Úřad pro ochranu osobních údajů

Doporučení ÚOOÚ č. 01/2025
ke kamerovým systémům umístěným ve školách a školských zařízeních
Přijato dne 15. ledna 2025

Úvod

Po vydání Metodiky k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů[1] (dále jen Metodika), která stanovuje a popisuje postup správců při zřízení a provozovaní kamerových systémů obecně, považuje Úřad pro ochranu osobních údajů za vhodné dále podpořit postup správců podrobnějším popisem týkajícím se konkrétních typově shodných zařízení, v tomto případě škol a školských zařízení (dále jen škol).

Toto doporučení se vztahuje na všechny školní kamerové systémy a fotopasti.

Kamerové systémy jsou poměrně často nasazovaným prostředkem dohledu ve školách na všech stupních. Nasazení kamerového systému v prostorách škol přitom může představovat zvlášť citelný zásah do práva na soukromí, a to i s ohledem na skutečnost, že v těchto zařízeních se zásadně formují vzorce chování dětí a mládeže, probíhají zde základní sociální interakce a děti/žáci/studenti, pedagogové a další zaměstnanci škol zde tráví značnou část dne. Je proto pochopitelné, že v zásadě všechny dozorové úřady EU věnují problematice zpracování osobních údajů prostřednictvím kamerových systémů náležitou pozornost, jak vyplývá i ze srovnání přístupu jednotlivých evropských dozorových úřadů ke kamerovému sledování ve školách.

Poznámka: V rámci škol mají své specifické postavení vysoké školy, u kterých je nutné zohlednit jejich akademické svobody a charakter otevřeného společenství spojeného s velkým rozsahem pravidelně přicházejících osob, což v podstatě vylučuje omezení zpřístupnění objektů těchto škol. Tomuto charakteru musí odpovídat i výběr technických a organizačních opatření k řešení mimořádných situací, přičemž některá z možných technických nebo organizačních opatření nemohou být z objektivních důvodů (například z důvodu nutnosti zachování volného přístupu do objektu) v tomto prostředí nasazena.

[1] Viz https://uoou.gov.cz/novinky/vse/nova-metodika-uradu-ke-kamerovym-systemum.

Základní ochranné funkce kamer

Školy, podobně jako jiní správci osobních údajů, si slibují od nasazení kamerového systému za ochrannými účely naplnění tří základních funkcí kamer – preventivní, reaktivní a důkazní.

- **Preventivní funkce** – Tato funkce spočívá v odrazení pachatele od nežádoucího jednání (na základě předchozí analýzy reálného ohrožení). Určitě lze uvažovat o tom, že rozšířené povědomí o nasazení konkrétního kamerového systému může předcházet opakování mimořádných událostí majetkového typu (vandalismus, sprejerství apod.). Naopak v případě mimořádných událostí typu fyzických útoků je třeba vzít v úvahu, že čelíme zpravidla pachatelům, při jejichž jednání nehraje vědomí přítomnosti kamer významnou roli. Skutečnost, že naplnění odrazující funkce není reálné, je zvlášť markantní v případě, kdy pachatelem fyzického útoku budou osoby, které mají pravidelný oprávněný přístup do budovy i se svými zavazadly (např. zaměstnanci, žáci, studenti). Určitou efektivitu preventivní funkce, srovnatelnou s efektivitou opatření zajišťujících řízení vstupu do prostor škol (fyzický dozor, čipy, turnikety, bezpečnostní rámy, místa pro odkládání zavazadel), by mohlo zajistit jedině nasazení kamer s moderními funkcemi (umělá inteligence) nebo detekce nebezpečných zvukových událostí na základě vysoké intenzity zvuku (střelba, křik, výbuch), za předpokladu, že je o nich subjekt předem informován a nedochází k nadměrnému zásahu do práv a svobod fyzických osob.
- **Reaktivní funkce** – V případě mimořádné události by pro naplnění reaktivní funkce měl kamerový systém vyvolat okamžitou reakci, která by zajistila omezení rozsahu a následků dané mimořádné události. Obecně platí, že kamery tuto funkci v zásadě mohou naplnit jen velmi omezeně. Zde je namístě zavést jiná opatření, která zamezí nebo ztíží postup pachatele (uzamykání některých místností/vytvoření útočišť v případě mimořádné události, rozesílání automatických varování o ohrožení – mobily, sirény, školní rozhlas, školení a výcvik k sebeobraně nebo postupu v podobných situacích a odeslání signálu pro bezprostřední zásah silových složek), případně využít kamery vybavené speciálními funkcemi nebo zařízení pro detekci nebezpečných zvukových událostí (křik, střelba, výbuch), které mohou urychlit reakci oprávněných osob na mimořádnou událost. Nasazení kamer provozovaných obvyklým způsobem by teoreticky mohlo být efektivním řešením jedině v kombinaci s permanentní přítomnosti zásahové skupiny aktivované na základě záběrů z kamer.

  Poznámka: Poněkud vyšší účinnost může mít kamerový systém přiměřeného rozsahu v případě, že existuje podezření na provedení fyzického útoku ještě před jeho zahájením (například na základě informace od oznamovatele), kdy

kamerový systém může umožnit identifikaci vstupu a přítomnosti pachatele v objektu.

- **Důkazní funkce** – Nejobvyklejší funkcí kamerových systémů je zajištění záznamu přítomnosti nebo jednání osob, které může být využito k doložení a vyšetření určitých událostí. S ohledem na invazivní charakter zpracování osobních údajů prostřednictvím kamerového dohledu je možné kamery nasadit jen takovým způsobem, aby nadměrně nezasahovaly do základních práv a svobod, zejména do práva na ochranu osobních údajů a soukromí subjektů údajů.

Účel zpracování a právní důvod

Nejběžnějším účelem provozování kamerových systémů ve školách je **ochrana majetku**. Při vhodném umístění a nastavení se kamerový systém může ukázat jako přiměřené opatření pro zajištění důkazní funkce při vyšetřování a řešení následků mimořádných událostí, ale i funkce preventivní (odrazující), byť v případech maskovaných pachatelů se jeho účinnost výrazně snižuje.

S účelem ochrany majetku bývá často deklarován účel **zvýšení bezpečnosti, ochrany zdraví a života osob**. Nasazení kamer ve školách za tímto účelem se stalo široce diskutovaným tématem v souvislosti s útokem např. na střední škole ve Žďáru nad Sázavou či střelbou na Filozofické fakultě Univerzity Karlovy v Praze. Statistická vyhodnocení přínosu kamerových systémů pro omezení nebo zabránění mimořádné události typu fyzického útoku ve školách oficiálně nejsou k dispozici. Případné rozsáhlé rozmisťování kamer uvnitř škol (mimo uzlová místa, jako jsou vstupy do objektů, v případě vysokých škol i křížení pochozích koridorů), se však z hlediska naplnění účelu zvýšení bezpečnosti, ochrany zdraví a života jeví přinejmenším jako sporné.

Některé školy rovněž uvažují o zavedení kamerového systému pro účel **zabránění šikaně**. Instalace kamer za tímto účelem se nejeví jako přiměřené řešení pro omezení tohoto problému, protože po jejich nainstalování je pravděpodobné, že bude šikana vytěsněna ze záběru kamer do jiných prostor, kde kamery nejsou (toalety) nebo mimo objekty škol, přičemž účelu nebude dosaženo. Navíc se může výrazně omezit i možnost tento závažný výchovný problém detekovat a následně řešit.

Poznámka: Ustanovení § 30 zákona č. 561/2004 Sb., školský zákon, ukládá řediteli školy vydat školní řád a řediteli školského zařízení vnitřní řád, které mimo jiné upravují i ochranu dětí, žáků a studentů před sociálně patologickými jevy a před projevy diskriminace, nepřátelství. V této souvislosti Ministerstvo školství, mládeže a tělovýchovy, Česká školní inspekce, případně jiné odborné organizace a asociace poskytují organizační, metodickou, poradenskou i materiální podporu, jak řešit ve škole nebo školském zařízení negativní události, nevhodné chování nebo šikanu dětí, žáků a studentů. ***Vzhledem k existenci jiných účinných nástrojů, které méně zasahují do***

soukromí se kamerový systém stává posledním a vcelku nejméně účinným prostředkem na řešení šikany ve škole nebo školském zařízení.

V době covidové pandemie se rozšířilo používání video a audio přenosů za účelem **zachování výuky v krizových podmínkách**. Tento přenos obrazu a zvuku při on-line distanční výuce, případně i zkoušení lze považovat za zvláštní případ využití kamerového systému, přičemž není pochyb, že i v tomto případě dochází ke zpracování osobních údajů. Právním titulem zpracování osobních údajů za účelem zachování výuky, případně i zkoušení je plnění zákonné povinnosti.[2] Nicméně i pro toto zpracování by měl správce plnit relevantní povinnosti dle obecného nařízení, zejména dodržovat zásady zpracování osobních údajů (zejména minimalizace zpracování) podle čl. 5, informační povinnost podle čl. 13, povinnost vést záznamy o činnostech zpracování podle čl. 30 a povinnost zabezpečení zpracování podle čl. 32 obecného nařízení. Ministerstvo školství mládeže a tělovýchovy vydalo k problematice distančního vzdělávání metodiku[3], která se dané problematiky z hlediska zpracování a ochrany osobních údajů dotýká jen okrajově, kdy např. metodikou požadovaný autorizovaný přístup žáků a učitelů by bylo možno považovat za jedno z technických a organizačních opatření podle čl. 32 obecného nařízení.

Poznámka 1: Využití a nastavení kamer se může při distanční výuce lišit u žáků/studentů a u pedagogů s cílem minimalizovat zásah do soukromí.

Poznámka 2: Další digitalizaci školství, jako je rozšiřování distanční výuky žáků a studentů (on-line audio a video přenosem) na dobu mimo krizové podmínky, zavádění distančního zkoušení žáků a studentů, a to včetně ověřování jejich identity při těchto činnostech, by si zřejmě vyžádalo úpravu příslušných právních předpisů. V případě vysokých škol je již distanční forma nebo kombinace prezenční a distanční formy výuky součástí právních předpisů[4], a tak by její forma a náležitosti mohly být upraveny i vnitřními předpisy vysoké školy.

V naprosté většině případů bude právním důvodem provozování kamerového systému ve školách oprávněný zájem[5] správce.

Poznámka: Pokud by škola byla součástí prvku kritické infrastruktury (např. lékařské fakulty v rámci nemocnic) nebo by šlo o subjekty nakládající s chemickými, biologickými, radiologickými, jadernými škodlivinami, výbušninami a zbraněmi, které by mohly vyhovovat průřezovým kritériím pro stanovení prvků kritické infrastruktury, potom by kamerový systém byl realizován jako jedno z možných technických a organizačních opatření k zajištění ochrany prvku kritické infrastruktury a jeho umístění

[2] Viz § 25 a § 184a zákona č. 561/2004 Sb., školský zákon, a § 95c zákona č. 111/1998 Sb., o vysokých školách.
[3] Viz https://www.edu.cz/methodology/metodika-pro-vzdelavani-distancnim-zpusobem-2/.
[4] Viz § 44 zákona č. 111/1998 Sb., o vysokých školách.
[5] Čl. 6 odst. 1 písm. f) GDPR.

a parametry by se řídily právními předpisy a dalšími dokumenty (metodikami) připravenými pro zajištění povinností subjektu kritické infrastruktury.

Před nasazením kamerového systému na základě právního důvodu oprávněného zájmu správce je třeba provést balanční test, jehož cílem je vybrat takovou variantu řešení, která na základě existujícího reálného ohrožení naplní požadované účely s nejmenším možným dopadem do soukromí subjektů údajů. V rámci balančního testu by měl správce zvážit různé varianty řešení, tzn. jak varianty bez použití kamerového systému, tak varianty kombinující kamerový systém s jinými prostředky či opatřeními, které by mohly zajistit dosažení stanoveného účelu, například omezený počet kamer v kombinaci se vstupem na čipy vydané jednotlivým subjektům údajů (pro řízení vstupu), nebo omezený počet kamer v kombinaci s dohledem ostrahy (pro řízení vstupu), nebo omezený počet kamer v kombinaci se specializovanými nátěry fasád (pro omezení poškozování fasád objektů) apod.

Úřad pro ochranu osobních údajů nedoporučuje využití institutu souhlasu subjektů údajů jako právního základu, protože tento právní základ není dlouhodobě udržitelný, a to jak s ohledem na osoby navštěvující školu pravidelně (zaměstnanci, děti/žáci/studenti, zákonní zástupci žáků do určitého věku, učitelé a jiní zaměstnanci), které mohou souhlas nejenom neposkytnout, ale i kdykoliv odvolat, tak i s ohledem na osoby navštěvující školu nepravidelně nebo nahodile (např. poštovní doručovatelé, řemeslníci provádějící opravy v objektech, inspekce apod.), u kterých už vůbec nelze počítat s tím, že by měli důvod souhlas udělit.

Omezení zásahu do soukromí

Míru zásahu do soukromí ovlivňují v případě kamerových systémů následující parametry a nastavení kamerového systému:

- Umístění kamer – Např. kamera umístěná u vstupu do objektu představuje obecně menší zásah do soukromí než kamera umístěná přímo v učebnách.
- Počet kamer – Např. jediná kamera monitorující vstup subjektů údajů do objektu představuje obecně menší zásah do soukromí než velký počet kamer monitorující téměř nepřetržitě chování subjektů údajů.
- Režim kamer – Např. v počítačové učebně umístěná kamera, která je v provozu mimo dobu vyučování či přítomnosti oprávněných subjektů, nebo kamera s řízeným spouštěním (na základě hladiny intenzity zvuku nebo na základě pokynu obsluhy při výskytu mimořádných událostí apod.), představuje obecně menší zásah do soukromí než tatáž kamera v nepřetržitém provozu.
- Záběry kamer – Např. v počítačové učebně umístěná kamera, která snímá vstupní dveře, představuje obecně menší zásah do soukromí než tatáž kamera, která snímá celý prostor učebny.

- Využívání některých speciálních funkcí kamer – Např. běžné kamery představují obecně menší zásah do soukromí než kamery se záznamem zvuku, biometrické kamery či kamery používající umělou inteligenci pro analýzu záběrů v reálném čase. U kamerových systémů, které jsou využívány ke zpracování zvláštních kategorií osobních údajů (nejčastěji přicházejí do úvahy právě kamery s využitím biometrického rozpoznávání obličeje), musí správce kromě právního důvodu podle čl. 6 obecného nařízení určit a doložit rovněž právní důvod podle čl. 9 obecného nařízení.
- Doba uložení kamerového záznamu – Např. záběry uchovávané po dobu 72 hodin představují obecně menší zásah do soukromí než záběry uchovávané po dobu několika měsíců, a to z hlediska zvýšeného rizika jejich zneužití, nepřehlednosti uchovaných záznamů apod.
- Kromě toho ovlivňuje míru zásahu do soukromí i frekvence výskytu osob ve sledovaném prostoru.

Balanční test

V rámci balančního testu musí správce posoudit, zda nad jeho oprávněným zájmem, případně oprávněným zájmem třetích osob (např. ochrana majetku) nepřevažují zájmy, základní práva nebo svobody subjektů údajů, jejichž údaje zamýšlí prostřednictvím kamer zpracovávat**.** Je tedy odpovědností správce, aby takový test provedl. Proto Úřad předem nevylučuje umístění kamer kdekoliv v objektech škol, protože by to předjímalo výsledek balančního testu[6]. Nicméně je zřejmé, že pro některé umístění kamer bude pozitivní výsledek balančního testu pro správce velmi nepravděpodobný, typicky se bude jednat o kamery ve sborovnách, v kabinetech, ve třídách v době vyučování, kamery přenášející zvuk (s výjimkou distančního vzdělávání), kamery s využitím biometrického rozpoznávání obličeje, kamery ve sprchách a na toaletách apod. Takové kamery totiž velmi pravděpodobně budou představovat řešení, při kterém míra narušení práv a zájmů subjektů údajů výrazně převáží nad mírou zajištění práv a zájmů správce nebo třetích stran, přičemž v rámci balančního testu bude zpravidla možné nalézt přiměřenější řešení.

Z hlediska míry zásahu do soukromí lze umístění kamer rozdělit pro účely provedení balančního testu[6] a nastavení technických a organizačních opatření[7] do několika skupin:

- **Kamery s malým zásahem do soukromí**: kamery monitorující perimetr pozemků a objektů (při zachování zásady minimalizace monitorování okolních prostor), parkovací místa u škol na jejich pozemcích, případně jakékoliv kamery, zaměřené na možná místa vniknutí do prostor školy, které fungují pouze v době, kdy se

[6] Viz kapitola 3.2.1 Metodiky.
[7] Viz kapitola 3.9.3 Metodiky.

v záběru kamery nemá žádná osoba oprávněně vyskytovat (např. běžně nevyužívaná zadní branka areálu, střecha, oplocené plochy mezi pavilony bez přístup žáků či jiných osob).

- **Kamery se středním zásahem do soukromí**: kamery u vstupů do škol, šatny pro odložení svrchních oděvů (kabáty, čepice, obuv), vstupy do vybraných učeben (např. učebny se zařízením, kde jsou při mimořádné události způsobeny poměrně vysoké škody a následné narušení vyučování – počítačové, jazykové učebny), omezené záběry na ohrožená zařízení (jídelní a nápojové automaty, lednice, kopírky), omezené záběry na křížení pochozích koridorů u rozsáhlých škol.

  Poznámka: Je potřeba pečlivě vyhodnotit, zda šatny slouží pouze k odkládání svrchních oděvů. Pokud by v takových šatnách docházelo (třeba i nahodile) k převlékání například i do cvičebních úborů, byl by zásah do soukromí podstatně vyšší.
- **Kamery s vysokým zásahem do soukromí**: kamery v šatnách u tělocvičen a bazénů (pokud jsou vyhrazeny jiné prostory pro převlékaní subjektů údajů), chodby škol, hřiště, školní jídelny se záběrem na strávníky nebo personál.
- **Kamery s velmi vysokým zásahem do soukromí**: kamery v učebnách, kabinetech, kamery s využitím biometrického rozpoznávání obličeje, kamery se zvukovým záznamem, školní družiny

Rozdělení kamer do výše uvedených skupin lze využít v rámci balančního testu pro stanovení koeficientu zásahu do soukromí, viz kapitola 3.2.1 Metodiky, bod 2) „Posouzení dosažení účelu jinými prostředky (varianty) – kritérium potřebnosti", a také výslednou přehledovou tabulku ve vzorovém balančním testu, vzor 3 Metodiky. Nicméně je třeba také zohlednit i další nastavení a parametry kamer (viz níže). Zároveň je samozřejmě třeba při hodnocení variant též zohlednit jiná variantní řešení bez využití kamer nebo s omezeným využitím kamer v kombinaci s jinými opatřeními, s dopady do soukromí ještě nižšími nebo nulovými.

Rozdělení kamer do výše uvedených skupin lze též využít pro zařazení do tříd dle kapitoly 3.9.2 Metodiky, avšak vždy s ohledem i na další parametry a nastavení kamer (viz níže).

Správce při umístění některých kamer musí také zvážit problém monitorování zaměstnanců na pracovišti dle ustanovení § 316 zákona č. 262/2006 sb., zákoník práce. Přitom lze konstatovat, že u škol bude možné uplatnit výjimku pro zvláštní povahu činnosti zaměstnavatele podle § 316 odst. 2 uvedeného zákona, jen zcela výjimečně.

Poznámka: O uplatnění této výjimky by zřejmě bylo možné uvažovat (velmi vzácně u některých středních a vysokých škol) v případech, kdy zaměstnanci nebo studenti pracují se zbraněmi a výbušninami, případně s nebezpečnými chemickými či infekčními látkami.

Jak však bylo uvedeno výše, při zařazení kamery do skupiny z hlediska míry zásahu do soukromí musí být brán ohled i na další parametry a nastavení kamerového systému. Rizika zásahu do soukromí tak lze dále omezit. Například pokud u některých kamer zvolíme režim záznamu mimo obvyklou provozní dobu, mohou být takové kamery zařazeny do skupiny s nízkým zásahem do soukromí (například na hřištích s režimem monitorování po provozní době). Rovněž u kamer provozovaných pouze v režimu on-line se míra zásahu do soukromí může v určitých případech snížit. Ovšem jakkoliv může mít provozování kamer v režimu on-line výrazný dopad na zvolená technická a organizační opatření[8], pro účely zpracování balančního testu zůstává u některých kamer zásadní vlastní umístění a záběr kamer a režim provozování kamer nehraje významnou roli, typicky například u kamer umístěných v šatnách se pro účely balančního testu zásah do soukromí při režimu on-line nijak výrazně nesníží.

Doba uložení záznamu

Nezbytná doba uložení kamerových záznamů (pokud jsou pořizovány) musí být správcem stanovena, zdůvodněna a dokumentována jako nezbytně nutná pro zajištění účelu. Metodika v kapitole 3.1.5 uvádí příklad právě ze školství, kdy je možné běžnou dobu uložení stanovit na 7 dní s odůvodněním kratšími prázdninami, státními svátky a ředitelskými volny a na 3 týdny v době hlavních prázdnin z důvodu nepřítomnosti subjektů údajů. Pokud by však škola pronajímala sportoviště nebo se ve školní jídelně vařilo v době prázdnin pro některé další subjekty, potom delší dobu uložení nelze u dotčených kamer aplikovat.

Místo uložení kamerových záznamů

V zásadě mohou být kamerové záznamy uloženy:

- lokálně na paměťových zařízeních správce (školy),
- lokálně na paměťových zařízeních zpracovatele (například bezpečnostní služby),
- vzdáleně s využitím cloudových služeb.

Pokud půjde o vzdálené uložení kamerových záznamů s využitím cloudových služeb, musí správce v některých případech vyhodnotit (pokud například nevyužije poskytovatele cloudových služeb v ČR) též rizika vznikající při předávání kamerových záznamů do třetích zemí[9] a navrhnout přiměřená opatření (včetně volby vhodného poskytovatele cloudu) k jejich omezení. Poskytovatel cloudových služeb se většinou

[8] Viz tabulka 1 Metodiky.
[9] Viz https://uoou.gov.cz/profesional/predavani-osobnich-udaju-do-tretich-zemi-1.

bude nacházet v pozici zpracovatele, a správce by pak musel též plnit požadavky obecného nařízení týkající se uzavírání vztahů se zpracovateli[10].

Úřad doporučuje v tomto případě prověřit:

- zemi/země uložení kamerových záznamů,
- zda země uložení kamerových záznamů je zemí s odpovídající úrovní ochrany osobních údajů,
- přiměřenost technických a organizačních opatření zajišťujících bezpečný transfer a zabezpečení osobních údajů ve třetí zemi.

Poznámka 1: Kromě technických a organizačních opatření nabízených poskytovatelem cloudových služeb by měl správce analyzovat, zda nepotřebuje další dodatečná technická a organizační opatření přijatá na své straně k zajištění vhodných záruk ochrany osobních údajů v třetí zemi.

Poznámka 2: Určitým vodítkem, pokud bude zvolena možnost uložení kamerových záznamů v cloudu, by mohl být katalog cloud computingu na webových stránkách Digitální informační agentury[11], kde jsou jednotlivé služby cloud computingu předmětem ex-ante kontroly, zda má nabízená služba vlastnosti vyžadované pro zařazení do příslušné bezpečnostní úrovně pro využívání cloud computingu orgány veřejné správy.

Závěr

Při nasazení kamerového systému v rámci škol by tedy měl být zvolen následující postup:

- Správce osobních údajů popíše **existenci reálného ohrožení** (buď u konkrétního objektu, nebo typově shodného objektu), které hodlá omezit.
- Zváží možné **varianty řešení** (včetně variant bez umístění kamer).
- Pokud má být správcem osobních údajů škola, nemůže do **volby řešení** zasahovat jiný subjekt (například zřizovatel).
  Poznámka: Pokud by to byl zřizovatel školy, kdo určí účel a prostředky zpracování, navrhne umístění a parametry kamerového systému a bude mít (výhradní) přístup ke kamerovým záznamům, bude správcem osobních údajů tento zřizovatel, a nikoliv vlastní škola. V takové situaci však zřizovatel musí dobře zvážit účel zpracování, protože zajištění některých účelů (typicky zabránění šikaně, bezpečnost osob ve škole apod.) spadá do působnosti vlastní školy, a nikoliv jejího zřizovatele.

[10] Viz kapitola 3.4 Metodiky.
[11] Viz https://www.dia.gov.cz/oha/katalog-cloud-computingu/.

- Správce osobních údajů **přiměřeně zabezpečí zpracování osobních údajů** proti ztrátě důvěrnosti, dostupnosti a integrity osobních údajů, a to prostřednictvím přijetí technických a organizačních opatření.
- Navrhované řešení správce **konzultuje s pověřencem pro ochranu osobních údajů** (je-li jmenován), a to zejména z hlediska vyhodnocení a výběru řešení, včetně jeho parametrů (u kamerového systému včetně umístění kamer, počtu kamer, doby uložení záznamu apod.) a zabezpečení zpracování osobních údajů.
- Správce pravidelně **vyhodnocuje účinnost zvoleného řešení**, případně upravuje jeho parametry.
- Správce **zajišťuje práva subjektů údajů** dle obecného nařízení (zejména zajištění informovanosti subjektu údajů a právo na přístup k osobním údajům).