Kamerové systémy pohledem auditora

Mgr. Stanislav Klika
Director, Risk Advisory Services
BDO Audit s.r.o.
Stanislav.Klika@bdo.cz

Kamerové systémy a ochrana soukromí

Kamerové systémy jsou považovány za moderní a účinnou ochranu osob a majetku. Mohou však rovněž představovat velký zásah do soukromí sledovaných lidí. Toto riziko je více patrné zejména v případě, kdy dochází k rozsáhlému systematickému monitorování veřejně přístupných prostor či v kombinaci s využitím prostředků pro zpracování biometrických dat.

Do budoucna lze očekávat další rozvoj kamerových systémů a jejich častější nasazení při prosazování zájmů firem a různých organizací. Technický pokrok v této oblasti bude zřejmě ještě umocněn pokrokem ve zlepšování systémů umělé inteligence a přechodem na výkonnější 5G sítě.

Nastíněný vývoj také povede k většímu tlaku na správce a zpracovatele osobních údajů, regulátory a zástupce veřejnosti, pokud jde o pojetí soukromí a jeho ochranu.

Výhodu budou mít ty společnosti a organizace, které disponují účinným systémem ochrany osobních údajů a které již dnes zvládají náročné požadavky vyplývající z GDPR[1]. Interní auditoři mohou svým objektivním a metodickým přístupem velkou měrou přispět k tomu, že organizace tyto výzvy zvládnou.

Následující text je pojat jako pomůcka pro auditory a další příslušné pracovníky, kteří se nastavením a fungováním kamerového systému v organizaci budou zabývat. Jsou nastíněna hlavní rizika při provozování kamer a také opatření k jejich zmírnění. Při psaní článku jsem vycházel především ze zkušeností, které jsme získali při auditech nebo nastavování kamerových systémů u různých správců ze soukromého a z veřejného sektoru v České republice i v zahraničí. Doporučení vycházejí také z přísných požadavků Úřadu pro ochranu osobních údajů, které uplatňuje při kontrolách provozovatelů kamerových systémů.

Kamerový monitoring a GDPR

Sledování osob pomocí kamerových systémů nemusí vždy podléhat regulaci GDPR. Pokud není pořizován kamerový záznam, nejde z hlediska GDPR o zpracování osobních údajů a pravidla GDPR se na takovou činnost neuplatní. I v takovém případě však provozovatel kamer musí respektovat právo osob na soukromí.

Osobní údaje shromažďované pomocí kamerových systémů mají z povahy věci charakter obrazových záznamů. Stále častěji se však v praxi můžeme setkat s průmyslovými kamerami, které umožňují zaznamenávat

1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

také zvuk. Správci osobních údajů si však často nejsou vědomi, že některé z kamer touto schopností disponují. Přitom je takové, byť neúmyslné, zpracování zpravidla nepřiměřeným zásahem do soukromí a může znamenat porušení GDPR.

Pořizování běžných kamerových záznamů by nemělo být považováno za zpracování zvláštních kategorií osobních údajů („citlivých" údajů). O zpracování biometrických údajů totiž půjde teprve v těch případech, kdy budou obrazové záznamy zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby.

V drtivé většině případů budou správci osobních údajů kamerový monitoring podkládat právním titulem „oprávněné zájmy" podle čl. 6 odst. 1 písm. f) GDPR. Proto budou kamerové systémy typicky vyžadovat provedení tzv. balančního testu. Lze dodat, že zpracování na základě uděleného souhlasu není z praktického hlediska vhodné.

Provozovatel kamerového systému – správce osobních údajů by měl zajistit dodržení všech základních zásad GDPR. V souvislosti s kamerami to znamená především zohlednění zásad zákonnosti, korektnosti a transparentnosti, účelového omezení, minimalizace údajů, omezení uložení a integrity a důvěrnosti dat. Provozovatel kamer by tak měl provést revizi kamerového systému, a pokud to bude v daném případě relevantní, realizovat následující kroky spočívající v:

- stanovení účelu pořizovaného záznamu,
- nastavení záběrů kamer tak, aby kamery nezasahovaly nadměrně do soukromí monitorovaných osob,
- nastavení doby uchování kamerového záznamu,
- označení prostor zabíraných kamerovým systémem a zajištěním detailních informací o pořizování záznamu,
- zabezpečení kamerového systému a záznamů a
- vytvoření nezbytné dokumentace.

Stanovení účelu pořizovaného záznamu

Správce je povinen před zahájením zpracování stanovit účel zpracování osobních údajů. V souvislosti s kamerovými systémy takovým účelem nejčastěji bývá ochrana života a zdraví, ochrana majetku, včetně prevence před vandalizmem, a možnost opatření důkazů pro případná soudní a jiná řízení.

„Pořizování běžných kamerových záznamů by nemělo být považováno za zpracování zvláštních kategorií osobních údajů (‚citlivých' údajů)."

Nastavení záběrů kamer

Kamerový systém by měl přispívat k naplňování stanoveného účelu. Proto by kamery neměly zabírat prostory, které k dosažení daného účelu není třeba snímat. Následující modelová doporučení se vztahují k typickým situacím. Vždy je však nutné každý jednotlivý snímek posoudit vzhledem ke kontextu sledování a povaze zabíraných prostor. Často bude záležet také na detailech, jako je kvalita snímání či možnost přiblížení záběrů.

Ve většině případů by kamery neměly snímat prostory či nemovitosti, které nepatří danému správci. Výjimku budou tvořit zejména přímo přilehlá veřejná prostranství, jako jsou chodníky nebo části silnic či jiné cizí nemovitosti, pokud to bude možné legitimně odůvodnit. Takovým důvodem bude nejčastěji možnost identifikace pachatele (např. zaznamenání sprejera při činu).

V souladu s GDPR bude tedy snímání nemovitostí správce, parkoviště, které správce využívá nebo pláště budovy správce, včetně přilehlého chodníku či silnice. Zpravidla nevhodné bude snímání protilehlých budov, jejich oken či vchodů. Problematické může být také sledování zaměstnanců, včetně recepčních nebo obsluhy různých přepážek či výrobní linky. Účelem takového sledování by neměla být kontrola výkonu těchto zaměstnanců, ale ideálně zajištění jejich bezpečnosti. Správce by měl být schopen doložit tvrzená bezpečnostní rizika a současně zajistit, aby bylo sledování těmto rizikům přiměřené.

V případě problematických záběrů je nutné zhodnotit, zda je kamerový monitoring dostatečně vyvážen legitimním zájmem na sledování. Snímky, u kterých převáží zájem subjektů údajů na ochraně soukromí nad zájmem správce, bude nutné upravit. Obvykle lze požadované úpravy docílit vhodným vymaskováním části snímku nebo změnou úhlu náklonu kamery.

Délka doby uchování kamerového záznamu

Z GDPR vyplývá, že by kamerový záznam neměl být uložen déle, než je to nezbytné pro stanovený účel kamerového monitoringu. Obecně se doporučuje délka uložení nepřesahující několik dní. Z návrhu metodického pokynu Evropského sboru pro ochranu osobních údajů[2] (dříve Pracovní skupina WP29) vyplývá, že by měl správce dobu uložení delší než 72 hodin pečlivě odůvodnit.

2 Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím video zařízení, verze pro veřejnou konzultaci ze dne 10. 7. 2019

V praxi se pak doby uložení záznamů zpravidla pohybují v rozmezí tří až 14 dnů. Spíše výjimečně se setkáváme s reálnou potřebou uchovávat záznamy po delší dobu. Doba uložení trvající několik dní je v běžných případech k naplnění stanoveného účelu kamerového sledování dostačující. Řešili jsme však i případy, kdy s ohledem na objektivní okolnosti byla relevantní doba uchování i v délce několika měsíců.

Označení prostor zabíraných kamerovým systémem

Jedním z cílů GDPR je, aby lidé měli svoje osobní údaje pod kontrolou. Takový cíl by však nebyl možný, pokud by současně nedisponovali informacemi o tom, kdo, k čemu a jak jejich údaje používá.

Řešení informační povinnosti u kamer spočívá především v umístění informačních cedulí při vstupech do monitorované oblasti. Cedulky by měly být viditelné z dostatečné vzdálenosti a dobře čitelné. Za tímto účelem je vhodné, aby obsahovaly piktogram kamery. Dále by mělo být uvedeno, že prostor je monitorován kamerovým systémem se záznamem, jednoznačná identifikace správce osobních údajů a kontakt, kde je možné získat více informací o zpracování osobních údajů a kde mohou subjekty údajů uplatnit svoje případné požadavky.

„Problematické může být také sledování zaměstnanců, včetně recepčních nebo obsluhy různých přepážek či výrobní linky.“

Často se setkáváme s nedostatky s označením správce, který je za dané zpracování odpovědný. Není vždy zcela nezbytné tohoto správce jmenovitě na informační ceduli uvádět, pokud z okolností jednoznačně vyplývá jeho identita. Pro vyloučení pochybností však takový postup doporučujeme, zvláště pokud jsou kamery umístěny na nemovitosti, kde má provozovnu více firem nebo organizací. Další rozšířenou nepřesností je uvádění bezpečnostní agentury, která pro správce kamerový systém obsluhuje, namísto tohoto správce.

Realizace práv subjektů údajů a zásad zpracování osobních údajů

Správce se v souvislosti s provozováním kamerového systému bude setkávat s požadavky subjektů údajů nebo například policie. Faktická realizace těchto požadavků bude odvislá od technických možností a funkcionalit záznamového zařízení. Při výběru záznamového zařízení by měl správce zohlednit, zda toto zařízení umožňuje vyhledávat a mazat části záznamů, tyto záznamy exportovat nebo například umožňuje vymaskování záběrů. Moderní zařízení těmito funkcionalitami zpravidla již disponují.

Zabezpečení kamerového systému

GDPR ukládá správcům a zpracovatelům povinnost zajistit bezpečnost osobních údajů. Jak je však patrné z pokut uložených v členských státech Evropské unie či jak vyplývá z kontrol vykonaných Úřadem pro ochranu osobních údajů, zabezpečení údajů (resp. plnění požadavků podle čl. 32 GDPR) je spíše slabším článkem ve zpracování osobních údajů.

Provozovatel kamerového systému se musí zaměřit na všechny prvky jím provozovaného kamerového systému, včetně kamer, případné kabeláže a záznamových zařízení.

Součástí bezpečnosti je zejména nastavení přístupů a oprávnění uživatelů a vedení provozního deníku. V ideálním případě záznamové zařízení umožňuje vedení systémových logů, a lze tak zpětně dohledat, kdo, kdy a co dělal s kamerovými záznamy. Je také důležité, aby obsluha kamerového systému byla řádně proškolena.

Dokumentace kamerového systému

Správce osobních údajů odpovídá za prokázání souladu s GDPR, a to především v souvislosti s případnými kontrolami ze strany Úřadu pro ochranu osobních údajů. To je jedním z důvodů, proč je třeba vést dostatečnou dokumentaci kamerového systému.

Součástí takové dokumentace by mělo být zejména posouzení nezbytnosti zvoleného řešení, analýza rizik, záznamy o činnostech zpracování, detailní popisy kamerového systému, včetně přijatých organizačních a technických opatření, vnitřní předpisy, příslušná provozní a smluvní dokumentace a doložení plnění informační povinnosti.

Součástí dokumentace by měly být také provedené balanční testy a případně také posouzení vlivu na ochranu osobních údajů.

„Účelem takového sledování by neměla být kontrola výkonu těchto zaměstnanců, ale ideálně zajištění jejich bezpečnosti.“

Provedení balančního testu

Jak bylo uvedeno výše, správci zpravidla zakládají zpracování osobních údajů formou kamerového monitoringu na právním titulu „oprávněné zájmy“[3]. Způsobem jak ověřit, zda lze uvedeným právním titulem zpracování podložit, je tzv. balanční test.

Balanční test zkoumá, zda je možné v konkrétním případě osobní údaje zpracovávat, tedy zda nad oprávněnými zájmy správce nebo třetí strany zpracovávat osobní údaje nepřevažují zájmy subjektů údajů. V rámci balančního testu se mj. ověřuje, zda lze stanoveného účelu dosáhnout méně invazivními prostředky.

V praxi se setkáváme buď s pouze formálně provedenými testy, nebo naopak s dlouhými slohovými cvičeními, z kterých není na první pohled patrné, co je závěrem, a případně co lze nejlépe učinit k dosažení kladného výsledku testu.

Že se Úřad pro ochranu osobních údajů skutečně zajímá, zda a jak kvalitně byly provedeny balanční testy, je patrné například z nedávno zveřejněných informací o kontrolách uzavřených Úřadem v prvním pololetí roku 2019 (např. kontrola TOP 09, SPD či Student Agency).

Provedení posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů (DPIA) je povinné v případě, kdy je pravděpodobné, že určité zpracování bude mít (s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování) za následek vysoké riziko pro práva a svobody fyzických osob. Může se stát, že se správce ocitne v situaci, kdy bude mít povinnost takové posouzení provést.

Vodítka k určení, zda je nutné DPIA provést, stanoví například metodické doporučení Úřadu pro ochranu osobních údajů „K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)“. Jiným vhodným materiálem je také metodický pokyn bývalé Pracovní skupiny WP29 č. WP 248 [4]. Podle tohoto pokynu by měl správce vypracovat posouzení vlivu na ochranu osobních údajů v případě, kdy identifikuje přítomnost alespoň dvou rizikových faktorů zpracování, které pokyn popisuje. V souvislosti s kamerovými systémy je z povahy věci naplněno systematické sledování zpravidla veřejně přístupných prostor a u mnoha správců také zpracování rozsáhlého objemu dat. Do budoucna bude zřejmě častější také zpracování biometrických osobních údajů. ■

[3] Zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

[4] Guidelines on Data Protection Impact Assessment (DPIA) and determining whetherprocessing is “likely to result in a high risk” for the purposes of Regulation 2016/679.