1.6 Legislatíva

> **Upozornenie:** Túto kapitolu sme starostlivo pripravili, no právo v oblasti UI sa rýchlo mení. Pravidlá sa mohli od zverejnenia zmeniť, preto si vždy overte aktuálnu právnu situáciu a v prípade potreby ju prispôsobte vnútroštátnym predpisom. Táto kapitola nepredstavuje právne poradenstvo.

Hlavné posolstvo

- Akt EÚ o UI je právnym základom. Európske pravidlá pre UI platia od augusta 2024 a postupne nadobúdajú účinnosť až do roku 2027. Vzťahujú sa nielen na technologické firmy, ale aj na školy.
- Gramotnosť v oblasti UI je povinnosťou, nie kurzom na odškrtnutie. Školy musia podporovať svojich zamestnancov pri budovaní gramotnosti v oblasti UI.
- Viaceré spôsoby používania UI sú úplne zakázané. Patrí medzi ne: odvodzovanie emócií žiakov z tvárových alebo hlasových údajov, UI, ktorá zneužíva zraniteľnosť detí na skresľovanie ich správania, a budovanie databáz na rozpoznávanie tváre alebo odvodzovanie znakov ako rasa či náboženstvo z biometrických údajov.
- Riziko závisí od rozhodnutia, nie od samotného produktu. Bežné nástroje na písanie, výskum, preklad a plánovanie hodín nie sú vysoko rizikové len preto, že sa používajú v škole. Vysoko rizikovými sa stávajú vo chvíli, keď ovplyvňujú prijímanie, vzdelávaciu dráhu, výsledky skúšok alebo pracovné rozhodnutia.
- Nie všetko, čo vygeneruje UI, potrebuje označenie. Povinnosť zverejnenia leží predovšetkým na poskytovateľovi; materiál skontrolovaný učiteľom s ľudskou redakčnou kontrolou je z tejto povinnosti vyňatý.
- Vysoko riziková UI potrebuje človeka, ktorý ju môže prehlasovať. Výstup UI nikdy nie je konečným rozhodnutím. Musíte poznať jej obmedzenia a byť schopní jej výstup odmietnuť alebo zmeniť.
- Akt o UI dopĺňa ostatné právo, nenahrádza ho. Vnútroštátne právo v oblasti ochrany osobných údajov, školstva, pracovného práva, ochrany detí a autorského práva platí naďalej popri ňom.
- GDPR upravuje údaje, nielen samotný nástroj. Aj systém UI, ktorý je v poriadku podľa Aktu o UI, môže byť naďalej neprípustný, ak spracúva osobné údaje o žiakoch alebo zamestnancoch bez platného právneho základu.

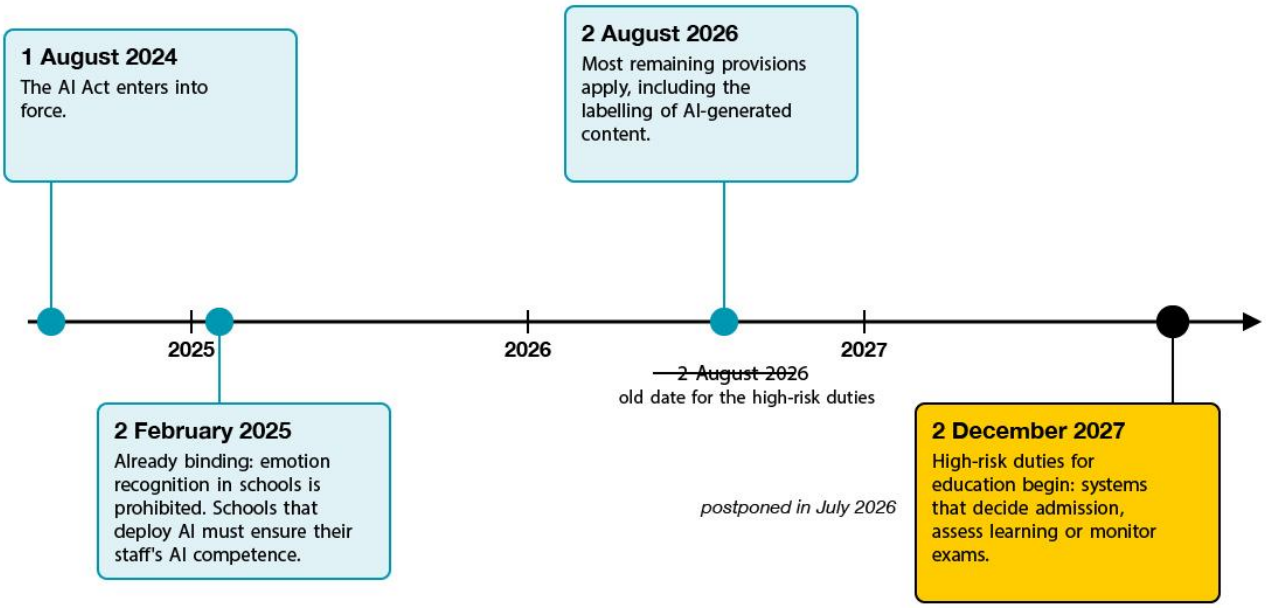
> “ Ak si z tejto stránky zapamätáte len jednu vetu: Používajte UI na podporu svojho profesijného úsudku, nie na jeho nahradenie — prísnejšie pravidlá platia hneď,

> ako UI pomáha rozhodovať o známkach, vzdelávacích dráhach alebo o ľuďoch.

Akt EÚ o umelej inteligencii

Akt EÚ o UI (Nariadenie (EÚ) 2024/1689) je jednotným, na riziku založeným súborom pravidiel EÚ pre umelú inteligenciu. Namiesto regulácie konkrétnych produktov klasifikuje systémy UI podľa rizika, ktoré predstavujú, a s tým spája príslušné povinnosti — od úplného zákazu pre malú skupinu postupov, cez dodatočné povinnosti pre „vysoko rizikové“ použitia, až po žiadne osobitné pravidlá pre bežné nástroje. Priamo sa uplatňuje vo všetkých členských štátoch, na verejné aj súkromné organizácie rovnako.

Akt nadobúda účinnosť postupne, krok po kroku. Platí od 1. augusta 2024; od 2. februára 2025 sú už záväzné nižšie uvedené zakázané postupy a povinnosť budovať gramotnosť v oblasti UI (čl. 4); od 2. augusta 2026 sa uplatňuje väčšina jeho zostávajúcich ustanovení.



Obr. 1: „Plán postupu v oblasti UI“ (obrázok vytvorený pomocou UI)

Kto je zodpovedný za používanie UI?

Ak škola zavedie systém UI a má nad ním kontrolu, je za obvyklých okolností zavádzajúcim subjektom škola alebo školský orgán (čl. 3 ods. 4). Učiteľ zvyčajne nie je samostatným

zavádzajúcim subjektom, ak nástroj používa podľa pokynov školy, musí sa však aj tak riadiť týmito pokynmi a všetkými príslušnými školskými pravidlami a pravidlami ochrany osobných údajov.

Učitelia musia vedieť, čo používajú

Školy a školské orgány musia prijať primerané opatrenia na podporu rozvoja gramotnosti v oblasti UI u tých, ktorí v ich mene používajú systémy UI (čl. 4). Akt o UI nešpecifikuje konkrétnu úroveň kompetencie, certifikát ani formu školenia. Tie skôr závisia od použitého systému UI, spôsobu jeho používania a od toho, koho sa môže dotýkať.

Postupy UI úplne zakázané pre školy

Akt o UI úplne zakazuje osem postupov UI (čl. 5); štyri z nich sa priamo týkajú škôl:

1. Používanie systémov UI vo vzdelávacích inštitúciách na odvodzovanie emócií alebo zámerov z biometrických údajov (napríklad z tvárových alebo hlasových charakteristík žiakov) je vo všeobecnosti zakázané. Existujú úzke výnimky na zdravotné alebo bezpečnostné účely (čl. 3 ods. 39; čl. 5 ods. 1 písm. f)).
2. Systémy UI, ktoré zneužívajú niečiu zraniteľnosť z dôvodu veku (ako v prípade detí), zdravotného postihnutia alebo sociálnej či ekonomickej situácie spôsobom, ktorý skresľuje ich správanie a spôsobuje im škodu, sú zakázané bez ohľadu na zámer (čl. 5 ods. 1 písm. b)).
3. Budovanie alebo rozširovanie databázy na rozpoznávanie tváre prostredníctvom necieleného zberu obrázkov z internetu alebo z kamerových záznamov je zakázané. Toto je relevantné, ak škola zvažuje nástroj na rozpoznávanie tváre na evidenciu dochádzky alebo dohľad nad skúškami (čl. 5 ods. 1 písm. e)).
4. Používanie biometrických údajov na kategorizáciu ľudí s cieľom odvodiť chránené znaky, ako je rasa, politické názory, náboženstvo alebo sexuálna orientácia, je zakázané. Toto je relevantné pre akýkoľvek biometrický nástroj, napríklad softvér na dohľad nad skúškami, ktorý presahuje svoj deklarovaný účel (čl. 5 ods. 1 písm. g)).

Potrebuje obsah vygenerovaný UI vždy označenie?

Ak študenti priamo komunikujú so systémom UI, ako je napríklad chatbot, musia byť informovaní, že komunikujú s UI. Zvyčajne je za jasné oznámenie tejto skutočnosti zodpovedný poskytovateľ systému (čl. 50 ods. 1).

Školy a učitelia musia označiť deepfakes alebo text vygenerovaný UI a zverejnený k veciam verejného záujmu, ak sa používajú vo výučbe (čl. 50 ods. 4). Táto povinnosť sa neuplatňuje, ak obsah vygenerovaný UI prešiel účinnou ľudskou kontrolou alebo redakčným dohľadom a osoba či inštitúcia preberá redakčnú zodpovednosť za jeho zverejnenie. Pracovný list vytvorený s pomocou UI a skontrolovaný učiteľom preto automaticky nevyžaduje označenie.

Kedy sa UI vo vzdelávaní stáva vysoko rizikovou

Bežné nástroje na písanie, preklad, výskum a plánovanie hodín nie sú vysoko rizikové len preto, že sa používajú pri práci. Klasifikácia závisí od zamýšľaného účelu systému, nielen od toho, ktorý konkrétny produkt sa používa (čl. 6 · Príloha III).

Systémy UI môžu byť klasifikované ako vysoko rizikové, ak sú určené na to, aby:

Pre učiteľov	Pre školy
• rozhodovali o prístupe, prijatí alebo zaradení žiakov do vzdelávacích či odborných inštitúcií a programov; • hodnotili výsledky učenia žiakov alebo usmerňovali ich vzdelávací proces; • posudzovali primeranú úroveň vzdelania, ktoré žiak dostane alebo ku ktorému môže mať prístup; alebo • odhaľovali zakázané správanie žiakov počas skúšok. (Príloha III, bod 3)	• prijímali alebo vyberali učiteľov, vrátane preverovania žiadostí; • rozhodovali o zmluvných podmienkach, povýšení alebo ukončení pracovného pomeru učiteľa; • prideľovali úlohy na základe správania alebo osobnostných vlastností učiteľa; alebo • hodnotili výkon učiteľov. (Príloha III, bod 4)

Obmedzený kontrolný alebo prípravný nástroj môže tiež spadať mimo kategórie vysokého rizika, ak výrazne neovplyvňuje rozhodnutie. Vzdelávací systém, ktorý profiluje jednotlivcov, sa však vždy považuje za vysoko rizikový.

Čo vysoko riziková UI znamená pre školy a učiteľov

Klasifikácia systému UI ako vysoko rizikového automaticky nevylučuje jeho používanie v školách. Vysoko rizikové systémy však so sebou prinášajú povinnosti (čl. 26):

Tieto povinnosti pre vysoko rizikovú UI vo vzdelávaní platia od 2. decembra 2027 — vyššie uvedené zákazy a povinnosť gramotnosti v oblasti UI však platia už dnes.

Pre učiteľov	Pre školy
• používali ju len na schválený účel a dodržiavali jej pokyny; • nepovažovali jej výstup za konečné rozhodnutie; • poznali jej hlavné obmedzenia a pravdepodobné zdroje chýb; • dávali si pozor na nadmerné spoliehanie sa na zdanlivo presvedčivé výsledky; a • boli pripravení jej výstup odmietnuť alebo zmeniť.	• zabezpečili kompetentný a oprávnený ľudský dohľad; • zabezpečili, aby všetky vstupné údaje, ktoré majú pod kontrolou, boli relevantné a dostatočne reprezentatívne; • monitorovali systém a reagovali na riziká alebo vážne incidenty; • uchovávali automaticky generované záznamy najmenej šesť mesiacov, ak majú tieto záznamy pod kontrolou; a • vopred informovali žiakov, učiteľov alebo dotknuté osoby, keď systém napomáha rozhodovaniu, ktoré sa ich týka.

Verejné orgány a súkromné organizácie poskytujúce verejné služby môžu byť tiež povinné vykonať posúdenie vplyvu na základné práva pred použitím vysoko rizikovej UI (čl. 27). Verejné orgány a organizácie konajúce v ich mene môžu byť navyše povinné zaregistrovať systém v databáze EÚ (čl. 49). Či je za to zodpovedná škola alebo jej zriaďovateľ, závisí od národného školského systému.

Akt o UI nie je jediným relevantným zákonom

Akt o UI nenahrádza európske ani vnútroštátne predpisy o ochrane osobných údajov, školstve, pracovnom práve a účasti zamestnancov, ochrane detí či autorskom práve (čl. 2 ods. 7). Napríklad skutočnosť, že nástroj nie je vysoko rizikový, neznamená, že doň smiete nahrávať práce žiakov alebo ich osobné údaje.

Nástroj môže byť podľa Aktu o UI prípustný, no napriek tomu zakázaný právom na ochranu osobných údajov alebo pravidlami vašej školy.

GDPR

GDPR (Nariadenie (EÚ) 2016/679) je zákon EÚ o ochrane osobných údajov. Zohráva podpornú úlohu popri Akte o UI: zatiaľ čo Akt o UI sa pýta, či a ako sa systém UI vôbec smie používať, GDPR si kladie užšiu otázku — smú sa tieto konkrétne údaje o tejto konkrétnej osobe spracúvať týmto spôsobom? Splnenie požiadaviek jedného predpisu automaticky neznamená splnenie požiadaviek druhého.

- Uplatňuje sa hneď, ako sú v hre osobné údaje. Mená, školské e-mailové adresy, práce žiakov, hlasové nahrávky, prepisy, fotografie, známky, dochádzka a údaje o pokroku v

učení — všetko sa počíta ako osobné údaje (čl. 4). Väčšina nástrojov UI používaných na hodinách sa dotýka aspoň jedného z nich.
- Na ich spracúvanie potrebujete právny základ. Školy sa zvyčajne opierajú o zákonnú povinnosť alebo o úlohu vo verejnom záujme; možný je aj súhlas, ten však musí byť daný slobodne a v prípade mladších žiakov ho musí udeliť rodič alebo zákonný zástupca (čl. 6, čl. 8).
- Niektoré údaje potrebujú osobitnú ochranu. Zdravotné informácie, biometrické údaje a údaje odhaľujúce rasový či etnický pôvod, náboženstvo alebo podobné znaky sú „osobitnou kategóriou údajov“ a v zásade sú neprípustné bez konkrétnej výnimky (čl. 9) — jeden z dôvodov, prečo Akt o UI osobitne zakazuje viaceré postupy biometrického odvodzovania v školách.
- Vedzte, kto je zodpovedný. Škola je zvyčajne „prevádzkovateľom“; poskytovateľ UI, ktorý spracúva údaje v mene školy, je „sprostredkovateľom“ a potrebuje zmluvu o spracúvaní údajov, ktorá jasne stanovuje jeho povinnosti (čl. 28). Overte si to skôr, než nový nástroj zavediete v celej škole.
- Údaje opúšťajúce EÚ potrebujú záruku. Mnohé obľúbené nástroje UI sú hostované mimo EÚ. Osobné údaje tam smú putovať len vtedy, ak existuje rozhodnutie o primeranosti alebo iná schválená záruka, ako sú štandardné zmluvné doložky (čl. 44).
- Žiaci a zamestnanci si zachovávajú svoje práva. Môžu sa opýtať, aké údaje sa o nich uchovávajú, žiadať ich opravu alebo vymazanie a namietať proti rozhodnutiam založeným výlučne na automatizovanom spracúvaní, ktoré sa ich významne dotýka (čl. 15–čl. 22) — právo, ktoré platí popri požiadavkách Aktu o UI na ľudský dohľad nad vysoko rizikovými systémami a posilňuje ich.

V praxi: predtým, ako do nástroja UI vložíte skutočné údaje žiakov alebo zamestnancov, overte si, či ho vaša škola schválila, nezdieľajte viac osobných údajov, než si úloha vyžaduje, a keď nástroj len skúšate, uprednostnite anonymizované alebo vymyslené príklady.

Kde nájsť pomoc

Presadzovanie práva je v každej krajine EÚ organizované inak. Keďže vnútroštátne kompetencie sa môžu meniť, použite aktuálny zoznam vnútroštátnych orgánov dohľadu nad trhom vedený Európskou komisiou. Ktokoľvek (učiteľ, žiak, rodič) môže na tento orgán podať sťažnosť, ak sa domnieva, že bol porušený Akt (čl. 85). Ak vysoko rizikový systém, ako napríklad nástroj na prijímacie konanie alebo dohľad nad skúškami, viedol k rozhodnutiu, ktoré významne ovplyvňuje žiaka, môže žiak (alebo jeho rodičia) tiež požiadať o vysvetlenie tohto individuálneho rozhodnutia (čl. 86).

Vnútroštátne pravidlá pre vašu krajinu

Akt o UI platí v celej EÚ, no orgány presadzovania práva, školské právo a prax v oblasti ochrany osobných údajov sa v jednotlivých krajinách líšia. Sem budú doplnené poznámky špecifické pre jednotlivé partnerské krajiny Playbooku:

- Rakúsko
- Česko
- Nemecko
- Lotyšsko
- Poľsko
- Slovensko
- Slovinsko
- Španielsko

Revision #4
Created 2026-09-01 09:13:36 UTC by Alexander
Updated 2026-10-20 15:32:32 UTC by Alexander