Metodika

k návrhu a provozování kamerových systémů
z hlediska zpracování a ochrany osobních údajů

Verze 0.98.3 ze dne 24. dubna 2023

Obsah

1. Úvod

V roce 2012 Úřad pro ochranu osobních údajů vydal publikaci Provozování kamerových systémů s podtitulem Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů. Tato metodika byla v určité době nejstahovanější publikací Úřadu. Mezitím uběhlo několik let. S přijetím nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále též GDPR nebo obecné nařízení o ochraně osobních údajů), a následně také Pokynů Evropského sboru pro ochranu osobních údajů č. 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky (dále jen Pokyny EDPB 3/2019), došlo k určitým změnám (např. zrušení registrace zpracování osobních údajů, upřesnění výkladu práv subjektů údajů), kterými se povinnosti správců pozměnily nebo upravily. V souvislosti s těmito změnami vyvstala také možnost či potřeba dokument aktualizovat a upravit. Předkládaný dokument Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů aplikuje požadavky obecného nařízení o ochraně osobních údajů na specializované zpracování osobních údajů kamerovými systémy.

Metodika (jak již název napovídá) není dokumentem, jehož dodržování by bylo pro jakýkoliv subjekt povinné. Správce může najít jiný způsob splnění povinností daných obecným nařízením o ochraně osobních údajů (například postupem dle jiné metodiky, nebo prostým shromážděním dokladů o plnění jednotlivých požadavků GDPR při zřízení a provozování kamerového systému). Cílem metodiky je přispět k jasnějšímu výkladu některých povinností v oblasti zpracování osobních údajů kamerovými systémy. Metodiku mohou využít všechny subjekty podílející se na zřízení nebo provozu kamerových systémů, a to s cílem:

- vytvoření kamerového systému, který co nejméně zasahuje do práv a svobod subjektů údajů, a přitom zachovává/zajišťuje práva a svobody správce;
- provozování kamerového systému v souladu s obecným nařízením o ochraně osobních údajů.

2. Popis kamerového systému

2.1.Technický popis kamerového systému

Kamerový systém zahrnuje:

- provádění operací zpracování v rámci kamerového systému
    - generování snímků, tj. vytvoření obrazu skutečného světa v definovaném použitelném formátu,
    - přenos snímků v rámci systému,
    - zobrazení, zpracování a ukládání snímků (poslední dva jen u kamer se záznamem).
- řízení kamerového systému
    - správa činností a některých údajů, která zahrnuje zpracování příkazů pracovníka a provedení činností systémem, které se netýkají přímo zpracování

osobních údajů (generování upozornění a poplachů), a dále například vytvoření a správa metadat, systémových dat a externích zdrojů dat,
    - připojení kamerového systému k jiným systémům (může sem patřit kontrola přístupu, požární poplach, správy budov, automatické rozpoznávání registračních značek při vpuštění pro parkování apod.),
- bezpečnost kamerového systému, tj. zajištění dostupnosti, důvěrnosti a integrity údajů, které se realizuje prostřednictvím přijatých technických a organizačních opatření.

2.2 Stupeň identifikace (osoby)

Stupně velikosti obrazu, jak je definuje norma,[1] mohou být použity k určení míry identifikace osoby jak v online kamerových systémech, tak v kamerových systémech se záznamem. Hodnoty jsou odvozeny od systému PAL, takže v jiných systémech (s jiným digitálním rozlišením) musí být údaje dle jednotlivých stupňů modifikovány na srovnatelnou úroveň (i zde uvádí převodní tabulku citovaná norma):

monitorování – cíl zabírá 5 % výšky obrazu v systému PAL, nebo více než 80 mm na pixel,
zjištění – cíl zabírá 10 % výšky obrazu v systému PAL, nebo více než 40 mm na pixel,
pozorování – cíl zabírá 25 % výšky obrazu v systému PAL, nebo více než 16 mm na pixel,
rekognoskace – cíl zabírá nejméně 50 % obrazu v systému PAL, nebo více než 8 mm na pixel,
identifikace – cíl zabírá nejméně 100 % obrazu v systému PAL, nebo více než 4 mm na pixel,
prozkoumání – cíl zabírá 400 % obrazu v systému PAL nebo více než 1 mm na pixel, tj. záběr zabírá jen část postavy,

Stupně velikosti obrazu ***monitorování a zjištění*** mohou být při řešení mimořádných událostí využity v on-line systémech, které umožňují rychlou reakci pozorovatele v případě takové události mezi neidentifikovanými subjekty nebo jiného typu mimořádné události (požár, povodeň, havárie apod.). V oblasti zpracování osobních údajů tyto dva stupně velikosti obrazu (***monitorování, zjištění***) při nasazení kamerových systémů se záznamem nemají smysl, resp. nelze určit účel, pro který by měly být provozovány, protože bez vynaložení nepřiměřeného úsilí (například kombinaci s dalším informacemi získanými mimo kamerový systém) neumožňují identifikovat účastníky mimořádné události. Využití kamerových systémů s takovým rozlišením (ať už v režimu on-line nebo v režimu se záznamem) není považováno za zpracování osobních údajů. Stupeň velikosti obrazu ***pozorování a rekognoskace*** může být použit v oblasti zpracování osobních údajů jak v online systémech, tak v kamerových systémech se záznamem, a provedení identifikace je jen omezené, a to pouze ve spojení s dalšími znaky nebo dalšími charakteristikami nebo objekty spojenými s osobou, jako je oblečení, standardní chování (pravidelné pochůzky), použité pomůcky nebo nástroje (hole, vozíky, nářadí), domácí zvířata (psi), automobil, stavba v okolí (rodinný dům) apod. Stupně velikosti obrazu ***identifikace a prozkoumání*** mohou být použity jak v online systémech, tak v kamerových systémech se záznamem a umožňují ztotožnění osob.

Možnost identifikace osob ovlivňují ještě další faktory [světelné podmínky, světelné odrazy, dočasné zakrytí (listí, dočasný mobiliář, osoba), maskování osoby (např. rouška nebo

[1] Viz ČSN EN 62676-4 Dohledové systémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace.

respirátor, kapuce, čepice, sluneční brýle), intenzita pohybu v záběru (při intenzivním pohybu osob může například dojít k nemožnosti identifikace konkrétní osoby, protože je překryta jinými pohybujícími se osobami)]. Tyto faktory by měly být zohledněny při návrhu kamerového systému s ohledem na jeho účel.

2.3 Popis operací zpracování

Kamerový systém se záznamem: Zpracování obrazového záznamu z kamerového systému (snímání, přenos, zobrazení, zpracování, ukládání, výmaz), a to včetně využití fotopastí.
Kamerový systém v režimu online: Prohlížení online záběrů z kamerového systému (snímaní, přenos, zobrazení). Kamerový systém využívaný v režimu online představuje zpracování osobních údajů, jak vyplývá například z § 29 Pokynů EDPB 3/2019.

3. Požadavky na zpracování osobních údajů kamerovým systémem

3.1 Zásady zpracování osobních údajů

3.1.1. Korektní, zákonné a transparentní zpracování osobních údajů

Korektní, transparentní a zákonné zpracování osobních údajů je zajištěno zejména prostřednictvím určení právního základu zpracování osobních údajů, dodržováním práv subjektů údajů (řešeno v části 3.2) a zabezpečením osobních údajů (řešeno v části 3.8).
U kamerových systémů přicházejí v úvahu následující právní základy zpracování osobních údajů:

- **Zpracování je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby.**[2]

  Tento právní základ se v praxi využívá nejčastěji. Správce dokládá (viz balanční test), že oprávněný zájem existuje, přičemž u kamerových systémů je dán existencí reálného ohrožení, které lze doložit:

  - mimořádnými událostmi v monitorované oblasti – týkajícími se přímo monitorovaného objektu, případy z okolí/okolních objektů, policejními případy nebo statistikami týkající se příslušného území, NEBO
  - statisticky častým výskytem bezprostředního nebezpečí v druhově obdobných objektech (čerpací stanice) nebo v objektech s výskytem cenných hodnot nebo vysokých objemů peněžních prostředků (klenotnictví, banky, pošty) apod., daným například počtem mimořádných událostí za rok, NEBO
  - mimořádnými událostmi a bezprostředním nebezpečím týkajícím se veřejných dopravních prostředků s doloženým výskytem vyššího počtu mimořádných událostí, tj. na určitých trasách, v určitých hodinách nebo zajišťujících dopravu na určité akce, a to například počtem mimořádných událostí na trasu za rok.

[2] Čl. 6 odst. 1 písm. f) GDPR.

Trvající existence oprávněného zájmu se pravidelně vyhodnocuje.

- **Zpracování se provádí na základě souhlasu subjektů údajů.**[3]

  Využití tohoto právního základu ÚOOÚ nedoporučuje, pro úplnost je však uveden. Zpracování kamerových záznamů postavené na souhlasu je totiž jen problematicky dlouhodobě udržitelné, protože postačuje odvolání souhlasu jednoho ze subjektů údajů, případně nesouhlas jednoho z nových subjektů údajů, do jehož práv a soukromí kamerový systém zasahuje, a správce musí kamerový systému omezit nebo vypnout. Proto se uplatní ne příliš často, a to v případech, kde není možné provozovat kamerový systém na jiném právním základě, a pouze tam, kde je možné vymezit okruh monitorovaných osob – některé kamery v bytových domech a školách. Následující text řeší pouze problém náležitostí souhlasu se zpracováním osobních údajů, pokud jsou osobní údaje zpracovány na jeho základě:

  - týká se pouze subjektů údajů, které se v monitorovaném objektu/prostoru vyskytují pravidelně (např. žáci, studenti, obyvatelé domu apod.),
  - za nezletilé nebo nesvéprávné subjekty údajů uděluje souhlas jejich zákonný zástupce (u nezletilých souhlas zákonného zástupce požadovat do věku 15 let;[4] od tohoto věku se předpokládá, že subjekt údajů dokáže posoudit rozsah a hloubku zásahů do soukromí a je tedy schopen udělit souhlas se zpracováním osobních údajů sám),
  - udělení souhlasu se naopak netýká subjektů údajů, jako jsou návštěvy, dodavatelé (včetně dodavatelů poštovních zásilek) a další osoby vstupující do monitorovaného objektu/prostoru nahodile/krátkodobě /nepravidelně,
  - udělení souhlasu musí být svobodným, vědomým a informovaným projevem vůle subjektu údajů, případně jeho zákonného zástupce (udělení souhlasu musí být jasně odlišitelné a nesmí být součástí dokumentů pro uzavření jiných vztahů),
  - správce musí být schopen doložit platný souhlas subjektů údajů po celou dobu zpracování osobních údajů,
  - subjekt údajů, případně i jeho zákonný zástupce, musí být před nebo nejpozději při udělení souhlasu informován o zpracování osobních údajů,[5]
  - v případě zásadních změn v rozmístění a nastavení kamerového systému (týká se změny účelu zpracování, zvýšení počtu kamer, přesunu kamer nebo záběru kamer do prostor se zvýšenou ochranou soukromí, změny režimu kamerového systému ve smyslu rozšíření doby monitorování, prodloužení doby uchování záznamu, snížení ochrany kamerového systému nebo kamerových záznamů) musí správce subjekty údajů o

[3] Čl. 6 odst. 1 písm. a) GDPR a kapitola 3.3 Pokynů EDPB 3/2019.
[4] § 7 zákona č. 110/2019 Sb., o zpracování osobních údajů.
[5] Čl. 13 a čl. 14 GDPR a zde níže kapitola 3.6.1.

těchto změnách informovat a získat jejich souhlas s takto zásadně změněným zpracováním osobních údajů,

- správce musí mít zpracovány postupy obsahující jasné a jednoznačné kroky pro situaci, kdy subjekt údajů souhlas se zpracováním osobních údajů odvolá, a pro situaci, kdy se objeví nový relevantní subjekt údajů, který souhlas se zpracováním osobních údajů neudělí.

- **Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce** [6] nebo **je zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje.**[7]

V úvahu přichází např. zákon č. 273/2008 Sb., o Policii ČR; zákon č. 553/1991 Sb., o obecní policii; zákon č. 17/2012 Sb., o celní správě; zákon 412/2005 Sb., o ochraně utajovaných informaci a o bezpečnostní způsobilosti apod.

Poznámka: Specifické podmínky provozování kamerových systémů tohoto typu, dané možností zákonného uplatnění výjimek z povinností správce dle GDPR, metodika neřeší, avšak i správcům takových kamerových systémů mohou některé části metodiky napomoci při návrhu a provozování těchto kamerových systémů takovým způsobem, aby co nejméně zasahovaly do práva na soukromí subjektů údajů.

3.1.2 Definice legitimních účelů pro zpracování osobních údajů

Účelem zpracování osobních údajů je identifikace osob vstupujících do záběru kamer nebo monitorování procesů a dějů, a to zejména pro následující účely (stanovené obvykle v návaznosti na doložení reálného ohrožení dle kapitoly 3.1.1.):

- zvýšení ochrany majetku (krádež, vloupání, vandalismus, přírodní pohromy, havárie),
- zvýšení bezpečnosti osob (napadení, loupež, krádež, jiná fyzická újma) = ochrana života a zdraví osob,

Doplňkové účely k předchozím mohou být:

- prevence mimořádných událostí a optimalizaci opatření pro snížení pravděpodobnosti výskytu mimořádných událostí (nepostačuje jako jediný účel),
- získávání důkazního prostředku pro příslušné odpovědné orgány (soudy a Policie ČR v případě trestných činů, obecní úřady v případě řešení přestupků, jiné veřejné subjekty pro výkon zákonem jim svěřených kompetencí apod.),
- získávání materiálu pro řešení pojistných událostí (s věcně příslušnou pojišťovnou).

Správce uvede účely platné pro jeho kamerový systém, případně jednotlivé kamery kamerového systému, pokud mají účel odlišný.

3.1.3 Minimalizace zpracovávaných údajů

Je nutné určit, zda je zpracováván obrazový záznam z kamerového systému (od snímání až po případné uložení a vymazání) nebo jen obraz z kamer. Nezbytně nutný rozsah zpracování osobních údajů je určen na základě provedení balančního testu k nasazení kamerového systému, který obecně sestává ze tří kroků:[8]

[6] Čl. 6 odst. 1 písm. e) GDPR.
[7] Čl. 6 odst. 1 písm. c) GDPR.
[8] Konkrétní příklad provedení balančního textu k nasazení kamerového systému viz vzor 3.

- **i) Posouzení dosažení účelu jinými prostředky (varianty) – kritérium potřebnosti**
  Posouzení spočívá v návrhu, porovnání a určení pořadí variant opatření, kterými lze dosáhnout stanoveného účelu, přičemž varianty kamerového systému mohou být typicky definovány:
  - ***počtem a umístěním kamer**, které minimalizují zásah do soukromí, a to pouze na nezbytných místech,*
  - ***nastavením záběru kamer,** kterým se minimalizuje zásah do soukromí (natočením kamery, rozostřením/zakódováním části záběru, vymaskováním, tj. zakrytím části záběru),*
  - ***režimem kamerového záznamu**, kterým se minimalizuje zásah do soukromí monitorovaných osob (kontinuální kamerový záznam, záznam na základě snímaní pohybu, záznam v době mimo přítomnost oprávněně vstupujících osob, záznam na základě pokynu obsluhy, automatické přepisování záznamu novým po určité době bez zásahu obsluhy apod.),*
  - ***deaktivováním některých funkcí kamer dalších součástí kamerového systému,** kterým se minimalizuje zásah do soukromí monitorovaných osob (pohyb/otáčení kamer, použití transfokátoru, rádiový přenos dat, pořizování zvukových záznamů, pořizování biometrických charakteristik),*
  - ***použitím jiných prostředků, než jsou kamerové systémy** (řízení přístupu do prostor – například vstupy na čipy, speciální nátěry – antivandal apod.),*
  - ***zohledněním nulové nebo stávající varianty***

  Poznámka: Správce navrhne varianty řešení, které v minimálně požadované úrovni zajistí jím definovaný účel. Tyto varianty porovná se stávajícím nebo nulovým řešením. Výsledkem porovnání je určení pořadí variant z hlediska nákladů, přínosů a zásahu do soukromí.
- **ii) Posouzení nezbytnosti vybrané varianty – kritérium vhodnosti**
  Poznámka: Zde se nejvýhodnější a nejpotřebnější varianta, vybraná v rámci i) posouzení dosažení účelu jinými prostředky, posuzuje z hlediska toho, zda je pro správce vhodná, tj. zda je její realizace nezbytná a přínosná. Proto by měla být provedena analýza nefinančních přínosů realizace, analýza škod a analýza návratnosti řešení. Pokud by některá z uvedených analýz měla záporný výsledek, bylo by nutné považovat vybranou variantu za nevhodnou a provést posouzení nezbytnosti zpracování osobních údajů pro variantu, která skončila v rámci i) posouzení dosažení účelu jinými prostředky jako další v pořadí, až k nalezení skutečně vhodné varianty.
- **iii) Posouzení přiměřenosti zpracování osobních údajů – kritérium poměřování**
  Poznámka: Správce provede porovnání v kolizi stojících práv a zájmů správce a práv a zájmů subjektů údajů, a to včetně analýzy očekávání subjektů údajů, analýzy postavení správce vůči subjektů údajů a popisu dodržování základních zásad zpracování osobních údajů. Pokud by posouzení přiměřenosti mělo záporný výsledek, bylo by nutné považovat vybranou variantu za nepřiměřenou a provést posouzení přiměřenosti pro variantu, která skončila v rámci i) posouzení dosažení účelu jinými prostředky jako další v pořadí, a která se zároveň v rámci ii) posouzení nezbytnosti ukázala jako vhodná.

3.1.4 Přesné a aktualizované údaje (jen u kamerových systémů se záznamem)

Vzhledem k charakteru zpracovávaných osobních údajů je přesnost a aktuálnost údajů omezena na požadavky:

- omezení možnosti neautorizovaných změn (střih, vymazání části záznamu, zásah do technický prostředků – neoprávněná manipulace), což je řešeno v rámci technických a organizačních opatření,
- pořizování záznamu v dostatečné kvalitě pro běžnou identifikaci vstupujících subjektů, což je řešeno v rámci požadavků při pořizování technických prostředků.
  Poznámka: Je zřejmé, že pořizování kamerového záznamu, který na základě své nízké kvality (nastavením kamer či technickými parametry kamerového systému, jako je rozlišení kamer) neumožňuje identifikovat osoby, nemůže ve většině případů plnit účel nasazení, s výjimkou preventivní či odstrašující funkce kamer, pro niž lépe poslouží atrapy kamer.

3.1.5 Nezbytně nutná doba uložení záznamů (jen u kamer se záznamem)

Doba uchování údajů by ve většině případů měla být stanovena v rozmezí jednoho až dvou dní, v zásadě by neměla přesáhnout 72 hodin.[9] Doba uložení je zdůvodněna [např. možností přítomnosti a prohlížení záznamů oprávněnou osobou; nepřítomností oprávněné osoby v určitých obdobích (v případě že oprávněná osoba nemá určeného zástupce), např. v době dovolených; obdobím uzavření objektu pro oprávněně vstupující; délkou reklamační lhůty, pokud je v záběru kamery například balení a expedice výrobků, ovšem bez záběru na zaměstnance; apod.] v rámci zpracování balančního testu případně v rámci posouzení vlivu na ochranu osobních údajů (dále též DPIA).

Poznámka 1: V zásadě může doba uložení vyplývat i z možnosti přístupu oprávněných osob ke kamerovým záznamům; v případě nepřetržitého přístupu postačuje doba uchování 1 den, v případě nepřítomnosti o víkendech 72 hodin. Pokud by byla doba uchování obrazových záznamů delší než 72 hodin, musí být součástí dokumentace jasné zdůvodnění, proč je nezbytná delší doba uchování kamerového záznamu.

Poznámka 2: Někdy je vhodná kombinace doby uchování, například v případě škol je obvyklá doba uchování 7 dní (daná například z důvodu existence státních svátků, ředitelského volna a kratších prázdnin) s tím, že o hlavních prázdninách může být tato doba prodloužena až na 3 týdny. Někdy také může být v rámci jednoho monitorovaného objektu rozdílná doba uchování u jednotlivých kamer, například u některých 3 dny, u jiných 3 týdny. Důvodem je to, že v záběru kamer s delší dobou uchování se subjekty většinou nevyskytují a kamery nejsou umístěny na frekventovaných místech (doba je stanovena dočasně, například o prázdninách, nebo trvale, například na perimetru objektu ústícího na pole, kdy u delší doby uchování není z hlediska záběru kamery zásah do soukromí významný).

Poznámka 3: Do doby uchování záznamu se nepočítá doba uchování záznamů mimořádných událostí pro orgány činné v trestním řízení, přestupkovém řízení nebo pro pojišťovny k vyřízení pojistné události, kdy je záznam uchován až do vyřízení mimořádné události, a pak teprve vymazán.

3.1.6 Zpracování zabezpečeným způsobem

Viz navrhovaná technická a organizační opatření v kapitole 3.8.

3.2 Zajištění práv subjektů údajů

Řešení problematiky zajištění práv subjektů údajů je navrženo takovým způsobem, aby správcům umožnilo vyhovět požadavkům na transparentnost daným článkem 12 obecného nařízení o ochraně osobních údajů.

3.2.1 Informace

[9] § 122 Pokynů EDPB 3/2019 (česká verze).

V případě kamerových systémů je informace subjektům údajů podávána ve více vrstvách, a to z toho důvodu, že před vstupem do monitorovaného prostoru není prakticky možné informovat subjekt údajů v plném rozsahu (velikost informační tabulky to neumožňuje).

3.2.1.1. Informace na první úrovni – základní informace (informační tabulka)

1. Označení monitorovaných prostor informačními tabulkami se provádí tak, aby subjekt údajů byl upozorněn na kamerový systém před vstupem do monitorovaného objektu nebo monitorovaných prostor, v každém případě před vstupem do záběru kamery.
2. Informační tabulky musí být u monitorovaného objektu/prostoru umístěny po celou dobu provozu kamerového systému.
3. Informační tabulky musí být dobře viditelné, tj. umístěné a navržené tak, aby byly nepřehlédnutelné (přibližně ve výšce očí a na místech, kudy musí subjekt údajů projít před vstupem do monitorovaných prostor).
4. Informační tabulky musí obsahovat alespoň piktogram/obrázek kamery, údaj o tom, že prostor je monitorován kamerovým systémem (se záznamem, pokud je pořizován), identifikaci správce a odkaz na kontaktní osobu (pověřenou správcem, např. na pověřence pro ochranu osobních údajů), odkaz na místo, kde je možné v písemné nebo digitální podobě získat o kamerovém systému podrobnější informaci (např. telefonní spojení, internetová adresa, QR kód, pracoviště pověřené osoby apod.), účel a právní základ zpracování osobních údajů a informace o právech subjektu údajů (např. větou „jako subjekt údajů máte možnost uplatnit vůči správci několik práv, zejména právo na přístup k osobním údajům a právo na výmaz svých osobních údajů“).[10]
5. Vzhled informační tabulky není předepsán, je však nezbytné, aby písmo bylo dobře čitelné, takže volba fontu/typu a velikosti písma hraje významnou roli.
6. Piktogram a text o tom, že objekt/prostor je monitorován kamerovým systémem (se záznamem), musí být viditelný/čitelný i z větší vzdálenosti (cca 2–5 m).
7. Odkaz na místo, kde je možné získat podrobnější informace (informace na druhé úrovni), musí být jednoznačný a místo snadno dostupné.
8. V případě, že jsou v objektu pravidelně přítomny slabozraké anebo nevidomé osoby, je vhodné jejich informovanost zajistit ještě jiným adekvátním způsobem (zvukovým oznámením, texty napsanými speciálním druhem písma apod.).
9. V případě některých objektů (hotely a některé další objekty určené ke krátkodobému bydlení, muzea apod.), v nichž dochází k četnému výskytu návštěvníků ze zemí mimo Českou republiku, se užijí vícejazyčné informační tabulky.

3.2.1.2 Informace na druhé úrovni – podrobná informace

Správce poskytuje subjektu údajů podrobné informace o zpracování osobních údajů kamerovým systémem v souvislosti s jeho povinností vyplývající z článku 13 a 14 obecného nařízení.

1. Poskytnutí informace probíhá v textové podobě, kterou lze vystavit na webu/zaslat/zapůjčit na požádání k prostudování.
3. Informace je snadno dostupná minimálně po dobu, kdy je objekt/prostor přístupný oprávněným subjektům údajů (například v pracovní/otevírací době).
4. Informace je dostupná po dobu, kdy zpracování osobních údajů probíhá (od zprovoznění kamerového systému do ukončení jeho provozu).

[10] § 114 až 116 Pokynů EDPB 3/2019.

5. Informaci je třeba udržovat v aktuálním stavu.
6. Obsah informace o kamerovém systému (viz vzor 1 v příloze):
    - účely zpracování (ochrana majetku apod.),
    - rozsah zpracování/kategorie osobních údajů (obrazový záznam kamerového systému),
    - identifikace správce (název, IČO, sídlo) a jeho zástupce nebo případně pověřence pro ochranu osobních údajů (jméno, příjmení a kontakt, tj. telefon, e-mail),
    - identifikace zpracovatele, pokud existuje (název, IČO, sídlo),
    - místo/místa zpracování (adresy),
    - právní základ zpracování a účely zpracování,
    - příjemce/kategorie příjemců zpřístupněných údajů (např. orgány činné v trestním řízení nebo správní orgány pro účely přestupkového řízení apod.),
    - předání osobních údajů do třetích zemí nebo mezinárodním organizacím,
    - počet kamer,
    - doba uchování záznamů, včetně způsobu vymazání údajů po uplynutí doby uchování (např. přepisem ve smyčce),
    - režim fungování kamer (např. na základě detekce pohybu, nepřetržitý, mimo pracovní dobu/vyučování apod.),
    - popis práv subjektu údajů vůči zpracovateli (dle čl. 13 až 22 obecného nařízení),
    - informace o automatizovaném rozhodování včetně profilování.

3.2.2 Přístup k osobním údajům (jen u kamerových systémů se záznamem)

V této části je řešen přístup subjektů údajů, ale i dalších oprávněných subjektů k osobním údajům. Pravidla pro přístup jsou pro všechny kategorie oprávněných subjektů obdobná.

3.2.2.1 Předávání kamerových záznamů **oprávněným subjektům:**

- ***subjektům údajů případně jejich zákonným zástupcům***[11] na základě jejich požadavku, a to v rozsahu obrazových záznamů uchovávaných o těchto subjektech (ostatní subjekty musí být na předaných záběrech anonymizovány);
- ***subjektům, kterým jsou kamerové záznamy poskytovány na základě souhlasu (všech) subjektů údajů, které jsou na záznamech zachyceny*** (např. obyvatelům domu, rodinným příslušníkům, zaměstnancům, a také hromadným sdělovacím prostředkům apod.);
- ***jiným spravujícím orgánům nebo správcům,*** typicky na základě povinnosti předávat kamerové záznamy vyplývající z právních předpisů (orgánům činným v trestním nebo přestupkovém řízení apod.), nebo pojišťovnám při řešení pojistných událostí.

3.2.2.2 Pravidla pro předávání **oprávněným subjektům:**

a. Subjekty, které žádají správce o poskytnutí záznamu z kamerového systému, by měly správci zaslat žádost obsahující specifikaci rozsahu požadovaného záznamu, zdůvodnění žádosti, a v případě subjektů, kterým je správce povinen předat záznamy z kamerového systému na základě zákona, také termín pro poskytnutí záznamu.

[11] Na základě práva na přístup k osobním údajům podle čl. 15 GDPR.

b. Správce může poskytnout kamerové záznamy orgánům činným v trestním řízení nebo správním orgánům pro vedení přestupkového řízení, případně pojišťovnám, i z vlastního rozhodnutí, a to v případě, že má podezření na spáchání trestného činu nebo přestupku nebo vzniku pojistné události, které jsou na záznamu zachyceny.
c. Pro vyřizování žádostí o poskytnutí záznamů z kamerových systémů i pro poskytnutí kamerových záznamů z vlastního rozhodnutí správce, vytvoří správce postupy, které stanoví a budou obsahovat:
    - kontaktní osoby správce pro předávání žádostí o poskytnutí dat,
    - posouzení oprávněnosti předání dat,
    - postup pro zpracování kopie záznamu, včetně stanovení osoby, která zajistí zpracování kopie,
    - určení osoby správce, která zajistí předání kopie kamerového záznamu žadateli nebo orgánům činným v trestním řízení nebo správním orgánům pro účely přestupkového řízení,
    - pokyny pro zpracování dokumentu o předání kopie kamerového záznamu, které zohlední následující doporučení:
        - protokol o předání kamerových záznamů, připravený orgány činnými v trestním řízení nebo správními orgány pro účely přestupkového řízení, lze použít bez nutnosti zpracování dalších dokumentů,
        - pokud dokument o předání zajišťuje přímo správce, Úřad doporučuje zpracovat předávací protokol, nebo záznam v rámci vedení provozního deníku, který bude obsahovat:
            - datum poskytnutí záznamu,
            - zdůvodnění poskytnutí záznamu (zejména právní důvod[12]):
                - v případě žádosti policie může jít o právní důvod plnění právní povinnosti,[13]
                - v případě pojistné události nebo podezření správce na trestný čin nebo přestupek, kde dochází k předání záznamu příslušným orgánům či pojišťovně na základě podezření správce či vzniklé škody, jde o předání na základě ochrany oprávněných zájmů správce,[14]
                - v ostatních případech, tj. přístup (např. individuální), šíření (on-line) nebo jakékoliv jiné zpřístupnění kamerových záznamů jiným subjektům jde o předání na základě souhlasu subjektu údajů,[15]
            - identifikaci žadatele o záznam (v případě žádosti oprávněných orgánů včetně čísla jednacího příslušného řízení nebo jiné specifikace příslušného řízení) nebo subjektu, kterému je záznam předáván z vlastního podnětu,

[12] Kapitola 4 Pokynů EDPB 3/2019.
[13] Čl. 6 odst. 1 písm. c) GDPR.
[14] Čl. 6 odst. 1 písm. f) GDPR.
[15] Čl. 6 odst. 1 písm. a) GDPR.

- specifikaci poskytnutých záznamů (datum pořízeného záznamu, čas odkdy dokdy),
- jméno a příjmení předávající osoby, včetně jejího podpisu,
- jméno a příjmení přejímající osoby, včetně jejího podpisu.

d. Pro účely poskytnutí záznamů z kamerového systému se za rozhodný den považuje den obdržení žádosti; jako přiměřená doba pro poskytnutí záznamu se považuje lhůta do 1 měsíce od obdržení žádosti, nebo je třeba respektovat termíny určené orgány činnými v trestním řízení.
e. Při poskytování kamerového záznamu subjektu údajů je třeba dodržet následující pravidla:
   - předkládají se pouze části pořízeného záznamu, na kterých je zaznamenán subjekt údajů žádající o poskytnutí záznamu (žadatel),
   - jiné subjekty údajů nesmí být na záznamu rozpoznatelné[16] (jejich obraz musí být rozostřen, záznam v příslušném místě rozmazán apod.), s výjimkou případů, kdy žadatel má jejich souhlas s tím, že může záznam obdržet i s jejich údaji. (*Poznámka: pokud by měl subjekt údajů podezření, že na záznamech může být zachyceno protiprávní jednání vůči jeho osobě, může současně požádat správce o omezení zpracování dle 3.2.5, které zajistí, že nedojde k vymazaní dotčených záběrů).*
f. Kamerový záznam se poskytuje v elektronické podobě (v tištěné podobě by mohly být poskytnuty jednotlivé záběry, pokud o to subjekt požádá), a to ve formátu běžně čitelném (např. MPEG-2, MPEG-4, JPEG-2000, H.263, H.264, H.265).
g. Za poskytnutí druhé a další kopie kamerových záznamů subjektu údajů může správce žádat přiměřenou úhradu nákladů spojených se zpracováním poskytovaného kamerového záznamu.
h. Nepřiměřené nebo zjevně neodůvodněné žádosti o kamerové záznamy mohou být správcem odmítnuty (opakované žádosti, žadatelem nedostatečně specifikovaný požadavek, který neomezuje dostatečně rozsah předávaných údajů) nebo správce může žádat přiměřený poplatek. Odmítnutí musí být zdůvodněno.

3.2.3 Právo na opravu (jen u kamerových systémů se záznamem)

Teoreticky lze předpokládat možnost využití práva na opravu pouze u kamerových systémů se záznamem. Ovšem charakter zpracovávaných osobních údajů (obrazový záznam), zjevně vylučuje možnost chyby nebo nepřesnosti osobních údajů. Správce je však povinen zajistit, aby s daty nemanipuloval nikdo neoprávněný, a aby o práci se záznamem oprávněných osob existoval záznam.

3.2.4 Právo na výmaz (jen u kamerových systémů se záznamem)

V případě kamerového systému má subjekt údajů (dále žadatel) právo podat žádost o výmaz osobních údajů. Zásady realizace práva na výmaz jsou následující:

[16] Čl. 15 odst. 4 GDPR.

- Správce upraví a zpřístupní formulář žádosti o vymazání záznamu zpracovaný takovým způsobem, aby na základě jeho vyplnění byl schopen v kamerovém záznamu údaje o žadateli nalézt (identifikace subjektu, časový údaj/rozmezí, kdy je subjekt zachycen).
- Správce vyřizuje žádosti o vymazaní záznamu do 30 dní od jejich obdržení, a to včetně odpovědi žadateli.
- Správce vymazává na žádost pouze části záznamu s žadatelem, které nezachycují mimořádné události, pro jejichž zachycení byl kamerový systém zřízen (plnění účelu).
- Vymazání se provádí např. smazáním záznamu, vystřižením části záznamu, rozmazáním části záznamu, vymaskováním části záznamu, na kterém je žadatel). Část záznamů zachycující mimořádné události správce vymazává teprve po jejich vyřízení příslušnými orgány (Policie ČR, soudy, orgány řešící přestupky, pojišťovny), pokud jim byly předány.
- Záznamy, u kterých je žadatelem uplatněno právo na omezení zpracování (omezení použití nebo uchování pro určení, výkon nebo obhajobu právních nároků žadatele nebo z důvodu vznesení námitky proti zpracování založenému na oprávněných zájmech správce), mohou být vymazány teprve poté, co bylo omezení zpracování správcem zrušeno.
- O vymazání záznamu se zpracovává protokol, který obsahuje:
    - Identifikaci žadatele o výmaz,
    - identifikaci vymazávaných záběrů (například datem a časovým údajem od-do),
    - identifikaci osoby, která výmaz provedla,
    - datum provedení výmazu.

3.2.5 Právo na omezení zpracování

Co se týče práva na omezení zpracování, v zásadě přicházejí v úvahu dva důvody podání žádosti na omezení zpracování:

- Žadatel požádal o omezení zpracování (údaje jsou pak uloženy bez jakékoliv změny) z důvodu určení, výkonu nebo obhajoby právních nároků. Takové kamerové záznamy potom mohou být nadále zpracovávány po dobu správcem určené doby uchování a po jejím uplynutí jen z těchto důvodů:
    - pro určení, výkon nebo obhajobu právních nároků žadatele,
    - pro potřeby orgánů činných v trestním nebo přestupkovém řízení nebo pro potřeby pojišťovny,
    - z důvodu veřejného zájmu EU nebo jejího členského státu.

  Poznámka: Posledně uvedený důvod je v případě kamerových záznamů velmi nepravděpodobný.

- Subjekt vznesl námitku proti zpracování kamerového záznamu u zpracování, které je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby.[17] Až do prokázání závažných důvodů správce, které převažují nad zájmy nebo právy a svobodami subjektů údajů (s využitím určení právního základu dle bodu 3.1.1 a analýzy nezbytnosti

[17] Čl. 21 GDPR.

nasazení kamerového systému dle bodu 3.1.3) nebo do vymazání záznamu, mohou být kamerové záznamy nadále zpracovávány jen z těchto důvodů:

- se souhlasem subjektu údajů, který o omezení požádal,
- pro určení, výkon nebo obhajobu právních nároků subjektu údajů,
- pro potřeby orgánů činných v trestním nebo přestupkovém řízení nebo pro potřeby pojišťovny,
- z důvodu veřejného zájmu EU nebo jejího členského státu.

Poznámka: Posledně uvedený důvod je v případě kamerových záznamů velmi nepravděpodobný.

Postup správce v takových případech:

- Správce upraví a zpřístupní formulář žádosti o omezení zpracování takovým způsobem, aby byl schopen identifikovat žadatele, identifikovat kamery, o které se jedná, identifikovat část kamerového záznamu, o který se jedná, a identifikovat důvod, proč se subjekt údajů domnívá, že zpracování neprobíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, nebo důvod určení, výkonu nebo obhajoby právních nároků).
- Správce obratem vyrozumí subjekt údajů, že žádost obdržel.
- Kamerové záznamy jsou u správce nebo zpracovatele uloženy beze změny.
- Pokud na základě analýzy dojde správce k závěru, že zpracování probíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, zašle tuto informaci do 30 dní subjektu údajů, který o omezení zpracování požádal, a vyrozumí jej, že omezení zpracování bude ke specifikovanému dni zrušeno.
- Pokud na základě analýzy dojde správce k závěru, že zpracování neprobíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, zašle tuto informaci do 30 dní subjektu údajů, který o omezení zpracování požádal, a vyrozumí jej, že data jsou vymazána a zpracování nadále ve stávajícím rozsahu nebude probíhat.
- Pokud subjekt údajů požádal o omezení zpracování z důvodu určení, výkonu nebo obhajoby právních nároků, potom správce zašle subjektu údajů požadavek na určení termínu ukončení omezení zpracování definované subjektem údajů, jinak budou údaje po jednom roce vymazány, pokud subjekt údajů nepotvrdí trvání omezení zpracování.

3.2.6 Právo na přenositelnost údajů (jen u kamerových systémů se záznamem)

Právo na přenositelnost údajů nedává u kamerových systémů pro subjekt údajů smysl. Je řešeno v rámci práva subjektu údajů na přístup k osobním údajům, kdy má subjekt údajů právo získat kamerové záznamy o své osobě (viz bod 3.2.2).

3.2.7 Právo vznést námitku proti zpracování

Právo vznést námitku proti zpracování se uplatní pouze u zpracování, které je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby.[18]

- Správce upraví a zpřístupní formulář práva vznést námitku takovým způsobem, aby byl schopen identifikovat žadatele, identifikovat kamery, o které se jedná, identifikovat část kamerového záznamu, o který se jedná, a identifikovat důvod, proč se subjekt

[18] Čl. 21GDPR.

údajů domnívá, že zpracování neprobíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, a to i automatizovaným způsobem (e-mailem, přes webové stránky správce apod.).

- Správce oznámí subjektu údajů přijetí žádosti.
- Správce na žádost odpoví do 30 dní od její obdržení.
- Správce provede analýzu existence závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů (k analýze využije údajů z určení právního základu dle bodu 3.1.1 a analýzy nezbytnosti nasazení kamerového systému dle bodu 3.1.3),
  Poznámka: Doporučuje se koncept takové analýzy zpracovat předem.
- Právo vznést námitku může být řešeno společně s právem na omezení zpracování, pokud se týká totožného zpracování a bylo podáno stejným subjektem.
- Pokud na základě analýzy dojde správce k závěru, že zpracování probíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, zašle tuto informaci do 30 dní subjektu údajů, který o omezení zpracování požádal, a vyrozumí jej, že zpracování bude opět zahájeno.
- Pokud na základě analýzy dojde správce k závěru, že zpracování neprobíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů, zašle tuto informaci do 30 dní subjektu údajů, který o omezení zpracování požádal, a vyrozumí jej, že data jsou vymazána a zpracování nadále ve stávajícím rozsahu nebude probíhat.

3.2.8 Automatizované individuální rozhodování, včetně profilování

Využití kamerového systému pro rozhodování založeném výhradně na automatizovaném zpracování včetně profilování není pravděpodobné, nicméně pokud by bylo realizováno, bylo by zřejmě spojeno s analýzou chování subjektů údajů nebo přímo se zpracováním zvláštních kategorií osobních údajů (zejména biometrické údaje typu rozpoznávání tváře nebo pohyb subjektů údajů). Proto by správce musel pečlivě zvážit nezbytnost realizace tohoto druhu využití kamerových systémů pro zajištění jím definovaného účelu.[19]

3.3 Zpracovatel

Pokud má správce najatého zpracovatele na provádění některých operací zpracování (případně i celého zpracování) v rámci provozování kamerového systému, potom musí dojít k uzavření zpracovatelské smlouvy [20] mezi správcem a zpracovatelem (nemusí být samostatná, může být součástí jiných smluvních dokumentů), která

- obsahuje definici předmětu zpracování osobních údajů (kamerový systém, druh objektu, umístění kamerového systému, povaha a účel zpracování, kategorie subjektů údajů),
- obsahuje operace zpracování, které provádí za správce zpracovatel, včetně časového rámce (do kdy správce zpracovatelskou operaci provede po obdržení dat),

[19] Čl. 22 GDPR.

[20] Čl. 28 GDPR, v případě kamerového systému jiný právní akt než smlouva mezi správcem a zpracovatelem není pravděpodobný.

- obsahuje dobu trvání smlouvy,
- obsahuje povinnosti zpracovatele,
  - pracovat dle pokynů správce (specifikovaných ve zpracovatelské smlouvě nebo v jiných dokumentech),
  - informovat správce, pokud by pokyn dle předchozí odrážky porušoval platné právní předpisy,
  - zachovávat mlčelivost o zpracovávaných osobních údajích,
  - zabezpečit zpracování (technická a organizační opatření) na základě požadavků specifikovaných ve zpracovatelské smlouvě,
  - před zapojením dílčího zpracovatele si vyžádat souhlas správce se zapojením daného dílčího zpracovatele do zpracování (u kamerových systémů však bude řetězení zpracovatelů řídkým jevem),
  - vymazat osobní údaje po vypršení platnosti zpracovatelské smlouvy nebo po jejím ukončení (pokud právo ČR nebo EU nepožaduje jinak),
  - umožnit provádění auditů, které se týkají zpracování osobních údajů (tj. kamerového záznamu) a spolupracovat při nich se správcem,
  - informovat správce o případných porušeních zákona nebo přestupcích zjištěných při zpracování kamerového záznamu (případně na základě pověření je oznamovat věcně příslušným orgánům za správce),
  - navrhnout správci postup v případě zjištění porušení zabezpečení osobních údajů.[21]

3.4 Záznamy o činnostech zpracování

Záznam o činnostech zpracování obsahuje identifikaci správce osobních údajů (název, adresa sídla, IČO), určení pověřené osoby (jméno, příjmení, tituly, adresa, telefon), identifikaci kamerového systému, na který se záznam vztahuje – správce jich může mít více (adresa umístění kamerového systému, počet kamer), účel, právní základ,[22] rozsah a dobu uložení osobních údajů, identifikaci příjemců osobních údajů, informace o předávání osobních údajů do třetích zemí (k němuž v drtivé většině případů nebude docházet) a informace o tom, zda dochází k automatizovanému rozhodování, včetně profilování.[23] Vzor 2 je obsažen v příloze.

3.5 Ohlašování porušení zabezpečení osobních údajů

Pokud se týče ohlašování porušení zabezpečení osobních údajů,[24] zde se správci doporučuje předem stanovit pro snazší a rychlejší způsob řešení bezpečnostních incidentů:

- odpovědnosti při řešení mimořádných událostí (organizačně i personálně),
- postupy oznamování mimořádných událostí (v rámci organizace, Úřadu pro ochranu osobních údajů, subjektům údajů),
- úpravu spolupráce se zpracovatelem (pokud zpracovatel existuje) při řešení mimořádných událostí,

[21] Srv. čl. 28 odst. 3 a čl. 33 odst. 2 GDPR.
[22] Právní základ není obligatorně GDPR vyžadován. Jeho uvedení je ale považováno za příklad dobré praxe.
[23] Čl. 30 GDPR.
[24] Čl. 33 a 34 GDPR.

- postupy klasifikace (závažnosti), šetření a vyhodnocení mimořádných událostí,
- pravidla a postupy revize technických a organizačních opatření na základě mimořádných událostí,
- pravidla vedení evidence a dokumentace mimořádných událostí.

3.6 Posouzení vlivu na ochranu osobních údajů (DPIA)

V rámci rozhodnutí, zda DPIA provádět, je nutno zpracovat analýzu, kterou bude zjištěno, zda se posouzení vlivu u zpracování kamerových záznamů/provozování kamerových systémů musí nebo nemusí provádět.[25]

3.7 Předávání do třetích zemí

Obecně je předávání kamerových záznamů do třetích zemí obtížně zdůvodnitelné a zpravidla k němu nebude docházet. V případě předávání orgánům činným v trestním řízení do třetích zemí zajišťuje případné předání do třetí země příslušný orgán činný v trestním řízení v České republice jako samostatný správce osobních údajů.[26]

3.8 Zabezpečení kamerových systémů

1) U kamerových systémů s vysokým rizikem pro práva a svobody subjektů údajů se návrh technických a organizačních opatření provádí v rámci řešení DPIA[27] (rozhodnutí na základě analýzy dle bodu 3.6).

2) U ostatních kamerových systémů provede návrh technických a organizačních opatření správce nebo zpracovatel (i prostřednictvím dodavatele) v rámci obecné povinnosti řízení rizik buď na základě vlastní analýzy nebo na základě klasifikace kamerových systémů z hlediska bezpečnosti (viz tabulka 1 v kapitole 3.8.2.1). Pro každý kamerový systém jsou opatření stanovována samostatně, ale v případech typově obdobných objektů, s typově rozmístěnými kamerami a s typovým nastavením (záběr, režim apod.) je možno technická a organizační opatření řešit v jednom dokumentu. Vždy je však nutno kamerové systémy, na které se technická a organizační opatření vztahují, jednoznačně identifikovat a popsat (pokud by se tak nestalo, byly by možné změny počtu kamer, umístění kamer a nastavení kamer bez nutnosti revize technických a organizačních opatření, což je nepřípustné).

3.8.1 Klasifikace kamerových systémů z hlediska bezpečnosti

Správce provede klasifikaci jím navrhovaného, provozovaného kamerového systému na základě stanovení dopadů a frekvence výskytu mimořádných událostí.

3.8.1.1 **Koeficient dopadů**

Stanovení dopadů: Správce nebo dodavatel stanoví dopady provozování kamerového systému na subjekty údajů nebo na správce podle citlivosti zpracovávaných kamerových záznamů, resp. podle důsledků neoprávněného přístupu, pozměnění nebo znepřístupnění kamerových záznamů. **Pro další výpočet vezme vyšší z obou hodnot**:

[25] Analýza se provádí podle návodu, který je obsažen v dokumentu Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (DPIA), uveřejněném na webové stránce Úřadu.

[26] Srv. čl. 48 GDPR.

[27] Metodika obecného posouzení vlivu na ochranu osobních údajů je zveřejněná na webové stránce Úřadu.

3.8.1.1.1 Koeficient dopadů na subjekty údajů

1. Může vést k nepohodlí subjektu údajů (podrážděnost, nutnost další komunikace se správcem).
2. Může vést k menší újmě [stres (pocit neustálého sledování), nepohodlí, drobné fyzické obtíže, nedostatek porozumění, časové nároky spojené s řešením dopadů].
3. Může vést k závažné újmě [napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny)].
4. Může vést k velmi závažné újmě, přímému ohrožení (dlouhodobě nepříznivý zdravotní stav, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení) či ztrátě života.

3.8.1.1.2 Koeficient dopadů na správce

1. Může způsobit krátkodobé nepříjemnosti (zdržení a podráždění zaměstnanců nebo členů statutárního orgánu správce). Náklady do 0,05 % ročního obratu.
2. Může negativně ovlivnit výkon zaměstnanců (stres zaměstnanců a členů statutárního orgánu správce, drobné fyzické a zdravotní obtíže). Náklady od 0,05 % do 2 % ročního obratu.
3. Může způsobit závažné, krátkodobé omezení (zhoršení zdravotního stavu zaměstnanců a členů statutárního orgánu, krátkodobá pracovní neschopnost). Náklady od 2,0 % do 10 % ročního obratu.
4. Může způsobit závažné dlouhodobé omezení (útoky na členy nebo zaměstnance společnosti, odchod zaměstnanců nebo členů statutárního orgánu, dlouhodobá pracovní neschopnost). Náklady vyšší než 10 % ročního obratu.

3.8.1.2 **Koeficient frekvence výskytu**

Správce nebo dodavatel stanoví frekvenci událostí, kdy dojde pokusu nebo k dokonanému pokusu o neoprávněný přístup, pozměnění nebo znepřístupnění kamerových záznamů (nebo obrazu z kamerového systému):

1. Frekvence výskytu není častější než jednou za pět let.
2. Frekvence výskytu se pohybuje v rozpětí od jednoho roku do pěti let.
3. Frekvence výskytu se pohybuje v rozpětí od jednoho měsíce do jednoho roku.
4. Frekvence výskytu se pohybuje v častějších intervalech než jednou za měsíc.

3.8.1.3 Koeficient míry porušení práv a zájmů subjektů údajů

Stanovení míry narušení práv: Správce nebo zpracovatel stanoví na základě umístění a parametrů kamer míru narušení práva a zájmů subjektů údajů:

1. žádná míra narušení – prostý kamerový záznam, umístění kamer a monitorování prostor, kam subjekty údajů obvykle nevstupují (například záznam v mimoprovozních hodinách, monitorování perimetru budov v některých místech apod.),
2. malá míra narušení – prostý kamerový záznam, monitorování prostor, kde se subjekty údajů nachází omezeně, nebo jde o prostory s omezeným výskytem citlivého chování nebo doby monitorování (plášť objektu, prostory u sklepů, sklady apod.),
3. střední míra narušení – monitorování prostor, kde může být zachyceno chování subjektů údajů (stav, doba a společnost), vstupy do obytných budov, škol, sociálních zařízení, zdravotnických zařízení, vstup do šaten ve školách, některé prostory prodejen,

4. vysoká míra narušení – monitorování vstupů do šaten, prostor šaten v bazénech (pokud jsou vyčleněny jiné prostory pro převlékání), některé prostory bazénů (například dojezd a nástup atrakcí), chodby škol, prostory pokladen, vstupy do kuřáren a odpočinkových místností, čekárny zdravotnických zařízení, výtahy,
5. velmi vysoká míra narušení – prostý kamerový záznam monitorování citlivých prostor jako jsou trvalá pracoviště při zvláštní povaze činnosti, biometrické kamerové záznamy, pořizování zvuku, pořizování polohy subjektů údajů při pohyblivých kamerách.

3.8.1.3 **Stanovení třídy bezpečnosti kamerového systému**

Kamerový systém se dělí dále do čtyř tříd podle dosažené hodnoty součinu: koeficient dopadů x koeficient frekvence x koeficient míry porušení práv a zájmů subjektů údajů.

třída 1 – Součin je menší než 6.

třída 2 – Součin je 8-27.

třída 3 – Součin je 32-48.

třída 4 – Součin je větší než 60.

3.8.2 Technická a organizační opatření

Pokud správce nebo zpracovatel (i prostřednictvím dodavatele) aplikuje technická a organizační opatření v závislosti na třídě kamerového systému, kterou stanovil, potom je seznam opatření uvedených v tabulce 1 povinný (nahrazuje analýzu provedou správcem). Nicméně návrh technických a organizačních opatření může na základě obecné povinnosti řízení rizik stanovit správce nebo zpracovatel (i prostřednictvím dodavatele) samostatně, jen musí být tato opatření přiměřená a zdůvodněná.

3.8.2.1 **Přehled opatření aplikovaných v jednotlivých třídách**

Opatření jsou formulována obecněji, v jednotlivých třídách může být způsob implementace některých opatření odlišný (monitorování a zaznamenávání činností může být učiněno softwarově, ale v jednodušších případech může být učiněno písemně za přítomnosti například dvou nezávislých osob). Zkratky použité v tabulce: P (povinné opatření), D (doporučené opatření).

Tabulka 1 – přehled opatření

č.	TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ	Tř. 1	Tř. 2	Tř. 3	Tř. 4
	OPATŘENÍ NA OCHRANU KAMER, DATOVÉHO PŘIPOJENÍ				
1.	detekce selhání KS (přerušení přenosu dat)		D	P	P
2.	detekce událostí (zakrytí nebo oslepení kamery)			D	P
3.	detekce nahrazení signálu kamery			D	P
4.	ochrana venkovních kamer a rozvodů před vlivy počasí	D	P	P	P
5.	ochrana datového připojení (kabelů apod.)	D	D	P	P
6.	odolnost proti útoku hrubou silou			D	P
	OPATŘENÍ NA OCHRANU ZÁZNAM. ZAŘÍZENÍ A DATOVÝCH NOSIČŮ*				
7.	umístění v chráněném prostoru	P	P	P	P

8.	evidence přístupu	P	P	P	P
	OPATŘENÍ NA OCHRANU ZOBRAZOVACÍHO ZAŘÍZENÍ (online obraz)				
9.	řízení přístupu osob do prostoru umístění zařízení	P	P	P	P
10.	řízení přístupu osob k obrazu	D	D	P	P
	OPATŘENÍ NA OCHRANU DAT (kamerových záznamů) *****				
11.	řízení přístupu k datům (autentizace, autorizace)	P	P	P	P
12.	monitorování a zaznamenávání činnosti (vyhledávání, přehrávání, vymazání, úprava, ukládání, tisk, předávání)	P	P	P	P
13.	autentizace dat (opatření proti narušení integrity dat) **	D	D	P	P
14.	ukládání údajů o čase	P	P	P	P
15.	bezpečný výmaz dat po uplynutí doby uchovaní	D	D	P	P
16.	zálohování				P
	OSTATNÍ OPATŘENÍ				
17.	ochrana před škodlivými kódy***	D	D	P	P
18.	školení obsluhy	P	P	P	P
19.	zpracování dokumentace	P	P	P	P
20.	řízení dodavatelů a zpracovatelů***	P	P	P	P

Poznámky:

* Neuplatní se u online kamerových systémů.

** V případě, kdy má sloužit jako důkazní prostředek pro orgány činné v trestním řízení, je doporučeno opatření implementovat.

*** Fakultativní, uplatní se, pokud je systém připojen do sítí, nebo pokud jsou do zpracování zapojeni zpracovatelé.

3.8.2.1 **Postup stanovení technických a organizačních opatření pro kamerový systém**

V případě užití kamerového systému je třeba učinit následující tři kroky:

1. Identifikace kamerového systému (aby bylo zřejmé, o jaký kamerový systém jde) a jeho popis (aby bylo zřejmé, na jaký stav kamerového systému se opatření vztahují):
   - kdo je jeho správce,
   - kdo je správcem pověřený zpracovatel/provozovatel (pokud existuje),
   - kdo je projektant a kdo dodavatel kamerového systému,
   - kde je umístěn kamerový systém (adresa),
   - počet instalovaných kamer,
   - popis záběrů kamer a jejich provozní režim,
   - popis technického řešení (jaké kamery, záznamové zařízení, rozvody apod.),
   - popis vyškolení obsluhy a zajištění údržby kamerového systému.

2. Popis technických a organizačních opatření
   U opatření použitých na konkrétní kamerový systém je třeba je zdokumentovat a doplnit podrobnější technický popis realizovaných opatření. V zásadě se však dá konstatovat, že při zpracování osobních údajů prostřednictvím kamerového systému lze definovat čtyři druhy hrozeb (u jednotlivých hrozeb jsou uvedena technická a organizační opatření, která budou uplatněna v závislosti na třídě kamerového systému):
   a) neoprávněný přístup k prostředkům kamerového systému ke kamerám

Přijatá technická a organizační opatření: výběr druhu kamer (omezuje možnost nepovoleného přístupu k obrazu přenášeného z kamer), umístění mimo běžný dosah osob pohybujících se ve sledovaném prostoru, kontrola jedné kamery druhou, bezpečnostní kryty kamer, záznam událostí (nebo i signalizace) – odpojení kamery, změny pozice kamery, ztráty záběru kamery (zatemnění nebo oslnění), nahrazení obrazových dat apod.

ke kabelovým rozvodům

Přijatá technická a organizační opatření: rozvody vedeny v chráničkách, lištách, pod omítkou, zakončení kabelů v uzamykatelném rozvaděči, oddělené rozvody kamerového systému od ostatních sítí apod.

k záznamovému zařízení nebo zobrazovacímu zařízení

Přijatá technická a organizační opatření: umístění v uzamykatelném objektu, v uzamykatelné místnosti, uzamykatelném zařízení, ochrana oken mříží, stálá ostraha, omezený počet vstupujících osob – evidence klíčů, vstup na základě karty/čipu apod., pohybová čidla, vstup do místnosti jen s dohledem nebo ve více osobách, evidence přístupu do místnosti apod.

b) neoprávněný přístup ke kamerovým záznamům (přístup neoprávněných osob)

Přijatá technická a organizační opatření: omezený přístup do objektu/do místnosti, řízení přístupu uživatele (přihlašovací jméno, heslo, PIN apod.), datové nosiče součástí záznamového zařízení (data nejsou ukládána externě, mimo záznamové zařízení), autentizace dat a vkládání údaje o čase, systém eviduje přístupy k záznamům, bezpečný výmaz/zničení nosičů dat, oddělení kamerového systému od datových sítí, zálohování dat, autentizace dat a vkládání údaje o čase apod.

c) neoprávněné čtení (i online), kopírování, přenos, úprava a vymazání kamerových záznamů

Přijatá technická a organizační opatření: řízení přístupu uživatele (přihlašovací jméno, heslo, PIN apod.), stanovení rolí uživatele (pro čtení, pro kopírování), datové nosiče součástí záznamového zařízení, autentizace dat a vkládání údaje o čase, antivirový software, bezpečný výmaz/zničení nosičů dat, systém eviduje přístupy k záznamům, eviduje práci se záznamy, tj. vyhledávání, přehrávání záznamů, vytváření kopií záznamů nebo práci se záznamy (střih a smazání), zálohování záznamů, oddělení kamerového systému od datových sítí, zápis údajů o čase do kamerových záznamů a vkládání autentizačních znaků, vytváří se zápisy v provozním deníku nebo protokoly o předání záznamů oprávněným osobám, přítomnost jen oprávněných osob při sledování záznamu nebo provádění kopie záznamů, školení obsluhy, ošetření servisu zařízení, bezpečnostní směrnice, určení administrátora a/nebo bezpečnostního správce systému apod.

d) živelní událost a povětrnostní podmínky

Přijatá technická a organizační opatřen v případě ohrožení počasím (déšť, sníh, vlhkost, slunce): kryty, clony.

Ve většině případů kamerových systémů lze brát živelní události ohrožující prostředky kamerového systému včetně dat (povodeň, požár, zásah bleskem apod.) jako zbytkové riziko, tj. hrozbu, kterou není třeba speciálně eliminovat nebo omezovat.

3. Způsob ověřování funkčnosti technických a organizačních opatření.
   Popis postupu kontrol funkčnosti technických a organizačních opatření (periodicita, kdo a jakým způsobem bude provádět, způsob zohlednění výsledků a doporučení kontroly) a způsobu sledování technického vývoje a případů porušení zabezpečení osobních údajů v oblasti kamerových systémů, včetně doporučení na eliminaci porušení zabezpečení a využití těchto informací ke zvýšení bezpečnosti v provozovaném kamerovém systému.

3.9. Dokumentace kamerového systému

Úplná dokumentace kamerového systému zahrnuje následující dokumenty:

1. záznam o činnostech zpracování (viz článek 30 GDPR) – 3.1.1, 3.1.2, 3.1.5, 3.4;
2. balanční test jako analýza nezbytnosti nasazení kamerového systému (viz článek 5 odst. 1 písm. c) a článek 35 odst. 7 písm. b) GDPR, § 26 Pokynů 3/2019) – 3.1.3;
3. analýza povinnosti zpracovat DPIA pro navrhovaný kamerový systém[28]; zpracovaná DPIA[29] (pokud bude povinná pro navrhovaný kamerový systém) nebo zpracovaná dokumentace technických a organizačních opatření (pokud DPIA nebude povinná) (viz článek 32 a 35 GDPR) – 3.6, 3.8;
4. projektová dokumentace kamerového systému (částečně čl. 24 obecného nařízení);
5. smluvní dokumentace včetně případné zpracovatelské smlouvy (dodavatel, provozovatel, společní správci, částečně viz článek 26 a 28 GDPR) – 3.3;
6. směrnice k provozování kamerového systému (fakultativně – může zahrnovat pravidla a postupy pro provozování kamerového systému, zajištění souhlasů subjektů údajů, zajištění práv subjektů údajů a řešení porušení zabezpečení osobních údajů, uvedené v následujících bodech) – se směrnicí musí být prokazatelně seznámeni všichni uživatelé kamerového systému;
7. doklady o udělení souhlasu subjektů údajů (v případě, že je právním základem zpracování souhlas subjektů údajů) – metodická část může být součástí směrnice k provozování kamerového systému (viz článek 7 GDPR) – 3.1.1;
8. zajištění informovanosti subjektů údajů (informační cedule a podrobná informace) a zajištění práv subjektů údajů (formuláře žádosti o výmaz, žádosti o omezení zpracování a námitky proti zpracování; dokumentace konkrétních žádostí o přístup, výmaz, omezení zpracování a námitek proti zpracování) – metodická část může být součástí směrnice k provozování kamerového systému (viz články 13 a 16 až 21 GDPR) – 3.2;
9. dokumentace k porušení zabezpečení osobních údajů (data breaches) – metodická část může být součástí směrnice k provozování kamerového systému (viz články 33 a 34 GDPR) – 3.5.

3.10 Upozornění k návrhu kamerového systému

1) V souvislosti s provozováním kamerového systému na pracovišti zaměstnavatele v pracovní době, které je místem výkonu práce zaměstnance, je nutné, kromě obecného nařízení o ochraně osobních údajů, aplikovat rovněž konkrétní ustanovení zákona č. 262/2006 Sb., zákoník práce, zejména § 316, který umožňuje zaměstnavateli

[28] Viz výše bod 3.6.

[29] Viz Metodika obecného posouzení vlivu na ochranu osobních údajů zpracovaná Úřadem pro ochranu osobních údajů a uveřejněná na jeho webu

zaměstnance monitorovat a jinak narušovat jeho soukromí pouze ze závažných důvodů spočívajících ve zvláštní povaze činnosti zaměstnavatele (například práce s infekčními agens, práce s vysoce výbušnými nebo jedovatými látkami). V případě, že takový důvod dán není, nemůže se zaměstnavatel ke sledování uchýlit, a to ani za předpokladu, že zaměstnanec udělí s monitorováním souhlas. Tento závěr je založen na skutečnosti, že ustanovení § 316 odst. 2 zákoníku práce je kogentní právní normou, od níž se tedy není možné odchýlit dohodou smluvních stran.

2) V případě pořizování zvukového záznamu (spolu s obrazovým záznamem) je třeba pečlivě posoudit, zda je jeho pořizování skutečně nezbytné pro naplnění účelu zpracování, protože pořizování zvukového záznamu představuje velký zásah do soukromí monitorovaných osob. *Poznámka: Lze předpokládat, že balanční test prokáže neopodstatněnost pořizování zvukového záznamu spolu s obrazovým v porovnání s jinými variantami řešení z hlediska míry zásahu do soukromí. V drtivé většině případů bude postačovat pro zajištění účelu a prokázání určité události pořízení obrazového záznamu.*
3) V případě, že jsou spolu s obrazovým záznamem (nebo i bez něj u kamerového systému provozovaného v režimu online) zpracovávány biometrické charakteristiky subjektů údajů (obličejové charakteristiky/markanty, charakteristiky chůze apod.) je také třeba pečlivě posoudit, zda je pořizování biometrických charakteristik skutečně nezbytné pro naplnění účelu zpracování, protože představuje zásadní zásah do soukromí monitorovaných osob. Navíc se v tomto případě jedná o zvláštní kategorii osobních údajů.
   Poznámka 1: I balanční test ve většině případů prokáže neopodstatněnost pořizování biometrických charakteristik v porovnání s jinými variantami řešení z hlediska míry zásahu do soukromí.
   Poznámka 2: Kamerový záznam pořízený a zpracovávaný obvyklým způsobem nepředstavuje zpracování zvláštní kategorie osobních údajů. V zásadě jde o vizuální identifikaci osoby v souvislosti s jejím určitým jednáním (například u spáchání trestného činu jde o zachycení pachatele bez ohledu na jeho národnost, náboženské vyznání, etnický původ, zdravotní stav či biometrické charakteristiky). To se nevylučuje s případným zpracováním latentních osobních údajů, které jsou obsaženy v části záznamu zobrazujícím mimořádnou událost, například biometrických charakteristik osob nebo i jiných osobních údajů, které po předání kamerového záznamu v rámci dalšího šetření extrahuje zvláštními nástroji Policie ČR jako nový samostatný správce. Správce je Policii ČR poskytuje v původním rozsahu, tzn. jako prostý kamerový záznam.
   Poznámka 3: V případě záměru zpracovávat biometrické údaje v rámci provozování kamerových systémů, a to zvláště na veřejně přístupných plochách (letiště, metro, nádraží apod.), je třeba zpracovat posouzení vlivu na ochranu osobních údajů (DPIA) dle kapitoly 3.8.
4) Monitorování veřejných prostranství je důvodné, pokud je založené na existenci reálného ohrožení (viz 3.1.1), musí však být omezeno na míru nezbytně nutnou, obvykle v rozsahu do 1,5-2 m od líce objektu nebo plotu (k omezení monitorování nežádoucích prostor může sloužit nastavení záběru kamer jejich natočením a rozmazáním nebo vymaskováním části záběru). Pokud by došlo k rozšíření záběru nad tento rozsah, musí to být pečlivě odůvodněno (zejména útokem na chráněné zájmy správce z místa mimo uvedenou vzdálenost).
5) Kamera umístěná u rodinného domu snímá vlastní nemovitost, a často také v přiměřené míře její hranici (viz předchozí bod 4), např. okrajové části okolních přilehlých zahrad, polí či veřejných komunikací. Používá-li majitel kameru jinak, může se dopustit přestupku proti občanskému soužití podle zákona o některých přestupcích.
   Poznámka: ÚOOÚ nemá kompetence k vedení řízení v případě individuálních sporů mezi majiteli obydlí, protože není oprávněn vstupovat do obydlí, které není používáno k podnikatelské činnosti, a nemůže proto ověřit režim provozu kamery v obydlí, ani prostá tvrzení protistran sporu a vysvětlení majitelů

kamer. Pokud není možné se s majitelem kamery/sousedem dohodnout, je možno takové jednání oznámit příslušné obci (komise k projednání přestupků), případně se obrátit na soud, a tím dosáhnout změny chování majitele kamery/souseda, například i odstranění kamery.

6) Doba uložení kamerového záznamu nesmí vyplývat z kapacity paměťového média, tedy z technických parametrů pořízeného kamerového systému, resp. snahy, co nejefektivněji využít pořízené technické prostředky, ale naopak musí vyplývat ze snahy o minimalizaci zásahu do soukromí s ohledem na organizační možnosti správce (podrobněji viz kapitola 3.1.5).

Vzor 1 - PŘÍKLAD INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM KAMEROVÉHO ZÁZNAMU NEBO PROSTŘEDNICTVÍM SLEDOVÁNÍ OBRAZU KAMER

Správce je povinen v souladu se zásadou transparentnosti informovat subjekty údajů o zpracování osobních údajů, které se jich týkají. Tento vzorový dokument uvádí příklad, jakým způsobem může správce subjektům údajů poskytnout řádnou informaci o rozsahu, účelu, době zpracování osobních údajů a další požadované informace v souvislosti s provozováním kamerového systému. Přitom se předpokládá, že všechny subjekty jsou rovněž informovány umístěním informačních tabulí u sledovaných prostor.

Správce osobních údajů	Název správce (IČO správce)	adresa správce: telefon správce: e-mail správce:
Kamerový systém	kamerový systém se záznamem pořizovaným na základě detekce pohybu var.: Kamerový systém v režimu online	adresa umístění: počet kamer:
Pověřenec pro ochranu osobních údajů/Pověřená osoba správce	Titul, jméno, příjmení pověřence pro ochranu osobních údajů/pověřené osoby	adresa: telefon: e-mail
Účel zpracování osobních údajů	Osobní údaje zaměstnanců jsou zpracovávány za účelem: • zvýšení ochrany majetku (krádež, vloupání, vandalismus), • zvýšení bezpečnosti osob (napadení, loupež, krádež, jiná fyzická újma) = ochrana života a zdraví osob, • prevence mimořádných událostí, • získávání důkazního materiálu pro příslušné odpovědné orgány (soudy a Policie ČR v případě trestných činů, obecní úřady v případě řešení přestupků), • získávání materiálu pro řešení pojistných událostí (s věcně příslušnou pojišťovnou).	
Právní základ zpracování osobních údajů	Zpracování je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby.	
Rozsah zpracovávaných osobních údajů	Obrazový záznam z kamerového systému var.: Obraz z monitorovaných prostor	
Doba uložení osobních údajů	Data jsou uchovávána po dobu … dní (obvykle 1-2 dny, max. do 72 hodin). Data jsou vymazávána přepisem ve smyčce.	
Příjemci osobních údajů	Orgány činné v trestním řízení v případě mimořádné události, Orgány činné v přestupkovém řízení v případě mimořádné události, Pojišťovny v případě řešení pojistné události, Subjekty údajů v případě jejich požadavku (jen záběry, kde se vyskytují tyto osoby, ostatní části jsou anonymizované). var. pro kamery v režimu online: Osobní údaje nelze předat jiným příjemcům.	

Předání do třetí země nebo mezinárodní organizaci	Správce nepředává osobní údaje do třetích zemí nebo mezinárodním organizacím. var.: Správce předává kamerové záznamy do Velké Británie mateřské společnosti… jako novému správci v rozsahu záznamu mimořádných událostí, a to za účelem nastavení technických a organizačních opatření v rámci skupiny společností... Velká Británie je na základě prováděcího rozhodnutí Komise ze dne 28. června 2021 podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů ve Spojeném království třetí zemí s odpovídající úrovní ochrany osobních údajů.
Práva subjektu údajů	• Právo na přístup k osobním údajům (čl. 15 GDPR) Zajištěno na základě žádosti subjektu údajů v rozsahu údajů o něm zpracovávaných. Obrazové záznamy jsou subjektům údajů poskytnuty v rozšířeném strojově čitelném formátu (doplnit jakém/jakých). • Právo na opravu osobních údajů (čl. 16 GDPR) Vzhledem k charakteru zpracovávaných osobních údajů (obrazový záznam) se právo na opravu neuplatní. Pomocí technických a organizačních opatření řešen neoprávněný zásah do kamerového záznamu. • Právo na výmaz osobních údajů (čl. 17 GDPR) Vzhledem k době uchování má subjekt údajů právo požádat o vymazání údajů, na kterých je zobrazen, pokud záznam nezachycuje mimořádnou událost. Jeho žádost bude vyřízena do 30 dní od obdržení. • Právo na omezení zpracování (čl. 18 GDPR) Subjekt údajů může vznést u správce námitku proti zpracování, a po dobu, než dojde k ověření, že oprávněné zájmy správce nepřevažují nad oprávněnými zájmy subjektů údajů, správce omezí zpracování osobních údajů na jejich ukládání. Pokud subjekt údajů osobní údaje potřebuje pro určení, výkon nebo obhajobu právních nároků, potom správce osobní údaje subjektu údajů uchová na základě jeho žádosti i po pominutí účelu zpracování nebo doby uložení kamerových záznamů. • Právo na přenositelnost údajů (čl. 20 GDPR) Neuplatní se, přenositelnost k novému správci nemá smysl, subjekt údajů však může uplatnit právo na přístup, kdy jsou mu poskytnuty obrazové záznamy o jeho osobě ve strojově čitelném formátu (viz výše). • Právo vznést námitku (čl. 21 GDPR) Subjekt údajů má právo vznést námitku např. prostřednictvím e-mailu správce uvedeného v hlavičce této informace. • Právo podat stížnost u dozorového úřadu (čl. 77 GDPR) Každý subjekt údajů (pokud se domnívá, že došlo k porušení obecného nařízení) má právo podat stížnost Úřadu pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7, tel. +420 234 665 111, e-mail posta@uoou.cz. var. pro kamery v režimu online: Právo na přístup k osobním údajům (čl. 15 GDPR), na opravu osobních údajů (čl. 16 GDPR), na výmaz osobních údajů (čl. 17 GDPR) a na přenositelnost údajů (čl. 20 GDPR) se neuplatní. • Právo na omezení zpracování (čl. 18 GDPR) a právo vznést námitku (čl. 21 GDPR) Subjekt údajů má právo vznést námitku např. prostřednictvím e-mailu správce uvedeného v hlavičce této informace. • Právo podat stížnost u dozorového úřadu (čl. 77 GDPR) Každý subjekt údajů (pokud se domnívá, že došlo k porušení obecného nařízení o ochraně osobních údajů) má právo podat stížnost Úřadu pro ochranu osobních

	údajů, Pplk. Sochora 27, 170 00 Praha 7, tel. +420 234 665 111, e-mail posta@uoou.cz.
Automatizované rozhodování včetně profilování	Správce nebude provádět automatizované rozhodování, včetně profilování.

Vzor 2 – PŘÍKLAD ZÁZNAMU O ČINNOSTECH ZPRACOVÁNÍ

Záznamy o činnostech zpracování dle čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů
I. Správce, účely zpracování, právní základ
Pořizování kamerového záznamu z monitorovaných prostor var.: Sledování obrazu kamer (online) z monitorovaných prostor **Správce:** Doplňte název správce, IČO správce, adresu správce, telefon správce, e-mail správce. Pověřená osoba správce: titul, jméno, příjmení, adresa, telefon a e-mail pověřence pro ochranu osobních údajů/pověřené osoby Umístění kamerového systému: Doplňte adresu umístění kamerového systému a počet kamer. **Účely:** - zvýšení ochrany majetku (krádež, vloupání, vandalismus), - zvýšení bezpečnosti osob (napadení, loupež, krádež, jiná fyzická újma) = ochrana života a zdraví osob - prevence mimořádných událostí, - získávání důkazního materiálu pro příslušné odpovědné orgány (soudy a Policie ČR v případě trestných činů, obecní úřady v případě řešení přestupků), - získávání materiálu pro řešení pojistných událostí (s věcně příslušnou pojišťovnou). **Právní základ:** - zpracování je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby - var.: zpracování se provádí na základě souhlasu subjektů údajů
II. Kategorie subjektů údajů
Osoby vstupující do monitorovaných prostor (žáci, studenti, obyvatelé domu, zaměstnanci, nakupující, další osoby vstupující do monitorovaných prostor apod.)
III. Kategorie osobních údajů
Obrazový záznam z kamerového systému var.: Obraz z monitorovaných prostor
IV. Kategorie příjemců
- orgány činné v trestním řízení v případě mimořádné události, - orgány činné v přestupkovém řízení v případě mimořádné události, - pojišťovny v případě řešení pojistné události, - subjekty údajů v případě jejich požadavku (jen záběry, kde se vyskytují tyto osoby, ostatní části jsou anonymizované), Správce nepředává osobní údaje příjemcům z třetích zemí.
V. Plánované lhůty pro výmaz jednotlivých kategorií osobních údajů
Data jsou uchovávána po dobu X dní.
VI. Obecný popis technických a organizačních bezpečnostních opatření
Následující výčet zahrnuje pokrytí nejpravděpodobnějších rizik zpracování; opatření k zabránění neoprávněnému přístupu k osobním údajům (řízení přístupu k datům), opatření proti ztrátě, odcizení nebo poškození dat (stanovení pravidel práce s paměťovými médii, umístění a ochrany záznamových zařízení), opatření v oblasti lidských zdrojů (stanovení pravidel pro práci s daty – stanovení rolí, proškolení osob) a opatření na ochranu dalších prostředků pro monitorování (kamery, kabely).

Vzor 3 - BALANČNÍ TEST KAMEROVÉHO SYSTÉMU, PŘÍKLAD ŘEŠENÍ ŠKOD V BYTOVÉM DOMĚ

Článek 6 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů umožňuje zpracovávat osobní údaje subjektu údajů na základě oprávněného zájmu správce osobních údajů či třetí strany. Pokud správce hodlá zpracovávat osobní údaje na základě oprávněného zájmu, je povinen provést balanční test (test vyváženosti) neboli test označovaný českým Ústavním soudem jako test proporcionality.

Balanční test má zohledňovat tři aspekty, které Pracovní skupina podle čl. 29 směrnice Evropského parlamentu a Rady 95/46/ES (WP29, předchůdce Evropského sboru pro ochranu osobních údajů) formulovala následovně:

i) důležitost oprávněného zájmu správce na zpracovávání osobních údajů;

ii) nezbytnost a důsledky zpracovávání osobních údajů pro subjekty údajů a

iii) zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.[30]

Ústavní soud v rámci testu proporcionality hodnotí tři kritéria, která jsou shodná se zmíněnými aspekty Balančního testu.[31] Dle Ústavního soudu by měl test proporcionality spočívat v posouzení následujících kritérií:

i) **kritérium vhodnosti**: zdali institut, omezující určité základní právo, umožňuje dosáhnout stanovený cíl;

ii) **kritérium potřebnosti (nutnosti)**: zdali by stanoveného cíle nemohlo být dosaženo jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod;

iii) **kritérium poměřování**: porovnání závažnosti obou v kolizi stojících základních práv, což spočívá ve zvažování empirických, systémových, kontextových i hodnotových argumentů.

Příklad bytového domu:

Bytový dům s 21 bytovými jednotkami, jedním vstupem a sklepními prostory v suterénu. Bytový dům se potýká s problémy, kdy dochází k posprejování fasády domu, ničení zámků u vstupních dveří, vykrádání sklepů a hodlá situaci řešit přijetím opatření včetně nasazení kamerového sledování.

Škody:

1. Poničena fasáda sprejery – předpoklady pro propočet:
    - několikrát ročně posprejováno,
    - rozsah poškození 25 m^2.

[30] Stanovisko WP29 č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/EC.

[31] Např. nález sp. zn. Pl. ÚS 3/14 ze dne 20. 12. 2016 (N 246/83 SbNU 793; 73/2017 Sb.), nález sp. zn. Pl. ÚS 4/94 ze dne 12. 10. 1994 (N 46/2 SbNU 57; 214/1994 Sb.).

2. Rozbité zámky u vchodových dveří:
    - 2× ročně.
3. Úklidové práce navíc.
4. Vykradené sklepy.

[*Poznámka 1: Intenzita posprejování za rok je u jednotlivých variant určena odhadem na základě:*

- *odrazujícího účinku kamerového systému (vědomí o existenci kamerového systému zbavuje původce incidentu pocitu bezpečné anonymity, na druhé straně intenzitu ovlivní režim kamerového systému, kdy v případě online dozoru může být na rozdíl od vyhodnocování záznamu kamer reakce správce okamžitá),*
- *odrazujícího účinku nátěru proti sprejerům (při dostatečně rychlém smytí výtvoru sprejera mizí částečně jeho motivace, protože nemůže svůj výtvor prezentovat).*

Poznámka 2: Vzhledem k tomu, že nátěr proti sprejerům vydrží 100 cyklů mytí, což při počtu mytí 12 za rok vychází zhruba na 8 let životnosti, byl zvolen srovnatelný časový úsek, ke kterému byly vztaženy náklady všech variant na 8 let.]

Definuje se účel zpracování:

Ochrana majetku, získání důkazních prostředků pro orgány činné v trestním řízení nebo získání důkazních prostředků pro pojišťovnu pro vyřízení pojistných událostí a prevence (odrazení pachatelů).

Zvažují se možná opatření:

Kamera na fasádě – je pořízen obrazový záznam, kamera s nočním viděním sleduje v omezené míře fasádu a přilehlý prostor (2 m od líce fasády), je zde určitý preventivní účinek (snížení frekvence událostí), účinnost proti sprejerům (záznam jako důkazní prostředek) je snížená, neboť mohou skrýt/maskovat svou tvář. Je to řešení, které nemusí úplně předcházet škodám.

Kamera u vstupu do objektu – je pořízen obrazový záznam, kamera s nočním viděním v omezené oblasti (cca 2 m ode dveří) zabírá osoby u vstupu nebo vstupující do objektu, nicméně může platit stejné jako v předchozím bodě (snížení frekvence událostí, ale jako důkazní prostředek v případě maskované cizí osoby je účinnost snížená). Je to řešení, které nemusí úplně předcházet škodám.

Kamera u sklepů – je pořízen obrazový záznam, kamera s nočním viděním zabírá osoby přicházející a odcházející chodbou ke sklepům. Lze předpokládat v kombinaci s dalšími opatřeními (omezení přístupu cizích osob do objektu) vysokou účinnost.

Ochranný nátěr – nátěr proti sprejerům je účinný, po nastříkání lze nasprejované obrazy 100× smýt bez nutnosti nanesení dalších vrstev (nicméně jsou společnosti, které po smytí nasprejovaných obrazců obnoví ochrannou vrstvu dalším nátěrem zdarma). Nelze použít jako důkazní prostředek a odrazující účinek spočívá v tom, že pokud je malba dostatečně rychle odstraněna, nemůže být autorem nikde prezentována. Zásah do soukromí není žádný.

Čipy – zajištění vstupu čipovými kartami – omezí ničení zámků a zabrání vstupu nepovoleným osobám (pokud je nevpustí někdo z obyvatel domu). Evidence přidělených čipů domácnostem (i jednočlenným), jsou přiděleny 3 čipy na domácnost. V případě mimořádné události kontrola průchozích čipů (tj. domácností) v určitou dobu.

Ceny:

Ceny jsou pouze ilustrativní, náhodně vyhledané na internetu pro účely zpracování příkladu, ceny určuje správce na základě podkladů nebo nabídek v konkrétní situaci.

1) Nátěry a mytí fasády (zasažená oblast 25 m^2, 12 cyklů ročně):
    - mytí fasády bez ochranného nátěru 300 Kč/m^2,
    - mytí fasády ochráněné nátěrem 144 Kč/m^2,
    - nátěr fasády 290 Kč/m^2,
    - nátěr proti sprejerům 990 Kč/m^2, vydrží 100 mycích cyklů, tj orientačně 8 let při 12 mycích cyklech ročně.
2) Přístup do objektu prostřednictvím čipového systému – cena 40 000 Kč (práce + materiál pro jedny vstupní dveře), cena 115 Kč/čip, náklady na provoz cca 2 000 Kč ročně, životnost čipového systému 8 let.
3) Přístup do objektu zámky – 5 000 Kč výměna zámku, včetně práce.
4) Kamerový systém – cena za 1 kameru 5 000 Kč, zařízení na uložení nahrávek 5 000 Kč, cena za práci 20 000 Kč/1 kamera, 22 000 Kč/2 kamery, 24 000 Kč/3 kamery, náklady na provoz cca 2 000 Kč/rok a kameru, životnost kamerového systému odhadem 8 let, poté je nutno kamerový systém vyměnit za nový.

i) Posouzení dosažení účelu jinými prostředky (varianty) – kritérium potřebnosti

1) VARIANTA 1 - NULOVÁ VARIANTA

Předpoklad – výtvory sprejerů jsou z fasády odstraňovány.

Škody:

1. Posprejovaná fasáda – předpoklady pro propočet:
    - 12x ročně posprejováno,
    - rozsah poškození 25 m^2,

   mytí fasády bez ochranného nátěru 300 Kč/m^2 (300x12x25 = 90 000 Kč/ročně),
   nátěr fasády 290 Kč/m^2 (290×12×25 = 87 000 Kč/ročně).
2. Rozbité zámky u vchodových dveří 2x ročně,
   zámky 2× ročně výměna 2×5 000 = 10 000 Kč včetně práce/ročně.
3. Úklidové práce navíc 15 000 Kč/ročně.
4. Vykradené sklepy škoda 25 000 Kč/ročně.

Celková škoda 237 177 Kč/rok; přepočteno za 8 let (kvůli vztažení na životnost nátěru proti sprejerům) 1 897 416 Kč/8 let.

Náklady:

Rovnají se škodám, tj. nákladům na odstranění škod 1 897 416 Kč/8 let.

Přínosy:

Nejsou u nulové varianty.

Zásahy do soukromí:

Žádné

2) VARIANTA 2 - 1 KAMERA NA FASÁDĚ, 1 U VCHODU a 1 U SKLEPŮ

předpoklady – snížení intenzity škod posprejováním fasády na hodnotu 4x ročně z důvodu odrazujícího účinku KS,

Škody:

1. Posprejovaná fasáda – předpoklady pro propočet:
    - 4× ročně posprejováno,
    - rozsah poškození 25 m^2

    mytí fasády bez ochranného nátěru 300 Kč/m^2 (300×4×25 = 30 000 Kč/ročně),
    nátěr fasády 290 Kč/m^2 (290×4×25 = 29 000 Kč/ročně).
2. Rozbité zámky u vchodových dveří 2x ročně,
    zámky 2x ročně výměna 2×5 000=10 000 Kč včetně práce/ročně.
3. Úklidové práce navíc 4 000 Kč/ročně.
4. Vykradené sklepy škoda 6 000 Kč/ročně.

Celková škoda 79 000 Kč/rok; přepočteno za 8 let (kvůli vztažení na životnost nátěru proti sprejerům) je to 632 000 Kč.

Náklady:

Odstranění škod 632 000 Kč/8 let.
Zřízení a provoz KS 92 000 Kč/8 let (15 000 + 5 000 + 24 000 + 48 000).
Celkem náklady 724 000 Kč/8 let.

Přínosy:

Úspora nákladů oproti nulovému stavu 1 897 416 - 724 000 = 1 173 416 Kč/8 let.

Zásahy do soukromí:

Zásah střední; daný tím, že je umístěna kamera u vchodu, který snímá kdo, s kým a v jakém stavu přichází domů, ve sklepech přichází obyvatelé domu nepravidelně a zřídka, u fasády je v záběru omezená oblast 1,5-2 m od fasády, která může zabírat kolemjdoucí jen v omezené míře.

3) VARIANTA 3 - 1 KAMERA NA FASÁDĚ, 1 U SKLEPŮ A NÁTĚR PROTI SPREJERŮM

předpoklady – snížení intenzity škod posprejováním fasády na hodnotu 3x ročně z důvodu odrazujícího účinku KS a rychlého smývaní nástřiků.

Škody:

1. Posprejovaná fasáda – předpoklady pro propočet:
    - 3× ročně posprejováno,
    - rozsah poškození 25 m^2,

    nátěr fasády 290 Kč/m^2 (290×1×25 = 7 250 Kč/8 let),
    nátěr fasády ochranným nátěrem 990 Kč/m^2 (990×1×25 = 24 750 Kč/8 let),
    mytí fasády s ochranným nátěrem 144 Kč/m^2 (144×3×25 = 10 800 Kč/ročně).
2. Rozbité zámky u vchodových dveří 2x ročně,
    zámky 2× ročně výměna 2×5 000 = 10 000 Kč včetně práce/ročně.
3. Úklidové práce navíc 4 000 Kč/ročně.
4. Poškozené a vykradené sklepy škoda 6 000 Kč/ročně.

Celková škoda 278 400 Kč/8 let.

Náklady:

Odstranění škod 278 400 Kč/8 let.
Zřízení a provoz KS 69 000 Kč/8 let (10 000 + 5000 + 22000 + 32 000).

Celkem náklady 347 400 Kč/8 let.

Přínosy:

Úspora nákladů oproti nulovému stavu 1 897 416 – 347 400 = 1 550 016 Kč/8 let

Zásahy do soukromí:

Zásah do soukromí je malý, kamery jsou umístěny u fasády a u sklepů, ve sklepech přichází obyvatelé domu nepravidelně a zřídka, u fasády je v záběru omezená oblast 1,5-2 m od fasády, která může zabírat kolemjdoucí jen v omezeném rozsahu a době. V záběrech kamer nejsou oblasti, kde by mělo docházet k projevům soukromého charakteru subjektů údajů.

4) VARIANTA 4 - 1 KAMERA U SKLEPŮ, VSTUP NA ČIPY, NÁTĚR PROTI SPREJERŮM

předpoklady – snížení intenzity škod posprejováním fasády na hodnotu 5x ročně z důvodu rychlého smývaní nástřiků.

Škody:

1. Posprejovaná fasáda – předpoklady pro propočet:
    - 5x ročně posprejováno,
    - rozsah poškození 25 m^2,

    nátěr fasády 290 Kč/m^2 (290×1×25 = 7 250 Kč/8 let),
    nátěr fasády ochranným nátěrem 990 Kč/m^2 (990×1×25 = 24 750 Kč/8 let),
    mytí fasády s ochranným nátěrem 144 Kč/m^2 (144×5×25 = 18 000 Kč/ročně).
1. Poničené čtecí čipové zařízení u vchodových dveří 2x ročně,
   2× ročně po 5 000 = 10 000 Kč/ročně, včetně práce.
2. Poškozené a vykradené sklepy škoda 2 000 Kč/ročně.

Celková škoda 272 000 Kč/8 let.

Náklady:

Odstranění škod 272 000 Kč/8 let.
Zřízení a provoz KS 46 000 Kč/8 let (5 000 + 5 000 + 20 000 + 16 000).
Zřízení čipového vstupního systému 63 245 Kč (životnost 8 let).
Celkem náklady 381 245 Kč/8 let.

Přínosy:

Úspora nákladů oproti nulovému stavu 1 897 416 - 381 245 = 1 516 171 Kč/8 let.

Zásahy do soukromí:

Zásah do soukromí je malý, ve sklepech přichází obyvatelé domu nepravidelně a zřídka. V záběru kamery nejsou oblasti, kde by mělo docházet k projevům soukromého charakteru subjektů údajů. V případě čipů je zpracována evidence přidělených čipů domácnostem (i jednočlenným), u mimořádné události proběhne kontrola průchozích domácností v určitou dobu.

5) VARIANTA 5 - VSTUP NA ČIPY A NÁTĚR PROTI SPREJERŮM (BEZ KAMER)

předpoklady – snížení intenzity škod posprejováním fasády na hodnotu 5x ročně z důvodu rychlého omývání nástřiků.

Škody:

1. Posprejovaná fasáda – předpoklady pro propočet:
    - 5× ročně posprejováno (není odrazující účinek kamer, pouze rychlým smytím odrazuje od častého opakování),

- rozsah poškození 25 m^2,

nátěr fasády 290 Kč/m^2 (290×1×25 = 7 250 Kč/8 let),
nátěr fasády 990 Kč/m^2 (990×1×25 = 24 750 Kč/8 let),
mytí fasády s ochranným nátěrem 144 Kč/m^2 (144×5×25 = 18 000 Kč/ročně).

2. Poničené čtecí čipové zařízení u vchodových dveří 2x ročně,
   2× ročně výměna 2×5 000 = 10 000 Kč včetně práce/ročně.
3. Úklidové práce navíc 4 000 Kč/ročně.
4. Poškozené a vykradené sklepy škoda 6 000 Kč/ročně.

Celková škoda za 8 let 336 000 Kč/8 let.

Náklady:

Odstranění škod 336 000 Kč/8 let.
Zřízení a provoz čipového systému 63 245 Kč (životnost 8 let).
Celkem náklady 399 245 Kč/8 let.

Přínosy:

Úspora nákladů oproti nulovému stavu 1 897 416 - 399 245 = 1 498 171 Kč/8 let.

Zásahy do soukromí:

Zásah do soukromí je malý, je zpracována evidence přidělených čipů domácnostem (i jednočlenným), u mimořádné události proběhne kontrola průchozích domácností v určitou dobu.

Výsledná přehledová tabulka

	Var. 1	Var. 2	Var. 3	Var. 4	Var. 5
Náklady	1 897 416	724 000	347 400	381 245	399 245
Koeficient nákladů	1	2	5	5	5
Přínosy	**0**	**1 173 416**	**1 550 016**	**1 516 171**	**1 498 171**
Koeficient přínosů	1	2	5	5	5
Zásah do soukromí	žádný	střední	malý	malý	malý
Koeficient zásahu	5	3	4	4	4
Součet koeficientů	7	7	14	14	14
Pořadí varianty	**5**	**4**	**1**	**2**	**3**

Z hlediska kritéria potřebnosti se jeví jako nejvýhodnější **VARIANTA 3 - JEDNA KAMERA NA FASÁDĚ, JEDNA KAMERA U SKLEPŮ A NÁTĚR PROTI SPREJERŮM**. Při stejném součtu koeficientů u variant 3, 4 a 5 má totiž varianta 3 nejvyšší absolutní hodnotu přínosů, a proto byla vyhodnocena jako nejlepší. (Vzhledem k srovnatelně velmi podobným hodnotám nákladů u variant 3, 4 a 5 byly u těchto variant stanoveny stejné koeficienty nákladů; analogicky byly stanoveny u variant 3, 4 a 5 stejné koeficienty přínosů s ohledem na srovnatelné hodnoty jejich přínosů.)

ii) Posouzení nezbytnosti zpracování osobních údajů v rámci vybraného řešení pro zajištění správcem definovaných účelů – kritérium vhodnosti

Analýza nefinančních přínosů:

Z hlediska subjektu údajů: preventivní/odrazující účinek navrhovaných řešení, tj. umístění informace o kamerovém systému a urychlené smytí nástřiků brzy po jejich objevení (neumožňuje prezentaci sprejerů). Možné zvýšení pocitu poškození soukromí.
Z hlediska obyvatel domu: relativní zvýšení pocitu bezpečí, zvýšení pohody (zejména z hlediska snížení počtu mimořádných událostí a rychlosti návratu k původnímu stavu – estetická nepospresejovaná fasáda).
Z hlediska správce: nastavení rutinních procedur řešení mimořádných událostí, pocit efektivně vynaložených prostředků.
Nefinanční přínosy nasazení kamerového systému jsou významné, ale ne natolik, aby samostatně zdůvodnily potřebnost nasazení zvoleného řešení.

Analýza škod:
Analýzu škod provedeme prostřednictvím vyhodnocení ročního rozsahu škod a jejich frekvence:

- koeficient rozsahu škod (jemuž má řešení předcházet):
  - vysoké škody (nad 50 000 Kč na majetku, závažné poškození zdraví, pracovní neschopnost delší než 21 dní, smrt) – hodnota 3,
  - střední škody (nad 5 000 do 50 000 Kč včetně na majetku, krátkodobá pracovní neschopnost do 21 dní) – hodnota 2,
  - malé škody (do 5 000 Kč včetně) – hodnota 1;
- koeficient frekvence událostí (které působí škody),
  - vysoká, tj. 1× za měsíc a častěji – hodnota 3,
  - střední, častěji než 1× za rok a zároveň méně často než 1 za měsíc – hodnota 2,
  - nízká, tj. méně často než 1× za rok – hodnota 1.

Oba určené koeficienty je nutno vynásobit, pokud je součin roven nebo vyšší než 3, je nasazení řešení opodstatněné. Pokud je součin nižší než 3, doporučuje se zvážit jiná opatření (než navrhované řešení), s výjimkou případů, ve kterých lze nefinanční přínosy nasazení řešení hodnotit jako velmi významné.
Konkrétně pro námi vybrané řešení (variantu 3)

1. Posprejovaná fasáda sprejery – předpoklady pro propočet:
   - 3× ročně posprejováno,
   - rozsah poškození 25 m^2,

   nátěr fasády 290 Kč/m^2 (290×1×25=7 250 Kč/8 let),
   nátěr fasády ochranným nátěrem 990 Kč/m^2 (990×1×25 = 24 750 Kč/8 let),
   mytí fasády s ochranným nátěrem 144 Kč/m^2 (144×3×25 = 10 800 Kč/ročně).
2. Rozbité zámky u vchodových dveří 2x ročně,
   zámky 2× ročně výměna 2×5 000 = 10 000 Kč včetně práce/ročně.
3. Úklidové práce navíc 4 000 Kč/ročně.
4. Poškozené a vykradené sklepy škoda 6 000 Kč/ročně.

Celková škoda 278 400 Kč/8 let. Průměrně je to 34 800 Kč/rok. Tato průměrná roční škoda odpovídá koeficientu rozsahu škod: střední škody (hodnota 2).
Frekvence událostí zpravidla 5× za rok (3x ročně posprejovaná fasáda a 2× ročně poškození zámku někdy spojené s vykradením sklepů). Tato roční frekvence odpovídá koeficientu frekvence: střední frekvence událostí (hodnota 2).

Součin koeficientů rozsahu škod a frekvence událostí je 2x2=4. Součin je tedy vyšší než 3, takže lze konstatovat, že nasazení vybraného řešení (varianty 3) je opodstatněné.

Analýza návratnosti řešení

Náklady:

Odstranění škod 278 400 Kč/8 let.

Zřízení a provoz KS 69 000 Kč/8 let (10 000 + 5 000 + 22000 + 32 000).

Celkem 347 400 Kč/8 let.

Přínosy:

Úspora nákladů oproti nulovému stavu 1 897 416 - 347 400 = 1 550 016/8 let.

Zjednodušená návratnost:

Poměr Přínosy/náklady = 1550016/347400 = 4,5. Je zřejmé, že předpokládané přínosy vybraného řešení (varianta 3) za uvažované osmileté období více než čtyřnásobně předčí jeho náklady.

Řešení se tedy správci finančně vyplatí, nasazení zvoleného řešení je opodstatněné.

Vzhledem k frekvenci a výši škod, návratnosti investice a nefinančním přínosům lze konstatovat vhodnost využití vybrané varianty pro zajištění práv správce a obyvatel domu.

iii) Posouzení přiměřenosti zpracování osobních údajů – kritérium poměřování

Posouzení přiměřenosti spočívá v porovnání na jedné straně práv a případných zájmů správce nebo třetí osoby (nejčastěji právo vlastnit majetek a jeho ochrana, svoboda podnikání, právo na informace, svoboda projevu, ochrana obydlí, ochrana života a zdraví apod.) nebo případných veřejných zájmů (např. veřejný pořádek, veřejné zdraví) a na druhé straně práv subjektu údajů (nejčastěji právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a ochranu jména, ochranu před neoprávněným zasahováním do soukromého a rodinného života, ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě apod.), zájmů subjektu údajů a případných dopadů na něj. Přičemž tímto posouzením správce dojde k závěru, zda existuje nebo neexistuje spravedlivý a přiměřený poměr mezi obhajobou práv a zájmů správce nebo třetích subjektů a veřejných zájmů, které mají být zajištěny zpracováním osobních údajů, na jedné straně, a zhoršením postavení základních práv subjektu údajů a dopadů na něj, k němuž v důsledku provedení zpracování osobních údajů dojde, na straně druhé. V našem případě provedeme posouzení přiměřenosti pro variantu 3 - JEDNA KAMERA NA FASÁDĚ, JEDNA KAMERA U SKLEPŮ A NÁTĚR PROTI SPREJERŮM. Pokud by posouzení přiměřenosti mělo záporný výsledek, bylo by nutné považovat vybranou variantu za nepřiměřenou a provést posouzení přiměřenosti pro variantu, která skončila v rámci i) posouzení dosažení účelu jinými prostředky jako další v pořadí, a která se zároveň v rámci ii) posouzení nezbytnosti ukázala jako vhodná.

Správce:

Míra zajištění práv a zájmů

- **správce** – ochrana majetku správce (ochrana fasády, snížení nákladů na úklid)
- **třetích osob** – ochrana majetku obyvatel domu (sklepy)
- **veřejných zájmů** – částečný vliv na veřejný pořádek (možnou identifikací pachatelů Policí ČR na základě předaných záznamů)

se při dané variantě 3, vzhledem k úsporám nákladů, kterých správce, a potažmo i obyvatelé domu, dosáhnou oproti stávajícímu (nulovému) stavu

- velmi významně zlepší (1 bod),
- ***významně zlepší (2 body),***
- středně zlepší (3 body),
- málo se zlepší (4 body),
- zůstane beze změny nebo se zhorší (5 bodů).

- **Nároky na činnost správce**, vzhledem k nutnosti prohlížet záznamy z kamerového systému pouze v případě výskytu mimořádných událostí (v ostatních případech se kamerový záznam kontinuálně přepisuje),
  - zůstanou beze změny nebo poklesnou (pod 100 % původního stavu) (1 bod),
  - ***málo narostou nebo téměř beze změny součinnosti (oproti původnímu stavu), méně než 1 hodina denně na zaměstnance, přepočtený počet vyčleněných zaměstnanců 1 a méně (2 body),***
  - středně narostou (do 150 % původního stavu), více než 1 hodina denně na zaměstnance, počet vyčleněných zaměstnanců 2-3 (3 body),
  - významně narostou (do 200 % původního stavu), více než 4 hodiny denně na zaměstnance, přepočtený počet vyčleněných zaměstnanců 4-19 (4 body),
  - velmi významně narostou (nad 200 % původního stavu), 8 hodin denně na zaměstnance, počet vyčleněných zaměstnanců 20 a více (5 bodů).
- **Případný dopad na správce při kompromitaci, pozměnění či znepřístupnění údajů,** stanovený dle metodiky DPIA, tabulka na straně 19, ale za celé zpracování, odpovídá úrovni 1/nízká [tzn. může negativně ovlivnit vztahy s jinými částmi správce, jinými subjekty nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání (nepříjemnosti se subjekty údajů, nutnost jednání s dalšími subjekty, negativní, někdy i veřejné reakce subjektů údajů apod.), může způsobit krátkodobé nepříjemnosti při zpracování osobních údajů (zdržení a podráždění zaměstnanců nebo členů správce, jiné zdravotní dopady nehrozí)] – **1 bod.**

Součet rovná se 5.

Subjekt údajů:

- **Míra narušení práv a zájmů subjektů údajů, kterou** lze charakterizovat především tím, že je zasaženo právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života obyvatel domu, ovšem vzhledem k umístění kamer na méně citlivých místech (na fasádě a u sklepů),
  - se sníží (1 bod),
  - zůstane beze změny 2 (body),
  - ***málo se zvýší (3 body)***,
  - významně se zvýší (4 body),
  - velmi významně se zvýší (5 bodů).

- **Nároky na součinnost subjektů údajů**, s ohledem na to, že součinnost subjektů údajů se při navrženém řešení nevyžaduje,
    - poklesnou (pod 100 % původního stavu) (1 bod),
    - ***zůstanou beze změny (beze změny součinnosti oproti původnímu stavu), nulová součinnost (2 body)***,
    - málo narostou (do 120 % původního stavu), malá součinnost do 1 hod/měsíc a subjekt (3 body),
    - středně narostou (pod 170 % původního stavu), střední součinnost od 1 do 5 hod/měsíc a subjekt (4 body),
    - významně narostou (nad 170 % původního stavu), významná součinnost nad 5 hodin/měsíc a subjekt (5 bodů).
- **Případný dopad na subjekt údajů při narušení důvěrnosti, pozměnění či znepřístupnění údajů**, stanovený dle metodiky DPIA, tabulka na straně 19, ale za celé zpracování, odpovídá v případě obyvatel domu při úniku záznamu kamer úrovni 1/nízká (finanční újma nehrozí, může vést k nepohodlí subjektu údajů) – **1 bod**.

Součet rovná se 6.

Vzhledem k výsledným hodnotám lze konstatovat, že zpracování osobních údajů má významný vliv na zajištění práv a zájmů správce (ochrana majetku), oproti tomu zásah do práv, svobod a zájmů subjektů údajů je malý (kamery monitorují fasádu a prostor u sklepů). Lze tedy uvést, že zajištění práv správce zpracováním osobních údajů je kompenzováno přiměřeným zhoršením zásahu do práv, svobod a zájmů subjektů údajů. Zhoršení postavení práv subjektů údajů ovlivňuje a omezuje na přijatelnou míru:

1) Analýza očekávání subjektů údajů od zpracování osobních údajů:

Neproběhl průzkum mezi subjekty údajů. V kontextu navrhovaného řešení lze předpokládat, že očekávání subjektu údajů od zpracování osobních údajů se neliší od skutečného stavu, který lze popsat tak, že monitorovány jsou subjekty procházející v záběru kamer, zejména ty, které poškozují majetek správce u fasády domu a majetek správce a obyvatel domu u sklepů. Záznamy jsou automatizovaně přemazávány v přiměřeném době s výjimkou mimořádných událostí. Záznamy mimořádných událostí mohou být předány orgánům činným v trestním řízení, případně pojišťovně. Na vyžádání subjektu údajů jim budou předány záznamy o jejich osobě, přičemž ostatní osoby na stejném záznamu budou anonymizovány (zakrytím, rozmazáním, vymaskováním apod.).

2) Analýza postavení správce:

Postavení správce (majitel objektu) vůči subjektům údajů (obyvatelé domu a další subjekty vstupující do monitorovaných prostor) není výrazně dominantní (realizaci řešení, včetně investice do zřízení kamerového systému budou schvalovat obyvatelé domu na schůzi).

3) Popis dodržování základních zásad zpracování osobních údajů

zákonnost, korektnost a transparentnost

- ***právní základ zpracování osobních údajů*** – Ochrana oprávněných zájmů správce a obyvatel domu, spočívá v ochraně před posprejováním vnější fasády objektu, rozlomením zámků u dveří, vykradením a poničením sklepů a znečištěním vnitřních prostor objektu.

- ***zajištění informovanosti subjektů údajů*** – Správce vysvětlí subjektům údajů jasným a uživatelsky přívětivým způsobem důvody, proč se domnívá, že zájmy nebo základní práva a svobody subjektů údajů nepřevažují nad zájmy správce, a vysvětlí jim rovněž ochranná opatření, která přijal na ochranu osobních údajů. Informovanost bude probíhat dvouúrovňově, jednak cedulkami (obsahují piktogram kamery, údaj o monitorování kamerovým systémem se záznamem, identifikaci správce, odkaz na kontaktní osobu, odkaz na web, kde je možné získat další informace, účel zpracování osobních údajů a text „jako subjekt údajů máte možnost uplatnit vůči správci několik práv, jakými jsou právo na přístup k osobním údajů a právo na výmaz svých osobních údajů“) umístěnými u vstupů, jednak informací o zpracování osobních údajů (obsahuje účely zpracování, rozsah zpracování, identifikaci správce, místo zpracování, právní základ zpracování, příjemci, počet kamer, umístění, doba uchování záznamů, přepis údajů ve smyčce, režim fungování kamer, popis práv subjektu údajů) umístěnými na webu správce, dále ve vývěsní skříňce v přízemí domu, a bude rozdána zástupcům jednotlivých domácností na schůzi.
- ***zajištění přístupu k osobním údajům*** – Osobní údaje jsou předávány
    - oprávněným subjektům, kterými jsou subjekty údajů, případně jejich zákonní zástupci na základě jejich požadavku (v rozsahu záznamů obrazových záznamů uchovávaných o těchto subjektech, ostatní subjekty budou na předaných záběrech anonymizovány),
    - subjektům, kterým jsou kamerové záznamy poskytovány na základě jejich žádosti o přístup k údajům a na základě souhlasu (všech) subjektů údajů, které jsou na záznamech zachyceny,
    - jiným správcům, a to orgánům činným v trestním a přestupkovém řízení a pojišťovnám při řešení pojistných událostí.

  K zajištění budou vypracována podrobnější pravidla přístupná na webu správce.
- ***zajištění práva na opravu*** – V případě kamerového záznamu se neuplatní, protože je u nich ukládán obraz, který zjevně nelze upravovat na základě podezření z chyby nebo nepřesnosti osobních údajů. Správce technickými a organizačními opatřeními zajistí, aby se záznamem nikdo neoprávněný nemanipuloval, a aby o práci se záznamem oprávněných osob existoval záznam.
- ***zajištění práva na výmaz*** – Vzhledem k tomu, že je záznam uchováván po omezenou dobu (7 dní, v období hlavních prázdnin 14 dní), pouze v případě mimořádných událostí je záznam o nich uchováván do doby uzavření případu příslušnými orgány (policie, soudy, pojišťovny), je právo na výmaz obtížně řešitelné. Ve lhůtě vyřízení (30 dní) bude až na výjimky (zachycení mimořádných událostí, uplatnění práva omezení zpracování) záznam již vymazán. Přesto má subjekt údajů právo podat žádost o výmaz, která musí být podána na určený kontakt zveřejněný na webu správce tak, aby bylo možno identifikovat žadatele a období, o které se jedná, žádost je vyřizována ve lhůtě (30 dní), včetně odpovědi žadateli, a výmaz (pokud je uplatnitelný) probíhá vystřižením, smazáním, rozostřením nebo vymaskováním části záznamu.

  Záznamy, u kterých je subjektem údajů uplatněno právo na omezení zpracování (omezení použití nebo uchování pro určení, výkon nebo obhajobu právních nároků subjektu údajů nebo z důvodu vznesení námitky proti zpracování založeném na

oprávněných zájmech správce), mohou být vymazány teprve poté, co bylo omezení zpracování zrušeno.

- ***zajištění práva na omezení zpracování*** – právo na omezení zpracování, pokud správce údaje již nepotřebuje se uplatní:
  - Pokud subjekt údajů požádal o omezení zpracování (údaje jsou pak uloženy bez jakékoliv změny) z důvodu určení, výkonu nebo obhajoby právních nároků. Takové kamerové záznamy potom mohou být nadále zpracovávány po dobu správcem určené doby uchování a poté jen z těchto důvodů (pro vlastní určení, výkon nebo obhajobu právních nároků subjektu údajů a pro potřeby orgánů činných v trestním nebo přestupkovém řízení nebo pro potřeby pojišťovny).
  - Pokud subjekt vznesl námitku proti zpracování kamerového záznamu. Až do prokázání závažných důvodů správce, které převažují nad zájmy nebo právy a svobodami subjektů údajů (viz celá tato analýza), nebo do vymazání záznamu mohou být kamerové záznamy nadále zpracovávány jen se souhlasem subjektu údajů, který o omezení požádal, nebo pro určení, výkon nebo obhajobu právních nároků subjektu údajů nebo pro potřeby orgánů činných v trestním nebo přestupkovém řízení nebo pro potřeby pojišťovny.

  Správce na svém webu zpřístupní popis postupů podání a vyřizování žádostí o omezení zpracování osobních údajů.
- ***zajištění práva na přenositelnost osobních údajů*** – není v případě kamerových systémů relevantní. Je řešeno v rámci práva subjektu údajů na přístup k osobním údajům, kdy má subjekt údajů právo získat kamerové záznamy o jeho osobě.
- ***zajištění práva na podání námitky proti zpracování osobních údajů*** – správce upraví a zpřístupní postup a formu práva vznést námitku na webu, přičemž zohlední následující aspekty (identifikace žadatele, identifikace kamer nebo jejich nastavení, zdůvodnění žádosti, termíny vyřízení žádosti, informace žadatele o postupu, analýza námitky, zdůvodnění výsledku analýzy, opatření správce).
- ***popis automatizovaného zpracování*** – automatizované zpracování není použito.

účelové omezení – Dle ii) posouzení nezbytnosti zpracování osobních údajů a i) posouzení dosažení účelu jinými prostředky se jeví vybrané řešení pro zajištění správcem definovaných účelů, kterými jsou ochrana majetku, získání důkazních prostředků pro orgány činné v trestním řízení nebo pojišťovnu a preventivní účely, jako přiměřené a účelné.

minimalizace údajů – Je zpracováván obrazový záznam z kamer umístěných u méně citlivých prostor (fasády, sklepy), údaje jsou zpracovávány pouze v případě mimořádných událostí, jinak je záznam kontinuálně přepisován, záběry kamer jsou omezeny na veřejných prostranstvích na míru nezbytně nutnou (cca 2 m od fasády, aby bylo možno identifikovat pachatele mimořádných událostí); doba uchování, viz níže v bodě omezené uložení.

přesnost – Přesnost osobních údajů je založena na charakteru osobních údajů (kamerový záznam) doplněného o opatření, která zabrání neoprávněné manipulaci s kamerovým záznamem (vymazání, krácení, prostřihání apod.), a o opatření, která zajistí vedení záznamů o oprávněné manipulaci s kamerovým záznamem.

omezené uložení – Navržená doba uchování osobních údajů je 7 dní (pro případ řešení mimořádné události o víkendech nebo kratších svátcích), v případě období hlavních prázdnin a dovolených může být prodloužena na 14 dní (z důvodu nepřítomnosti oprávněné osoby a dalších osob, jejichž sklepy mohou být zasaženy mimořádnou událostí).

zajištění integrity, dostupnosti a důvěrnosti osobních údajů – Vzhledem k tomu, že není potřeba zpracovávat DPIA, jsou pro minimalizaci rizik pro práva a svobody subjektů údajů navržena následující opatření vyplývající ze třídy kamerového systému stanovené dle této metodiky bod 3.8.1.3.

Stanovení třídy bezpečnosti kamerového systému je dán součinem koeficientu dopadů x koeficientu frekvence x koeficientu míry porušení práv a zájmů subjektů údajů = (1x1) x2 x3 = 6, to znamená **1. třída bezpečnosti kamerového systému.**

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ
OPATŘENÍ NA OCHRANU KAMER, DATOVÉHO PŘIPOJENÍ
detekce selhání KS (přerušení přenosu dat)
ochrana venkovních kamer a rozvodů před vlivy počasí
ochrana datového připojení (kabelů apod.)
OPATŘENÍ NA OCHRANU ZÁZNAM. ZAŘÍZENÍ A DATOVÝCH NOSIČŮ
umístění v chráněném prostoru
evidence přístupu
OPATŘENÍ NA OCHRANU DAT (kamerových záznamů)
řízení přístupu k datům (autentizace, autorizace)
monitorování a zaznamenávání činnosti (vyhledávání, přehrávání, vymazání, úprava, ukládání, tisk, předávání)
autentizace dat (opatření proti narušení integrity dat)
ukládání údajů o čase
bezpečný výmaz dat po uplynutí doby uchovaní
OSTATNÍ OPATŘENÍ
ochrana před škodlivými kódy
školení obsluhy
zpracování dokumentace
řízení dodavatelů a zpracovatelů

Závěr:
Zvolené řešení, tj. jedna kamera na fasádě, jedna kamera u sklepů a nátěr proti sprejerům, významně chrání práva správce a obyvatel domu (zejména ochrana majetku) a je přiměřené z hlediska zásahu do práv subjektů údajů (zejména právo ochranu před neoprávněným zasahováním do soukromého a rodinného života subjektů údajů), a to s přihlédnutím k postavení správce a subjektů údajů, možnému očekávání subjektů údajů od zpracování osobních údajů a analýzy dodržování základních zásad zpracování osobních údajů.