



Kamerový systém ve městě Dačice

Správcem zpracování osobních údajů je město Dačice, se sídlem Krajířova 27/I, 380 01 Dačice, IČO 00246476. Informace o kamerovém systému je možno získat na e-mailové adrese poverenec@dacice.cz, tel. 384 401 282 či na mestska.policie@dacice.cz na tel. 602 486 070.

Důvody pořízení městského kamerového dohlížecího systému (účel)

- snížení páchané majetkové trestné a přestupkové činnosti (zejména tzv. pouliční kriminality, např. krádeží, projevů vandalismu),
- snížení počtu násilné trestné a přestupkové činnosti (fyzického násilí)
- zlepšení stavu veřejného pořádku (např. snížení míry znečišťování veřejného prostranství)
- preventivní funkce (přítomnost kamer odrazuje pachatele nejen od páchaní trestné a přestupkové činnosti, ale i od dalších negativních sociálních patologických jevů)
- vytváření bezpečných zón a zvýšení pocitu bezpečí (v rizikových lokalitách nebo nočních hodinách, např. v parcích).

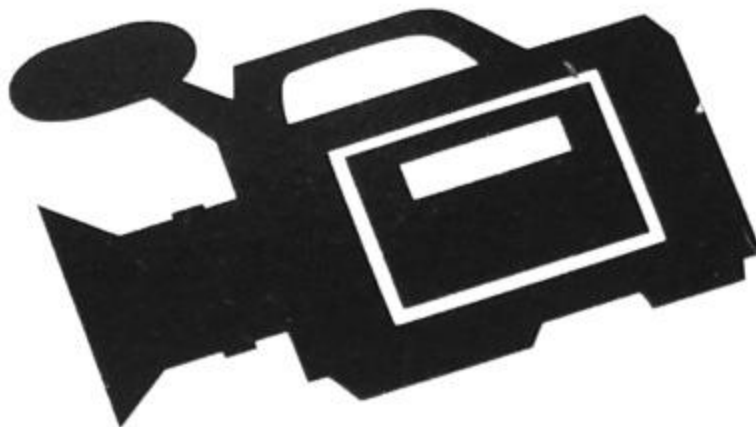
Právním základem pro budování městského kamerového systému je zákon č. 553/1991 Sb. o obecní policii a zákon č. 273/2008 Sb. o Polici ČR, který stanovil specifické podmínky pro provozování kamerových systému. Monitorování veřejného prostranství je tak prováděno ze zákona při výkonu veřejné moci a ve veřejném zájmu.

V roce prosinci 2025 byl městskou policií vybudován městský kamerového dohlížecího systému, na Palackého nám. v Dačicích, který obsahuje prvních 3 kamerové body a celkem 8 kamer s tím, že monitorovací pracoviště bylo zřízeno na stálé službě městské policie na Palackého nám. čp. 31. Nepřetržitý (24hodinový) monitoring provádí městská policie, ale záznamy si mohou vyžádat i policisté obvodního oddělení.

Souběžně s městským dohlížecím kamerovým systémem provozuje městská policie a město Dačice i vnitřní kamerový systém, který zejména slouží k ochraně vnitřních prostor budovy č.p. 4 (KD Beseda) a čp. 31 (služebna Městské policie Dačice) před jejím poškozením, dále pro zajištění ochrany života a zdraví osob.

Město Dačice disponuje směrnicí Rady města Dačice č. R2-2025 a směrnicí tajemníka T2-2025. Tyto směrnice stanoví postupy pro pořizování, uchovávání a správu audiovizuálních dat z kamerového systému provozovaného na objektech města Dačice v souladu s nařízením GDPR a zákonem o zpracování osobních údajů, a na základě zákona o obecní policii, podle něhož obecní policie zabezpečuje místní záležitosti veřejného pořádku, příp. plní další úkoly stanovené právními předpisy, a to mimo jiné tím, že přispívá k ochraně a bezpečnosti osob a majetku.

Informační tabulka – vzor pro použití – monitorované veřejné prostory



PROSTOR NÁMĚSTÍ JE MONITOROVÁN KAMEROVÝM SYSTÉMEM SE ZÁZNAMEM

Správcem zpracování je město Dačice, se sídlem Krajiřova 27/I, 380 01 Dačice, IČO 00246476. Informace o kamerovém systému je možno získat na e-mailové adrese poverenec@dacice.cz, tel. 384 401 282 či na mestska.policie@dacice.cz na tel. 602 486 070.



Záznam o činnosti - kamerový systém města Dačice:

Organizační zabezpečení:

Označení		
Proces		Interní procesy
Agenda/činnost		Provoz kamerového systému
Dokumenty s osobními údaji		Záznam z kamerového systému 8 kamer
Zákonnost zpracování osobních údajů	Souhlas subjektu údajů	Ne
	Plnění zákonné povinnosti organizace (uvést zákon), nebo pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci	Plnění úkolů ve veřejném zájmu
	Plnění smlouvy	Ne
	Ochrana životně důležitých zájmů subjektu údajů	Ne
	Oprávněný zájem správce (bez zákonných důvodů)	Zpracování je nezbytné pro ochranu oprávněných zájmů správce nebo třetí osoby.
Účel zpracování osobních údajů		Osobní údaje osob vstupujících do monitorovaných prostor jsou zpracovávány za účelem: <ul style="list-style-type: none"> • 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).
Kategorie osobních údajů	Základní osobních údaje	Obraz kamerového systému
	Zvláštní osobní údaje	
Kategorie subjektů údajů		Osoby vstupující do monitorovaných prostor a prostranství
Zdroje osobních údajů		Kamerový systém
Osobní údaje vč. jejich	Informační systém (IS)	IS kamerového systému (přístup zabezpečen uživ. jménem a heslem) 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).
	PC, server, cloud, přenositelné	
	Úložiště listinných forem	
Období uchovávání	Od kdy	Od zahájení snímání
	Doba uložení osobních údajů	10 dnů 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 či IZS, kdy je záznam uchován až do vyřízení mimořádné události, a pak teprve vymazán
Pracovníci správce, jimž mohou být osobní údaje zpřístupněny a důvod přístupu		Informatici – správa systému Strážníci Městské policie Dačice – výkon jejich činnosti dle zákona o obecní policii
Příjemci osobních údajů mimo správce a subjekt údajů		V případě mimořádné události orgány činné v trestním řízení nebo správní orgány pro účely přestupkového řízení, IZS, Pojišťovny v případě řešení pojistné události, Subjekty údajů v případě jejich požadavku (jen záběry, kde se vyskytují tyto osoby, ostatní části jsou anonymizované).
Druh zpracování osobních údajů		Se záznamem: snímání, přenos, zobrazení, zpracování, ukládání, výmaz On-line: snímání, přenos, zobrazení
Počet záznamů		10 dnů videozáznamu

Záznam s osobními údaji není předáván do třetích zemí nebo mezinárodním organizacím a není na něm aplikováno automatizované rozhodování ani profilování osobních údajů.

Formulář žádosti – vzor

Požadavek na informaci, změnu, omezení zpracování, nebo výmaz osobních údajů v rámci kamerového záznamu

Identifikace žadatele (dále „žadatel“)	
Jméno a příjmení	
Datum narození	
Adresa trvalého pobytu	
Identifikace dítěte *)	
Identifikace organizace, které je požadavek adresován (dále „organizace“)	
Název, sídlo, IČ	Město Dačice, se sídlem Krajířova 27/I, 380 01 Dačice, IČO 00246476, prostřednictvím Městské policie Dačice
Pověřenec organizace (dále „Pověřenec“)	JUDr. Eva Škodová, tel. 384 401 282, e-mail: poverenec@dacice.cz

*) pokud žádá zákonný zástupce za dítě, které je zobrazeno na kamerovém záznamu

Žádám organizaci, jako správce záznamu z kamerového systému, o (označte):

- poskytnutí kamerového záznamu (pokud není možno čas přesně určit, musí se žadatel dostavit na správcem určené místo za účelem přesného určení časového úseku pro export záznamu.)
- opravu/úpravu času na záznamu z kamerového systému (není nutná identifikace žadatele fotografií a popisem oblečení viz níže)
- omezení zpracování záznamu z kamerového systému z důvodu (ve zdůvodnění žádosti uvést důvod, proč se žadatel 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).
- vznesení námítky proti zpracování záznamu z kamerového systému (uplatnitelné pouze u kamer. Systémů provozovaných pro ochranu oprávněných zájmů správce nebo třetí osoby dle čl. 21 GDPR, ve zdůvodnění žádosti uvést důvod, proč se žadatel domnívá, že zpracování neprobíhá na základě závažných důvodů, které převažují nad zájmy nebo právy a svobodami subjektů údajů)
- výmaz záznamu z kamerového systému (žádosti nebude vyhověno v části záznamu, který zachycuje mimořádné události, pro jejichž zachycení byl kamerový systém zřízen – tyto budou vymazány až po jejich vyřízení příslušnými orgány).

Zdůvodnění žádosti:

.....
.....
.....
.....
.....
.....
.....
.....

Identifikace žadatele na kamerovém záznamu (je-li to pro vyřízení žádosti relevantní - organizace musí být schopna žadatele na základě níže uvedených skutečností na záznamu jednoznačně identifikovat):

- přílohou žádosti fotografie žadatele (z více úhlů pohledu, aby bylo možné identifikovat žadatele), na které je žadatel zobrazen tak, jak vypadal v níže uvedeném období pořízení záznamu,
- detailní popis oblečení, které měl žadatel na sobě v době pořízení záznamu a příp. popis věcí které nesl.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Identifikace kamery (kamer) snímající kamerový záznam jehož se žádost týká:

.....
.....

.....
.....
Žádost se týká části záznamu výše uvedené kamery (kamer) v období:
od data času..... do data..... času

Poučení:

Organizace má na vyřízení žádosti 30 dnů, které v odůvodněných případech může prodloužit až na 90 dnů. Uvedené osobní údaje budou zpracovávány pověřenými osobami organizace za účelem vyřízení této žádosti. V případě, že byste zjistili, že zpracování poskytnutých osobních údajů je v rozporu s ochranou Vašeho soukromého a osobního života, nebo v rozporu se zákonem, můžete organizaci požádat o vysvětlení a odstranění takto vzniklého stavu a máte právo podat stížnost u pověřence, nebo dozorového úřadu, kterým je Úřad na ochranu osobních údajů www.uoou.cz. Bližší informace o zpracování osobních údajů organizací a Vašich právech jsou uvedeny na www.dacice.cz v sekci GDPR anebo se informujte přímo u pověřence města Dačice pro ochranu osobních údajů na e-mailu poverenec@dacice.cz anebo na tel. 384 401 282.

V
.....

dne

Podpis žadatele

Stanovení úrovně technickoorganizačních bezpečnostních opatření

U kamerových systémů s vysokým rizikem pro práva a svobody subjektů údajů se návrh technických a organizačních opatření provádí v rámci řešení DPIA – z provedené analýzy vyplynulo, že tento kamerový systém může být s vysokým rizikem pro práva a svobody subjektů údajů.

1) Klasifikace kamerového systému z hlediska bezpečnosti na základě stanovení míry porušení práv a zájmů subjektů údajů

Specifikace jednotlivých tříd:

Třída 1 - malá míra porušení

- kamery bez záznamu (v režimu on-line); prostý kamerový záznam; umístění kamer a monitorování prostor, kam subjekty údajů obvykle nevstupují, například záznam jakéhokoliv prostoru v mimoprovozních hodinách (škola, úřad, hřiště), monitorování perimetru budov v některých místech apod.,
- 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, kontejnerová stání, parkovací místa, vstupy do administrativních budov apod.),

Třída 2 – střední míra porušení

- 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 pro odložení svrchního oděvu (kabáty, boty, čepice, tašky apod.) ve školách, divadlech, kinech a restauracích, některé prostory prodejen, kamery v automobilech, některé veřejné prostory (letišť, metro, nádraží, náměstí),

Třída 3 – vysoká míra porušení

- monitorování vstupů do šaten, prostor šaten pro odložení oděvu a osobních věcí (pokud jsou vyčleněny nemonitorované prostory pro převlečení) v tělocvičnách, bazénech, fitness a saunách, některé prostory bazénů (například dojezd a nástup atrakcí), chodby škol, prostory pokladen, vstupy do kuřáren a odpočinkových místností, čekárny zdravotnických zařízení, výtahy;

Třída 4 – velmi vysoká míra porušení

- prostý kamerový záznam monitorování citlivých prostor jako jsou trvalá pracoviště při zvláštní povaze činnosti, riziková pracoviště jednotlivých úřadů (napadání zaměstnanců); biometrické kamerové záznamy; pořizování zvuku; pořizování polohy subjektů údajů při pohyblivých kamerách.

Tabulka 1 – přehled opatření

č.	TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ	Tr. 1	Tr. 2	Tr. 3	Tr. 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 uchování	P	P	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

* 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 sítě, nebo pokud jsou do zpracování zapojeni zpracovatelé.

Zkratky použité v tabulce: P (povinné opatření), D (doporučené opatření)

**Závěr: Tento kamerový systém spadá do třídy 2 (tj. druhá hodnota níže).
(význam hvězdiček a zkratk viz předchozí strana)**

OPATŘENÍ NA OCHRANU KAMER, DATOVÉHO PŘIPOJENÍ

1. detekce selhání KS (přerušení přenosu dat) X D P P
2. detekce událostí (zakrytí nebo oslepení kamery) X X D P
3. detekce nahrazení signálu kamery X X 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 X D D P

OPATŘENÍ NA OCHRANU ZÁZNAM, ZAŘÍZENÍ A DATOVÝCH NOSIČŮ*

7. umístění v chráněném prostoru P P P P
 - umístění v uzamykatelných prostorách s omezeným přístupem osob s elektronickým bezpečnostním systémem
8. evidence přístupu P P P P
 - řešeno v rámci IS kamerového systému a knihy kamerového systému

OPATŘENÍ NA OCHRANU ZOBRAZOVACÍHO ZAŘÍZENÍ (online obraz)

9. řízení přístupu osob do prostoru umístění zařízení P P P P
 - přístup pouze oprávněným osobám, nebo za přítomnosti oprávněných osob
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
 - přístup chráněn heslem
12. monitorování a zaznamenávání činnosti (vyhledávání, přehrávání, vymazání, úprava, ukládání, tisk, předávání) P P P P
 - řešeno v rámci IS kamerového systému a knihy kamerového systému
13. autentizace dat (opatření proti narušení integrity dat) ** D D P P
14. ukládání údajů o čase P P P P
 - údaje o čase uloženy v rámci videozáznamu
15. bezpečný výmaz dat po uplynutí doby uchování P P P P
 - mazáno automaticky bez nutnosti zásahu obsluhy
16. zálohování XXXP

OSTATNÍ OPATŘENÍ

17. ochrana před škodlivými kódy*** D D P P
18. školení obsluhy P P P P
 - dodavatelem, nebo vyškoleným pracovníkem správce
19. zpracování dokumentace P P P P
 - log, soubor IS kamerového systému + Provozní kniha kamerového systému
20. řízení dodavatelů a zpracovatelů*** P P P P
 - dodavatel zvolen výběrovým řízením

2) Popis technických a organizačních opatření pro 4 druhy hrozeb:

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, bezpečnostní kryty kamer

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),

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,

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

Přijatá technická a organizační opatření: řízení přístupu uživatele (přihlašovací jméno, heslo), 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, zálohování záznamů, oddělení kamerového systému od datových sítí, 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 systému.

d) živelní událost a povětrnostní podmínky

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

3) Způsob ověřování funkčnosti technických a organizačních opatření:

Typ kontroly	Způsob kontroly	Odpovídá
periodická	1x měsíčně kontrola funkčnosti kamer a záznamového zařízení – fyzickou kontrolou záznamu z kamer 1x měsíčně vizuální kontrola fyzického porušení kamer	Administrátor kamerového systému
průběžná	Kontrola ukládání záznamu z kamer	Administrátor kamerového systému
průběžná	Sledování technického vývoje a porušování technického	Administrátor

	zabezpečení kamerových systémů	kamerového systému
nahodilá	Kontrola zabezpečení kamerového systému	Administrátor kamerového systému
Na základě události	Kontrola funkčnosti zabezpečovacích prvků v případě mimořádné události (porušení zabezpečení)	Administrátor kamerového systému
periodická	Město Dačice provede prostřednictvím starosty nebo jím pověřeného zaměstnance jednou za kalendářní rok kontrolu vedení Provozní knihy kamerového systému.	Správce za součinnosti Administrátora kamerového systému

Výsledky kontrol vč. návrhů ke zvýšení úrovně bezpečnosti vyplývajících z těchto kontrol budou předloženy vedoucímu odboru správního, který rozhodne o dalším postupu.

Posouzení úrovně rizikovosti zpracování osobních údajů

Posouzení úrovně rizikovosti zpracování osobních údajů

Hodnocení rizikovosti dle metodického pokynu ÚOOÚ „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů ver.01“



seznam-operaci-zpracovani-nepodlehajicic

Hodnoty:

- 1 – nízká hodnota
- 2 – významná hodnota
- 3 – kritická hodnota

Činnost s vysokým rizikem pro práva a svobody subjektů údajů obsahuje min. dvě kritické hodnoty, nebo jednu kritickou a pět významných hodnot

P.č.	Kritérium	Hodnocení
1	Zpracování zahrnuje monitorování subjektu údajů	Subjekty údajů jsou identifikované/identifikovatelné a rozpoznatelné 2
2	Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektu údajů	Jedná se o běžné údaje. 1
3	Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí	Omezená zranitelnost. 1
4	Zpracování osobních údajů velkého rozsahu	Zpracování osobních údajů malého rozsahu 1
5	Zpracování zahrnující snímání veřejně přístupných	Podrobná úroveň – místa veřejně 3

	prostor	přístupná	
6	Zpracování osobních údajů s omezeným ovlivněním subjekty údajů	Subjektem údajů neovlivnitelné zpracování a předání	3
7	Zpracování osobních údajů veřejně přístupných	Údaje jsou veřejně přístupné omezenému počtu subjektů	1
8	Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách	Jednoduchý nebo složitý systém bez propojení na jiná zpracování prováděna stejným správcem	1
9	Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele	Bez vazeb na jiné správce a/nebo zpracovatele.	1
10	Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení	Obdobné řešení u správce již někde nasazené nebo řešení nově nasazené u správce, ale jde o opakované řešení (nabízené na trhu dodavatelem se škálovatelným nastavením)	1

Závěr: 2x2 + 2x3 - činnost podléhá požadavku na analýzu DPIA.

DPIA – Kamerový systém na náměstí (veřejný prostor) analýza rizik pro ochranu osobních údajů

1. Popis zpracování

1.1 Účel

- Ochrana veřejného pořádku.
- Prevence přestupků a trestné činnosti (vandalismus, násilné incidenty).
- Bezpečnost osob na veřejném prostranství.
- Podpora práce městské policie a také policie České republiky.

1.2 Technické řešení

- Použitý předpoklad: 8 kamer s fixním nebo omezeně otočným zorným polem.
- Max. rozlišení 8MPX: 3840x2160/30fps, bez zvuku.
- Umístění na sloupu veřejného osvětlení a budovách v perimetru náměstí.
- Záznam ukládán na zabezpečený server městské policie.
- Bez automatizovaného rozpoznávání obličejů, bez analytiky identifikující osoby.

1.3 Kategorie údajů

- Obraz osob pohybujících se na veřejném prostranství.
- Vozidla a jejich SPZ.

1.4 Subjekty údajů

- Obyvatelé, návštěvníci, kolemjdoucí.
- Velký počet náhodných osob → zásah je zásadně citlivější než v neveřejném objektu.

1.5 Právní základ

- Plnění úkolu prováděného ve veřejném zájmu / výkon veřejné moci (čl. 6 odst. 1 f) GDPR) podle zákona o obecní policii.

- Požadavek nezbytnosti vyžaduje prokázání konkrétních problémů v lokalitě (incidents, kriminalita).

1.6 Doba uchování

- Obvyklé maximum: 10 dnů; delší uchování jen v případě incidentu.
- Delší standardní retenční doba je v prostředí veřejného prostranství obtížně obhajitelná.

1.7 Příjemci

- Městská policie (správce).
- Policie ČR při řešení incidentů.

2. Nezbytnost a proporcionalita

2.1 Odůvodnění nezbytnosti

- Opakované doložené požadavky Městské Police Dačice a Policie ČR z důvodu prevence a objasňování (krádeže, vandalismus, narušování veřejného pořádku),
- nedostatečnost méně invazivních opatření (policejní hlídky – nelze být všude pořád, posílení osvětlení – naráží na efektivitu a obtěžování světelným smogem, úprava prostoru – dochází k úpravám, výsledky jsou nedostatečné, požadavky pořádkových složek trvají).
- Zavedení kamer je přiměřený zásah do soukromí osob při zachování nastavených pravidel.

2.2 Minimalizace zásahu

- Kamery zabírají jen nezbytné části náměstí, nikoli celé plochy, pokud to není opodstatněné incidenty.
- Omezeno optické zoomování; nastaveny pevné či předdefinované pozice.
- Zakázáno manuální sledování jednotlivých osob bez konkrétního důvodu (zásada minimalizace).

2.3 Transparentnost

- Viditelné a čitelné informační tabule na všech přístupových místech.
- Specifikovat.

2.4 Pravidla pro přístup

- Přístup mají jen konkrétně určení strážníci.
- Logování přístupů je povinné.
- Zpětné vyhledávání v záznamech jen pro legitimní účel (objasnění incidentu).

3. Analýza rizik

Riziko	Pravděpodobnost	Dopad	Hodnocení
Sledování pohybu velkého množství lidí	střední	vysoký	vysoké
Neoprávněný přístup k záznamům	střední	vysoký	vysoké
Zásah do soukromí obyvatel okolních domů	nízká–střední	vysoký	střední–vysoké
Chybné použití zoomu (sledování jednotlivců)	střední	vysoký	vysoké
Únik nebo zneužití záznamů	nízká	vysoký	střední
Zobrazení SPZ a z toho vyplývající sekundární zneužití	nízká–střední	střední	střední

U veřejného prostranství jsou rizika objektivně vyšší.

4. Opatření ke snížení rizik

4.1 Organizační opatření

- Přesný Provozní řád kamerového systému: kdo může sledovat, kdy, jak – určeno směrnicí, vedena Provozní kniha kamerového systému.
- Povinnosti strážníků, zákaz „volného“ sledování osob.
- Povinné zaznamenávání každého nahlédnutí do záznamů.
- Jednou ročně audit zorných polí kamer.

4.2 Technická opatření

- Maskování oblastí mimo legitimní dohled (např. okna, soukromé plochy).
- Omezený přístup k NVR (dvoufaktorové ověření).
- Segmentovaná síť oddělená od běžného provozu úřadu.
- Automatické mazání záznamů po 10 dnech.
- Žádná biometrická analytika.

4.3 Opatření k omezení dopadu incidentů

- Incident response plan.
- Okamžité uzamčení přístupu při podezření na zneužití.
- Jednotné postupy pro předávání Policii ČR.

Rozmístění kamer a jejich zorné úhly

Zorné úhly kamer zabírajících veřejné prostranství:



Zakreslení umístění kamer zabírajících veřejné prostranství:



Znázornění pozic kamer zabírajících veřejné prostranství:



POZICE č. 3

