Warto wiedzieć…

AI w placówkach oświatowych a dane osobowe

Jak chronić dane osobowe w edukacji w dobie rozwoju sztucznej inteligencji?

Sztuczna inteligencja (ang. Artificial Intelligence, AI) coraz częściej wspiera nauczycieli i uczniów np. w nauczaniu zdalnym, analizie wyników czy personalizacji procesu nauki. Jednak korzystanie z AI może wiązać się z przetwarzaniem danych osobowych, co niesie potencjalne zagrożenia dla prywatności. Dlatego ważne jest świadome i odpowiedzialne korzystanie z tej technologii.

Zanim skorzystasz z AI w edukacji, sprawdź:

- ✓ Czy dany system AI jest zgodny z zasadami ochrony danych osobowych (RODO)?
- ✓ Czy masz zgodę na przetwarzanie danych uczniów?
- ✓ Kto ma dostęp do przetwarzanych informacji i czy są one odpowiednio zabezpieczone?
- ✓ Czy dane uczniów są wykorzystywane wyłącznie w celu edukacyjnym?

Podstawowe zasady ochrony danych w placówkach oświatowych:

1. Zachowaj bezpieczeństwo danych. Instytucje edukacyjne powinny wdrażać polityki ochrony danych i regularnie sprawdzać używane narzędzia cyfrowe pod kątem zgodności z przepisami o ochronie danych. Szczególną uwagę należy zwrócić na bezpieczeństwo danych przetwarzanych przez systemy AI, które mogą automatycznie gromadzić, analizować i udostępniać informacje.

2. Uzyskuj zgodę na przetwarzanie danych. Opiekunowie i uczniowie powinni wiedzieć, jakie dane są zbierane, w jakim celu i kto ma do nich dostęp. Zgoda na ich przetwarzanie musi być świadoma i dobrowolna.

3. Minimalizuj ilość zbieranych danych. W przypadku korzystania z systemów AI, upewnij się, że przetwarzane są wyłącznie dane niezbędne do działania algorytmów. Ogranicza to ryzyko naruszenia prywatności.

4. Zadbaj o edukację cyfrową. Warto być świadomym zasad bezpiecznego korzystania z AI oraz potencjalnych zagrożeń, tj. uprzedzenia algorytmiczne i decyzje podejmowane przez AI bez ludzkiego nadzoru.

5. Unikaj niekorzystnych aspektów profilowania. Podczas analizowania przez systemy AI postępów ucznia, zadbaj o to, by nie prowadziło to do uprzedzeń lub nieuczciwej oceny jego możliwości.

PAMIĘTAJ!

Dane osobowe przetwarzane w placówkach oświatowych mogą stanowić wrażliwe informacje, które wymagają szczególnej ochrony. Nieodpowiednie wykorzystanie z systemów AI może prowadzić do naruszeń prywatności, dyskryminacji czy nieautoryzowanego przetwarzania danych. Bez promowania i wdrażania wyżej wymienionych praktyk i wiedzy o ochronie danych sektor edukacyjny nie będzie mógł skutecznie wykorzystać potencjału nowych technologii!

URZĄD OCHRONY DANYCH OSOBOWYCH

Ważne terminy i pojęcia

Sztuczna inteligencja (AI)
to dziedzina informatyki zajmująca się tworzeniem systemów zdolnych do wykonywania zadań wymagających inteligencji ludzkiej. System AI na potrzeby wyraźnych lub dorozumianych celów wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne.

Dane osobowe
oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (art. 4 pkt 1 RODO).

Profilowanie
na podstawie RODO można określić jako zautomatyzowane przetwarzanie danych osobowych w celu oceny aspektów osobistych, w szczególności w celu tworzenia analiz lub prognoz odnośnie konkretnych osób. Użycie słowa „ocena" sugeruje, że profilowanie obejmuje pewien rodzaj oceniania lub ewaluacji osoby (np. ocena zdolności ucznia na podstawie jego wyników w nauce).

Cyberbezpieczeństwo
jest to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Prościej mówiąc, cyberbezpieczeństwo obejmuje działania podejmowane w celu ochrony systemów informatycznych i danych przed nieautoryzowanym dostępem, atakami i naruszeniami.

Cyfrowy ślad
to informacje tworzone podczas korzystania z Internetu, które mogą być później powiązane z użytkownikiem i analizowane przez AI i inne technologie.