Ochrona danych studentów w przypadku korzystania ze sztucznej inteligencji w szkolnictwie wyższym

Ochrona danych osobowych i bezpieczeństwo studentów w edukacji wspomaganej sztuczną inteligencją

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

CC BY NC ND

Cele nauczania

W skrócie

Celem niniejszego tematu jest ułatwienie wykładowcom zrozumienia najważniejszych zasad ochrony danych oraz stosowania najlepszych praktyk w celu ochrony danych studentów podczas korzystania z narzędzi AI w edukacji.

- Zrozumienie podstawowych zasad ochrony danych podczas wykorzystywania sztucznej inteligencji w szkolnictwie wyższym.
- Identyfikacja potencjalnych zagrożeń związanych z gromadzeniem, przetwarzaniem i przechowywaniem danych studentów.
- Zrozumienie znaczenia najważniejszych przepisów dotyczących ochrony danych oraz ich wpływu na praktykę dydaktyczną.
- Stosowanie praktycznych strategii mających na celu ochronę prywatności studentów i przestrzegania ich praw w środowiskach edukacyjnych wykorzystujących AI.
- Krytyczna refleksja nad rodzajami danych studentów, które mogą być wykorzystywane w sposób etyczny i zgodny z prawem w systemach edukacyjnych opartych na sztucznej inteligencji.

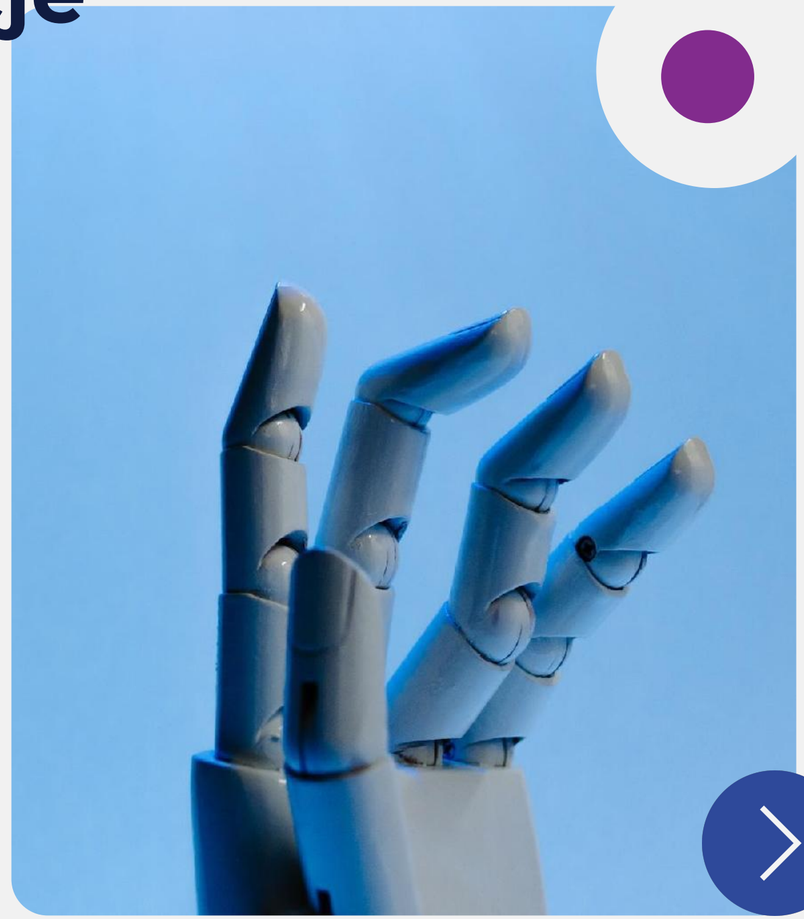
Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Najważniejsze koncepcje i definicje

PODSTAWOWE ZASADY OCHRONY DANYCH STUDENTÓW W EDUKACJI WSPIERANEJ PRZEZ SZTUCZNĄ INTELIGENCJĘ

Zrozumienie tych podstawowych zasad ma zasadnicze znaczenie dla wykorzystywania danych studentów w edukacji wspieranej przez sztuczną inteligencję w sposób zgodny z prawem, etyczny i przejrzysty.



Ochrona danych

Ochrona danych odnosi się do zasad i przepisów regulujących sposób gromadzenia, przetwarzania, przechowywania i udostępniania danych osobowych.

Minimalizacja danych

Minimalizacja danych oznacza, że należy gromadzić wyłącznie te dane, które są absolutnie niezbędne do realizacji uzasadnionych celów edukacyjnych.

Świadoma zgoda

Świadoma zgoda oznacza, że osoby fizyczne rozumieją, jakie dane są gromadzone i w jakim celu, oraz w razie potrzeby dobrowolnie udzielają wyraźnej zgody.

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Ochrona danych osobowych w szkolnictwie wyższym

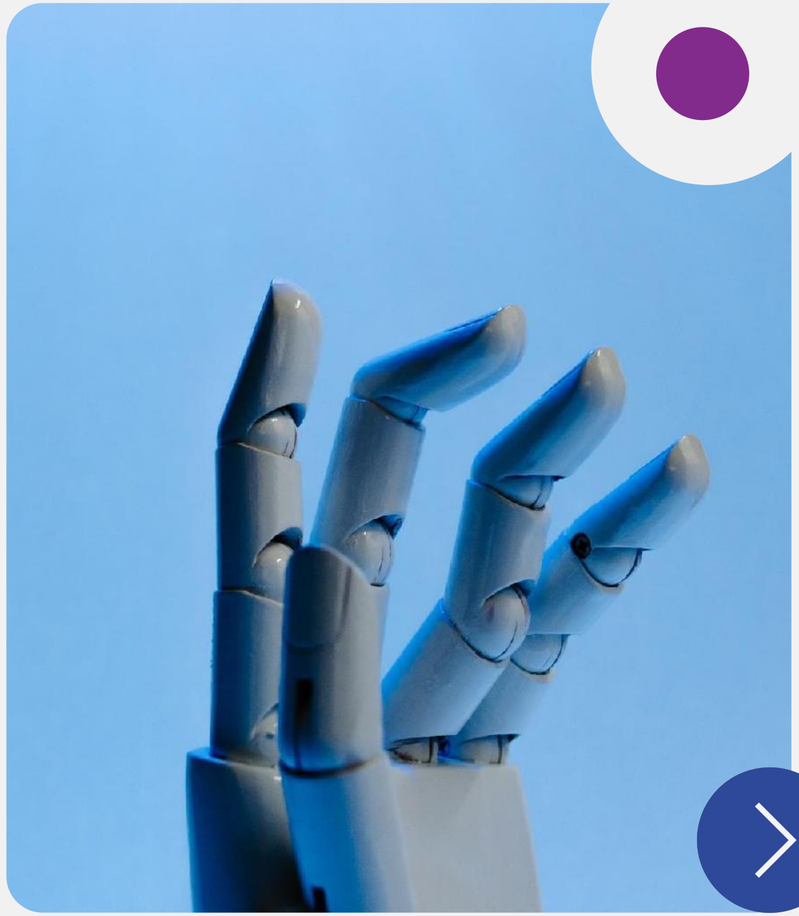
Zrozumienie, na czym polega ochrona danych osobowych w środowiskach edukacyjnych wykorzystujących sztuczną inteligencję.

Wykorzystanie narzędzi cyfrowych i systemów sztucznej inteligencji w szkolnictwie wyższym wiąże się z gromadzeniem, przetwarzaniem i przechowywaniem danych osobowych. Mogą one obejmować dane akademickie, identyfikatory cyfrowe, wzorce uczenia się, a w niektórych przypadkach również informacje wrażliwe.

Ochrona danych nie ogranicza się do zapewniania zgodności z prawem; stanowi ona część etycznej odpowiedzialności wykładowców i instytucji. Zapewnienie prywatności oznacza, że dane są wykorzystywane w sposób zgodny z prawem, proporcjonalny i przejrzysty.

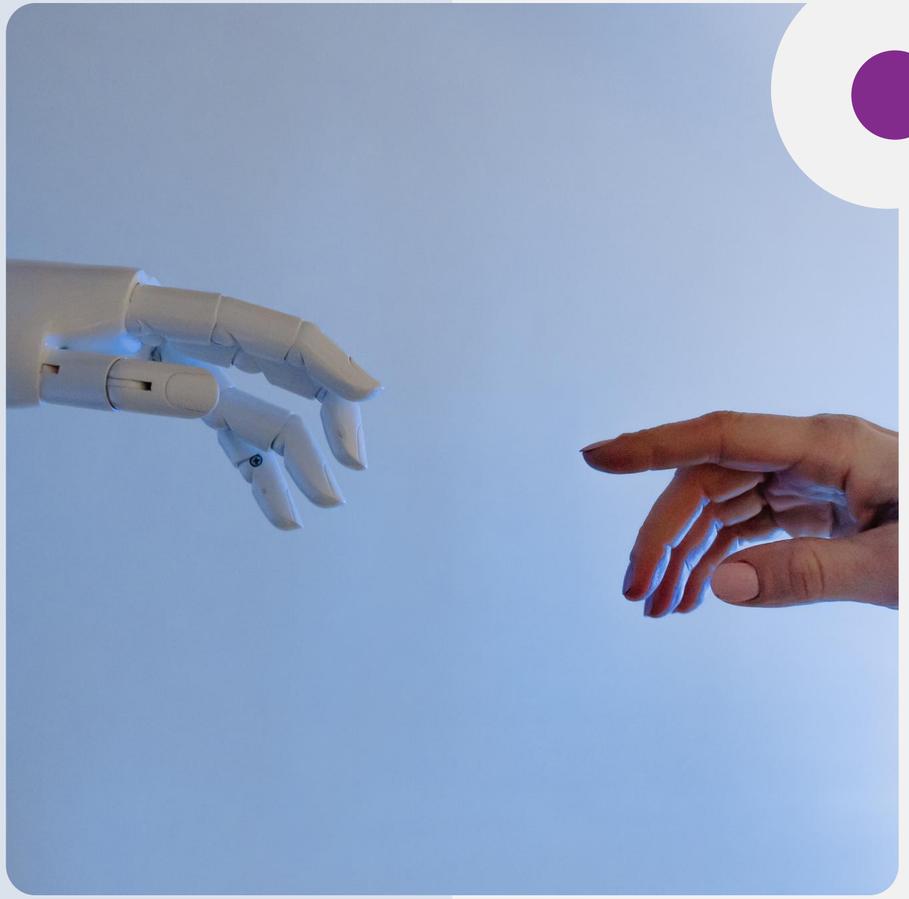
W praktyce dydaktycznej ochrona danych obejmuje:

- świadomość tego, jakie dane są gromadzone i w jakim celu,
- ograniczanie dostępu do danych osobowych,
- unikanie nieproporcjonalnego lub niewłaściwego wykorzystywania danych w procesach edukacyjnych wspieranych przez sztuczną inteligencję.



Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union



Ramy ochrony danych w szkolnictwie wyższym

Najważniejsze przepisy

Zrozumienie roli RODO w wykorzystywaniu danych osobowych w europejskim kontekście edukacyjnym

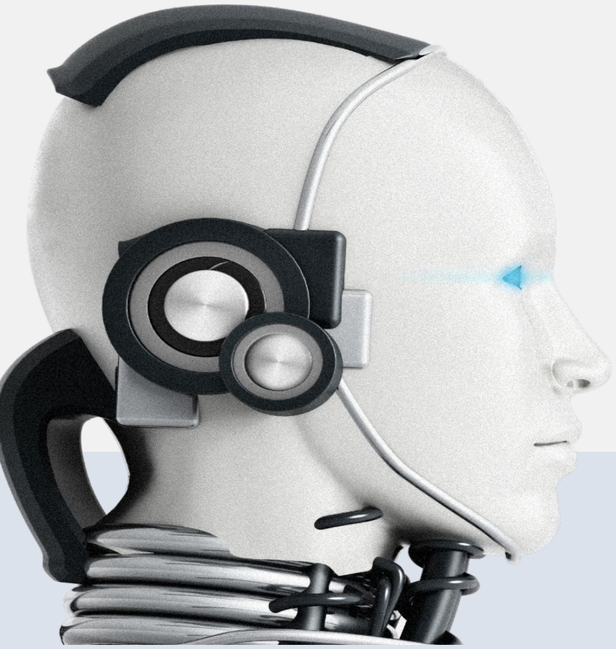
Ogólne rozporządzenie o ochronie danych (RODO – UE)

RODO stanowi podstawowe ramy prawne regulujące przetwarzanie danych osobowych w Unii Europejskiej. Ma zastosowanie do wszystkich uczelni wyższych, które gromadzą, przechowują lub przetwarzają dane osobowe dotyczące studentów, wykładowców lub pracowników administracyjnych.

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Najważniejsze zasady RODO mające znaczenie dla praktyki dydaktycznej:



- **Zgodność z prawem**, rzetelność i przejrzystość: dane muszą być przetwarzane w oparciu o ważną podstawę prawną oraz w przejrzysty sposób.
- **Ograniczenie celu**: dane mogą być wykorzystywane wyłącznie do określonych i uzasadnionych celów.
- **Minimalizacja danych**: należy gromadzić wyłącznie dane, które są absolutnie niezbędne.
- **Prawidłowość**: dane osobowe muszą być prawidłowe i aktualne.
- **Integralność i poufność**: należy zapewnić odpowiednie zabezpieczenia.
- **Odpowiedzialność**: instytucje muszą być w stanie wykazać zgodność z przepisami.

Kluczowe przesłanie.

W kontekście europejskim RODO stanowi nie tylko obowiązek prawny, ale także ramy regulujące odpowiedzialne i etyczne wykorzystanie narzędzi cyfrowych oraz sztucznej inteligencji w szkolnictwie wyższym.

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Ryzyko związane z danymi

Ryzyko związane z wykorzystywaniem danych w środowiskach edukacyjnych opartych na sztucznej inteligencji.

Wykorzystywanie narzędzi cyfrowych i systemów sztucznej inteligencji w szkolnictwie wyższym może wiązać się z ryzykiem, jeśli dane osobowe nie są odpowiednio zarządzane. Ryzyko to może mieć konsekwencje akademickie, prawne i etyczne dla studentów, wykładowców i instytucji.

Główne zagrożenia i ich potencjalne konsekwencje:

- **Naruszenia bezpieczeństwa danych na platformach edukacyjnych** → ujawnianie danych studentów i odpowiedzialność instytucji.
- **Gromadzenie większej ilości danych niż to konieczne** → naruszenie zasad RODO i spadek zaufania studentów.
- **Ocena oparta na sztucznej inteligencji bez weryfikacji przez człowieka** → niesprawiedliwe oceny lub decyzje akademickie.
- **Niejasne praktyki dotyczące danych** → studenci nie są świadomi tego, w jaki sposób wykorzystywane są ich dane.
- **Korzystanie z narzędzi zewnętrznych bez zabezpieczeń** → ryzykowne transfery danych poza kontrolą instytucji.

Przesyłanie prac studentów umożliwiających identyfikację na zewnętrzne platformy AI bez zgody instytucji może stanowić niezgodny z prawem transfer danych w świetle RODO i narażać instytucję na ryzyko prawne oraz utratę reputacji.

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Najlepsze praktyki w zakresie ochrony prywatności

Praktyczne strategie odpowiedzialnego wykorzystywania danych w środowiskach edukacyjnych opartych na sztucznej inteligencji.

Wdrożenie rygorystycznych praktyk w zakresie ochrony danych nie tylko ogranicza ryzyko prawne, ale także wzmacnia zaufanie i integralność akademicką podczas korzystania z narzędzi cyfrowych i opartych na sztucznej inteligencji.

Kluczowe zalecenia dla wykładowców

- **Oceniaj konieczność wykorzystania danych**: przed wdrożeniem narzędzia zastanów się, czy przetwarzanie danych osobowych jest rzeczywiście konieczne.
- **Przekazuj studentom jasne informacje**: wyjaśniaj, jakie dane są gromadzone, w jakim celu i jak długo będą przechowywane.
- **Stawiaj na narzędzia instytucjonalne lub zgodne z przepisami:** korzystaj z platform, które spełniają europejskie standardy ochrony danych.
- **Zapewniaj nadzór ludzki**: unikaj polegania wyłącznie na zautomatyzowanych systemach przy podejmowaniu istotnych decyzji akademickich.
- **Regularnie sprawdzaj ustawienia prywatności**: dostosowuj konfigurację zabezpieczeń i ograniczaj dostęp do danych osobowych.

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Należy zbierać tylko te dane, które są niezbędne do realizacji uzasadnionych celów edukacyjnych

Minimalizacja danych

Zasada minimalizacji danych jest jedną z podstawowych zasad RODO. Wymaga ona, by dane osobowe były adekwatne, istotne i ograniczone do tego, co jest absolutnie niezbędne do osiągnięcia określonego celu edukacyjnego.

W kontekście nauczania i wykorzystania sztucznej inteligencji oznacza to, że:

- Należy unikać gromadzenia dodatkowych informacji, które nie są niezbędne do realizacji działań edukacyjnych.
- Nie należy ponownie wykorzystywać danych do celów innych niż pierwotnie określone bez odpowiedniej podstawy prawnej.
- Należy ograniczać niepotrzebne przechowywanie danych historycznych lub wrażliwych.
- Należy rozważyć, czy zamiast danych osobowych umożliwiających identyfikację można wykorzystać dane zanonimizowane lub zagregowane.

Przykład praktyczny

**Jeżeli narzędzie AI wymaga danych osobowych do generowania analiz wyników, wykładowcy powinni zadać sobie pytanie:
Czy informacje umożliwiające identyfikację są rzeczywiście niezbędne, czy ten sam cel można osiągnąć przy użyciu danych zanonimizowanych?**

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Zanim zaczniesz korzystać z narzędzia AI w ramach swoich zajęć, zastanów się:

- Jakie dane osobowe udostępniam?
- Czy dane te są naprawdę niezbędne do osiągnięcia celu edukacyjnego?
- Czy ten sam efekt można osiągnąć, korzystając z mniejszej ilości informacji lub danych zanonimizowanych?
- Czy zapewniam przejrzystość i nadzór ze strony człowieka?

Rozpocznij ćwiczenie

Odpowiedzialne wprowadzanie innowacji wymaga świadomych i przemyślanych decyzji dotyczących wykorzystania danych studentów

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Źródła

- Parlament Europejski i Rada Unii Europejskiej. (2016). Rozporządzenie (UE) 2016/679 (ogólne rozporządzenie o ochronie danych). https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Europejska Rada Ochrony Danych (EDPB). (2020). Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych https://edpb.europa.eu
- Komisja Europejska. (2022). *Ethical guidelines on the use of artificial intelligence and data in teaching and learning for educators* (Wytyczne etyczne dotyczące wykorzystania sztucznej inteligencji i danych w nauczaniu i uczeniu się, przeznaczone dla nauczycieli). https://education.ec.europa.eu/news/ethical-guidelines-on-the-use-of-artificial-intelligence-and-data-in-teaching-and-learning-for-educators
- OECD. (2021). *OECD Digital Education Outlook 2021: Pushing the Frontiers with AI, Blockchain and Robots*. https://doi.org/10.1787/589b283f-en

Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

Im mniej danych osobowych jest wykorzystywanych, tym mniejsze ryzyko naruszenia prywatności i tym silniejsza ochrona prawna i etyczna.

Konsorcjum:

БИТ

ahe Akademia Humanistyczno Ekonomiczna w Łodzi

mecb Driving Excellence & Innovation

UNIVERSITÀ DI TORINO

canarias excelencia tecnológica

ACTA FOUNDATION

https://trustai.unibit.bg/

Projekt Trust AI

Wyłączenie odpowiedzialności: Finansowane przez Unię Europejską. Wyrażone poglądy i opinie stanowią wyłącznie poglądy autora (autorów) i niekoniecznie odzwierciedlają poglądy Unii Europejskiej lub Narodowej Agencji (NA). Ani Unia Europejska, ani NA nie ponoszą za nie odpowiedzialności.
Nr projektu: 2024-1-BG01-KA220-HED-000249185

Co-funded by the European Union

CC BY NC ND