Program nauczania

dot. ochrony danych

Uniwersytet Pedagogiczny we Fryburgu

Fryburg 2024

Co-funded by
the European Union

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Spis treści

Wstęp

W czasach, w których technologie cyfrowe przenikają każdy aspekt naszego życia, ochrona danych osobowych staje się kluczową kwestią. DataPro, pionierska inicjatywa edukacyjna w ramach programu Unii Europejskiej Erasmus Plus, uznaje za niezbędne edukowanie młodego pokolenia w celu szerokiego pojmowania ochrony danych jako podstawowego prawa człowieka. Niniejszy program nauczania został zaprojektowany z myślą o skomplikowanych realiach wykorzystywania i ochrony danych, mając na celu wyposażenie uczniów w wiedzę i narzędzia niezbędne do poruszania się po tym złożonym obszarze.

Nasze społeczeństwo w coraz większym stopniu opiera się na danych, a ogromne ilości informacji są przetwarzane każdego dnia, wpływając na prywatność jednostek i zbiorowe bezpieczeństwo. W tym kontekście projekt DataPro oferuje kompleksowe narzędzia edukacyjne, aby oświecić młode umysły na temat znaczenia prywatności danych i związanych z nią kwestii etycznych. Poprzez edukowanie uczniów na temat wieloaspektowego charakteru wykorzystania danych i kluczowego znaczenia ochrony danych osobowych, DataPro dąży do kultywowania obywatelskiej świadomości, przygotowując społeczeństwo do obrony swoich praw dotyczących danych.

Program nauczania określa szereg celów i konkretnych zadań mających pogłębić zrozumienie przez uczniów złożoności ochrony danych i uznania jej za istotną część praw człowieka. Poprzez ustrukturyzowane podejście obejmujące gromadzenie, adaptację i rozwój innowacyjnych narzędzi edukacyjnych, DataPro chce łączyć wiedzę teoretyczną z praktycznym zrozumieniem. Inicjatywa ta nie tylko koncentruje się na rozpowszechnianiu tych zasobów wśród szkół i interesariuszy edukacyjnych, ale także kładzie nacisk na aktywne zaangażowanie uczniów i nauczycieli w dynamiczny proces uczenia się.

Przewiduje się, że wpływ DataPro będzie znaczący. Poprzez integrację tego programu nauczania w środowiskach edukacyjnych, przewidujemy wychowanie pokolenia, które będzie nie tylko świadome znaczenia ochrony danych, ale także będzie posiadać

umiejętności w zakresie wdrażania najlepszych praktyk. Oczekuje się, że ta podstawowa wiedza będzie sprzyjać ulepszonym środkom ochrony prywatności i wpłynie na szersze postawy społeczne wobec ochrony danych i praw do prywatności w naszym coraz bardziej cyfrowym świecie.

Poprzez ustrukturyzowaną metodologię i wspólne wysiłki pod patronatem programu Erasmus Plus, DataPro dąży do realizacji tych założeń, znacząco przyczyniając się w ten sposób do rozwoju cyfrowej świadomości i odpowiedzialności wśród obywateli. Ten program nauczania służy jako latarnia morska dla innowacji edukacyjnych, prowadząc młode osoby w kierunku przyszłości, w której będą w stanie pewnie chronić swoje dane w zdigitalizowanym świecie.

1. Wprowadzenie

Program nauczania dotyczący ochrony danych, będący częścią projektu DataPro w ramach programu Unii Europejskiej Erasmus Plus, ma na celu wyposażenie młodych ludzi w niezbędną wiedzę i umiejętności, aby zrozumieli i poruszali się w zawiłościach ochrony danych. Program nauczania opiera się na kompleksowej strukturze kompetencji, podzielonej na odpowiednie obszary edukacyjne. Poniższe sekcje zawierają szczegółowy przegląd struktury programu nauczania.

W dzisiejszym cyfrowym świecie ochrona danych osobowych ma ogromne znaczenie. Młodzi ludzie dorastają w środowisku, w którym dane odgrywają kluczową rolę, czy to poprzez media społecznościowe, naukę online, czy komunikację cyfrową. Jednak wielu z nich brakuje świadomości zagrożeń i praw związanych z korzystaniem z technologii cyfrowych. Projekt DataPro ma na celu opracowanie kompleksowego rozwiązania edukacyjnego, które umożliwi uczniom kompetentne i bezpieczne zarządzanie swoimi danymi.

Program nauczania odzwierciedla obszary tematyczne, z których każdy obejmuje określone kompetencje i uwzględnia wcześniej zbadane przeszkody w nauce. W oparciu o ten program, programy nauczania dla poszczególnych krajów zostaną

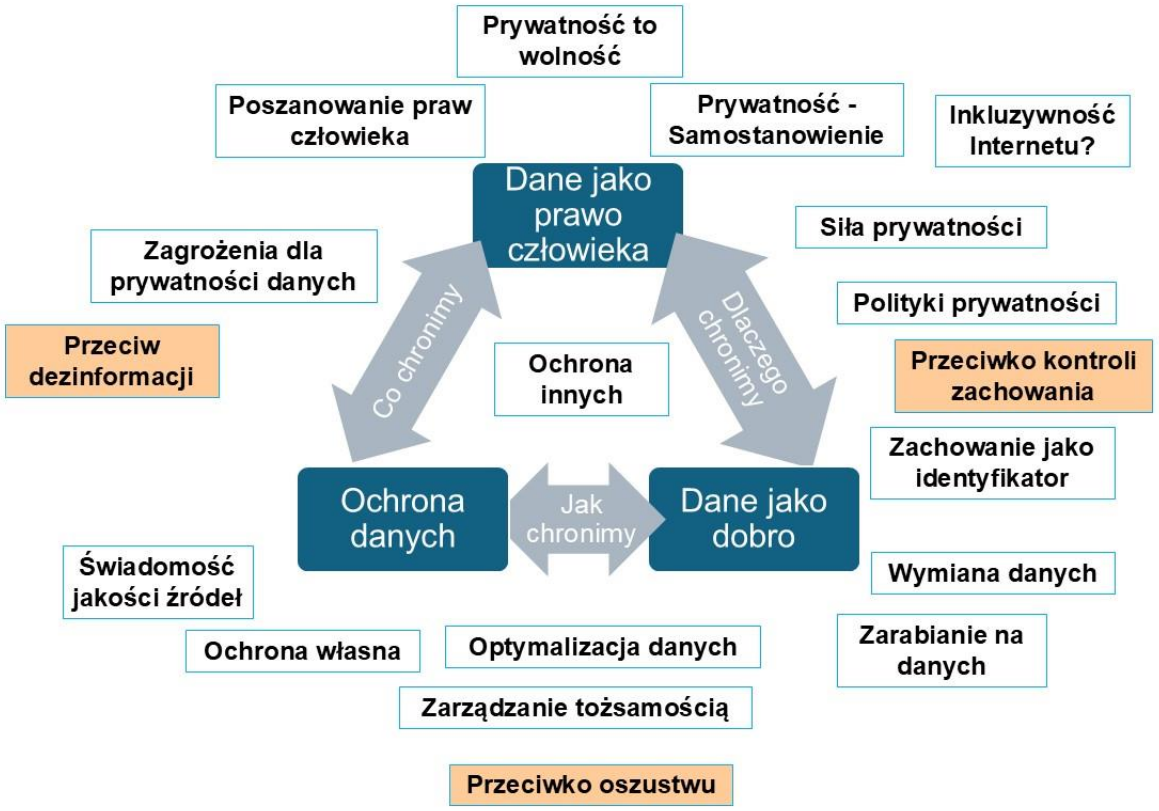
dostosowane do każdej grupy docelowej. Prototypy szkoleniowe w WP3 będą opierać się na teoretycznych podstawach rezultatów WP2.

Chociaż program nauczania w dużej mierze opiera się na DigComp Framework[1], jego ukierunkowany rozwój obejmował kilka etapów uzyskiwania informacji zwrotnych od członków konsorcjum i ekspertów w dziedzinie ochrony danych, w celu upewnienia się, że jest on kompleksowy i praktyczny. Z jednej strony pokazuje on, że ochrona danych jest zarówno indywidualnym prawem, jak i praktyką uwzględniającą ryzyko dla innych, a z drugiej strony, że dane mają często ukrytą wartość ekonomiczną. Program nauczania DataPro integruje te aspekty, aby wyposażyć uczniów w umiejętności ochrony swojej prywatności i odpowiedzialnego działania w przestrzeni cyfrowej.

2. Opis kompetencji

W tej sekcji program nauczania został opisany za pomocą dołączonej grafiki, która służy jako wizualna reprezentacja struktury kompetencji. Program nauczania DataPro składa się z trzech nakładających się na siebie obszarów: Ochrona danych, Prywatność jako prawo i Dane jako dobro. Odzwierciedla on wymagania aktywnego, autonomicznego i odpowiedzialnego członka demokratycznego, opartego na danych/informacjach społeczeństwa rynkowego.

[1] https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en



Program nauczania koncentruje się na trzech powiązanych ze sobą tematach:

- „Ochrona danych” jest najbardziej oczywistą częścią, ponieważ odnosi się do praktycznych aspektów ochrony danych i cyberbezpieczeństwa w rozumieniu wielu wytycznych.
- „Dane jako prawo człowieka” – z perspektywy edukacji ogólnej – odnosi się do znaczenia samostanowienia informacyjnego jako prawa człowieka.
- „Dane jako dobro” przyjmuje pespektywę ekonomiczną, z jednej strony, aby wyjaśnić, jak działa branża danych, a z drugiej strony, w jaki sposób osoby fizyczne mogą czerpać korzyści z wartości swoich danych.

Tak więc ogólnie kompetencje można wyjaśnić, odpowiadając na następujące trzy pytania: A. Jak mogę chronić moje prywatne dane (i moje zaufanie do informacji)? B.

Co sprawia, że ochrona danych jest prawem człowieka? C. Co sprawia, że dane są wartościowe (ekonomicznie)?

Te trzy obszary nie są odrębnymi wymiarami – w znacznym stopniu się pokrywają. Ochrona danych i prywatność jako prawo pokrywają się w zakresie tego, co i jak chronić oraz jak uwzględniać prawa prywatności innych osób. Oznacza to, że program nauczania nie tylko uczy, jak chronić własne dane, ale także wpaja szacunek do prywatności danych innych osób.

Prywatność jako prawo i Dane jako dobro nakładają się na siebie, ważąc (uzasadniony) interes firm opartych na danych w stosunku do prywatności. Program nauczania dotyczy równowagi między interesami korporacyjnymi w zakresie wykorzystania danych a indywidualnymi prawami prywatności, pomagając uczniom zrozumieć szersze implikacje ekonomii danych.

Ochrona danych i Dane jako dobro pokrywają się w zakresie wykorzystania danych. Dziedzina ta koncentruje się na praktycznych umiejętnościach potrzebnych do odpowiedzialnego i skutecznego zarządzania danymi osobowymi i ich wykorzystywania w różnych kontekstach.

Program nauczania DataPro nie zawiera poziomów kompetencji, ponieważ lista dostarczonych kompetencji jest uważana za fundamentalną dla społeczeństwa informacyjnego. Te podstawowe umiejętności i pojęcia są uważane za niezbędne, aby skutecznie i odpowiedzialnie funkcjonować w cyfrowo zintegrowanym świecie.

Kompetencje w zakresie rozpoznawania i radzenia sobie ze złośliwymi zachowaniami w Internecie są szczególnie podkreślane.

A. Jak chronić swoje dane (i zaufanie do informacji)?

Aby chronić swoje prywatne dane i utrzymać zaufanie do informacji, należy rozważyć następujące cele edukacyjne, które koncentrują się na umożliwieniu uczniom bezpieczniejszego i bardziej odpowiedzialnego poruszania się po cyfrowym świecie.

A.1 Zarządzanie tożsamością:

- *Bezpieczna identyfikacja*: Naucz się zabezpieczać swoją identyfikację elektroniczną za pomocą metod takich jak silne, unikatowe hasła i uwierzytelnianie dwuskładnikowe.
- *Świadomość użytkowania*: Regularnie zastanawiaj się, jak i gdzie można bezpiecznie wykorzystywać i udostępniać dane osobowe. Zrozum ryzyko związane z udostępnianiem danych osobowych.
- *Środki anonimowości*: Używaj środków do ukrywania tożsamości online: VPN, szyfrowane narzędzia komunikacji i przeglądarki nastawione na prywatność.

A.2 Ochrona własna:

- *Ustawienia komunikacji*: Stosuj środki zapobiegania otrzymywaniu niechcianych wiadomości lub e-maili, takich jak filtry antyspamowe i ustawienia poczty e-mail.
- *Zarządzanie śledzeniem*: Wdrażaj środki mające na celu ograniczenie i zarządzanie śledzeniem działań użytkownika w Internecie, w tym korzystanie z rozszerzeń przeglądarki blokujących moduły śledzące i pliki cookie.
- *Środki bezpieczeństwa*: Stosuj się do standardowych zasad bezpieczeństwa, takich jak używanie różnych, silnych haseł do różnych usług online, włączanie uwierzytelniania wieloskładnikowego, korzystanie z blokad biometrycznych, regularne aktualizowanie i instalowanie oprogramowania ochronnego.

A.3 Przeciwko dezinformacji:

- *Krytyczna ocena*: Regularnie pytaj, kto stoi za informacjami znalezionymi w Internecie, zwłaszcza w mediach społecznościowych. Ustal, kto może mieć interes w rozpowszechnianiu fałszywych wiadomości, jak np. boty, propagatorzy mowy nienawiści lub osoby tworzące komory pogłosowe (bańki).
- *Świadomość jakości źródeł:* Wiedz, że dezinformacja może być bardzo przekonująca, zwłaszcza przy użyciu zaawansowanych technologii, takich jak sztuczna inteligencja, które mogą tworzyć dopracowane wizualizacje. Zawsze kwestionuj jakość i źródło informacji.

A.4 Sprawdzanie informacji:

- *Sprawdzanie źródła*: Bądź przygotowany/a do korzystania z wielu źródeł w celu weryfikacji informacji. Pomaga to w rozpoznaniu i zrozumieniu różnych punktów widzenia lub uprzedzeń stojących za poszczególnymi informacjami i źródłami danych.
- *Rozpoznawanie uprzedzeń*: Naucz się identyfikować potencjalne uprzedzenia w informacjach, biorąc pod uwagę, że każde źródło danych może mieć nieodłączne uprzedzenia wynikające z jego pochodzenia lub celu.

A.5 Ochrona innych:

- *Rozważania dotyczące udostępniania danych*: Regularnie sprawdzaj, czy dane osobowe innych osób są udostępniane i czy mogą zostać niewłaściwie wykorzystane.
- *Świadomość prawna*: Miej świadomość, że udostępnianie informacji o innych może mieć poważne konsekwencje prawne. Przed udostępnieniem danych osobowych innych osób należy zawsze uzyskać ich zgodę.

A.6 Minimalizacja danych:

- *Kwestionowanie potrzeb*: Regularnie kwestionuj konieczność przechowywania i udostępniania danych osobowych. Stosuj praktyki, takie jak podawanie tylko niezbędnych informacji i używanie jednorazowych adresów e-mail lub numerów telefonów w stosownych przypadkach.

A.7 Przeciwko oszustwu:

- *Środki bezpieczeństwa*: Bądź świadomy/a powszechności ataków opartych na inżynierii społecznej (phishing) w różnych kanałach komunikacji, aby zapobiec nieuczciwemu pozyskiwaniu (cyfrowych) zasobów.

B. Co sprawia, że ochrona danych jest prawem człowieka?

W odniesieniu do ochrony danych jako prawa człowieka należy rozważyć następujące cele nauczania, które koncentrują się na zrozumieniu przez uczniów ochrony danych i jej implikacji:

B.1 Prywatność to wolność:

- *Fundamentalna wolność*: Prywatność jest niezbędna dla wolności, ponieważ pozwala jednostkom swobodnie wyrażać swoje opinie i żyć bez nadmiernej ingerencji. Jeśli inni mogą obserwować lub kontrolować zachowanie, wolność osobista jest zagrożona.

B.2 Prywatność - Samostanowienie:

- *Zarządzanie danymi*: Każdy ma prawo decydować o tym, jakie dane na jego temat są gromadzone, przetwarzane i wykorzystywane. To prawo do samostanowienia ma kluczowe znaczenie dla zachowania osobistej autonomii.
- *Ochrona przed automatyzacją*: Pamiętaj, że ochrona danych obejmuje prawo do niepodlegania w pełni zautomatyzowanym procesom decyzyjnym, które mogą mieć znaczący wpływ na osoby fizyczne.
- *Zapobieganie nadużyciom*: Ochrona danych osobowych pomaga chronić przed niechcianym monitoringiem, kradzieżą tożsamości, dyskryminacją i innymi formami niewłaściwego wykorzystania danych osobowych.

B.3 Siła prywatności:

- *Prawa dotyczące danych*: Znaj swoje prawa wobec firm wykorzystujących twoje dane, w tym prawo dostępu do przechowywanych danych, poprawiania nieścisłości, usuwania danych (Prawo do bycia zapomnianym) i składania skarg do władz.
- *Konieczność wyrażenia zgody*: Pamiętaj, że firmy zazwyczaj muszą uzyskać zgodę użytkownika na przetwarzanie jego danych osobowych. Regularnie sprawdzaj, czy wyrażenie takiej zgody jest konieczne.

- *Sprawdzanie konieczności zgody*: Często sprawdzaj konieczność wyrażenia zgody na wykorzystanie danych, aby upewnić się, że dane osobowe nie są bezpodstawnie wykorzystywane.

B.4 Poszanowanie praw człowieka:

- *Cyfrowa odpowiedzialność*: Bądź świadomy/a swojej odpowiedzialności za ochronę godności ludzkiej, wolności, demokracji i równości podczas działania w Internecie. Obejmuje to poszanowanie prywatności i praw dotyczących danych innych osób oraz opowiadanie się za odpowiedzialnymi praktykami w zakresie danych.

B.5 Zagrożenia dla prywatności danych:

- *Poziomy ryzyka*: Wiedz, że istnieją różne poziomy ryzyka dla prywatności związane z różnymi praktykami dotyczącymi danych. Niektóre procesy dotyczące danych, w szczególności te związane ze sztuczną inteligencją, wiążą się z wyższym ryzykiem
- *Zagrożenia związane ze sztuczną inteligencją*: Pamiętaj, że procesy i usługi oparte na sztucznej inteligencji mogą stwarzać ryzyko dla prywatności, często ze względu na zdolność AI do przetwarzania dużych ilości danych i wnioskowania o wrażliwych informacjach.

B.6 Inkluzywność Internetu:

- *Kwestionowanie źródeł informacji:* Ważne jest, aby regularnie sprawdzać, kto stoi za informacjami znalezionymi w Internecie, zwłaszcza w mediach społecznościowych. Należy wiedzieć, kto może czerpać korzyści z rozpowszechniania fałszywych informacji, zatrudniania botów, promowania mowy nienawiści i tworzenia baniek filtrujących.
- *Świadomość o podwójnej naturze Internetu:* Należy mieć świadomość, że Internet stwarza nowe możliwości uczestnictwa w życiu społecznym dla grup znajdujących się w trudnej sytuacji, ale może również przyczynić się do izolacji tych, którzy z niego nie korzystają.

B.7 Polityka prywatności:

- *Ocena polityki prywatności*: Rozwijaj umiejętność krytycznego analizowania i oceniania polityk prywatności aplikacji i usług. Obejmuje to zrozumienie, jakie dane są gromadzone, w jaki sposób są wykorzystywane oraz jakie prawa przysługują użytkownikowi w odniesieniu do jego danych.

C. Co sprawia, że dane są wartościowe (ekonomicznie)?

Ponieważ dane mają znaczną wartość ekonomiczną wpływającą również na uczniów, należy rozważyć następujące cele nauczania, które koncentrują się na prostych pojęciach ekonomicznych:

Zarabianie na danych:

- *Modele dochodowe*: Dowiedz się o głównych sposobach zarabiania pieniędzy przez firmy na danych osobowych i zagregowanych, np. jak poprzez platformy reklamowe i ulepszanie ukierunkowanych reklam (w tym reklam politycznych).
- *Ekonomia usług*: Pamiętaj, że większość bezpłatnych usług internetowych jest świadczona przez firmy nastawione na zysk, które często generują przychody dzięki danym użytkowników.

Zachowanie jako identyfikator:

- *Użycie danych*: Zauważ, że wzorce użytkowania i podłączone urządzenia mogą być wykorzystywane do optymalizacji usług online i ukierunkowanych reklam. Obejmuje to śledzenie zachowań użytkowników w celu dostarczania spersonalizowanych treści.
- *Strategie kontroli*: Poznaj strategie kontrolowania i ograniczania zakresu śledzenia zachowań, takie jak dostosowywanie ustawień prywatności i korzystanie z technologii zwiększających prywatność.

Przeciwko kontrolowaniu zachowań:

- *Świadomość mechanizmów*: Pamiętaj, że wiele platform cyfrowych wykorzystuje taktyki psychologiczne, takie jak nudging, grywalizacja i manipulacja, aby wpływać na zachowanie użytkowników. Rozpoznawaj te taktyki, aby platformy nie miały na ciebie nadmiernego wpływu.
- *Środki zapobiegawcze*: Stosuj strategie mające na celu zmniejszenie tych wpływów, takie jak ustalanie osobistych limitów użytkowania i krytyczna ocena konsumowanych treści.

Sprzedaż danych:

- *Świadomość o monetyzacji*: Pamiętaj, że wiele bezpłatnych usług komunikacyjnych (takich jak media społecznościowe) i treści online jest opłacanych z reklam lub sprzedaży danych użytkowników. Ten model ekonomiczny opiera się na monetyzacji danych osobowych.
- *Publiczne udostępnianie*: Wiedz, że wszystko co jest udostępniane publicznie w Internecie (np. obrazy, filmy, dźwięki) może być wykorzystywane do szkolenia systemów sztucznej inteligencji, które mogą mieć niepożądane funkcje śledzenia. Zachowaj ostrożność co do zakresu publicznego udostępniania danych.

3. Wnioski dla nauczycieli i ich kompetencje

Aby przekazać uczniom niezbędną wiedzę o technologiach cyfrowych, zachęcając do ich korzystnego i efektywnego wykorzystania, kluczowe są następujące kompetencje oparte na DigCompEdu Framework[2]:

Ochrona urządzeń i treści cyfrowych:

- Przekazuj wiedzę o ochronie urządzeń cyfrowych przed zagrożeniami (złośliwe oprogramowanie i uszkodzenia fizyczne), przy użyciu oprogramowania antywirusowego, regularnych aktualizacji i bezpiecznych haseł.

- Nauczaj uczestników identyfikowania i reagowania na zagrożenia, takie jak phishing, ransomware, kradzież tożsamości i cyberprzemoc.

Znajomość środków bezpieczeństwa i ochrony:

- Nauczaj o bezpiecznych nawykach przeglądania, uwierzytelniania dwuskładnikowego i korzystania z bezpiecznych sieci, takich jak VPN.
- Podkreślaj znaczenie ochrony danych osobowych, zrozumienia, co należy udostępniać online i zarządzania silnymi, unikatowymi hasłami.

Ochrona danych osobowych i prywatności:

- Powtarzaj, aby nie udostępniać poufnych informacji na niezabezpieczonych stronach internetowych i czytać politykę prywatności usług cyfrowych.
- Nauczaj, jak skonfigurować ustawienia prywatności w mediach społecznościowych i na innych platformach.

Bezpieczne korzystanie i udostępnianie danych osobowych:

- Edukuj w zakresie bezpiecznego udostępniania danych osobowych, szyfrowania danych wrażliwych i dostrzegania potencjalnych szkód wynikających z niewłaściwego wykorzystania danych.

Zrozumienie polityk prywatności:

- Wyjaśniaj znaczenie polityk prywatności w usługach cyfrowych i nauczaj uczniów ich czytania i rozumienia w celu podejmowania świadomych decyzji.

Unikanie zagrożeń zdrowotnych:

- Przedstawiaj sposoby zapobiegania konsekwencjom dla zdrowia wynikającym z długotrwałego korzystania z urządzeń cyfrowych, takim jak zmęczenie oczu, zła postawa i wpływ na zdrowie psychiczne.

Ochrona przed zagrożeniami cyfrowymi:

- Edukuj w zakresie identyfikowania, unikania i zgłaszania cyberprzemocy, internetowych przestępców i innych szkodliwych zachowań.

Promowanie dobrostanu i integracji społecznej:

- Podkreślaj pozytywne aspekty technologii cyfrowych we wspieraniu więzi społecznych i praktyk sprzyjających integracji społecznej.

Świadomość oddziaływania na środowisko:

- Nauczaj o wpływie technologii cyfrowych na środowisko, w tym o odpadach elektronicznych i zużyciu energii.

Monitorowanie i ochrona dobrostanu:

- Aktywnie monitoruj aktywności online w celu zapewnienia dobrostanu i interweniuj w razie potrzeby, aby zapobiec szkodliwym zachowaniom.
- Bądź przygotowany/a do podjęcia natychmiastowych działań przeciwko zagrożeniom dla dobrostanu uczniów, takim jak cyberprzemoc.

Zachęcanie uczniów do traktowania swoich danych jak pieniędzy

Ważnym aspektem, który nie został uwzględniony w ramach DigCompEdu, a mianowicie w bieżących działaniach, jest wartość danych jako dobra. Dlatego chcielibyśmy dodać: **Docenianie danych jako dobra.**

Uczniowie powinni nauczyć się rozumieć wartość swoich danych osobowych, podobnie jak cenią pieniądze. Obejmuje to dostrzeżenie znaczenia ochrony ich danych, rozumienie, w jaki sposób można je spieniężyć lub wykorzystać, oraz podejmowanie świadomych decyzji dotyczących ich udostępniania.