

Aktuální povinnosti, které se týkají škol

Aktuální povinnosti škol v oblasti umělé inteligence (AI) a Aktu o AI (AIA) vycházejí především z kombinace nového nařízení EU a zpřísněných požadavků na ochranu osobních údajů (GDPR) v digitální éře. Rok 2026 přináší nutnost hlubší analýzy technologií, které školy používají.

Zde je výčet klíčových povinností:

1. Provádění posouzení FRIA (Posouzení dopadů na základní práva)

Školy, které nasazují systémy AI, jsou v terminologii Aktu o AI považovány za **zavádějící subjekty** (deployery).

- **Vysoce rizikové systémy:** AI systémy používané ve **vzdělávání** (např. pro hodnocení studentů nebo nábor zaměstnanců) jsou klasifikovány jako **vysoce rizikové**.
- **Povinnost FRIA:** Školy jako veřejnoprávní subjekty nebo soukromé subjekty poskytující veřejné služby mají povinnost provést toto posouzení před nasazením systému. FRIA hodnotí širší spektrum práv než jen soukromí – zaměřuje se na **diskriminaci**, lidskou důstojnost, transparentnost a rovný přístup ke vzdělávání.

2. Aktualizace a rozšíření DPIA o „AI-ready“ optiku

Škola musí provádět posouzení vlivu na ochranu osobních údajů (DPIA) vždy, když hrozí vysoké riziko pro práva jednotlivců, což je u AI téměř pravidlem.

- **Riziko reidentifikace:** V rámci DPIA již nestačí posoudit riziko úniku dat. Musí být explicitně hodnoceno **riziko reidentifikace** prostřednictvím AI útoků.
- **Konec tradiční anonymizace:** Školy si musí uvědomit, že v éře AI pouhé smazání jmen (např. z výsledků testů pro statistiku) nestačí. AI dokáže díky tzv. **mozaikovému efektu** identifikovat studenta z kontextuálních fragmentů (např. kombinace bydliště, věku a specifické události).
- **Red teaming:** U kritických AI systémů by mělo být DPIA doplněno o praktické testování (etický hacking), zda lze z „anonymních“ dat identitu studenta skutečně dovodit.

3. Zajištění lidského dohledu (Human in the Loop)

- U jakéhokoli automatizovaného rozhodování, které má na studenty významné dopady (např. automatické vyhodnocování testů ovlivňující přijetí na školu), musí být zajištěn **lidský dohled**.
- AI nesmí být v pozici rozhodovací autority, ale pouze **asistenta**.

4. Transparentnost a informační povinnost

Školy musí studenty, rodiče i pedagogy jasně informovat o:

- Schopnostech používaných AI systémů a jejich bezpečnostních opatřeních.
- Důsledcích a rizicích jejich zneužití.
- Možnosti požádat o odstranění škodlivého obsahu (např. v případě generování nevhodných obrázků či deepfakes).

5. Ochrana dětí před škodlivým obsahem generovaným AI

V souvislosti s rozvojem generativní AI (např. modely jako Grok) jsou školy povinny:

- Zavádět robustní ochranná opatření proti zneužití osobních údajů studentů k vytváření **intimních snímků** či hanlivých zobrazení.
- Poskytovat studentům i rodičům informace o těchto rizicích přizpůsobené věku.

6. Správa „rozpočtu soukromí“ a práce s daty

Při trénování vlastních modelů nebo analýzách dat by školy měly prosazovat přístup:

- **Synthetic-first:** Místo reálných dat žáků používat **syntetická data**, která statisticky zachovávají vlastnosti původního souboru, ale neobsahují vazbu na konkrétní studenty.
- **Diferenciální soukromí:** Vkládání „digitálního šumu“ do výstupů AI, aby z nich nešlo zpětně odvodit identitu konkrétního jednotlivce.

Školám se doporučuje aktualizovat své metodiky nejpozději do srpna 2026, aby odpovídaly technologické realitě, kdy AI dokáže prolomit starší formy anonymizace během několika sekund.

Co se mění v roli pověřence pro školu v roce 2026

V roce 2026 dochází k zásadnímu posunu v roli pověřence pro ochranu osobních údajů (DPO), a to zejména v organizacích veřejného sektoru, jako jsou školy. Role se mění z auditora formálních náležitostí na **architekta datové bezpečnosti**.

Zde jsou klíčové změny a nové výzvy pro pověřence ve školství v roce 2026:

1. Rozšíření odpovědnosti o novou legislativu (AI Act a NIS2)

Pověřenec se již nezabývá pouze GDPR, ale musí se orientovat v celém balíku nových digitálních předpisů:

- **Akt o umělé inteligenci (AI Act):** Školy, které nasazují AI systémy (např. pro hodnocení studentů), musí nově provádět **Posouzení dopadů na základní práva (FRIA)**. Pověřenec je klíčovou osobou, která musí posoudit rizika diskriminace, zásahy do lidské důstojnosti a zajistit transparentnost AI systémů.
- **Kybernetická bezpečnost (NIS2/nový ZKB):** Pověřenec musí úzce spolupracovat s IT oddělením při implementaci bezpečnostních opatření a rozumět tomu, jak se promítají do ochrany dat.

2. Aktualizace procesů DPIA a „AI-ready“ optika

Pověřenci musí radikálně přehodnotit strategie posuzování vlivu na ochranu osobních údajů (DPIA):

- **Konec tradiční anonymizace:** V éře AI už k ochraně soukromí nestačí smazání jmen. AI dokáže reidentifikovat osoby z kontextuálních fragmentů (tzv. mozaikový efekt).
- **Nové povinnosti v DPIA:** Pověřenec musí nově v DPIA explicitně hodnotit **riziko reidentifikace prostřednictvím AI útoku**.
- **Správa „rozpočtu soukromí“:** Pověřenec se stává arbitrem při nastavování metod jako diferenciální soukromí (vkládání digitálního šumu do dat) nebo při prosazování přístupu „synthetic-first“ (používání syntetických dat místo reálných údajů žáků).

3. Zesílený dohled ÚOOÚ nad postavením pověřenců

Úřad pro ochranu osobních údajů (ÚOOÚ) ve svém **kontrolním plánu pro rok 2026** výslovně uvádí, že si posvítí na postavení pověřenců ve veřejném sektoru:

- Úřad bude kontrolovat, zda jsou pověřenci **dostatečně a včas zapojováni** do všech záležitostí souvisejících s ochranou dat.
- Bude se prověřovat, zda školy poskytují pověřencům **odpovídající zázemí a zdroje** pro výkon jejich funkce.

4. Využívání AI jako pracovního nástroje

Pověřenci v roce 2026 začínají sami využívat AI nástroje (např. NotebookLM) ke zefektivnění své práce:

- **Analýza dokumentace:** AI pomáhá s revizí tisíců smluv a směrnic, identifikuje chybějící klauzule nebo nesoulad s legislativou.
- **Vyřizování žádostí:** Automatizace kategorizace žádostí subjektů údajů (přístup, výmaz) a sledování lhůt.
- **Školení:** Generování personalizovaných školicích materiálů a testů pro pedagogy a zaměstnance školy.

5. Specifické agendy škol

Pověřenec musí metodicky vést školu v aktuálních citlivých oblastech:

- **Kamerové systémy:** Aplikace doporučení ÚOOÚ 01/2025 pro školy. Úřad trvá na tom, že kamery samy o sobě nezabrání šikaně a jejich instalace musí být podložena přísným balančním testem.
- **Školní matrika:** Pověřenec musí dohlížet na to, aby škola nevyžadovala nadbytečné souhlasy tam, kde je zpracování uloženo zákonem (např. údaje o zdravotním stavu v matrice).
- **Marketing:** Správné nastavení souhlasů pro používání fotografií a videí studentů po ukončení jejich studia.

V roce 2026 se tedy role pověřence profesionalizuje směrem k technickému porozumění systémům a proaktivnímu řízení rizik spojených s digitalizací školství.

Na co se zaměří ÚOOÚ při kontrole škol v roce 2026

Úřad pro ochranu osobních údajů (ÚOOÚ) ve svém **kontrolním plánu pro rok 2026** a v navazujících metodikách vytyčil několik klíčových oblastí, na které se u veřejných subjektů, včetně škol, zaměří.

Mezi hlavní priority kontrolní činnosti patří:

1. Postavení a role pověřence (DPO)

Úřad se v roce 2026 zaměří na **postavení pověřenců ve veřejném sektoru**. Kontroly budou prověřovat, zda školy:

- **Včas a dostatečně zapojují pověřence** do všech záležitostí souvisejících s ochranou dat.
- Poskytují pověřencům **odpovídající zázemí a zdroje** pro výkon jejich funkce.
- Zajišťují, aby role pověřence nebyla ve střetu zájmů a odpovídala požadavkům GDPR.

2. Transparentnost a informační povinnost

V rámci celoevropské koordinované akce (CEF) se ÚOOÚ v roce 2026 soustředí na dodržování **zásady transparentnosti**. Pro školy to znamená nutnost mít v pořádku informační dokumenty, které studentům a rodičům jasně vysvětlují, jak a proč se jejich údaje zpracovávají.

3. Nadužívání souhlasů (zejména školní matrika)

Úřad dlouhodobě kritizuje chybnou praxi, kdy školy vyžadují **souhlas rodičů tam, kde je zpracování uloženo zákonem**. Typickým příkladem je vedení údajů ve **školní matrice** (včetně údajů o zdravotním stavu), které škole ukládá školský zákon. V takovém případě je vyžadování souhlasu považováno za klamání subjektu údajů a porušení GDPR.

4. Kamerové systémy

Školy zůstávají pod dohledem v souvislosti s **Doporučením č. 01/2025 ke kamerovým systémům ve školách**. ÚOOÚ trvá na tom, že:

- Samotná přítomnost kamer nedokáže zabránit šikaně nebo agresivnímu chování.
- Instalace kamer musí být podložena **přísným balančním testem** a nelze je instalovat v prostorách určených k odpočinku nebo na toaletách.

5. Marketing a fotografie studentů

Častým terčem stížností i kontrol je **používání fotografií a videí studentů** pro marketingové účely školy. Školy musí zajistit:

- **Granularitu souhlasu** (oddělený souhlas pro fotky, videa, různé kanály).
- Správné ošetření souhlasu u končících studentů (např. před maturitou), aby nebyla narušena **dobrovolnost souhlasu** kvůli nerovnému vztahu mezi školou a žákem.

ÚOOÚ rovněž upozorňuje, že v roce 2025 zaznamenal **rekordní nárůst stížností** (meziročně o 68 %), k čemuž přispívá i využívání AI nástrojů veřejností k psaní strukturovaných podání. Lze tedy očekávat, že kromě plánovaných kontrol budou školy čelit i častějším kontrolám incidentním na základě podnětů rodičů.