowych i usługach online.
- Potrafią zidentyfikować kluczowe aspekty RODO (GDPR).
- Rozumieją, kogo dotyczy RODO i co stanowi dane osobowe.
- Potrafią analizować studia przypadków w celu identyfikacji braku zgodności i ryzyka.
- Potrafią zastosować wiedzę do proponowania rozwiązań codziennych problemów z prywatnością.

Licencja:

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC 4.0) Międzynarodowe.