Pokyny ke zpracování osobních údajů prostřednictvím videozařízení

1 Nutnost definovat zákonnost a účel zpracování

1.1 Ve většině případů se jedná o **oprávněný zájem** správce osobních údajů a s tím související účel – ochrana majetku:

- Musí se jednat o závažný oprávněný zájem, který převažuje nad zájmy, právy a svobodami subjektu údajů (v žádném případě nesmí být kamery instalovány na sociálních zařízeních, v šatnách, zachycující stoly určené k odpočinku či ke stravování apod.)
- Takové zpracování musí být nezbytné – je vhodné si položit otázku, zda nelze účel naplnit jinými způsoby (např. oplocení pozemku, zavedení pravidelných pochůzek, využívání vrátných, lepší osvětlení, bezpečnostní zámky, nerozbitná okna a dveře apod.)
- Oblast snímaných prostor by měla být co nejvíce omezená a správce by měl využívat technické prostředky k tomuto omezení jako je např. blokování nebo rozostření nerelevantních prostor (např. prostory, které zabírají kromě pokladny i stoly, kde se lidé stravují, nebo kromě vchodu do budovy i přilehlý chodník či parkoviště apod.).
- Doporučujeme oprávněnost zdokumentovat historií – např. vážné incidenty v minulosti (datum, způsob, finanční ztráta)

1.2 V některých případech se může jednat o úkol prováděný **ve veřejném zájmu** nebo **při výkonu veřejné moci**

1.3 Zcela výjimečně pak o zpracování na základě **souhlasu**

2 Zpřístupnění videozáznamů třetím stranám

2.1 Předání musí odpovídat původně stanovenému účelu. Záznam pořízený za účelem ochrany majetku se v případě škody na majetku může předat právnímu zástupci správce případně donucovacím orgánům, záznam však nemůže být předán např. marketingové společnosti pro vyhodnocení návštěvnosti

2.2 Nezapomeňte, že každé takové předání musí být řádně zdokumentované a odůvodněné (např. písemná žádost Policie ČR, záznam o předání v Knize ke kamerovému systému apod.)

3 Zpracování zvláštních kategorií údajů

- např. biometrické údaje, zdravotní stav, náboženské vyznání, členství v odborech, politické názory apod.

Údaje shromážděné prostřednictvím videa mohou být použity k odvození dalších informací pro dosažení jiného účelu (např. zmapování zvyků jednotlivce). Je tedy velmi důležité, abyste měli pod kontrolou záběry jednotlivých kamer. Proto navrhujeme provést následující kroky:

- Projděte všechny záběry a položte si otázku, zda zabírají opravdu pouze ty prostory, které zabírat mají v souladu se stanoveným účelem
- Nedochází ke snímání veřejných prostor – např. kostela, vchod do specializovaného zdravotnického zařízení (psychiatrie, léčení závislostí) apod.?
- Nejsou pořizovány záznamy z akcí, které mají politický podtext, případně ze schůzí odborové organizace?
- Používáte metodu rozpoznávání obličeje (zpracování biometrických údajů)?

Pokud dojdete k závěru, že zpracováváte zvláštní kategorii údajů, pak je nutné toto zpracování provádět pouze na základě výjimek dle č. 9, odst. 2 GDPR. V tomto případě doporučujeme kontaktovat vašeho pověřence pro ochranu osobních údajů a v každém případě zpracovat Posouzení vlivu (viz bod 8).

4 Práva subjektu údajů

4.1 Subjekt má právo si vyžádat informaci, zda byl v určeném čase a místě nahráván, případně si může vyžádat i tuto nahrávku. Správce má pak povinnost informovat subjekt údajů, zda k nahrávání dochází/docházelo a v případě, že je to možné mu nahrávku zpřístupnit. Nesmí však dojít k omezení práv a svobod třetích osob – v tomto případě se doporučuje rozostřit obraz, kde se nachází třetí osoby, případně odmítnout předání, pakliže by úpravy záznamu byly technicky neproveditelné.

4.2 Pokud správce automaticky maže veškeré záznamy například do dvou dnů, může subjekt údajů získat přístup jen k této informaci (neboť materiál byl již smazán), ale pouze pokud žádost byla podána správci po těchto dvou dnech! Zde upozorňujeme na správci často využívané účelové pozdržování odpovědi na žádosti s cílem neposkytnout požadované údaje se zdůvodněním, že je nahrávka již smazána. Na tuto praktiku je kontrolní orgán citlivý a vždy je lepší dát si práci se zdůvodněním, proč je nemožné nahrávku poskytnout (technická náročnost, výskyt třetích osob apod.), než žádost účelově pozdržet do doby automatického smazání záznamu.

5 Transparentnost a informační povinnost

- doporučuje se používat tzv. 2 vrstvy informací

5.1 **První vrstva** – umístění varovného oznámení před vchodem do monitorovacích prostor – **informační cedule**, která bude umístěna přibližně ve výši očí, bude dostatečně velká a informace na ní budou uvedeny dostatečně velkým písmem (velikost by měla být podobná jako u ostatních informačních tabulí). Tato cedule by měla dle Sboru obsahovat následující informace:

- Identita správce + kontakt na pověřence/správce
- Právní titul a účel
- Informaci, zda se jedná o zařízení se záznamem
- Informaci, zda jsou záznamy předávány a případně komu
- Práva subjektu údajů

- Odkaz na podrobnější informace – např. na webové stránky, recepci apod.

5.2 **Druhá vrstva** – musí obsahovat všechny povinné informace dle článku 13 GDPR. Přístup k těmto informacím musí být možný i bez vstupu do monitorované oblasti. Toho lze dosáhnout např. odkazem na webové stránky nebo uvedením tel. čísla.

6 Doba zpracování

6.1 Opět upozorňujeme, že doba uchovávání záznamů by měla být v řádu několika dnů (v návaznosti na účel). V odůvodněných případech lze tuto dobu prodloužit o další dny – víkendy, svátky apod. Evropský sbor zmiňuje hranici **72 hodin**, za touto hranicí je nutné mít k dispozici rozsáhlejší argumentaci pro legitimitu účelu a nezbytnost uchování! Tedy opět doporučujeme vypracovat Posouzení vlivu.

7 Technická a organizační opatření

7.1 Správci údajů by měli vytvořit interní rámec a politiku, kde budou popsána technická a organizační opatření. Proto doporučujeme vypracovat **Směrnici pro provoz kamerového systému** a **Posouzení vlivu na ochranu osobních údajů**, pokud je potřebné.

7.2 Příklady relevantních organizačních opatření:

- Určit osoby zodpovědné za správu a provoz kamerového systému
- Stanovit účel a rozsah
- Určit přípustné a zakázané použití (např. zákaz skrytých kamer)
- Definovat opatření týkající se transparentnosti (viz bod 5)
- Definovat způsob nahrávání, délku uchovávání záznamů, délku archivace v případě bezpečnostních incidentů
- Určit osoby, které musí absolvovat příslušné školení a kdy
- Vyjmenovat osoby/pozice, které mají přístup k záznamům a za jakým účelem
- Stanovit provozní postupy (např. kým a odkud je monitorováno, jak postupovat v případě porušení ochrany dat)
- Stanovit postupy při nákupu videozařízení, instalaci a údržbě (včetně instalace nových kamer)
- Stanovit postupy v případě incidentu a nápravné postupy

7.3 Příklady relevantních technických opatření:

- Ochrana proti krádeži, vandalismu, náhodným poškozením apod.
- Ochrana přenosu záznamů komunikačními kanály zabezpečenými proti narušení
- Šifrování dat
- Používání antivirových systémů, firewallů apod.
- Zabezpečení prostor, kde dochází k ukládání záznamů proti neoprávněnému přístupu třetích stran
- Umístění monitorů takovým způsobem, aby je mohli vidět pouze oprávnění operátoři
- Stanovení postupů pro udělení, změnu a odvolání fyzického a logického přístupu

- Ověřování a autorizace uživatelů – dostatečná síla hesla a frekvence jeho změny
- Logování operací

8 Posouzení vlivu na ochranu osobních údajů

8.1 Správci jsou povinni provádět Posouzení vlivu na ochranu osobních údajů (DPIA), pokud je pravděpodobné, že daný typ zpracování dat může mít za následek vysoké riziko pro práva a svobody fyzických osob, pokud zpracování představuje rozsáhlé systematické monitorování veřejně přístupných prostor nebo pokud správce zamýšlí zpracovávat zvláštní kategorie údajů ve velkém měřítku.

8.2 Z výše uvedeného je důvodné předpokládat, že videodohled bude ve většině případů vyžadovat Posouzení vlivu. Zde doporučujeme kontaktovat vašeho pověřence pro ochranu osobních údajů, který by vám měl v této záležitosti doporučit další postup.

Závěrem je nutno uvést, že právě **Posouzení vlivu** je nejen v mnoha případech nutný, ale i velmi užitečný nástroj, který správci osobních údajů pomůže zmapovat rozsah zpracování, jeho zákonnost, účely a s tím související oprávněnost. Na základě této analýzy pak správce může přijmout všechna potřebná opatření, aby toto zpracování bylo v souladu se zásadami GDPR a aby se tak vyhnul zbytečným pokutám!