



DETEKTYWI PRYWATNOŚCI.

MISJA: ODPORNOŚĆ CYFROWA

ogólnopolska gra terenowa dla szkół podstawowych
II etap edukacyjny: klasy IV-VI



MATERIAŁ DLA NAUCZYCIELA / KOORDYNATORA

SCENARIUSZ I METRYCZKA

- **Organizator:** Urząd Ochrony Danych Osobowych
- **Autorki:** Marta Mikołajczyk, Justyna Fijałkowska, Urząd Ochrony Danych Osobowych
- **Konsultacja merytoryczna:** dr Lena Tkaczyk, dr Adam Gogacz, Ośrodek Rozwoju Edukacji
- **Data pilotażu:** 15 – 23 października 2026 r. (ewaluacja do 26 października 2026 r.)

SPIS TREŚCI

WPROWADZENIE	3
CEL GRY	4
INSTRUKCJE ORGANIZACYJNE	6
ZASADY	9
PRZEBIEG GRY	12
➤ ETAP I: WPROWADZENIE (POWITANIE DRUŻYN I PRZEDSTAWIENIE ZASAD)	12
➤ ETAP II: STACJE WYZWAŃ – PRZEBIEG GRY	13
• STACJA 1: Twoje prawa to Twoje supermoce - Tarcza prywatności RODO	13
• STACJA 2: Mroczny labirynt manipulacji i monetyzacji danych	14
• STACJA 3: Dwie twarze maszyny (korzyści i zagrożenia AI)	15
• STACJA 4: Lustro kłamstw - deepfake i dezinformacja	15
• STACJA 5: Wypuszczony balonik czyli pułapki wizerunku	16
• STACJA 6: Zatruty haczyk - phishing	17
➤ ETAP III: PODSUMOWANIE I EWALUACJA	17
LISTA MATERIAŁÓW POTRZEBNYCH DO REALIZACJI GRY	20
LIST PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH	20
KLASOWY KODEKS OCHRONY PRYWATNOŚCI	23



WPROWADZENIE

Edukacyjna gra terenowa pt. „Detektywi Prywatności: Misja: odporność cyfrowa”, została przygotowana z myślą o uczniach klas 4-6. Gra realizowana jest w ramach programu edukacyjnego „Twoje dane – Twoja sprawa” Prezesa Urzędu Ochrony Danych Osobowych, którego celem jest edukacja uczniów i nauczycieli na temat skutecznej ochrony danych osobowych, kompetencji niezbędnej do odpowiedzialnego i bezpiecznego funkcjonowania w środowisku cyfrowym. Program jest realizowany pod patronatem honorowym Ministra Edukacji i Rzecznika Praw Dziecka.

Gra umożliwia rozwijanie kluczowych kompetencji uczniów w zakresie ochrony prywatności, bezpieczeństwa informacyjnego oraz higieny cyfrowej. Uczestnicy uczą się rozpoznawać zagrożenia występujące w przestrzeni internetowej, podejmować świadome decyzje dotyczące udostępnienia informacji o sobie oraz odpowiedzialnie korzystać z technologii.

Uczniowie pracują w zespołach i odwiedzają kolejne stacje z zadaniami, gdzie rozwiązują praktyczne problemy, analizują sytuacje z życia codziennego oraz podejmują decyzje wymagające krytycznego myślenia. Projekt jest formą nauki przez działanie, która angażuje uczestników, wzmacnia współpracę, rozwija kompetencje społeczne oraz sprzyja trwałemu przyswajaniu wiedzy poprzez doświadczenie i działanie.

Zadania odnoszą się do rzeczywistych wyzwań, z którymi dzieci spotykają się każdego dnia podczas korzystania z internetu i urządzeń cyfrowych. Dzięki temu rozwijają umiejętności bezpiecznego funkcjonowania w świecie nowych technologii, budują odporność na manipulację, dezinformację i cyberzagrożenia oraz kształtują nawyki odpowiedzialnego korzystania z sieci z poszanowaniem prywatności własnej i innych osób.



CEL GRY

Głównym celem edukacyjnej gry terenowej „Detektywi prywatności. Misja: odporność cyfrowa” jest kształtowanie u uczniów świadomych, odpowiedzialnych i bezpiecznych postaw w przestrzeni cyfrowej, poprzez rozwijanie kompetencji w zakresie ochrony danych osobowych, ochrony prywatności, bezpieczeństwa informacyjnego oraz dobrostanu cyfrowego. Gra wspiera uczniów w zdobywaniu praktycznych umiejętności niezbędnych do bezpiecznego korzystania z internetu i nowych technologii, rozwija krytyczne myślenie oraz uczy odpowiedzialnego podejmowania decyzji w sytuacjach związanych z przetwarzaniem danych osobowych i korzystaniem z usług cyfrowych. Łączy elementy współpracy i zabawy, zwiększa zaangażowanie uczestników oraz sprzyja trwałemu przyswajaniu wiedzy i kształtowaniu właściwych nawyków cyfrowych. Może być realizowana w ramach pracy projektowej obejmując działania wychowawcze, profilaktyczne, wiedzę przedmiotową z zakresu informatyki oraz edukacji zdrowotnej.

Cele szczegółowe

Uczestnik gry:

- rozwija kompetencje w zakresie ochrony danych osobowych i prywatności oraz bezpieczeństwa informacyjnego i cyberbezpieczeństwa;
- kształtuje odporność cyfrową poprzez analizowanie zagrożeń oraz podejmowanie świadomych i odpowiedzialnych decyzji podczas korzystania z technologii;
- stosuje zasadę „Zatrzymuję się. Myślę. Decyduję świadomie” przed udostępnieniem informacji o sobie lub innych osobach;
- rozpoznaje próby manipulacji, dezinformacji, cyberprzemocy oraz mechanizmy wpływu wykorzystywane w środowisku cyfrowym;
- rozumie wartość danych osobowych oraz konsekwencje ich nieprzemyślanego udostępniania, w tym mechanizmy profilowania i monetyzacji danych;
- potrafi ocenić wiarygodność informacji i źródeł internetowych oraz krytycznie analizować treści publikowane w sieci;
- rozwija umiejętność reagowania na zagrożenia cyfrowe, takie jak phishing, wyłudzenia danych, kradzież tożsamości, deepfake, oszustwa internetowe czy manipulacyjne interfejsy (dark patterns tzw. zwodnicze interfejsy projektowe);

- 
- poznaje sposoby ochrony swoich kont, urządzeń i danych oraz zasady bezpiecznego korzystania z aplikacji i serwisów internetowych;
 - rozwija umiejętności sprzyjające zachowaniu dobrostanu cyfrowego, ucząc się świadomego, zrównoważonego i odpowiedzialnego korzystania z technologii oraz rozpoznawania ryzyka związanego z nadmiernym korzystaniem z urządzeń cyfrowych;
 - kształtuje postawy szacunku wobec prywatności i wizerunku własnego oraz innych osób, rozumiejąc znaczenie świadomego publikowania treści i zasad uzyskiwania zgody na rozpowszechnianie wizerunku;
 - rozwija kompetencje społeczne, w tym współpracę, komunikację, odpowiedzialność za podejmowane decyzje oraz rozwiązywanie problemów w zespole;
 - wzmacnia poczucie sprawczości i odpowiedzialności za własne bezpieczeństwo w świecie cyfrowym oraz bezpieczeństwo innych użytkowników.



INSTRUKCJE ORGANIZACYJNE

Gra organizowana jest w ramach ogólnopolskiego programu edukacyjnego Prezesa Urzędu Ochrony Danych Osobowych „Twoje dane – Twoja sprawa”. Szczegółowe informacje na temat zapisów i realizacji programu znajdują się na stronie UODO: www.uodo.gov.pl/tdts. W ramach programu dzielimy się wiedzą ekspercką w formie konferencji, szkoleń, webinarów i materiałów edukacyjnych. Rekrutacja do XVII edycji trwa do 31 października 2026 roku.

- **Etap edukacyjny:** II etap edukacyjny: szkoła podstawowa, klasy IV-VI.
- **Przedmioty*:** edukacja zdrowotna (dział: Internet i profilaktyka uzależnień), informatyka (dział: Bezpieczeństwo i kultura cyfrowa), zajęcia z wychowawcą.
- **Proponowany czas realizacji:** 3 jednostki lekcyjne, łącznie 135 minut (10 min. wprowadzenie, 70 min. właściwa rozgrywka na stacjach, 40 min. tworzenie plakatów z zasadami przez grupy oraz Klasowego Kodeksu Ochrony Prywatności, 15 min. podsumowanie, ewaluacja).
- **Formy pracy:** praca zespołowa, praca projektowa w małych grupach zadaniowych (4-5 osób).
- **Miejsce realizacji:** przestrzeń szkoły/ teren wokół szkoły.

Uzasadnienie:

Współczesne środowisko cyfrowe przestało być dla młodego pokolenia jedynie narzędziem technologicznym – stało się przestrzenią kształtowania tożsamości, relacji społecznych i postaw życiowych. Uczniowie klas 4-6 posługują się nowymi technologiami w sposób intuicyjny, a jednak ich wiedza o ryzykach związanych z ochroną prywatności ma często charakter deklaracyjny i nie przekłada się na codzienne nawyki.

Gra uczy młodego człowieka krytycznego myślenia, świadomego zarządzania własnym wizerunkiem oraz podmiotowego korzystania z prawa do odmowy poprzez stwierdzenie „Nie zgadzam się” oraz w myśl zasady „Zatrzymuję się. Myślę. Decyduję świadomie”.

*Spójność gry z podstawą programową kształcenia ogólnego

Gra stanowi aktywizujące narzędzie do realizacji zapisów podstawy programowej dla klas IV-VI w zakresie następujących przedmiotów:



➤ **Edukacja zdrowotna – dział. Internet i profilaktyka uzależnień**

Uczeń:

- rozumie jak budować odporność i bezpieczeństwo cyfrowe;
- zagrożenia wynikające z niewłaściwego używania technologii informacyjno-komunikacyjnych, takie jak uzależnienie od Internetu i gier komputerowych, phishing, deepfake, kradzież tożsamości;
- rozumie korzyści i zagrożenia związane ze sztuczną inteligencją.

➤ **Edukacja informatyczna dział. Bezpieczeństwo i kultura cyfrowa**

Uczeń:

- bezpiecznie i odpowiedzialnie porusza się w cyberprzestrzeni oraz korzysta z urządzeń nowych technologii;
- przestrzega zasad ochrony danych osobowych i wizerunku zgodnie z prawem;
- rozumie konsekwencje nieświadomego udostępniania informacji o sobie i innych w sieci (cyfrowy ślad, sharenting);
- rozwija kompetencje krytycznego myślenia wobec treści i manipulacji w sieci (dezinformacja, profilowanie, zwodnicze interfejsy projektowe tzw. dark patterns).

Cele programu edukacyjnego Prezesa UODO „Twoje dane – Twoja sprawa”

Gra bezpośrednio wpisuje się w priorytety edukacyjne 17. Edycji programu, takie jak:

- budowanie odporności cyfrowej – kształtowanie nawyku refleksji przed każdym kliknięciem i przekazaniem danych;
- wspieranie bezpiecznych działań w przestrzeni cyfrowej, sprzyjających ochronie danych osobowych, w tym danych dotyczących zdrowia;
- rozwój sprawczości i asertywności – wyposażenie ucznia w prawo do ochrony prywatności i umiejętności wycofania zgody lub odmowy jej udzielenia;
- rozumienie monetyzacji danych – uświadomienie uczniom, że w świecie cyfrowym usługa „darmowa” opłacana jest ich danymi osobowymi, uwagą i prywatnością;
- zrozumienie działania algorytmów, mechanizmów gier hazardowych w sieci i manipulacji utrudniających podejmowanie świadomych decyzji w zakresie ochrony prywatności w świecie cyfrowym;

- 
- odpowiedzialne zarządzanie wizerunkiem – zrozumienie nieodwracalnych skutków publikacji w sieci (metafora wypuszczonego balonika);
 - podkreślenia wartości ochrony danych osobowych w dobie dynamicznego rozwoju nowych technologii oraz postępującej cyfryzacji życia społecznego.

Podsumowując, gra terenowa wpisuje się w aktualne priorytety programu „Twoje dane Twoja sprawa” oraz odpowiada na nowe wyzwania związane z cyfrowym środowiskiem życia dzieci i młodzieży. Warto również podkreślić, że nowelizacja prawa w kwestii ograniczenia używania telefonów w szkole wzmacnia działania szkoły na rzecz higieny cyfrowej i przeciwdziałania uzależnieniom, zapewnienia bezpieczeństwa, a także dobrostanu i ochrony prywatności uczniów. Przerwa od telefonu, to również okazja do rozmowy, ruchu zabawy i budowania relacji. Służy proponowana gra terenowa, która rozwija kompetencje społeczne uczniów. Jej tematyka łączy ochronę danych osobowych i prywatności z higieną cyfrową, bezpieczeństwem informacyjnym, ochroną wizerunku, przeciwdziałaniem manipulacji oraz świadomym korzystaniem z nowych technologii i sztucznej inteligencji. Istotnym kontekstem jej realizacji w związku z wprowadzeniem ustawowych ograniczeń korzystania z telefonów w szkołach podstawowych, jest wzmacnianie działań na rzecz koncentracji, dobrostanu, budowania relacji społecznych i higieny cyfrowej. Gra terenowa stanowi praktyczne narzędzie, które pokazuje uczniom, że ochrona prywatności nie oznacza rezygnacji z technologii, lecz umiejętność świadomego i odpowiedzialnego decydowania, kiedy i w jaki sposób z niej korzystać, aby chronić siebie i swoje dane osobowe. Gra poprzez proponowane aktywności i zadania wspiera rozwój odporności cyfrowej i odpowiedzialnego korzystania z narzędzi cyfrowych. Zaplanowane zadania przekładają wiedzę o ochronie danych osobowych na konkretne sytuacje i decyzje, z którymi uczniowie spotykają się na co dzień.



ZASADY

1. Nauczyciel jako mentor i przewodnik

Prowadzący nie podaje wiedzy, ale prowadzi uczniów poprzez pytania pogłębiające, nie jest strażnikiem poprawności wiedzy. Nie ocenia zachowań i odpowiedzi uczniów, lecz prowokuje do myślenia poprzez pytania np. „Po co aplikacji te dane?”, „Kto ma dostęp do tych danych?”, „Do czego aplikacja potrzebuje dane?”, „Co się stanie w przyszłości z Twoimi danymi udostępnionymi w sieci?”. Poprzez pytania otwarte stymuluje uczniów do samodzielnego wyciągania wniosków.

2. Przygotowanie przestrzeni

Wymagana jest organizacja 6 stacji w różnych częściach szkoły lub w terenie. Do sprawnego przebiegu gry, w zależności od liczby drużyn, proponujemy zaangażowanie 6 lub 12 osób do obsługi stacji.

3. Przygotowanie stacji od 1 do 6

Na każdą stację należy wydrukować „Karty pracy dla drużyny” (liczba egzemplarzy powinna być równa liczbie drużyn), „Kartę mentora – opiekuna stacji”, „Klucz odpowiedzi dla mentora – opiekuna stacji” oraz tabliczkę z „Pigułką wiedzy” i fragment Kodu Odporności Cyfrowej, które otrzymuje opiekun stacji. Opiekun stacji odgrywa rolę mentora, który nie podaje gotowych odpowiedzi ani ocen, tylko zadaje pytania, które pobudzają uczniów do dyskusji, analizy i samodzielnego wyciągania wniosków. Jeśli drużyna podaje błędną lub niepełną odpowiedź, mentor nie krytykuje zespołu, lecz zadaje jedno z pytań pomocniczych zawartych na karcie mentora. Zaliczenie stacji następuje w momencie, gdy uczniowie własnymi słowami sformułują prawidłowo zasadę ochrony prywatności.

4. Zasada działania

Gra opiera się na pracy zespołowej (grupy 4-5 osobowe). Na każdej z sześciu stacji czeka wyzwanie. Uczniowie uczą się poprzez doświadczenie i dyskusję. Każda drużyna dysponuje zasobem 12 żetonów tzw. **żetonów decyzji**. Uczniowie otrzymują kopertę tzw. „**Portfel prywatności**” z żetonami. Do każdej stacji przypisane są po dwa żetony. Uczniowie na stacjach nie tylko udzielają odpowiedzi, ale muszą podjąć decyzję i właściwie odpowiedzieć.

Podejmowanie nieprzemyślanych lub ryzykownych decyzji na stacjach skutkuje utratą żetonu,



Kod zawiera istotny przekaz dla uczniów, aby zawsze pamiętali, że od każdego z nas i naszych codziennych decyzji i uwagi zależy, czy nasze dane będą bezpieczne. Gra kończy się sformułowaniem i akceptacją klasowego „Kodeksu Ochrony Prywatności” oraz odpowiedzią na pytanie: „Co po dzisiejszej grze zrobisz inaczej w internecie?”.

7. Ewaluacja

Najważniejszym punktem wykonywanych zadań jest faza refleksji po każdej rozgrywce, formułowanie zasad oraz to, w jaki sposób uczniowie argumentują swoje wybory. Jeśli grupa popełni błąd na stacji, nie otrzymuje gotowej odpowiedzi, a jest naprowadzana pytaniami. Istotne jest zrozumienie, na czym polega ochrona prywatności oraz praktyczne stosowanie zasad przygotowanych przez uczniów, a także wnioski i refleksja nad tym, co zrobią inaczej następnym razem w sferze ochrony swojej prywatności.





PRZEBIEG GRY

➤ ETAP I: WPROWADZENIE (POWITANIE DRUŻYN I PRZEDSTAWIENIE ZASAD)

Nauczyciel wita uczniów i tłumaczy cel i zasady gry „Detektywi prywatności. Misja: odporność cyfrowa”

„Uwaga! System bezpieczeństwa jest zagrożony. Ktoś próbuje wykraść Wasze dane. Alert dotyczy naruszenia prywatności. Waszą misją jako detektywów prywatności jest skuteczna ochrona przed utratą prywatności i nabywanie odporności w świecie cyfrowym. Waszym zadaniem jest zdobycie „Kodu odporności cyfrowej”, zachowanie jak największej liczby „Żetonów decyzji” oraz opracowanie zasad, które będą stanowiły podstawę Waszego bezpieczeństwa i ochrony Waszej prywatności w świecie cyfrowym”.

Od tej pory wcielacie się w rolę detektywów prywatności. Każda drużyna (4-5 osób) otrzymuje kopertę tzw. „Portfel prywatności” zawierający 12 „Żetonów decyzji”, do którego również włożycie fragmenty „Kodu Odporności Cyfrowej”.

Waszym zadaniem jest odnalezienie 6 stacji. Każda drużyna rozpoczyna grę od innej stacji według otrzymanej mapy przygotowanej dla drużyny. Na każdej stacji czeka wyzwanie. Jeśli jako drużyna postąpiacie nieostrożnie, podejmiecie złą decyzję rozwiązując zadania – stracie żeton z „Portfela prywatności”.

Waszym celem jest dotarcie do końca gry, z jak największą liczbą „Żetonów decyzji” oraz ułożenie z fragmentów hasła „Kodu Odporności Cyfrowej”. Następnie przygotujecie zasady do stworzenia klasowego Kodeksu Ochrony Prywatności, na podstawie tego co się dowiedzieliście podczas gry.

Każda grupa (drużyna) otrzymuje pakiet startowy – kopertę z żetonami decyzji oraz mapę stacji. Po przybyciu na stację macie 60 sekund na zapoznanie się z „Pigułką wiedzy”. Na rozwiązanie zadań na każdej ze stacji, macie około 8 minut.

Zadaniem opiekunów stacji - mentorów jest przekazanie Wam „Kart pracy dla drużyny” i ewentualna pomoc w rozwiązaniu zadań poprzez naprowadzanie pytaniami. Nie wolno udzielać odpowiedzi i podpowiadać drużynie. Czas start!”

Uwaga: Jeśli po przybyciu na stację okaże się, że ktoś już przy niej jest, czekacie na swoją kolej, w wyznaczonym przez opiekuna stacji miejscu.



➤ ETAP II: STACJE WYZWAŃ – PRZEBIEG GRY

Cel misji: rozwiązanie zadań, zachowanie jak największej liczby żetonów decyzji i odkrycie „Kodu Odporności Cyfrowej”, a następnie sformułowanie zasad ochrony prywatności.

Po przejściu wszystkich stacji i zebraniu fragmentów Kodu Odporności Cyfrowej, każda drużyna przygotowuje zasady ochrony prywatności, aby następnie wspólnie wypracować klasowy Kodeks Ochrony Prywatności.

Na koniec misji każda drużyna otrzymuje potwierdzenie ukończenia misji w formie dyplomu.

Następnie po zakończeniu gry nauczyciel wypełnia elektroniczną ankietę ze strony UODO i otrzymuje potwierdzenie.



STACJA 1: Twoje prawa to Twoje supermoce - Tarcza prywatności RODO

Cel stacji

Uczniowie poznają podstawowe znaczenie RODO oraz wybrane prawa związane z ochroną danych osobowych. Uczą się rozpoznawać sytuacje w których mogą skorzystać ze swoich praw.

Zadania dla drużyny i mentora – opiekuna stacji

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Podsumowanie i wnioski – ważna zasada

Znajomość swoich praw pomaga lepiej chronić swoją prywatność.

Wskazówka dla nauczyciela

Warto podkreślić, że nie wszystkie prawa działają w każdej sytuacji. Przykładowo wycofywanie zgody dotyczy przetwarzania opartego na zgodzie, a prawo do usunięcia danych, nie jest prawem bezwzględny.

ZŁOTA ZASADA STACJI 1

SUPERMOC DETEKTYWA PRYWATNOŚCI

Supermoc zmiany zdania – zgodę wyrażoną w aplikacji lub grze możesz w każdej chwili wycofać.

Wycofanie zgody musi być tak samo łatwe, jak jej wyrażenie.

Kiedy aplikacja czy inna osoba żąda od Ciebie za dużo danych, skorzystaj ze swojej cyfrowej supermocy i powiedz: „NIE ZGADZAM SIĘ!”



STACJA 2: Mroczny labirynt manipulacji i monetyzacji danych

Cel stacji

Uczniowie dostrzegają związek między pozornie darmowymi grami i usługami, a utratą prywatności, uwagą i zrachowaniami użytkowników internetu. Rozpoznają podstawowe techniki manipulacji, w tym zwodnicze wzorce projektowe (dark patterns) oraz sygnały mogące wskazywać na problematyczne korzystanie z gier.

Zadania dla drużyny i mentora – opiekuna stacji

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Podsumowanie i wnioski – ważna zasada

Jeśli coś jest „za darmo”, warto sprawdzić, czym płacimy – pieniędzmi, danymi osobowymi czy swoją uwagą.

ZŁOTA ZASADA STACJI 2

SUPERMOC DETEKTYWA PRYWATNOŚCI

Kontrola czasu i asertywność w udostępnianiu danych osobowych – zanim usiądziesz do gry, ustal z rodzicami jasny limit czasu i go przestrzegaj. Kiedy gra wymaga dostępu do mikrofonu lub kontaktów, zastanów się czy to jest konieczne do działania gry. Jeśli nie – po prostu odmów.



STACJA 3: Dwie twarze maszyny (korzyści i zagrożenia AI)

Cel stacji

Pokazanie uczniom, że sztuczna inteligencja może być przydatnym narzędziem, ale korzystanie z niej wymaga krytycznego myślenia oraz dbałości o prywatność.

Zadania dla drużyny i mentora – opiekuna stacji

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Podsumowanie i wnioski – ważna zasada

Sztuczna inteligencja może halucynować i podawać nieprawdziwe informacje. Zawsze należy je sprawdzać w wiarygodnych źródłach. Nie wolno też wpisywać danych osobowych swoich oraz danych innych osób do narzędzi sztucznej inteligencji.

ZŁOTA ZASADA STACJI 3

SUPERMOC DETEKTYWA PRYWATNOŚCI

AI to nie pamiętnik! Nigdy nie wpisuj do AI swoich haseł, problemów, sekretów ani żadnych danych osobowych. Stosuj zasadę: Jeśli nie powiedziałbyś czegoś obcej osobie na ulicy – nigdy nie wpisuj tego do narzędzi AI. Im mniej informacji o sobie udostępniasz w internecie, tym lepiej (zasada minimalizacja danych). Nie udostępniaj danych, które powinny być szczególnie chronione np. dane o zdrowiu.



STACJA 4: Lustro kłamstw - deepfake i dezinformacja

Cel stacji

Rozwijanie krytycznego myślenia wobec zdjęć, filmów i innych treści publikowanych w internecie. Uczniowie poznają zjawisko deepfake i uczą się, że obraz lub nagranie nie zawsze przedstawia prawdziwe sytuacje. Technologia może służyć do tworzenia dezinformacji.



Zadania dla drużyny i mentora – opiekuna stacji

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Podsumowanie i wnioski – ważna zasada

To, co widzisz w internecie, nie zawsze jest tym, co wydarzyło się naprawdę.

ZŁOTA ZASADA STACJI 4

SUPERMOC DETEKTYWA PRYWATNOŚCI

Zatrzymuję się. Myślę. Sprawdzam. Powiedzenie „zobaczyć lub usłyszeć nie znaczy uwierzyć”.

Zawsze sprawdzam, czy informacja jest prawdziwa.

Ustal z rodzicami tajne „hasło rodzinne” (np. „zielony ogórek”), aby w razie podejrzanego telefonu natychmiast zweryfikować, czy naprawdę po drugiej stronie jest ktoś bliski.



STACJA 5: Wypuszczony balonik czyli pułapki wizerunku

Cel stacji

Uświadomienie uczniom, że publikacja zdjęcia lub informacji w internecie może mieć długotrwałe konsekwencje. Kształtowanie odpowiedzialnego podejścia do własnego wizerunku i wizerunku innych osób. Wizerunek jest daną osobową podlegającą ochronie prawnej.

Zadania dla drużyny i mentora – opiekuna stacji

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Podsumowanie i wnioski – ważna zasada

Zanim opublikujesz zdjęcie pomyśl, czy za rok nadal byś chciał, aby ta informacja lub zdjęcie było dostępne. Ważna jest ochrona wizerunku i poszanowanie wizerunku innych osób.

ZŁOTA ZASADA STACJI 5

SUPERMOC DETEKTYWA PRYWATNOŚCI

Pamiętaj, że „Internet nie zapomina”. Zanim udostępnisz czyjeś zdjęcie, zawsze zapytaj o zgodę. Udostępnianie zdjęcia w internecie jest jak wypuszczenie balonu z dłoni – od razu tracisz nad nim kontrolę, a z sieci niezwykle trudno cokolwiek usunąć. Przemyśl dwa razy, zanim klikniesz „Wyślij” i udostępnisz swoje dane osobowe.

STACJA 6: Zatruty haczyk - phishing

Rozwijanie umiejętności rozpoznawania prób wyłudzenia danych i innych form manipulacji w komunikacji cyfrowej.

Opiekun stacji przekazuje „Pigułkę wiedzy” drużynie. Uczniowie mają 1 min., aby zapoznać się z materiałem. Następnie przekazuje drużynie kartę pracy i uczniowie rozwiązują przygotowane zadania. Mentor nie podaje odpowiedzi. Zadaje pytania pomocnicze i odnosi przykłady do codziennych sytuacji uczniów.

Nie klikaj automatycznie w podejrzone linki.

ZŁOTA ZASADA STACJI 6
SUPERMOC DETEKTYWA PRYWATNOŚCI
Nie klikaj w “zatrute haczyki”! Jeśli otrzymasz niepokojącą wiadomość z żądaniem podania hasła lub kliknięcia w link – natychmiast zamknij okno wiadomości i powiadom dorosłego, aby zgłosić phishing.

Nie klikaj w “zatrute haczyki”! Jeśli otrzymasz niepokojącą wiadomość z żądaniem podania hasła lub kliknięcia w link – natychmiast zamknij okno wiadomości i powiadom dorosłego, aby zgłosić phishing.

Gdy wszystkie grupy wrócą z wykonanymi zadaniami, przejdźcie do najważniejszej części – podsumowania i budowania sprawczości. Technologia przecież nie jest zła sama w sobie, zagrożeniem jest nieodpowiedzialne działanie. Dlatego ważna jest wiedza na temat praw jakie



posiadamy, ale także stosowanie zasad, aby lepiej dbać o swoje bezpieczeństwo i ochronę prywatności w internecie.

1. Odczytanie Listu Prezesa UODO

2. Analiza „Portfeli prywatności” z żetonami decyzji

Prowadzący analizuje, ile żetonów zachowały poszczególne grupy. Dyskusja o zasadach ochrony prywatności i o tym, jak łatwo w pośpiechu oddać swoją prywatność, tak jak żetony w grze. Podkreśla, że brak dbania o prywatność naraża każdego człowieka na ryzyka, które stanowią realne krzywdy dla drugiego człowieka. Z kolei przedłużanie czasu przed ekranem odbiera nam, czas na sen, sport, zabawę i budowanie relacji.

3. Przygotowanie klasowego Kodeksu Ochrony Prywatności i akceptacja jego zasad przez wszystkich uczestników gry.

Po ukończeniu rozgrywki, odczytaniu Listu Prezesa UODO oraz analizy „Portfeli prywatności”, uczniowie układają „Kod Odporności Cyfrowej”. Nauczyciel zadaje uczniom pytania dotyczące tego czego dowiedzieli się podczas gry i jakie zasady warto stosować w celu ochrony swojej prywatności w Internecie. Każda drużyna zapisuje zasady na osobnych karteczkach, a następnie uczniowie grupują w podobne tematycznie obszary. Jeśli dzieci pominęły ważny obszar uwzględniony niżej, nauczyciel zadaje pytania pomocnicze, aby naprowadzić je na uzupełnienie punktu.

W kolejnym kroku uczniowie przygotowują wspólny plakat zawierający zasady klasowego Kodeksu Ochrony Prywatności. Na dole plakatu dzieci umieszczają Kod Odporności Cyfrowej „Twoje dane – Twoja sprawa. Zatrzymuję się. Myślę. Decyduję świadomie”. Na zakończenie wszyscy uczniowie zatwierdzają Kodeks. Plakat zostaje powieszony w sali lekcyjnej jako oficjalny wkład w obchody Dnia Ochrony Danych Osobowych.

Warto wiedzieć że 28 stycznia obchodzony jest Dzień Ochrony Danych Osobowych.

Tego dnia w 1981 roku w Strasburgu podpisano Konwencję 108 jeden z najstarszych międzynarodowych dokumentów dotyczący ochrony danych osobowych. Dzień ten świętujemy, aby przypomnieć wszystkim mieszkańcom Europy, że ich prywatność, dane osobowe, są cenne i wymagają ochrony. Polska obchodzi ten dzień od 2007 roku. Stworzony Kodeks Ochrony Prywatności jest Waszym wkładem w obchody Dnia Ochrony Danych



Osobowych – 28 stycznia. Dzień ten akcentuje historyczny i międzynarodowy aspekt danych osobowych podkreślając, że nie jest to tylko szkolna lekcja, ale ogólrnoeuropejska tradycja.

Uwaga

Dodatkowo do przygotowania zasad klasowego Kodeksu można wykorzystać „**Test 3 pytań**” jako testu przed każdym kliknięciem. Zanim coś udostępnisz lub klikniesz „Zgadzam się”, zadaj sobie 3 pytania:

- Czy ja tego chcę, czy gra/aplikacja wymusza to na mnie np. pod presją czasu?
- Po co udostępniam? Kto to zobaczy i co się z tymi danymi stanie za 1 rok czy 5 lat?
- Czy chciałbym/chciałabym, żeby to co udostępniłem/łam zobaczył mój nauczyciel, rodzic lub przyszły szef?

Zapiszcie na plakacie kluczowe filtry, które uczniowie muszą nałożyć przed każdym kliknięciem i udostępnianiem swoich danych w internecie. Kodeks jest podpisywany przez klasę.

4. Podsumowanie i wnioski

Nauczyciel zadaje najważniejsze pytanie podsumowujące „**Co po dzisiejszej grze zrobisz inaczej następnym razem w Internecie?**”. Na koniec nauczyciel podsumowuje grę stwierdzeniem: „Macie prawo do edukacji, do zabawy w grach i korzystania z AI. Ale macie też podstawowe prawo do prywatności. Od Waszego zdrowego rozsądku i tego, czy potraficie powiedzieć „nie” lub „stop”, zależy, czy będziecie bezpieczni. Waszą największą supermocą jest umiejętność powiedzenia „Zatrzymuję się. Myślę. Decyduję świadomie”. Powinniście też wiedzieć, że kiedy aplikacja lub gra żąda za dużo informacji, możecie po prostu odmówić.

Uwaga

Warto podkreślić, że wycofanie zgody lub powiedzenie „NIE ZGADZAM SIĘ”, to nie brak współpracy, czy spełnienia koniecznych wymagań, lecz przejaw dojrzałości i dbania o swoje granice. Prawdziwa siła nie polega na tym, co świat i technologia mogą zrobić z Waszymi danymi. Prawdziwa siła polega na tym, co Wy zdecydujecie się z nimi zrobić.

5. Gratulacje i wręczenie dyplomów dla drużyn

6. Wysłanie ankiety ewaluacyjnej w formie elektronicznej za pośrednictwem strony UODO

7. Potwierdzenie realizacji gry dla nauczycieli.



LISTA MATERIAŁÓW POTRZEBNYCH DO REALIZACJI GRY

Lista umożliwia sprawne przygotowanie wszystkich materiałów przed przeprowadzeniem gry. Wszystkie elementy zostały podzielone na pakiety według przeznaczenia (dla prowadzącego, drużyn, opiekunów stacji oraz na podsumowanie).

1. Pakiet dla nauczyciela

- ☐ **Scenariusz i przebieg gry terenowej:** 1 egz. – opis celów, zasad i przebiegu oraz metryczka metodyczna potwierdzająca zgodność z podstawą programową.
- ☐ **List Prezesa UODO:** 1 egz. do odczytania uczniom przed przystąpieniem do tworzenia Kodeksu
- ☐ **[Mapa stacji:** Liczba egzemplarzy powinna być równa z liczbą drużyn. Każda drużyna powinna rozpoczynać od innej stacji.
- ☐ **Wzór klasowego Kodeksu Ochrony Prywatności:** 1 egz. jako materiał pomocniczy do przygotowania Kodeksu przez uczniów w formie plakatu.
- ☐ **[Dyplomy dla drużyn i potwierdzenie dla nauczyciela (po wypełnieniu ankiety ewaluacyjnej)]**

2. Pakiety dla drużyn

- ☐ **Pisak:** długopis lub ołówek
- ☐ **Koperty drużynowe** – 1 koperta na fragmenty Kodu Odporności Cyfrowej dla każdej drużyny
- ☐ **Portfel prywatności:** 1 koperta z 12 żetonami decyzji na każdą drużynę (po 2 żetony na stację)
- ☐ **Mapa stacji z wypełnioną tabelą:** 1 egz. na drużynę (każda drużyna rozpoczyna od innej stacji)

3. Materiał dla opiekuna stacji – mentora (po 1 pakiecie na punkt)

- ☐ **Pigułka wiedzy (stacje 1–6):** karta A4 do udostępnienia drużynie na stacji
- ☐ **Karty pracy dla drużyny (stacje 1–6):** 1 egz. dla każdej drużyny na stacji
- ☐ **Karta mentora – opiekuna stacji (stacje 1–6):** 1 egz. z pytaniami i instrukcją

- 
- ☐ **Klucz odpowiedzi dla mentora – opiekuna stacji(stacje 1–6):** 1 egz. z kluczem odpowiedzi
 - ☐ **Paski z określonym fragmentem Kodu Odporności Cyfrowej:** 1 fragment Kodu na stację dla każdej drużyny.

4. Materiały na podsumowanie

- ☐ **Arkusze papieru i przybory papiernicze** do przygotowania plakatu klasowego **Kodeksu Ochrony Prywatności.**
- ☐ **Dyplomy dla drużyn**



**LIST PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH
DO UCZESTNIKÓW GRY EDUKACYJNEJ
„DETEKTYWI PRYWATNOŚCI. MISJA: ODPORNOŚĆ CYFROWA”**



Drodzy Detektywi Prywatności!

Drodzy Uczniowie i Uczennice!

gratuluję Wam ukończenia tej niezwykłej misji! Przechodząc przez kolejne stacje gry terenowej, udowodniliście, że potraficie myśleć samodzielnie, rozbrajać cyfrowe pułapki i odróżniać fakty od iluzji i dezinformacji w sieci.

Żyjemy w świecie, w którym komputery, smartfony, gry, aplikacje i sztuczna inteligencja towarzyszą nam na każdym kroku. To wspaniałe narzędzia, które dają ogromne możliwości. Pamiętajcie jednak, że w świecie cyfrowym Wasze dane osobowe – Wasze imię, numer telefonu, lokalizacja, a także Wasz wizerunek i głos – mają ogromną wartość. Są częścią Waszej godności i historii, której nikt nie powinien Wam odbierać.

Często słyszy się, że w sieci trzeba uważać i odpowiedzialnie korzystać z nowych technologii. I to jest prawda. Chcę, abyście pamiętali, że w cyfrowym świecie to Wy jesteście gospodarzami. Waszą największą supermocą, nie są szybkie kciuki na ekranie smartfona, ale umiejętność zatrzymania się i uważności. Zapamiętajcie złotą zasadę cyfrowego detektywa: „Zatrzymuję się. Myślę. Decyduję świadomie!”. Pamiętajcie również, że macie pełne prawo chronić swoją prywatność. Kiedy jakaś aplikacja, gra lub nieznajoma osoba w sieci żąda od Was zbyt wiele np. podania haseł, prywatnych informacji czy przesłania zdjęcia – macie prawo odmówić. To nie jest oznaka słabości, ale dowód prawdziwej cyfrowej dojrzałości i siły.

Dbajcie o swoich kolegów i koleżanki. Zanim wrzucicie czyjeś zdjęcie do Internetu, czy na forum grupowe, zawsze zapytajcie o zgodę. Pamiętajcie, że prawdziwy detektyw prywatności chroni nie tylko siebie, ale stoi też na straży bezpieczeństwa innych.

Teraz przed Wami ostatnie, najważniejsze zadanie. Połączcie swoje siły i na podstawie tego, co przeżyliście dzisiaj w grze, stwórzcie Wasz klasowy Kodeks Ochrony Prywatności. Niech te zasady, będą Waszą codzienną tarczą ochronną, a Kodeks stanie się Waszym oficjalnym wkładem w obchody Dnia Ochrony Danych Osobowych, który świętujemy 28 stycznia. W tym szczególnym Dniu organizowanych jest wiele wydarzeń edukacyjnych, aby przypomnieć wszystkim mieszkańcom Europy, że ich prywatność i dane osobowe są cenne i wymagają ochrony, szczególnie w szybko zmieniającym się świecie nowych technologii. Mam nadzieję, że przygotowany Kodeks będzie stanowił cenny element obchodów Dnia Ochrony Danych Osobowych w Waszej szkole.

Jestem z Was bardzo dumny i oficjalnie witam Was w gronie ekspertów ds. prywatności i ochrony danych osobowych.

Łączę serdeczne pozdrowienia,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych



KLASOWY KODEKS OCHRONY PRYWATNOŚCI

Materiał pomocniczy dla nauczyciela na podstawie wniosków z gry. Wzór Kodeksu stanowi listę kontrolną dla nauczyciela. Pozwala na sprawne uporządkowanie wniosków dzieci i upewnienie się, że klasa uwzględniła kluczowe zasady wypracowane na 6 stacjach wyzwań. W Kodeksie mogą być uwzględnione zasady ochrony prywatności ważne dla klasy nawet jak nie są zawarte w zaproponowanym materiale.

1. Moje dane osobowe mają wartość i podlegają ochronie

Imię, nazwisko, PESEL, adres, numer telefonu, wizerunek i głos to moje cenne dane osobowe. Mam prawo chronić swoją prywatność i powiedzieć „**NIE ZGADZAM SIĘ**”, gdy aplikacja lub gra żąda ich za dużo.

2. Mam supermoc zmiany zdania (wycofanie zgody)

Zgodę wyrażoną na przetwarzanie moich danych osobowych przykład w aplikacji, na portalu czy w grze mogę w każdej chwili wycofać. Zrezygnowanie z usługi jest moim prawem i musi być tak samo proste, jak jej wyrażenie na początku.

3. Hasła to klucze do mojego cyfrowego domu

Tworzę silne, trudne do odgadnięcia hasła na przykład do gier, poczty. Nigdy nie zdradzam ich nikomu, nawet najlepszemu przyjacielowi.

4. Wiem, że nic w sieci nie jest za darmo

Rozumiem, że za „darmowe” aplikacje i gry płacę swoimi danymi osobowymi, uwagą i czasem. Nie daję się manipulować cyfrowym pułapką, presji czasu, ukrytym przyciskiem umożliwiającym odmowę udostępniania danych osobowych (*dark patterns*) i stosuję z rodzicami limity czasu przed ekranem.

5. Asystent AI to program, a nie pamiętnik

Nie wpisuję do chatbotów sztucznej inteligencji (AI) moich haseł, sekretów, adresów ani problemów osobistych. Zawsze weryfikuję odpowiedzi AI w potwierdzonych źródłach (podręcznikach, u ekspertów, czy z nauczycielem, rodzicem), ponieważ narzędzia sztucznej inteligencji potrafią zmyślać (tzw. halucynować).

6. Szanuję wizerunek i pamiętam o „metaforze wypuszczonego balonika”

Wizerunek to dane osobowe. Zanim opublikuję zdjęcie lub film na przykład z kolegą lub koleżanką, zawsze pytam o jego zgodę oraz jego rodziców. Pamiętam, że raz



wrzucone zdjęcie, może być przez kogoś wykorzystane i przekazane dalej, dlatego dane osobowe wymykają się nam spod kontroli jak balonik.

7. Dezinformacja i fałszywe nagrania lub obrazy

Wiem, że obraz, film i głos można sfałszować za pomocą sztucznej inteligencji (AI).

Nie podaję dalej wiadomości, informacji bez sprawdzenia źródła i nigdy nie używam cyfrowych narzędzi do krzywdzenia innych osób.

8. Mamy z rodziną „hasło rodzinne”

Ustalam z rodziną tajne hasło rodzinne, aby natychmiast potwierdzić, czy dzwoni osoba bliska, która zna hasło rodzinne, na przykład w razie podejrzanego telefonu dotyczącego przekazania pieniędzy lub danych osobowych.

9. Nie klikam w zatrute haczyki (phishing)

Nie otwieram podejrzanych linków z SMS-ów czy wiadomości. Każdy podejrzany SMS przesyłam bezpłatnie na **numer 8080 (CERT Polska)**, a o zdarzeniu powiadamiam osobę dorosłą.

10. Stosuję złotą zasadę cyfrowego detektywa

Przed każdym kliknięciem, udostępnieniem zdjęcia, czy wysłaniem wiadomości zadaję sobie **test 3 pytań**:

- Czy ja tego chcę, czy gra/aplikacja wymusza to na mnie np. pod presją czasu?
- Po co udostępniam? Kto to zobaczy i co się z tymi danymi stanie za 1 rok czy 5 lat?
- Czy chciałbym/chciałabym, żeby to co udostępniłem/łam zobaczył mój nauczyciel, rodzic lub przyszły szef?

ŚWIADOMA AKCEPTACJA ZAPISÓW KODEKSU

Ustalone zasady akceptują wszyscy uczniowie.s



„Twoje dane – Twoja sprawa”

ogólnopolski program edukacyjny Prezesa UODO,
który pomaga uczniom i nauczycielom zrozumieć zasady ochrony prywatności
w cyfrowym świecie.

PATRONI HONOROWI



Minister
Edukacji



Rzecznik
Praw Dziecka



Urząd Ochrony Danych Osobowych
Departament Inicjatyw Edukacyjnych

ul. Stanisława Moniuszki 1a, 00-014 Warszawa

e-mail: tdts@uodo.gov.pl

www.uodo.gov.pl