



Úřad pro ochranu
osobních údajů

Kamerové systémy ve školách a školských zařízeních s důrazem na doporučení ÚOOÚ č. 1/2025

Praha dne 4. června 2025



Zaměření doporučení

- Na co se doporučení vztahuje:
 - Školy a školská zařízení
 - Veřejné, soukromé, církevní
 - Mateřské, základní, střední, vysoké (specifické postavení)
 - Komerové systémy se záznamem i formou online přenosu
 - Fotopasti
- Na co se nevztahuje:
 - Atrapy kamerových systémů
 - Komerové systémy jejichž pomocí nedochází ke zpracování osobních údajů (např. panoramatické kamery, více viz [kapitola 2.2 Stupeň identifikace \(osoby\) Metodiky ÚOOÚ ke kamerám](#) (str 6))
 - Nahodilé pořízení jednotlivého záznamu (např. na mobilní telefon)



Funkce kamerových systémů

- Preventivní – primární funkce odrazení pachatele od nežádoucího jednání
- Reaktivní – hlavní cíl je vyvolat okamžitou reakci
- Důkazní – cílem je zajištění záznamů přítomnosti nebo jednání osob, které může být využito k doložení či vyšetřování určitých událostí. Nejobvyklejší funkce.



Účel a právní titul

- Účel
 - Nejčastěji se jedná o ochranu majetku či zdraví osob
 - Pro zabránění šikany neefektivní
- Právní titul
 - Ve většině případů se jedná o oprávněný zájem správce či třetí strany
 - Plnění právní povinnosti – ve zvláštních případech jako je např. distanční výuka v některých mimořádných situacích uzavření škol či zákazu přítomnosti dětí, žáků nebo studentů ve školách (§184 a školského především v návaznosti na krizové opatření vyhlášené podle krizového zákona či postup dle § 95b zákona o vysokých školách)
 - Souhlas je v případě většiny kamerových systémů neaplikovatelný
 - V případě zpracování zvláštní kategorie osobních údajů (např. biometrické údaje) nutno nalézt výjimku ze zákazu zpracování této kategorie dle čl. 9 odst. 2 GDPR
- V případě monitorování zaměstnanců na pracovišti nutno zohlednit ustanovení § 316 zákoníku práce
- V případě využití AI nutno aplikovat AI Act (Nařízení Evropského parlamentu a Rady (EU) 2024/1689



Stanovení rolí

- Správcem bude typicky škola
- V případě zapojení třetí osoby (např. bezpečnostní agentura) je nutno uzavřít zpracovatelskou smlouvu dle čl. 28 GDPR (lze postupovat dle standardních smluvních doložek mezi správcí a zpracovatelem podle čl. 28 odst. 7, které upravuje [Prováděcí rozhodnutí Komise \(EU\) 2021/915 ze dne 4. června 2021](#))
- Forma zpracování prostřednictvím společných správců bude v praxi minoritní



Balanční test

- Přesná forma či přesný obsah nejsou právními předpisy stanoveny
- Oprávněný zájem dle čl. 6 odst. 1 písm. f) GDPR musí být zákonný a formulován dostatečně konkrétně
- V rámci Metodiky ÚOOÚ ke kamerám je doporučeno balanční test z hlediska zpracování osobních údajů kamerovým systémem provést ve čtyřech postupných krocích:
 - 1) Popis existence reálného ohrožení
 - 2) Posouzení dosažení účelu jinými prostředky (varianty) – kritérium potřeby
 - 3) Posouzení nezbytnosti vybrané varianty – kritérium vhodnosti
 - 4) Posouzení přiměřenosti zpracování osobních údajů – kritérium poměrování
- Nepovinný vzor balančního testu kamerového systému, ve věci řešení škod v bytovém domě je uveden v rámci [přílohy č. 3 Metodiky ÚOOÚ ke kamerám](#) (str 41-56)



Rozdělení kamer do skupin pro účely provedení balančního testu a nastavení organizačních opatření

- Kamery s malým zásahem do soukromí
 - (např. kamery monitorující perimetr pozemků, parkovací místa u škol na jejich pozemcích)
- Kamery se středním zásahem do soukromí
 - (např. kamery u vstupů do škol, do některých učeben)
- Kamery s vysokým zásahem do soukromí
 - (např. kamery v šatnách, u tělocvičen a bazénů – pokud jsou vyhrazeny jiné prostory pro převlékání, chodby škol, školní jídelny se záběrem na strávníky a personál)
- Kamery s velmi vysokým zásahem do soukromí
 - (např. kamery v učebnách, školních družinách, kabinetech, s využitím zvukového záznamu či s technologií rozpoznávání obličejů)

Rozdělení kamer do skupin pro účely provedení balančního testu a nastavení organizačních opatření

- Rozdělení kamer do v předchozím snímku uvedených skupin lze využít v rámci balančního testu pro stanovení koeficientu zásahu do soukromí, viz [kapitola 3.2.1 Metodiky ÚOOÚ ke kamerám, bod 2\)](#) „Posouzení dosažení účelu jinými prostředky (varianty) – kritérium potřeby“ (str 13), a také výslednou přehledovou tabulku ve vzorovém balančním testu, [vzor 3 Metodiky ÚOOÚ ke kamerám](#) (str 47)
- Rozdělení kamer do výše uvedených skupin lze též využít pro zařazení do tříd dle [kapitoly 3.9.2 Metodiky ÚOOÚ ke kamerám](#) (str 28-32), avšak vždy s ohledem i na další parametry a nastavení kamer



Omezení zásahu do soukromí

- Umístění kamer – (kamera u vchodu do budovy x kamera v šatně)
- Počet kamer (jedna kamera x množství kamer)
- Režim kamer (kamera snímající kontinuálně celé vyučování x kamera spínající se na základě intenzity zvuku)
- Záběry kamer (kamera u vchodu do učebny x kamera v učebně)
- Využívání některých speciálních funkcí kamer (kamera pořizující videozáznam x kamera pořizující záznam zvuku, či biometrické kamery nebo kamery využívající umělou inteligenci)
- Doba uchování (uchování po dobu 72 hodin x uchování po dobu několika měsíců)
- Frekvence výskytu osob ve sledovaném prostoru (prostor s nahodilým výskytem osob x prostor s pravidelně vysokou fluktuací osob)



Úřad pro ochranu
osobních údajů

Balanční test – méně rizikový kamerový systém

1. Krátký ale výstižný popis reálného ohrožení
2. Popis rozmístění a nastavení kamerového systému, aby bylo zřejmé, že jde o méně rizikový kamerový systém. Porovnání variant (minimálně: stávající varianta x navrhovaná varianta x alternativní varianta)
3. Krátký popis míry zásahu do práv a zájmů subjektů údajů (jen slovně) a krátký popis, jak budou dodržována práva subjektu údajů



Technická a organizační opatření

- Ve většině případů lze aplikovat třídu 2 – střední míra porušení dle [Metodiky ke kamerám](#) (str. 30)
- Jedná se tedy o tyto opatření:
 - Ochrana vnitřních i venkovních kamer
 - Umístění záznamového zařízení a datových nosičů v chráněném prostoru
 - Evidence přístupů (logování)
 - Řízení přístupu osob do prostoru umístění zařízení (u online obrazu)
 - Řízení přístupu k datům (autentizace, autorizace)
 - Monitorování a zaznamenávání činnosti (vyhledávání, přehrávání, vymazání, úprava, ukládání, tisk, předávání)
 - Ukládání údajů o čase
 - Bezpečný výmaz dat po uplynutí doby uchování
 - Školení obsluhy
 - Zpracování dokumentace
 - Ochrana před škodlivými kódy (uplatní se, pokud je systém připojen do sítí, nebo pokud jsou do zpracování zapojeni zpracovatelé)
 - Řízení dodavatelů a zpracovatelů (uplatní se, pokud je systém připojen do sítí, nebo pokud jsou do zpracování zapojeni zpracovatelé)



Úřad pro ochranu
osobních údajů

Záznam o činnostech zpracování

- Dle čl. 30 GDPR, tyto záznamy obsahují ([viz vzor č. 2: Metodiky ke kamerám](#), (str 40)):
 - Správce (např. škola)
 - Účely zpracování, právní základ (např. ochrana majetku a zdraví osob, oprávněný zájem správce nebo třetí osoby)
 - Kategorie subjektů údajů (např. osoby vstupující po monitorovaných prostor: především žáci, učitelé, zákonní zástupci žáků, zaměstnanci externích dodavatelů)
 - Kategorie osobních údajů (např. obrazový záznam z kamerového systému)
 - Kategorie příjemců (např. orgány činné v trestním řízení, pojišťovna)
 - Plánované lhůty pro výmaz jednotlivých kategorií osobních údajů (např. data jsou uchována po dobu 7 dní ve školním roce, v období tzv. velkých prázdnin po dobu 3 týdnů)
 - Obecný popis technických a organizačních bezpečnostních opatření pro nejpravděpodobnější rizika zpracování;
 - opatření k zabránění neoprávněnému přístupu k osobním údajům (řízení přístupu k datům),
 - opatření proti ztrátě, odcizení nebo poškození dat (stanovení pravidel práce s paměťovými médii, umístění a ochrany záznamových zařízení),
 - opatření v oblasti lidských zdrojů (stanovení pravidel pro práci s daty – stanovení rolí, proškolení osob) a opatření na ochranu dalších prostředků pro monitorování (kamery, kabely).

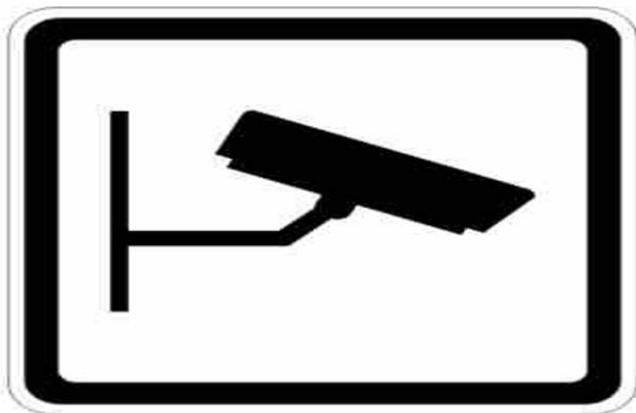


Informační povinnost

- Nutno označit monitorovaný prostor tak, aby subjekt údajů byl upozorněn na kamerový systém před vstupem do tohoto prostoru
- Informační tabulky musí být u monitorovaného objektu/prostoru umístěny po celou dobu provozu kamerového systému
- Informační tabulky musí být dobře viditelné, tj. umístěné a navržené tak, aby byly nepřehlédnutelné (přibližně ve výšce očí a na místech kudy musí subjekt údajů projít před vstupem do monitorovaných prostor)
- U kamerových systémů je pro plnění uvedené povinnosti dle čl. 13 GDPR prakticky nutné využití vrstevnatého přístupu (tj. první vrstva - piktogram se základními informacemi a s odkázáním na druhou vrstvu – např. odkaz na webové stránky pomocí URL či QR kódu, kde lze nalézt zbývající informace)
- Obecný vzor pro plnění tzv. druhé vrstvy je uveden v rámci [přílohy č. 1 Metodiky ÚOOÚ ke kamerám](#) (str 38)



Úřad pro ochranu
osobních údajů



Tento objekt je monitorován kamerovým systémem

Provozovatel/Správce:

Úřad pro ochranu osobních údajů

tel.: 234 665 111 IČO 70837627

Účel zpracování osobních údajů

Zvýšení ochrany majetku (krádež, vloupání, vandalismus),
bezpečnosti osob (napadení, loupež, jiná fyzická újma) a prevence mimořádných událostí

Právní základ zpracování osobních údajů

Zpracování je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby - čl. 6 odst. 1 písm. f) GDPR

Práva subjektu údajů

Subjekt údajů má možnost uplatnit vůči správci práva garantovaná mu GDPR, např. právo na přístup k osobním údajům

Podrobnější informace o zpracování osobních údajů prostřednictvím kamerového systému, včetně práv subjektu údajů
a kontaktu na pověřence pro ochranu osobních údajů, jsou k dispozici na recepci a na webové stránce www.uoou.cz



Úřad pro ochranu
osobních údajů





Úřad pro ochranu
osobních údajů

Místo uložení kamerových záznamů

- Lokálně na paměťových zařízeních správce (typicky prostory školy)
- Lokálně na paměťových zařízeních zpracovatele (např. bezpečnostní agentura)
- Vzdáleně s využitím cloudových služeb
 - Může být problematické v případě dodavatelů mimo EHP,
 - Předávání osobních údajů do třetích zemí řeší kapitola V GDPR, viz příslušná [sekce](#) webových stránek ÚOOÚ
 - Určitým vodítkem pro výběr vhodného poskytovatele může být [katalog cloud computingu](#) na webových stránkách DIA



Další povinnosti správce

- Nastavení mechanismu ohledně výkonu práv subjektu údajů (především právo na přístup k osobním údajům dle čl. 15 GDPR, právo vznést námitku dle čl. 21 GDPR, právo na omezení zpracování dle čl. 18 GDPR)
- Ohlašování případů porušení zabezpečení osobních údajů dle čl. 33 GDPR
 - Ohlášení nutno vůči ÚOOÚ učinit do 72 hodin od okamžiku, kdy se správce o porušení dozvěděl. Pokud není ohlášení Úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění
 - Ohlašovat není třeba případy, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby
 - Pokud je pravděpodobné, že případ bude mít za následek vysoké riziko pro práva a svobody dotčených osob je nutné bez zbytečného odkladu informovat i tyto osoby (čl. 34 GDPR)
 - Více viz příslušná [sekce](#) webových stránek ÚOOÚ
- Registrační povinnost byla zrušena



Úřad pro ochranu
osobních údajů

Spolupráce s pověřencem pro ochranu osobních údajů

- Pověřenec může být konzultován při postupu řešení (návrh variant, parametry řešení)
- Správce výběr varianty a její parametry předkládá pověřenci ke stanovisku
- Zapojení pověřence do vyřizování žádostí subjektu údajů či ohlašování porušení zabezpečení
- Pověřenec by měl alespoň participovat na tvorbě příslušné dokumentace (záznamy o činnostech zpracování, informační povinnost apod.)
- Pověřenec může kontrolovat, zda jsou dodržována navržená technická a organizační opatření



Úřad pro ochranu
osobních údajů

Nejčastější chyby

- Chybějící dokumentace
 - Informační povinnost, záznamy o činnostech zpracování, bilanční test
- Nevhodné umístění a nastavení kamery
- Nedostatečné zabezpečení kamerového systému
- Nevhodně zvolená doba uchování
- Absence logování
- Nezapojení pověřence pro ochranu osobních údajů
- Nedostatečná revize/aktualizace související dokumentace
- Nesprávná aplikace souhlasu
- Nedostatečné proškolení personálu



Jak postupovat při zpracování osobních údajů v rámci kamerového systému – závěrečné shrnutí

- Definování konkrétních účelů (např. ochrana majetku či zdraví osob) a právních titulů (např. oprávněný zájem správce)
- Odůvodnění nezbytnosti předmětného zpracování (např. v případě oprávněného zájmu provedení balančního testu – při existenci reálného ohrožení a porovnání variant)
- Stanovení rolí (otázka odpovědnosti)
- Zpracování záznamu o činnostech zpracování a další příslušné dokumentace
- Nastavení mechanismů týkajících se práv subjektu údajů (především plnění informační povinnosti a práva na přístup k osobním údajům)
- Zabezpečení osobních údajů – prostřednictvím technických a organizačních opatření
- Periodické vyhodnocování účinnosti zvoleného řešení



Zahraniční zkušenosti

- Přístup evropských dozorových Úřadů:
 - Převážně restriktivní přístup. Vychází z přesvědčení, že kamerové sledování sociální komunikace představuje výrazný zásah do práva na soukromí a zasahuje nevhodným způsobem do procesu budování sociálních vazeb a vzorců chování dětí.
 - Nastavení režimu kamerového sledování rozlišují vyučovací či provozní dobu školy, v jejímž průběhu je sledování prostor školy v zásad vyloučeno, a dobu mimo vyučování, kdy je škola uzavřena.



Užitečné odkazy

- [Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů - ÚOOÚ](#)
- [Guidelines 1/2024 on processing of personal data based on Article 6\(1\)\(f\) GDPR – EDPB](#)
- [Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky - EDPB](#)
- [Metodika pro distanční vzdělávání - za podmínek stanovených v § 184 školského zákona – MSMT](#)
- [Doporučení ÚOOÚ č. 1/2025 ke kamerovým systémům ve školách – ÚOOÚ](#)
- [Katalog cloud computingu - DIA](#)



Úřad pro ochranu
osobních údajů

Děkuji za pozornost a přeji
příjemný den

Mgr. Petr Ševčík