

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Kamerové systémy ve školách podle doporučení Úřadu pro ochranu osobních údajů: Jen chtít nestačí

Kamerové systémy jsou stále častějším tématem a způsobem cíleným na ochranu majetku, života, zdraví, ale i prevenci násilného či jinak závažného jednání. V poslední době se jejich použití rozšířilo také do škol a školských zařízení. Přístup škol ke kamerovým systémům je zpravidla obdobný. Chtěly by. Ale měly by? V článku vycházejícím z aktuálního doporučení a metodiky ÚOOÚ upozorňujeme na některé praktické aspekty právní úpravy, které ředitelé škol při rozhodování o pořízení kamerového systému mnohdy opomíjejí.

V reakci na čím dál častější nasazování kamerových systémů ve školách vydal počátkem tohoto roku Úřad pro ochranu osobních údajů[1] doporučující dokument[2], který navazuje na metodiku zveřejněnou v loňském roce[3] a který si klade za cíl podpořit postup škol při zavádění a provozování kamerových systémů. Nadcházející text z těchto dokumentů (a také ze zkušeností autorky) z nich vychází a je relevantní jak pro kamerové systémy se záznamem, tak pro ty v režimu on-line (monitoringové kamery) a pro fotopasti.

Přístup škol ke kamerovým systémům je zpravidla obdobný. Chtěly by. Ale měly by?

Článek si neklade za cíl detailně popsat všechny povinnosti a úskalí zavádění kamerového systému, ale spíše upozornit na praktické aspekty právní úpravy, které si ředitelé škol při rozhodování o pořízení kamerového systému mnohdy neuvědomují.

Prevence, reakce nebo důkaz?

Jedna z prvních otázek, kterou si musí správce[4] položit, zní: Jakou funkci má kamerový systém plnit? ÚOOÚ jako nejčastější identifikuje funkci preventivní, reaktivní a důkazní. Pokud má kamerový systém být **preventivním opatřením**, pak by se správce měl ptát a zjišťovat, zda nasazení kamerových systémů povede ke snížení výskytu šikany, odcizení věcí a podobných jevů. Právě tato racionální úvaha a provedení analýzy reálného ohrožení v praxi mnohdy chybí a kamerový systém pak nemůže plnit svou funkci.

U **reaktivní funkce** je otázkou, zda kamerový systém okamžitě reaguje a omezuje následky mimořádné události. Sám o sobě totiž k tomu obvykle způsobilým není. Nedávné tragické události ukázaly, že v případech útoků či střelby budou efektivnější a pružnější odlišná opatření, jako jsou školení o prevenci chování v krizových situacích, únikový plán, automatické rozesílání výstražných SMS či sirény.

Nejčastěji je proto jejich využití zdůvodňováno **funkcí důkazní**. Právě ta ale bude mnohdy nejinvazivnější – a tedy z pohledu ochrany osobních údajů nejproblematictější.

Jaký je účel kamerového systému a co k jeho využití opravňuje správce?

Na rozdíl od správného určení funkce neklade stanovení účelu kamerových systémů zpravidla potíže. V kontextu škol jde většinou o ochranu života, zdraví a majetku, zvýšení bezpečnosti či prevenci šikany nebo jiného závadného chování. Využívání kamer k prevenci šikany však kritizuje ÚOOÚ a označuje je za „poslední a vcelku nejméně účinný prostředek na řešení šikany“. To souvisí nejen s rizikem vytlačení závadného chování na místa, kde kamery nejsou (např. toalety), ale i s množstvím jiných nástrojů, které může škola využít k prevenci a řešení šikany a dalších sociálně-patologických jevů[5].

Stejně jako v případě jiných operací zpracování i v případě kamerových systémů navíc platí, že k němu správce musí mít jeden ze šesti vymezených **právních titulů**[6]. Nejpriléhavějším a nejčastějším z nich bude oprávněný zájem. Ten sice umožňuje správci zpracovávat osobní údaje prostřednictvím kamerového systému, avšak pouze za splnění poměrně přísných a přesně daných podmínek. Klíčovým je tzv. balanční test, v němž musí správce posoudit, zda jeho zájem (např. ochrana majetku, života nebo zdraví) převyší zájmy subjektů údajů, zejména tehdy, je-li subjektem údajů dítě, tedy osoba mladší 18 let, což bude ve školách téměř pravidlem. Při tom se správce musí vypořádat s možnými variantami řešení a méně invazivními (byť pro školu mnohdy méně pohodlnými) způsoby dosažení sledovaného cíle.

Správce, který by se povinnosti zpracovat balanční test chtěl zprostit tím, že si opatří souhlas žáků a jiných osob, které budou kamerami snímány, by s touto strategií ve většině případů spíše neuspěl. Využití souhlasu je v tomto případě problematické kvůli absenci jeho dobrovolnosti a informovanosti, a u žáků navíc naráží na věkovou hranici, protože souhlas se zpracováním osobních údajů mohou děti udělit až od 15 let[7].

Všechny správce navíc bude tížit povinnost vyhotovení analýzy rizikovosti a případně také odborně-technického posouzení vlivu na ochranu osobních údajů (DPIA)[8], který se v některých ohledech může s balančním testem (pokud byl zpracován) prolínat.

Ve vztahu k zaměstnancům pak musí správce zohlednit také zákonný zákaz sledování zaměstnanců na pracovišti[9].

Další povinnosti a zásady zpracování

Jaké další povinnosti a limity stanoví metodika a právní úprava? V souvislosti s jakýmikoliv kamerovými systémy je nejčastěji potřeba mít na paměti jednu ze základních zásad GDPR, kterou je **minimalizace údajů**[10]. Tu lze lakonicky řečeno přeložit takto: čím méně, tím lépe – a to ve všech ohledech. Zásah do soukromí v případě kamerových systémů je totiž nezpochybnitelný, a proto má-li již k němu dojít, je potřeba, aby se tak dělo v co nejmenším rozsahu (zde je uvažováno umístění a počet kamer, jejich režim, záběry atp.). V tomto ohledu nejinvazivnější a také nejproblematictější by byly kamery v učebnách, kamery využívající biometrické rozpoznávání obličeje nebo kamery se zvukovým záznamem, ale také kamery na chodbách škol, hřištích, ve školních jídelnách nebo v šatnách u tělocvičen.

Zpracování musí být také **transparentní, zákonné a korektní**, čehož praktickým a naprosto nezbytným průmětem je dostatečně rozpracované víceúrovňové informování před vstupem do monitorovaných prostor (pouhý vykřičník či text „*prostor je monitorován kamerovým systémem*“ je nedostatečný a tuto povinnost nesplňuje). Údaje dále nesmějí být dále zpracovávány způsobem, který je s předem stanoveným účelem zpracování neslučitelný (**účelové omezení** zpracování). **Přesnost** osobních údajů je zpravidla zajišťována povahou zpracování bez dalšího.

Osobní údaje – zde především v podobě kamerových záznamů – nesmějí být ukládány po dobu delší, než je nezbytně nutné (zásada **omezení uložení**). Obvyklá a ÚOOÚ bez problému akceptovatelná

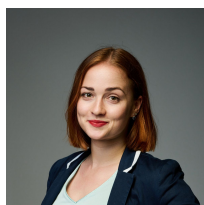
lhůta uchování je 72 hodin. V praxi se tato hodnota mnohdy překračuje až na 30 a více dní, což však bude obvykle nezákonný přístup, pokud takto dlouhá doba uložení není odůvodněna zvláštními provozními nebo jinými významnými důvody. Konečně musí být přijata dostatečná technická a organizační opatření, která osobní údaje ochrání před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením (zásada **integrity a důvěrnosti**). To zahrnuje také způsob uložení záznamů z kamerových systémů, zvláště pokud by správce hodlal využít služeb zahraničních cloudových úložišť.

Pokud k provozování kamerových systémů či k monitorování kamer využívá škola externí subjekt, musí s ním uzavřít smlouvu o zpracování osobních údajů[11]. Ve většině případů bude také škola povinna zohlednit zpracování v rámci záznamů o činnostech zpracování (evidenčních listech)[12].

Shrnutí aneb Jak z toho ven

Povinností, které musí škola, která chce nebo potřebuje zavést kamerový systém, splnit, je celá řada, a i samotná metodika a doporučení ÚOOÚ upozorňují pouze na některé z nich. Nejedná se však o žádné přelomové povinnosti, pouze o praktická upozornění (a ze strany ÚOOÚ do určité míry také přátelská předtím, než začnou kamerové systémy být předmětem masivnějších kontrol) na právní úpravu, která závazná a účinná již téměř sedm let[13].

Proto pokud jste ředitel či jiný zástupce školy, která uvažuje o tom, že by kamerové systémy pořídila, anebo která je již používá, ale dosud si příliš nelámala hlavu s povinnostmi, které to může přinášet, zbystřete. Právní úprava a ochrana, kterou nastavuje, dává smysl, i když může být v prvotních počátcích, zvláště bez odpovídajícího právního zázemí, obtížně uchopitelná. Stejně jako v jiných oblastech zpracování osobních údajů, či spíše v rámci kamerových systémů obzvláště platí, že se jedná o systém, u něž nestačí jednorázově zpracovat informační tabulku nebo zásady a vylepit je na nástěnku. Naopak, ochrana osobních údajů je živým organismem, o který je potřeba pravidelně pečovat - kontrolovat jej, aktualizovat informační dokumenty i vnitřní předpisy, nastavovat nová technická a organizační opatření, vyřizovat žádosti subjektů údajů, zodpovídat dotazy - a tyto činnosti konzultovat s právní službou a/nebo s pověřencem pro ochranu osobních údajů (DPO). Metodika a doporučení, z nichž tento článek vzešel, k tomu jen podává pomocnou ruku.



Mgr. Karolína Volčíková,
spolupracující advokátka



HSP & Partners advokátní kancelář s.r.o.

Vodičkova 710/31
110 00 Praha 1

Tel.: +420 734 363 336
e-mail: sekretariat.praha@akhsp.cz

[1] Dále také jen jako „ÚOOÚ“.

[2] Doporučení ÚOOÚ č. 1/2025 ke kamerovým systémům umístěným ve školách a školských zařízeních, ze dne 15. 1. 2025.

[3] Metodika ÚOOÚ k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, ze dne 8. 2. 2024.

[4] Tedy subjekt ve smyslu čl. 4 odst. 7 GDPR (nařízení Evropského parlamentu a Rady (EU) č. 2016/679), který o zpracování rozhoduje a který za něj odpovídá. Prakticky vzato se bude jednat o školu jednajícím prostřednictvím svého statutárního orgánu – ředitele – rozhodujícího ve věcech a v působnosti školy.

[5] Metodika konkrétně poukazuje na organizační, metodickou, poradenskou a materiální pomoc, kterou v oblasti řešení šikany a jiných sociálně-patologických jevů, projevů diskriminace a nepřátelství nabízí a poskytuje MŠMT, Česká školní inspekce i další odborné organizace a asociace.

[6] Právní tituly jsou v zákoně stanoveny taxativně a jejich existenci je správce povinen prokázat. Jedná se o souhlas, plnění smlouvy, plnění právní povinnosti, ochranu životně důležitých zájmů, provádění úkolu ve veřejném zájmu či při výkonu veřejné moci, nebo v souvislosti s kamerovými systémy nejčastěji aplikovatelný oprávněný zájem (čl. 6 odst. 1 GDPR).

[7] § 7 zákona č. [110/2019](#) Sb., o zpracování osobních údajů

[8] čl. 35 GDPR

[9] § 316 odst. 2 zákona č. [262/2006](#) Sb., zákoníku práce

[10] čl. 5 odst. 1 písm. c) GDPR

[11] čl. 28 GDPR

[12] čl. 30 GDPR

[13] GDPR nabylo účinnosti 25. 5. 2018, zákon č. [110/2019](#) Sb., o zpracování osobních údajů, pak 24. 4. 2019.

Další články:

- [DEAL MONITOR](#)
- [Tři dekády v advokacii a otevřený pohled na to, co profesi i justici nejvíc škodí](#)
- [DEAL MONITOR](#)
- [Vybrané otázky poskytování zdravotních služeb na dálku](#)
- [DEAL MONITOR](#)
- [„Za každou kauzou je živý příběh“](#)
- [Ombudsman na Maltě - základní parametry a role. A v čem bychom se mohli poučit i my v Česku?](#)
- [DEAL MONITOR](#)
- [DEAL MONITOR](#)
- [Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo](#)
- [DEAL MONITOR](#)