Kamerové systémy se záznamem – analýza z hlediska GDPR

David Janota, červen 2018

Úvod

Jednoznačně nejčastější dotazy, které na auditech podle GDPR dostáváme se týkají kamerových systémů. Představitele firem zajímají odpovědi na otázky jako např. zda mohou mít na pracovišti kamery, kam mohou mířit, koho můžou natáčet, jak mohou data uchovávat, apod. Jelikož ani samotný Úřad pro ochranu osobních údajů nevydal žádný průkazně jasný materiál, kterým by se firmy mohly při implementaci řídit, přinášíme tento dokument a naše doporučení, podložené mimo jiné analýzou výsledků kontrol UOOU. Předem upozorňujeme, že se jedná o náš názor, který není v žádném případě soudně vymahatelný, jedná se čistě o náš pohled na toto téma.

Informace v tomto dokumentu se týkají výlučně **kamerových systému se záznamem.**

Právní rámec

Na kamerové sledování i pořizování záběrů osob se primárně vztahují ustanovení občanského zákoníku upravujícího podmínky ochrany soukromí, osobnosti a podoby člověka. V případě pořizování záznamu obydlí člověka jde o zásah do soukromí upravený v § 86 občanského zákoníku, který stanoví, že nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod.[1]

Provoz kamerového systému podléhá pravidlům GDPR (resp. jakékoliv ochrany osobních údajů) v momentě, kdy je toto prováděno automaticky a kdy je možno z uchovaného záznamu vyčíst charakteristické znaky osoby, typicky obličeje, ale také např. chůze. Důvod je jasný: dle GDPR (čl. 4, odst. 1) je osobní údaj „veškeré informace o identifikované nebo identifikovatelné fyzické osobě“ a „identifikovatelná fyzická osoba je fyzická osoba, kterou lze přímo či nepřímo identifikovat“. Z toho plyne první, bohužel z hlediska důvodu zavedení kamerového systému poněkud paradoxní zásada:

Aby se nejednalo o osobní údaj, osoba na kamerovém záznamu nesmí být přímo či nepřímo identifikovatelná.

Pokud tedy např. potřebujete kamerový záznam z důvodu detekce osob (ve smyslu někdo tam je, ale nemá tam být) v nějakém prostoru (např. zakázaném), pak je vhodné kameru dát do takové vzdálenosti (příp. snížit softwarové datový tok a tím rozlišení), aby nebylo možné rozlišit, o jakou osobu jde.

Zákonné důvody zpracování

Pro kamerový záznam platí stejné zásady jako pro všechny osobní údaje zpracovávané u správce: aby bylo zpracování legální, musí mít daný správce splněn jeden z šesti zákonných důvodů zpracování. Pro připomenutí, jedná se o (GDPR, čl. 6, odst. 1):

1. Souhlas
2. Plnění smlouvy
3. Právní povinnost
4. Životně důležité zájmy subjektu nebo jiné osoby

[1] UOOU, K provozování kamerových systémů, dostupné online na https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

5. Veřejný zájem nebo výkon veřejné moci
6. Oprávněný zájem správce

V této analýze úmyslně vynecháme souhlas. Lze jej samozřejmě použít v případě, kdy nelze použít žádný jiný právní důvod, nicméně souhlas je dle GDPR článku 7, odst. 3 kdykoliv odvolatelný. Dále vynecháme plnění smlouvy (např. natáčení reklamy u herců), veřejný zájem (natáčení zásahů příslušníků Policie ČR), životně důležité zájmy subjektu (monitorování pacientů na jednotce IP) a právní povinnost, nejvíc nás bude zajímat oprávněný zájem správce.

Zásady zpracování při oprávněném zájmu správce

Před jakýmkoliv zpracováním osobních údajů při použití oprávněného zájmu správce je nutno provést tzv. test proporcionality (test rovnováhy), zda je tento důvod oprávněný. V případě, pokud bude subjekt údajů reagovat námitkou proti zpracování, je nutno mu sdělit výsledky testu rovnováhy. Bohužel, na test rovnováhy není vydán UOOU žádný předpis nebo výkladové stanovisko, což se snad v budoucnu změní. V současné době doporučujeme sepsat na jedné straně práva subjektu a na straně druhé důvody, proč je kamerový systém zaveden.

Při použití kamerového systému je nutné dodržet několik hlavních zásad. Asi nikoho nepřekvapí, že nelze monitorovat prostory určené k ryze soukromým úkonům, např. WC nebo šatny. Dalším naprosto neoddiskutovatelným pravidlem je, že data včetně přenosových cest musí být zabezpečena a minimalizován počet osob (doporučili bychom maximálně dvě[2]). A samozřejmě je nutno mít sepsánu interní směrnici, definován proces porušení bezpečnosti ochrany osobních údajů (pravidla viz GDPR, čl. 33) a přistupující osoby povinně vyškolit.

Další důležitá zásada říká, že:

Kamerový systém je možno použít v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou stejně účinnou cestou.

Z toho plyne, že je nutno velmi dobře zvážit (a toto zdůvodnit), zda kombinací jiných prostředků (např. elektronickým zabezpečovacím systémem, čipováním zboží, apod.) nedosáhne správce stejného cíle se stejným účinkem. To jde ruku v ruce s tzv. principem minimalizace údajů – pokud data nepotřebuji k danému účelu, nesbírám je.

Není povoleno snímat laicky řečeno cokoliv, co není vaše, typicky tedy není možné snímat chodník, cestu, apod.

Dalším důležitým parametrem je doba uchovávání záznamů. UOOU říká, že „doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému ..... v zásadě však nepřesahující několik dnů ..... po uplynutí této doby vymazána[1]“. Pro shrnutí:

Smyčka by měla být dlouhá maximálně týden, data by poté měla být smazána.

Poslední zásada je jasná:

Osoba musí být o kamerovém systému informována nejen povinným piktogramem, ale i dalšími informacemi.

[2] V době tvorby této analýzy nebyl stále vydán oficiální návod pro stanovení vodítek pro nutnost vytvoření studie DPIA. V neoficiální je uvedeno (kritérium č. 5), že dané kritérium není kritické, ani důležité, pokud k daným datům přistupují max. 2 osoby.

Zde platí, že informace musí být poskytovány všem osobám, které se pracovišti mohou vyskytnout a to i náhodně, tzn. není např. možno tyto informace uvést na intranetu. Měly by obsahovat minimálně:

- určení totožnosti správce
- účel dohledu
- o době uchovávání záznamu
- (nepovinně) informace o tom, v jakých případech bude záběry zkoumat management společnosti
- (nepovinně) o případech, kdy budou záběry poskytnuty orgánům činným v trestním řízení.

Připomínáme, že se pořád bavíme o zpracování osobních údajů, takže i pro takové zpracování musí správce zabezpečit všechna pravidla definována v GDPR, např. možnost podat námitku, definovat účel, vypracovat informační povinnost, apod.

Praktické příklady

Několik důležitých citací z dokumentu pracovní skupiny WP29[3], ve kterých považují či nepovažují instalaci kamerového systému za oprávněný:

- ANO u stadionu nebo zastávkách MHD či prostředcích MHD v případě, že dojde k několika násilným aktům v blízkosti stadionu nebo pokud dojde opakovaně k napadení osob v autobusech v příměstských oblastech nebo v blízkosti autobusových zastávek.
- NE ve vozech MHD pro případ prevence inzultace řidičů autobusů a znečišťování vozidel
- NE u kontejnerů s cílem identifikace občanů, kteří se dopustí menších přestupků, jako je vyhazování pytlů s odpadky mimo kontejnery.
- NE odhalování osob odpovědných za příležitostné krádeže v prostorách bazénů.
- NE kamerové systémy zaměřené přímo na kontrolu kvality a objemu pracovní činnosti ze vzdáleného místa

Výsledky kontrol UOOU

V následujícím textu je uvedeno několik výsledků kontrol UOOU za 2. pololetí roku 2017.

- Kamerový systém na prostory, kde jsou umístěny výrobní linky.
    - Účel: kontrola výrobního procesu, bezpečnost zaměstnanců a prevence úrazů[4].
    - Výsledek: dochází k monitorování zaměstnanců (ani případné střídání zaměstnanců na jednotlivých pozicích nevede k tomu, že by nebyli významnou část pracovní doby monitorováni).
    - Návrh: snímání pouze striktně omezeného prostoru, kde je zvýšené nebezpečí úrazu zaměstnanců.
    - Sankce: neuložena, stav byl ihned napraven.
- Kamerový systém na dveře a venkovní prostory ve vlastnictví výrobní firmy
    - Účel: ochrana majetku
    - Výsledek: přípustné, dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. (ochrana práv a právem chráněných zájmů).
- Kamerový systém v bytovém domě
    - Účel: ochrana majetku

[3] Viz Stanovisko 4/2004, WP29.

[4] Zdůvodněno tím, že vedoucí pracovník může zajistit pomoc zraněnému zaměstnanci a následnou analýzou záznamu zjistit, jak přesně k úrazu došlo.

    - Výsledek: s výjimkou venkovní kamery (záběr i na parkoviště) přípustné dle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. (ochrana práv a právem chráněných zájmů).
    - Sankce: 5000 Kč, stav ihned napraven
- Kamerový systém v bytovém domě II.
    - Účel: nedefinován
    - Výsledek: porušení povinnosti správce osobních údajů, kamery jsou instalovány tak, že primárně sledují vchody do jednotlivých bytů, v daném případě přitom výrazně zasahují do soukromí obyvatel a tento zásah převažuje nad právem majitele bytového domu na ochranu jeho práv a právem chráněných zájmů.
    - Sankce: neznámá
- Kamerový systém městské části
    - Účel: monitorování veřejného prostranství a v budově sídla, dále na pracovištích
    - Výsledek: používání informačních cedulek, které byly nevhodné z hlediska jejich velikosti nebo v několika případech obsahovaly zavádějící text. Dále zaclonění vnějších kamer, postupné odstraňování nadbytečných kamer, vyměněny informační cedulky.
    - Sankce: 50 000 Kč

Pozor, tyto sankce byly uděleny před platností GDPR, v současné době mohou být mnohem vyšší.

Doporučení a závěr

Jak bylo řečeno v úvodu, UOOU nevydal žádné konkrétní návody, jak se s těmito systémy vypořádat. Uvádíme proto seznam doporučení zejména na základě důsledného sledování výsledků kontrol a na základě všech zásad uvedených v předchozím textu. Zároveň upozorňujeme na fakt, že striktní aplikování těchto zásad může snížit pravděpodobnost udělení pokuty, nikoliv se jí ale bezpečně vyhnout.

1. Velmi dobře definujte účel a doložte, že ke sledování kamerovými systémy máte dobrý důvod (časté krádeže, rizikový prostor, apod.), doložte do testu proporcionality (rovnováhy).
2. Proveďte a sepište analýzu, že neexistuje jiný prostředek ke stanovenému účelu než kamerový systém (pokud existuje, kamery raději odinstalujte).
3. Délku smyčky stanovte maximálně týden.
4. Nikdy nesledujte komplexně celý prostor (např. tzv. rybí oko v rohu), pouze prostory, ve kterých se může něco zvláštního stát (úraz, vstupní dveře, pokladna, apod.)
5. Snažte se zvolit takový úhel, ve kterém není vidět obličej dané osoby (např. kamera na výrobní lince snímající pouze ruce, kamera na nákladové rampě snímající pouze výkladový prostor tahače, apod.).
6. Pokud z nějakého důvodu musíte snímat celý prostor, musí být vzdálenost tak velká, aby nemohlo dojít k identifikaci dané osoby, ale např. pouze k identifikaci podezřelé aktivity (osoba v nebezpečném prostoru, apod.).
7. Zacloňte kamery tak, aby nesnímaly žádný veřejný prostor (chodníky, parkoviště, apod.)
8. Zaměřte se na analýzu toho, zda se v daném úhlu kamery nevyskytuje převážně definovaná skupina pracovníků po definovanou časovou jednotku (např. záběr na recepci s recepční).
9. Důkladně zabezpečete jak přenosové cesty (https, VPN, vlastní okruh WiFi), tak samotný záznam (šifrování, serverovna s klíčem).
10. Minimalizujte počet přistupujících osob k záznamu.
11. Všude instalujte raději větší tabule, uveďte na nich všechny definované informace (viz výše).
12. Definujte záznamy zpracování (defacto mírně modifikovaná datová mapa).
13. Sepište a vystavte (např. na internetu) informační povinnost dle čl. 13 a 14.
14. Proveďte si analýzu, zda je nutno vypracovat DPIA a pokud bude výsledek kladný, vypracujte DPIA.
15. Pokud už dojde ke kontrole z UOOU, aktivně spolupracujte a snažte se daný problém odstranit ještě během kontroly.