

1.6 Przepisy prawne

Najważniejsze przesłanki

- **Unijny AI Act to podstawa prawna.** Unijny zbiór przepisów dotyczących SI obowiązuje od sierpnia 2024 r. i jest wdrażany stopniowo do 2027 r. Dotyczy nie tylko firm technologicznych, ale też szkół.
- **Kompetencje w zakresie SI to obowiązek, a nie kurs do odhaczenia.** Szkoły muszą wspierać personel w budowaniu kompetencji w zakresie SI.
- **Kilka zastosowań SI jest wprost zakazanych.** Wśród nich: wnioskowanie o emocjach uczniów na podstawie danych z twarzy lub głosu, SI wykorzystująca podatność dzieci w celu zniekształcenia ich zachowania oraz budowanie baz danych rozpoznawania twarzy czy wnioskowanie o cechach takich jak rasa czy religia na podstawie danych biometrycznych.
- **Ryzyko zależy od decyzji, nie od produktu.** Zwykłe narzędzia do pisania, wyszukiwania, tłumaczenia czy planowania lekcji nie są wysokiego ryzyka tylko dlatego, że są używane w szkole. Stają się wysokiego ryzyka, gdy wpływają na przyjęcie, ścieżkę kształcenia, wynik egzaminu lub decyzje zatrudnieniowe.
- **Nie wszystko, co wygenerowane przez SI, wymaga oznaczenia.** Obowiązek ujawnienia spoczywa głównie na dostawcy; materiał zweryfikowany redakcyjnie przez nauczyciela jest z niego zwolniony.
- **SI wysokiego ryzyka wymaga człowieka, który może ją unieważnić.** Wynik działania SI nigdy nie jest decyzją ostateczną. Musisz rozumieć jej ograniczenia i być w stanie ją zignorować lub uchylić.
- **AI Act nakłada się na inne prawo, nie zastępuje go.** Krajowe prawo ochrony danych, oświatowe, pracy, ochrony dzieci i autorskie nadal obowiązują równolegle.
- **RODO reguluje dane, nie tylko narzędzie.** Nawet system SI zgodny z AI Act może być niedozwolony, jeśli przetwarza dane osobowe uczniów lub personelu bez ważnej podstawy prawnej.

„Jeśli zapamiętasz z tej strony tylko jedno zdanie: Używaj SI, by wspierać swój profesjonalny osąd, a nie go zastępować – surowsze zasady obowiązują, gdy tylko SI zaczyna pomagać w podejmowaniu decyzji o ocenach, ścieżkach edukacyjnych lub ludziach.

Unijny AI Act

Unijny AI Act (Rozporządzenie (UE) 2024/1689) to jednolity, oparty na ryzyku zbiór przepisów UE dotyczących sztucznej inteligencji. Zamiast regulować konkretne produkty, klasyfikuje systemy SI według ryzyka, jakie stwarzają, i nakłada odpowiednie obowiązki – od całkowitego zakazu dla niewielkiej grupy praktyk, przez dodatkowe obowiązki dla zastosowań „wysokiego ryzyka”, aż po brak szczególnych zasad dla narzędzi codziennego użytku. Obowiązuje bezpośrednio w każdym państwie członkowskim, zarówno w organizacjach publicznych, jak i prywatnych.

Rozporządzenie wchodzi w życie etapami. Obowiązuje od 1 sierpnia 2024 r.; od 2 lutego 2025 r. wiążące są już zakazane praktyki opisane niżej oraz obowiązek budowania kompetencji w zakresie SI ([Art. 4](#)); od 2 sierpnia 2026 r. zastosowanie znajdzie większość pozostałych przepisów.

Kto odpowiada za wykorzystanie SI?

Jeśli szkoła wprowadza i kontroluje system SI, to zazwyczaj to szkoła lub organ prowadzący szkołę jest „podmiotem stosującym” ([Art. 3\(4\)](#)). Nauczyciel zwykle nie jest odrębnym podmiotem stosującym, gdy korzysta z narzędzia zgodnie z instrukcjami szkoły, ale nadal musi przestrzegać tych instrukcji oraz wszystkich odnośnych zasad szkolnych i dotyczących ochrony danych.

Nauczyciele muszą? wiedzieć?, z czego korzystają?

Szkoły i organy prowadzące muszą podjąć odpowiednie działania, by wspierać rozwój kompetencji w zakresie SI wśród osób korzystających w ich imieniu z systemów SI ([Art. 4](#)). AI Act nie określa konkretnego poziomu kompetencji, certyfikatu ani formy szkolenia. Zależą one raczej od konkretnego systemu SI, sposobu jego użycia i tego, kto może zostać nim dotknięty.

Praktyki SI całkowicie zakazane w szkołach

AI Act całkowicie zakazuje ośmiu praktyk związanych z SI ([Art. 5](#)); cztery z nich bezpośrednio dotyczą szkół:

- Wykorzystywanie systemów SI w placówkach edukacyjnych do wnioskowania o emocjach lub intencjach na podstawie danych biometrycznych (takich jak cechy twarzy lub głosu ucznia) jest co do zasady zakazane. Istnieją wąskie wyjątki dla celów medycznych lub bezpieczeństwa ([Art. 3\(39\)](#); [Art. 5\(1\)\(f\)](#)).
- Systemy SI wykorzystujące czyjaś podatność wynikającą z wieku (jak w przypadku dzieci), niepełnosprawności lub sytuacji społecznej czy ekonomicznej, w sposób zniekształcający zachowanie tej osoby i wyrządzający jej szkodę, są zakazane niezależnie od intencji ([Art. 5\(1\)\(b\)](#)).

- Budowanie lub rozszerzanie bazy danych rozpoznawania twarzy poprzez nieukierunkowane pozyskiwanie obrazów z internetu lub z nagrań monitoringu jest zakazane. Ma to znaczenie, jeśli szkoła rozważa narzędzie rozpoznawania twarzy do sprawdzania obecności lub nadzoru egzaminów ([Art. 5\(1\)\(e\)](#)).
- Wykorzystywanie danych biometrycznych do kategoryzowania osób w celu wnioskowania o chronionych cechach, takich jak rasa, poglądy polityczne, religia czy orientacja seksualna, jest zakazane. Ma to znaczenie dla każdego narzędzia opartego na biometrii, takiego jak oprogramowanie do nadzoru egzaminów, które wykracza poza swój deklarowany cel ([Art. 5\(1\)\(g\)](#)).

Czy tre?? wygenerowana przez SI zawsze wymaga oznaczenia?

Jeśli uczniowie wchodzi w bezpośrednią interakcję z systemem SI, takim jak chatbot, muszą zostać poinformowani, że wchodzi w interakcję z SI. Zwykle odpowiedzialność za jasne poinformowanie o tym spoczywa na dostawcy systemu ([Art. 50\(1\)](#)).

Szkoły i nauczyciele muszą ujawniać deepfake'i lub tekst wygenerowany przez SI publikowany w sprawach interesu publicznego, gdy są one wykorzystywane na lekcji ([Art. 50\(4\)](#)). Ten wymóg nie ma zastosowania, gdy treść wygenerowana przez SI przeszła efektywną weryfikację i kontrolę redakcyjną człowieka, a dana osoba lub instytucja przyjmuje odpowiedzialność redakcyjną za jej publikację. Karta pracy wspomagana SI, zweryfikowana przez nauczyciela, nie wymaga więc automatycznie oznaczenia.

Kiedy SI w edukacji staje si? wysokiego ryzyka

Zwykle narzędzia do pisania, tłumaczenia, wyszukiwania i planowania lekcji nie są wysokiego ryzyka tylko dlatego, że są wykorzystywane w pracy. Klasyfikacja zależy od zamierzonego celu systemu, a nie po prostu od tego, jaki produkt jest używany ([Art. 6](#) · [Annex III](#)).

Systemy SI mogą zostać zaklasyfikowane jako wysokiego ryzyka, gdy są przeznaczone do:

Dla nauczycieli	Dla szkół
-----------------	-----------

• decydowania o dostępie, przyjęciu lub przydziale uczniów do placówek i programów edukacyjnych lub zawodowych; • oceniania wyników nauczania uczniów lub sterowania ich procesami uczenia się; • oceniania odpowiedniego poziomu kształcenia, jaki uczeń otrzyma lub do jakiego może uzyskać dostęp; lub • wykrywania zakazanych zachowań uczniów podczas egzaminów. (Annex III, pkt 3)	• rekrutacji lub selekcji nauczycieli, w tym przeglądania zgłoszeń; • decydowania o warunkach umowy, awansie lub rozwiązaniu stosunku pracy nauczyciela; • przydzielania zadań na podstawie zachowania lub cech osobistych nauczyciela; lub • oceniania wyników pracy nauczycieli. (Annex III, pkt 4)
--	---

Ograniczone narzędzie sprawdzające lub przygotowawcze może również nie zostać zaklasyfikowane jako wysokiego ryzyka, jeśli nie wpływa istotnie na decyzję. Jednak system edukacyjny profilujący osoby zawsze jest uznawany za wysokiego ryzyka.

Co SI wysokiego ryzyka oznacza dla szkół? i nauczycieli

Zaklasyfikowanie systemu SI jako wysokiego ryzyka nie wyklucza automatycznie jego wykorzystania w szkołach. Systemy wysokiego ryzyka wiążą się jednak z obowiązkami ([Art. 26](#)):

Te obowiązki dla SI wysokiego ryzyka w edukacji zaczną obowiązywać od 2 grudnia 2027 r. – natomiast wymienione wyżej zakazy i obowiązki budowania kompetencji w zakresie SI obowiązują już dziś.

Dla nauczycieli	Dla szkół
• korzystać z niego wyłącznie w zatwierdzonym celu i przestrzegać jego instrukcji; • nie traktować jego wyniku jako decyzji ostatecznej; • rozumieć jego główne ograniczenia i prawdopodobne źródła błędów; • uważać na nadmierne poleganie na pozornie przekonujących wynikach; oraz • być przygotowanym, by zignorować lub uchylić jego wynik.	• zapewnić kompetentny i upoważniony nadzór ludzki; • zapewnić, by wszelkie dane wejściowe pod jej kontrolą były trafne i wystarczająco reprezentatywne; • monitorować system i reagować na zagrożenia lub poważne incydenty; • przechowywać automatycznie generowane dzienniki zdarzeń przez co najmniej sześć miesięcy, gdy pozostają pod jej kontrolą; oraz • z wyprzedzeniem informować uczniów, nauczycieli lub osoby dotknięte skutkami, gdy system wspomaga podejmowanie decyzji ich dotyczących.

Podmioty publiczne oraz organizacje prywatne świadczące usługi publiczne mogą być również zobowiązane do przeprowadzenia oceny skutków dla praw podstawowych przed zastosowaniem SI wysokiego ryzyka ([Art. 27](#)). Organy publiczne oraz organizacje działające w ich imieniu mogą

dodatkowo być zobowiązane do zarejestrowania systemu w unijnej bazie danych ([Art. 49](#)). To, czy odpowiada za to szkoła, czy jej organ prowadzący, zależy od krajowego systemu oświaty.

AI Act to nie jedyne prawo, które ma znaczenie

AI Act nie zastępuje europejskich ani krajowych przepisów dotyczących ochrony danych, oświaty, zatrudnienia i partycypacji pracowniczej, ochrony dzieci czy prawa autorskiego ([Art. 2\(7\)](#)). Na przykład fakt, że narzędzie nie jest wysokiego ryzyka, nie oznacza, że wolno przysyłać do niego prace uczniów czy ich dane osobowe.

Narzędzie może być dopuszczalne na gruncie AI Act, a mimo to zakazane przez prawo ochrony danych lub zasady obowiązujące w Twojej szkole.

RODO

RODO (Rozporządzenie (UE) 2016/679) to unijne prawo o ochronie danych osobowych. Pełni rolę uzupełniającą wobec AI Act: podczas gdy AI Act pyta, czy i jak dany system SI wolno w ogóle stosować, RODO pyta, czy te konkretne dane o tej konkretnej osobie wolno przetwarzać w ten konkretny sposób.

- Ma zastosowanie, gdy tylko w grę wchodzi dane osobowe. Imiona i nazwiska, szkolne adresy e-mail, prace uczniów, nagrania głosu, transkrypcje, zdjęcia, oceny, obecność i dane o postępach w nauce – wszystko to liczy się jako dane osobowe ([Art. 4](#)).
- Niektóre dane wymagają dodatkowej ochrony. Informacje o zdrowiu, dane biometryczne oraz dane ujawniające pochodzenie rasowe lub etniczne, religię czy podobne cechy to „szczególne kategorie danych” i co do zasady są niedostępne bez konkretnego wyjątku ([Art. 9](#)) – to jeden z powodów, dla których AI Act osobno zakazuje w szkołach kilku praktyk wnioskowania biometrycznego.
- Wiedz, kto za co odpowiada. Szkoła jest zwykle „administratorem”; dostawca SI przetwarzający dane w imieniu szkoły jest „podmiotem przetwarzającym” i potrzebuje umowy powierzenia przetwarzania danych określającej jego obowiązki ([Art. 28](#)). Sprawdź to, zanim wdrożysz nowe narzędzie w całej szkole.
- Dane opuszczające UE potrzebują zabezpieczenia. Wiele popularnych narzędzi SI jest hostowanych poza UE. Dane osobowe mogą tam trafić tylko wtedy, gdy istnieje decyzja stwierdzająca odpowiedni poziom ochrony lub inne zatwierdzone zabezpieczenie, takie jak standardowe klauzule umowne ([Art. 44](#)).
- Uczniowie i personel zachowują swoje prawa. Mogą zapytać, jakie dane są o nich przechowywane, zażądać ich poprawienia lub usunięcia oraz sprzeciwić się decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, które istotnie ich dotyczą ([Art. 15–Art. 22](#)) – prawo to działa równolegle do wymogu nadzoru ludzkiego nad systemami wysokiego ryzyka z AI Act i je wzmacnia.

Gdzie szuka? pomocy

Egzekwowanie przepisów jest zorganizowane w każdym kraju UE inaczej. Ponieważ odpowiedzialności krajowe mogą się zmieniać, korzystaj z aktualnej [list of national market-surveillance authorities](#) Komisji Europejskiej [lista krajowych organów nadzoru rynku]. Każdy (nauczyciel, uczeń, rodzic) może złożyć skargę do takiego organu, jeśli uzna, że doszło do naruszenia przepisów rozporządzenia ([Art. 85](#)). Gdy system wysokiego ryzyka, taki jak narzędzie do decyzji o przyjęciu lub nadzoru egzaminu, doprowadził do decyzji istotnie wpływającej na ucznia, uczeń (lub jego rodzice) mogą również zażądać wyjaśnienia tej indywidualnej decyzji ([Art. 86](#)).

Zasady krajowe dla Twojego kraju

AI Act obowiązuje w całej UE, ale organy egzekwujące, prawo oświatowe i praktyka ochrony danych różnią się w zależności od kraju. Uwagi dotyczące poszczególnych krajów partnerskich Playbooka zostaną tu dodane:

- Austria
- Czechy
- Niemcy
- Łotwa
- Słowacja
- Słowenia
- Hiszpania

Revision #2

Created 2026-09-01 09:14:31 UTC by Alexander

Updated 2026-09-02 09:54:23 UTC by Alexander