

# **Dokumentace technických a organizačních opatření**

Verze	1.
Datum verze	1.9.2024
Vypracovali	Mgr. Markéta Maříková, Mgr. Jiří Kothánek
Schválil	Mgr. Jiří Kothánek
Klasifikace	Pro vnitřní potřebu

# Obsah

1 Úvod	3
2 Základní pojmy, základní informace	3
2.1 Základní pojmy	3
Správce osobních údajů	4
2.2 Důvody vypracování Dokumentace	4
2.3 Postup realizace	5
2.4 Orgány školy které budou zahrnuty do Dokumentace technických a organizačních opatření	5
3 Rozsah zpracování osobních údajů a předávání osobních údajů	5
3.1 Zpracovávané kategorie osobních údajů	6
3.2 Zpracovávaný rozsah citlivých osobních údajů	6
3.3 Kategorie subjektů údajů	6
3.4 Poskytování osobních údajů do zahraničí, příjemci osobních údajů	6
4 Technické opatření a účel zpracování	7
4.1 Technický popis kamerového systému	7
4.2 Stupeň identifikace (osoby)	7
4.3 Jak bude kamerový systém provozován	8
4.3.1 Zavedená technická opatření, která budou aplikována i na kamerový systém	8
4.4 Kybernetické zabezpečení	8
4.5 Kde budou kamery umístěny	9
4.6 Jak bude na kamery upozorňováno, kdo bude obsluhovat kamerový systém	9
4.6.1 Upozornění na kamerový systém	9
4.6.2 Obsluha kamerového systému	9
4.7 Nezbytně nutná doba uložení záznamů, archivace	9
4.8 Skartace <sup>10</sup>	
4.9 Zpracovávání osobních údajů na základě souhlasu a automatizovaného rozhodování včetně profilování	10
5 Posouzení potřebnosti, vhodnosti a přiměřenosti zpracování	10
5.1 Popis účelu zpracování a oprávněného zájmu správce	10
5.2 Je či bylo možné stanoveného účelu zpracování dosáhnout i jiným způsobem? Kritérium potřebnosti (nutnosti) a kritérium vhodnosti	10
5.3 Jaké jsou důsledky pro subjekty údajů?	10
5.4 Jsou přijaty vhodné záruky (bezpečnostní a technická opatření) pro eliminaci dopadů pro subjekty údajů?	11
5.5 Porovnání oprávněného zájmu školy s právy subjektů údajů. Kritérium poměrování	11
6 Posouzení rizik pro práva a svobody subjektů údajů	11
6.1 Posouzení toho, jaká rizikovost dopadá na subjekt údajů v rámci pořízení záznamu	12
6.2 Rizikovost při úniku dat a přijatá opatření	12
7 Nezbytná dokumentace	12
8 Organizační zabezpečení	12
8.1 Princip minimalizace zpracovávaných osobních údajů	12
8.1.1 Počet a umístění kamer	13
8.1.2 Nastavení záběru kamer a deaktivace některých funkcí kamer a dalších součástí kamerového systému	13
8.1.3 Doba uložení kamerového záznamu	13
8.2 Zajištění práv subjektu údajů	13
8.3 Postupy a pravidla v oblasti poskytování záznamů z kamerového systému (práva subjektů údajů)	13
8.3.1 Zásady pro předávání kamerových záznamů oprávněným subjektům	14
8.4 Práva zaznamenaných subjektů údajů	14
8.5 Provoz kamerového systému na pracovišti zaměstnanců	15
9 Plánovaná opatření včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s obecným nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob	15
10 Závěrečné zhodnocení	16

# Dokumentace technických a organizačních opatření

Základní škola T. G. Masaryka a Mateřská škola Písek, Čelakovského 24, 397 01 Písek, (dále jen „**správce nebo škola**“) poskytuje, v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**Obecné nařízení**“) a zákonem č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, informace o zpracování osobních údajů a o právech subjektů údajů v oblasti ochrany osobních údajů.

## 1 Úvod

Základním cílem této Dokumentace technických a organizačních opatření (dále jen „**Dokument**“) je stanovit technická a organizační opatření v souvislosti se zahájením provozu kamerového systému v prostorách Základní školy T.G. Masaryka a Mateřské školy Písek, Čelakovského 24, sídlem Čelakovského 24, 397 01 Písek (dále jen „**kamerový systém**“) tak, aby byla minimalizována či vyloučena míra rizikovitosti zpracování osobních údajů zaznamenaných osob prostřednictvím kamerového systému.

Právním rámcem v této oblasti je Obecné nařízení, zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „**ZzoÚ**“), zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“), zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „**zákoník práce**“) a zákon č. 561/2004 Sb., o předškolním, základním, středním a vyšším odborném školství (školský zákon), ve znění pozdějších předpisů.

---

## 2 Základní pojmy, základní informace

Níže budou upřesněny základní pojmy obsažené v rámci tohoto Dokumentu a základní informace vztahující se k provozovateli kamerového systému a správci osobních údajů pořízených prostřednictvím kamerového systému.

### 2.1 Základní pojmy

Pro účely tohoto Dokumentu se níže uvedenými pojmy rozumí:

1. **Osobní údaj:** veškeré informace o fyzické osobě nebo fyzické osobě podnikající (např. jméno, adresa, datum narození, rodné číslo atd...) na základě kterých lze tuto osobu identifikovat.
2. **Citlivé osobní údaje:** osobní údaje, které vypovídají o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filosofickém přesvědčení nebo členství v odborové organizaci, genetický údaj, biometrický údaj zpracovávaný za účelem jedinečné identifikace fyzické osoby, údaj o zdravotním stavu, o sexuálním chování, o sexuální orientaci a údaj týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření.
3. **Zpracování osobních údajů:** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděna pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
4. **Správce:** právnická nebo fyzická osoba, v tomto případě Základní škola T.G. Masaryka a Mateřská škola Písek, Čelakovského 24, 397 01 Písek, která určuje účely a prostředky zpracování osobních údajů.

5. **Zpracovatel:** fyzická nebo právnická osoba, nebo subjekt, který zpracovává osobní údaje pro Správce.
6. **Subjekt údajů:** Subjektem údajů se rozumí fyzická osoba nebo fyzická osoba podnikající, k níž se osobní údaje vztahují.
7. **Anonymizace:** technika, která se používá na osobní údaje tak, aby bylo dosaženo nevratného znemožnění identifikace.
8. **Pověřenec pro ochranu osobních údajů:** osoba, která posuzuje činnost správce či zpracovatele, zda je v souladu s platnou právní úpravou, informuje je, radí, dává doporučení.

Kontaktní údaje na Správce, pověřence pro ochranu osobních údajů a osobu odpovědnou za danou agendu:

<b>Správce osobních údajů</b>	Základní škola T.G. Masaryka a Mateřská škola Písek, Čelakovského 24 Čelakovského 24, 397 01 Písek IČO: 70943150 DIČ: CZ70943150 Tel: 380425341 e-mail: info@tgmpisek.cz datová schránka: cvrms7h
<b>Pověřenec pro ochranu osobních údajů</b>	Mgr. Markéta Maříková, Tel: 382 330 773, e-mail: marketa.marikova@mupisek.cz
<b>Osoba odpovědná za danou agendu</b>	Mgr. Jiří Kothánek, ředitel školy tel. 380 425 343, e-mail: jiri.kothanek@tgmpisek.cz

## 2.2 Důvody vypracování Dokumentace

zahájení provozu kamerového systému v rámci prostor školy, je činností, která spadá do oblasti článku 35 odst. 3 písm. c) Obecného nařízení.

Vypracování tohoto dokumentu předcházelo vydání **Stanoviska pověřence pro ochranu osobních údajů k provedení posouzení vlivu na ochranu osobních údajů** (dále jen „**stanovisko**“) v rámci kterého byla odůvodněna povinnost pro vypracování tohoto Dokumentu a balančního testu, který tvoří obsah článku 5 tohoto Dokumentu.

Provoz kamerového systému byl „z výše uvedeného důvodu přezkoumán prvně z pohledu právních předpisů a z nich plynoucích povinností. Výsledkem je, že žádný právní předpis nestanovuje povinnost zavedení kamerového systému na Základní školy T. G. Masaryka, Čelakovského 24, PSČ: 397 01, Písek, proto nelze na tuto novou činnost aplikovat ustanovení § 10 zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.“

S touto činností tudíž souvisí provedení posouzení vlivu na ochranu osobních údajů (dále jen „**DPIA**“), a to dle článku 35 odst. 3 písm. c) Obecného nařízení o ochraně osobních údajů. Před započítím provedení DPIA bylo uskutečněno zhodnocení výše uvedené činnosti dle dokumentu vydaného Úřadem pro ochranu osobních údajů s názvem „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (verze 1.0)“. Tento dokument se dělí na dvě části, a to na první část s názvem „Seznam druhů operací zpracování osobních údajů, které nepodléhají posouzení vlivu na ochranu osobních údajů“ a na druhou část s názvem „Seznam druhů operací zpracování osobních údajů, které podléhají posouzení vlivu na ochranu osobních údajů s přesně stanoveným postupem řešení“.

Dle uvedeného dokumentu a dle provedeného zhodnocení nutnosti provedení DPIA, jsem dospěla k závěru, že uvedená činnost zpracování osobních údajů nespadá do první části

*dokumentu, tudíž by bylo nutné DPIA provést. Druhá část dokument však provedení DPIA, u provozu kamerového systému v rámci budovy Základní školy T. G. Masaryka, Čelakovského 24, PSČ: 397 01, Písek, nestanovuje. Hodnocení rizikovosti dosáhlo ve 3 kritériích nízké hodnoty a v 7 kritériích významné hodnoty. DPIA není, dle dokumentu, nutné provést. Není tedy pravděpodobné, že by zpracování osobních údajů mohlo mít za následek vysoké riziko pro práva a svobody fyzických osob.*

*Dle nové Metodiky k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů vydané Úřadem pro ochranu osobních údajů v roce 2024, je však doporučeno vypracovat Dokumentaci technických a organizačních opatření.*

*Před započítím vypracování Dokumentace technických a organizačních opatření je nutné provést rovněž balanční test z primárního důvodu zpracování, kterým je oprávněný zájem správce plynoucí z ustanovení článku 6 odst. 1 písm. f) Obecného nařízení o ochraně osobních údajů.*

**Z důvodů výše uvedených nedoporučuji provést DPIA, doporučuji však vypracovat balanční test a Dokumentaci technických a organizačních opatření<sup>1</sup>.**

## **2.3 Postup realizace**

Dokument bude obsahovat jednotlivá technická a organizační zabezpečení, v rámci kterých bude zajištěna ochrana záznamů pořízených prostřednictvím kamerového systému umístěného v budovách a prostorách školy. V Dokumentu bude dále zhodnocena míra rizikovosti zpracování osobních údajů v souvislosti s dopadem na subjekty údajů, které budou kamerovým systémem zaznamenány. Rovněž budou shrnuty dokumenty, které bude nutné, v souvislosti s provozem kamerového systému, vypracovat a bude vymezen rozsah zpracování osobních údajů a subjektů údajů a v závěru bude provedeno zhodnocení celé problematiky. Dokument bude taktéž obsahovat balanční test.

## **2.4 Orgány školy, které budou zahrnuty do Dokumentace technických a organizačních opatření**

Do Dokumentu budou zahrnuty následující orgány:

- Základní škola T.G. Masaryka a Mateřská škola Písek, Čelakovského 24, Čelakovského 24, 397 01 Písek.

---

## **3 Rozsah zpracování osobních údajů a předávání osobních údajů**

Před započítím provozu kamerového systému je nutné vymežit rozsah zpracování. Jak již bylo popsáno výše, bylo uskutečněno zhodnocení činnosti provozu kamerového systému dle dokumentu vydaného Úřadem pro ochranu osobních údajů s názvem „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (verze 1.0)“, ze kterého plyne, že zpracování osobních údajů prostřednictvím kamerového systému bude pouze v malém rozsahu, a to dle těchto kritérií:

### **Zpracování osobních údajů:**

- do 5000 subjektů údajů nebo méně než 0,5 % populace ČR nebo dotčených států;
- o a/nebo do 2 přístupujících osob/zaměstnanců správce;
- o a/nebo s 1-4 místy zpracování/pobočkami;

---

<sup>1</sup> Stanovisko pověřence pro ochranu osobních údajů ze dne 30.08.2024

- o a úroveň nejméně obce z hlediska původu/umístění subjektů údajů<sup>2</sup>.

### 3.1 Zpracovávané kategorie osobních údajů

Posouzeny byly veškeré osobní údaje, u nichž bude docházet k jejich zpracování Správcem v souvislosti s provozem kamerového systému v budovách a prostorách školy.

Osobní údaje, u nichž bude docházet ke zpracování osobních údajů v případě monitoringu prostřednictvím kamerového systému je **podoba a obrazové informace o chování a jednání zaznamenaných osob - vizuální identifikační údaje ve formě kamerového záznamu.**

### 3.2 Zpracovávaný rozsah citlivých osobních údajů

Citlivé osobní údaje jsou vymezeny ZOOÚ v ustanovení § 66 odst. 6 takto: *citlivým osobním údajem se rozumí osobní údaj, který vypovídá o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filosofickém přesvědčení nebo členství v odborové organizaci, genetický údaj, biometrický údaj zpracovávaný za účelem jedinečné identifikace fyzické osoby, údaj o zdravotním stavu, o sexuálním chování, o sexuální orientaci a údaj týkající se rozsudků v trestních věcech a trestných činů nebo souvisejících bezpečnostních opatření.* Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu, než je tomu u obecných osobních údajů, proto je jím věnován samostatný článek 9 Obecného nařízení.

**V rámci provozování kamerového systému nebude docházet ke zpracování citlivých osobních údajů.**

### 3.3 Kategorie subjektů údajů

Do kategorie subjektu údajů, které mohou být zachyceny kamerovým systémem, budou spadat:

- zaměstnanci školy;
- žáci školy;
- všechny osoby vstupující do monitorovaného prostoru – veřejnost;
- osoby spolupracující se školou v rámci smluvního vztahu.

### 3.4 Poskytování osobních údajů do zahraničí, příjemci osobních údajů

Správce bude oprávněn předat zaznamenané osobní údaje získané prostřednictvím kamerového systému další osobě zejména tehdy, pokud proto svědčí některý z právních důvodů. Především bude moci správce takto činit tehdy, vyplývá-li mu tato povinnost či oprávnění z příslušného právního předpisu.

Příjemci záznamů z kamerového systému mohou být:

- orgány činné v trestním řízení;
- orgány státní správy a samosprávy;
- soudy;
- pojišťovny;
- advokáti;
- subjekt údajů, k němuž se váží zachycené osobní údaje;
- další subjekty, kterým pro předání bude svědčit právní důvod.

---

<sup>2</sup> Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů (verze 1.0), str. 11

V rámci činnosti Správce nebude docházet k předávání osobních údajů do třetích zemí.

---

## 4 Technické opatření a účel zpracování

Kamerový systém bude provozován na základě oprávněného zájmu správce a rovněž v rámci plnění úkolů ve veřejném zájmu na základě následujících právních předpisů a za těmito účely:

- 1) Účelem provozování kamerového systému bude ochrana zdraví, majetku a bezpečnosti všech žáků, pracovníků a návštěvníků školy a hájení dalších zájmů správce v souladu s posláním školy vymezeném v **zákoně č. 561/2004 Sb. o předškolním, základním, středním a vyšším odborném školství (školský zákon), ve znění pozdějších předpisů.**
- 2) Dále pak bude sloužit k zajištění důkazního materiálu v případě zjištění případů porušování školního řádu, konkrétně pak vandalizmu, poškození majetku, šikany, krádeží, neoprávněného vstupu, dopravních přestupků, znečišťování prostor apod. Dále pak bude napomáhat řešení případných nenadálých situací. **Dosavadní opatření nebyla účinná.**

### 4.1 Technický popis kamerového systému

Kamerový systém bude zahrnovat:

- Kamery umístěné v budovách a prostorách školy;
- Softwarové a hardwarové řešení navržené dodavatelem;
- Technická, organizační a bezpečnostní opatření (viz tento Dokument);
- Mazání kamerového záznamu (přehrání jiným záznamem) po uplynutí stanovené doby (viz tento Dokument);
- Operace zpracování osobních údajů, které budou provozovány 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;
- Bezpečnost kamerového systému - zajištění dostupnosti, důvěrnosti a integrity údajů, které se realizuje prostřednictvím přijatých technických a organizačních opatření.
- Možnost vygenerování, přenositelnost, výmaz a omezení zpracování.

### 4.2 Stupeň identifikace (osoby)

**Subjekt údajů bude identifikovatelný v následujících případech:**

- Postava v záběru bude zabírat více než 25 % výšky obrazu, resp. na jeden pixel obrazu případně méně než 40 mm reálné výšky postavy. Hodnoty jsou odvozeny od systému PAL, takže v jiných systémech (s jiným digitálním rozlišením) musí být údaje dle jednotlivých stupňů přepočteny na srovnatelnou úroveň (i zde uvádí převodní tabulku citovaná norma)<sup>3</sup>.
- Pokud by postava v záběru nespĺňovala výše uvedená kritéria, ale došlo by ke splnění v případě využití digitálního zoomu, bude osoba rovněž identifikovatelná.

---

<sup>3</sup> Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, str. 7

### 4.3 Jak bude kamerový systém provozován

Kamerový systém bude provozovat správce.

Softwarová a technická řešení a zabezpečení a údržbu kamerového systému budou zajišťovat proškolení zaměstnanci Správce a údržbu, opravy atd. dodavatel kamerového systému (případně jiná odborná firma), který nebude v pozici zpracovatele osobních údajů.

#### 4.3.1 Zavedená technická opatření, která budou aplikována i na kamerový systém

- 1) Přístup k elektronickým datovým souborům bude zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy.
- 2) Kamery budou zabezpečeny proti běžnému poškození a umístěny tak, aby byly ve výšce, bez možnosti bezproblémového dosahu kolemjdoucích.
- 3) Rovněž budou zabezpečeny veškeré kabely a technika související s kamerovým systémem.
- 4) Bude stanoven řízený přístup k datům a seznam osob oprávněných manipulovat se zaheslovaným počítačem umístěným v ředitelně školy (dále jen „**počítač**“), který bude napojen na záznamy kamerového systému, ostatním osobám bude manipulace s ním zakázána.
- 5) Bude provedeno školení oprávněných osob po stránce technické.
- 6) Budou doplněny a dále vedeny záznamy o přístupu k počítači.
- 7) Budou nahlášeny odpovědné osobě, které zajistí neprodleně opravu kamerového systému (bude také proveděn zápis o odstranění závady).
- 8) Obsluhu kamerového systému budou zajišťovat pověřené osoby a softwarová a technická řešení a zabezpečení a údržbu kamerového systému bude zajišťovat dodavatel kamerového systému (nebo jiná odborná firma), který nebude v pozici zpracovatele osobních údajů.
- 9) Budou doplněny Záznamy o činnostech zpracování pro kamerový systém.
- 10) Veřejnost bude seznámena s informacemi o umístění kamer ve škole při vstupech do budov školy.
- 11) Bude provedeno školení všech oprávněných osob v oblasti ochrany osobních údajů.
- 12) Bude provedena ochrana rozvodů před poškozením a vlivy počasí.
- 13) Bude zajištěna evidence přístupů.
- 14) Bude provedeno zajištění odolnosti kamer proti útoku hrubou silou.

### 4.4 Kybernetické zabezpečení

V rámci kybernetické bezpečnosti budou zajištěna následující opatření:

- 1) zajištění bezpečnosti přenosových cest;
- 2) zajištění bezpečnosti datových nosičů, na nichž jsou záznamy z kamer;
- 3) zajištění kybernetické bezpečnosti na technice, na které se budou záznamy zpracovávat;
- 4) zajištění ochrany datového připojení (kabelů atd.);
- 5) zajištění evidence přístupů;
- 6) řízení přístupů k datům (autentizace, autorizace);
- 7) monitorování a zaznamenávání činnosti (vyhledávání, přehrávání, vymazávání, úprava, ukládání, tisk, předávání);
- 8) opatření proti narušení integrity dat – autentizace dat;
- 9) ukládání údajů o čase;
- 10) bezpečný výmaz dat po uplynutí stanovené doby;
- 11) zálohování dat do výmazu po uplynutí stanovené doby.



## 4.5 Kde budou kamery umístěny

Kamery budou umístěny v prostorách Školy, viz. příloha č. 4 tohoto Dokumentu.

## 4.6 Jak bude na kamery upozorňováno, kdo bude obsluhovat kamerový systém

### 4.6.1 Upozornění na kamerový systém

- 1) Před každým vstupem do Školy musí být umístěna informační tabulka tak, aby každý subjekt vstupující do monitorovaného prostoru byl informován o provozu kamerového systému v budově ještě před vstupem do monitorovaného objektu.
- 2) Informační tabulky musí být umístěny po celou dobu provozu kamerového systému a musí být umístěny tak, aby byly nepřehlédnutelné (přibližně ve výšce očí vstupujících subjektů, na místě nepřehlédnutelném před vstupem do monitorovaného objektu a umístěny tak, aby byl nepřehlédnutelný z větší vzdálenosti cca 2,5 metru. Písmo musí být dobře čitelné.
- 3) Informační tabulky musí obsahovat: „piktogram/obrázek kamery (příloha č. 1 tohoto Dokumentu), údaj o tom, že prostor je monitorován kamerovým systémem, identifikaci správce a odkaz na pověřence pro ochranu osobních údajů, odkaz na místo, kde je možné v písemné nebo digitální podobě získat o kamerovém systému podrobnější informaci - telefonní spojení, internetová adresa, účel a právní základ zpracování osobních údajů a informace o právech subjektu údajů“.<sup>4</sup>

### 4.6.2 Obsluha kamerového systému

- 1) Obsluhu kamerového systému z hlediska záznamového zařízení budou provádět pouze proškolení zaměstnanci školy.
- 2) Softwarová a technická řešení a zabezpečení a údržbu kamerového systému budou zajišťovat proškolení zaměstnanci školy a rovněž dodavatel kamerového systému (případně jiná odborná firma), který nebude v pozici zpracovatele osobních údajů.

## 4.7 Nezbytně nutná doba uložení záznamů, archivace

Počítač bude umístěn v kanceláři ředitele školy. Archivaci bude provádět pouze ředitel školy, nebo jím pověřená osoba. Archivace záznamu všech kamer se bude provádět automaticky na záznamovém zařízení, které bude uloženo v samostatné uzamykatelné místnosti a v samostatné uzamykatelné skříni (racku). Po uplynutí 96 hodin bude záznam automaticky nenávratně smazán (přehrán novým záznamem). O využití záznamu jako důkazního materiálu bude rozhodovat ředitel školy, nebo jeho statutární zástupce. Policii České republiky nebo správním orgánům či dalším příjemcům bude vydán záznam zachyceného incidentu (důkazního materiálu) pouze na základě písemné žádosti. Formulář Žádosti o vydání záznamu z kamerového systému (dále jen „**Žádost**“) bude řádně vyplněn. Po převzetí záznamu žadajícím bude tento plně odpovědný za jeho využití a ochranu osobních údajů proti zneužití. Žádost o vydání záznamu z kamerového systému bude tvořit přílohu interní směrnice k provozování kamerového systému a rovněž tvoří přílohu č. 3 Dokumentu.

Škola bude archivovat záznamy po dobu 96 hodin. Jedná se o delší časový úsek, než doporučených 72 hodin, a to z důvodu zajištění důkazních prostředků tak, aby mohly být uplatněny i v případě, že bude např. událost/skutečnost zjištěna za delší časový úsek (přes víkend), aby mohla škola vyhodnotit získaný důkazní materiál i po oznámení učiněném v pondělí, když by se čin stal v pátek. Delší časový úsek, nežli 96 hodin, nebude překročen.

---

<sup>4</sup> Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů

Do doby uchování záznamů nebude možno zahrnout dobu, po kterou jsou záznamy uchovávány z důvodu mimořádných událostí pro orgány činné v trestním řízení, pojišťovny, přestupkové řízení, soudní řízení atd., kdy ke smazání dochází až poté, co skončí řízení, vyřízení pojistné události atd.

#### **4.8 Skartace**

Po uplynutí 96 hodin bude záznam z kamerového systému automaticky nenávratně smazán (přehrán novým záznamem). Není tudíž nutné řešit procesní stránku skartačního řízení.

#### **4.9 Zpracovávání osobních údajů na základě souhlasu a automatizovaného rozhodování včetně profilování**

Vzhledem k technickému řešení a naplňování právního důvodu zpracování dle článku 6 odst.1 písm. f) Obecného nařízení a článku 6 odst. 1 písm e) Obecného nařízení a ustanovení § 5 písm. b) ZzoÚ, **budou osobní údaje subjektů údajů zpracovávány bez souhlasu.**

Při pořizování záznamů z kamerového systému **nebude docházet k automatizovanému rozhodování včetně profilování** dle článku 22 Obecného nařízení.

---

## **5 Posouzení potřebnosti, vhodnosti a přiměřenosti zpracování**

Z důvodu, že kamerový systém je provozován primárně na základě článku 6 odst. 1 písm f) Obecného nařízení, bylo nutné rovněž provést balanční test, který tvoří obsah tohoto článku 5.

### **5.1 Popis účelu zpracování a oprávněného zájmu správce**

Zpracování osobních údajů prostřednictvím kamerového systému bude probíhat primárně na základě oprávněného zájmu správce. Účelem provozování kamerového systému je ochrana zdraví, majetku a bezpečnosti všech žáků, pracovníků a návštěvníků školy a hájení dalších zájmů správce v souladu s posláním školy vymezeném v **zákoně č. 561/2004 Sb. o předškolním, základním, středním a vyšším odborném školství (školský zákon), ve znění pozdějších předpisů**. Dále pak kamerový systém bude sloužit k zajištění důkazního materiálu v případě zjištění případů porušování školního řádu, konkrétně pak vandalizmu, poškození majetku, šikany, krádeží, neoprávněného vstupu, dopravních přestupků, znečišťování prostor apod. Dále pak bude napomáhat řešení případných nenadálých situací.

### **5.2 Je či bylo možné stanoveného účelu zpracování dosáhnout i jiným způsobem? Kritérium potřebnosti (nutnosti) a kritérium vhodnosti.**

Dosud uvedené v bodu 5.1. škola řešila zvýšeným dohledem pedagogických pracovníků, častější kontrolou ze strany zaměstnanců školy, dotazováním zainteresovaných a poškozených osob atd. Vzhledem k neúčinnosti dosavadních opatření a rozlehlosti a počtu monitorovaných prostor ve vlastnictví školy nebude možné jinak efektivně zaručit naplnění sledovaného účelu.

### **5.3 Jaké jsou důsledky pro subjekty údajů?**

Jednotlivé kamery budou zachycovat pohyb osob v monitorovaném prostoru/objektu školy, čímž bude docházet k zachycení jejich fyzické podoby a obrazové informace o chování a jednání zaznamenaných osob. Tímto bude docházet k určitému zásahu do soukromí daných osob a rovněž ke zpracování takto získaných osobních údajů v situaci, kdy budou zachyceny kamerami.

#### **5.4 Jsou přijaty vhodné záruky (bezpečnostní a technická opatření) pro eliminaci dopodů pro subjekty údajů?**

Jednotlivé kamery budou umístěny tak, aby monitorovaly výhradně prostory za daným účelem, kde se budou osoby pohybovat standardním způsobem, kdy záznam nebude nijak zásadně narušovat jejich soukromí. Před samotným vstupem do monitorovaných prostor budou nepřehlédnutelně umístěny informace o tom, že je prostor monitorován (viz tento dokument článek 4.6.1). Pokud by osoby vstupující do těchto prostor měly zájem o podrobnější informace o provozu kamerového systému, bude obsahovat informace odkaz, kde bude možné tyto podrobnější informace získat. Software pro zpracování záznamů bude zpracovávat jako celek, aniž by umožňoval hledání konkrétních osob. Záznamy pořízené z kamer budou uloženy jen po nezbytně nutnou dobu a přístup k nim bude výrazně omezen. Záznamové zařízení bude umístěno v kanceláři ředitele školy, která je vedena jako režimové pracoviště s omezeným přístupem. Přístup do záznamového zařízení bude podmíněn heslem (další technická, bezpečnostní a organizační opatření jsou obsahem tohoto Dokumentu).

#### **5.5 Porovnání oprávněného zájmu školy s právy subjektů údajů. Kritérium poměrování.**

Při zpracování osobních údajů prostřednictvím kamerového systému bude docházet k zásahu do práv subjektů údajů, které budou ale vyvolány nezbytností při realizaci účelu zpracování, který spočívá primárně v ochraně zdraví, majetku a bezpečnosti všech žáků, pracovníků a návštěvníků školy a hájení dalších zájmů správce v souladu s posláním školy vymezeném v **zákoně č. 561/2004 Sb. o předškolním, základním, středním a vyšším odborném školství (školský zákon), ve znění pozdějších předpisů**. K zásahu do práv subjektu údajů dochází jen v minimální míře. Riziko zneužití uložených záznamů bude regulováno na minimum prostřednictvím přijatých technických a organizačních opatření. Konkrétně se bude jednat o to, že kamery budou zaznamenávat monitorovaný prostor jen v nezbytně nutném rozsahu, záznamy budou uloženy jen na nezbytně nutnou dobu, záznamové zařízení bude umístěno na režimovém pracovišti s omezeným přístupem. Lze tedy konstatovat, že k zásahu do práv subjektu údajů bude docházet jen v nezbytně nutném rozsahu s ohledem na realizaci účelu zpracování, který nebude možné realizovat jiným způsobem. Rizika pro subjekt údajů budou eliminována prostřednictvím realizovaných technických a organizačních opatření.

Oprávněný zájem školy, v důsledku neúčinných dosavadních opatření, bude převažovat nad zájmy subjektů údajů. Z tohoto důvodu školapřistoupí k instalaci kamerového systému.

---

## **6 Posouzení rizik pro práva a svobody subjektů údajů**

Ochrana práv subjektu údajů a mlčenlivost v souvislosti s provozem kamerového systému se budou řídit platnými právními předpisy, včetně právních předpisů v oblasti ochrany osobních údajů. Tato povinnost bude trvat i po skončení pracovního poměru. Obsluha kamerového systému nebude oprávněna poskytovat jakékoliv informace sdělovacím prostředkům. Informace bude sdělovat pouze ředitel školy, nebo jeho statutární zástupce. Ochrana práv občana v rámci kamerového systému bude v souladu s ústavním zákonem č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů, Obecným nařízením a dalšími dotčenými právními předpisy.

Se záznamem z kamerového systému bude možné nakládat pouze v souladu s dotčenými právními předpisy.

## **6.1 Posouzení toho, jaká rizikovitost dopadá na subjekt údajů v rámci pořízení záznamu**

Rizikovitost dopadu na subjekt údajů v rámci pořízení záznamu z kamerového systému v případě nepáchání protiprávní jednání, bude minimální. V případě páchání protiprávního jednání nebo pokusu, bude postupováno dle dotčených právních předpisů.

## **6.2 Rizikovitost při úniku dat a přijatá opatření**

Rizikovitost při úniku dat v případě zjevného rozpoznání subjektu údajů v případě, kdy nebude páchat protiprávní jednání, bude minimální. V případě páchání protiprávního jednání nebo jeho pokusu bude rizikovitost vysoká a z tohoto důvodu zavedl Správce opatření pro případ úniku dat a postup ohlašování a oznamování takového úniku Úřadu pro ochranu osobních údajů a také subjektu údajů, o němž záznam unikl, formou formulářů a šablon, které tvoří přílohu č. 2 tohoto Dokumentu a jiným zákonem stanoveným orgánům dle jiného právního předpisu. Správce v případě úniku dat dodržuje ustanovení článku 33 a 34 Obecného nařízení a rovněž ustanovení plynoucí ze ZzoÚ.

---

## **7 Nezbytná dokumentace**

Nezbytná dokumentace kamerového systému bude zahrnovat následující dokumenty, kdy některé z nich budou rovněž tvořit přílohy směrnice pro provoz kamerového systému:

- 1) Vedení záznamů o činnostech zpracování, které byly pro oblast provozu kamerového systému současně provozovaného správcem vypracovány, budou doplněny o kamerový systém;
- 2) Zhodnocení povinnosti zpracovat DPIA, která byla provedena před vypracováním tohoto Dokumentu a jejíž výsledky tvoří obsah článku 2.2. tohoto Dokumentu.
- 3) Projektová dokumentace kamerového systému, která tvoří přílohu č. 4 tohoto Dokumentu.
- 4) Smluvní dokumentace včetně případných zpracovatelských smluv;
- 5) Směrnice pro provoz kamerového systému včetně stanovení postupů pro vyřízení žádosti o poskytnutí záznamu z kamerového systému, která bude doplněna o kamerový systém;
- 6) Informační tabulky (příloha č. 1);
- 7) Žádosti k uplatnění práv subjekty údajů;
- 8) Zásady ochrany osobních údajů;
- 9) Formuláře a šablony pro případ úniku dat (příloha č. 2);
- 10) Předávací protokol videozáznamu;
- 11) Žádost o poskytnutí kamerového záznamu z kamerového systému (příloha č. 3).

---

## **8 Organizační zabezpečení**

Správce a oprávněné osoby, kteří budou oprávněni nakládat s kamerovým systémem či kamerovými záznamy, budou povinni při shromažďování a zpracovávání osobních údajů pořízených prostřednictvím kamerového systému dodržovat ustanovení článku 5 Obecného nařízení.

### **8.1 Princip minimalizace zpracovávaných osobních údajů**

V rámci provozu kamerového systému bude nutné dodržovat princip minimalizace zpracovávaných osobních údajů, který souvisí s následujícími opatřeními:

### 8.1.1 Počet a umístění kamer

Počet kamer v rámci provozu kamerového systému byl omezen na nezbytně nutný rozsah (viz příloha č. 4).

### 8.1.2 Nastavení záběru kamer a deaktivace některých funkcí kamer a dalších součástí kamerového systému

Kamery zahrnuté do kamerového systému budou namířeny tak, aby zaznamenávaly pouze nezbytně nutné prostory školy a případně pouze malý prostor před budovou (do 2,5 metru od pláště budovy, či budou namířeny tak, aby subjekty procházející před budovou nebyly identifikovatelné.

Nastavení kamerového záběru a vizuální zobrazení u jednotlivých kamer bude zahrnuto do interní směrnice pro provoz kamerového systému. Kamery budou statické, v případě, že by kamery byly vybaveny možností pohybu/otáčení, bude tato funkce vypnuta a nebude docházet k jejímu využití. V případě, že by kamery byly vybaveny funkcí zoomu, bude tato funkce rovněž vypnuta. K jejímu využití by mohlo docházet v případě, že by došlo, ze strany zaznamenaného subjektu údajů, ke spáchání protiprávního činu. Kamery budou rovněž vybrány tak, aby nedisponovaly funkcemi rádiového přenosu dat, pořizováním zvukového záznamu či pořizováním biometrických charakteristik. Pokud by byly dodavatelem dodány kamery, které disponují těmito funkcemi, budou tyto funkce ze strany dodavatele deaktivovány. Rovněž bude takto přistoupeno k dalším funkcím, které by zvyšovali riziko zpracování osobních údajů zaznamenaných subjektů.

### 8.1.3 Doba uložení kamerového záznamu

Toto opatření je upraveno v článku 4.7 a 4.8 tohoto Dokumentu.

## 8.2 Zajištění práv subjektu údajů

Správce bude povinen zajistit informace dle článku 13 a 14 Obecného nařízení transparentním způsobem, a to formou tzv. vrstvení informací:

- 1) První vrstva: upraveno v článku 4 pododstavci 4.6.1.
- 2) Druhá vrstva: Správce bude poskytovat informace v textové podobě v kanceláři školy a u pověřence pro ochranu osobních údajů. Informace budou vtěleny do Zásad ochrany osobních údajů – kamerový systém.

Z důvodu usnadnění práv subjektům údajů budou revidovány vypracované žádosti o uplatnění práv dle článku 15-22 Obecného nařízení.

## 8.3 Postupy a pravidla v oblasti poskytování záznamů z kamerového systému (práva subjektů údajů)

Záznamy z kamerového systému budou moci být poskytnuty, po posouzení oprávněnosti předání dat, následujícím subjektům údajů:

- 1) **subjektům údajů případně jejich zákonným zástupcům**, v souvislosti s právem na přístup k osobním údajům dle ustanovení článku 15 Obecného nařízení o ochraně osobních údajů, na základě jejich požadavku, a to pouze tehdy, vyskytuje se tento subjekt údajů či jeho zákonný zástupce na kamerovém záznamu a pouze v rozsahu jeho osobních údajů;
- 2) **správním orgánům nebo správcům**, na základě povinnosti předávat kamerové záznamy vyplývající z právních předpisů (orgánům činným v trestním nebo přestupkovém řízení apod.), případně pojišťovněm při řešení pojistných událostí,

nebo třetím osobám po prokázání oprávněného zájmu, pokud situaci neřeší orgány činné v trestním řízení nebo orgány činné v občansko-právních sporech (například řešení bezpečnostních incidentů v rámci pronajatých prostor nebo pojistných událostí těchto osob)<sup>5</sup>.

### 8.3.1 Zásady pro předávání kamerových záznamů oprávněným subjektům

- 1) Subjekty, které žádají správce o poskytnutí záznamu z kamerového systému, budou muset doložit správci či pověřenci pro ochranu osobních údajů 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.
- 2) Správce bude oprávněn poskytnout kamerové záznamy orgánům činným v trestním řízení nebo správním orgánům pro vedení přestupkového řízení, případně pojišťovně, i z vlastního rozhodnutí, a to v případě, že bude mít podezření na spáchání trestného činu nebo přestupku nebo vzniku pojistné události, které jsou na záznamu zachyceny
- 3) Rozhodným dnem pro poskytnutí kamerového záznamu bude den, kdy bude doručena žádost o poskytnutí kamerového záznamu. Lhůta, která bude brána jako přiměřená pro poskytnutí kamerového záznamu, bude 1 měsíc, samozřejmě budou žádosti vyřizovány bez zbytečného odkladu, případně bude nutné řídit se právními předpisy v případě, kdy jednotlivý subjekt na předání kamerového záznamu má nárok ze zákona.
- 4) Při poskytování kamerového záznamu subjektu údajů bude třeba dodržet následující pravidla:
  - předkládají se pouze části pořízeného záznamu, které se týkají subjektu údajů žádajícího o poskytnutí záznamu (žadatel),
  - jiné osoby, jejichž pohyb se netýká subjektu údajů, nesmí být na záznamu rozpoznatelné (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 (pokud by měl subjekt údajů podezření, že na záznamech může být zachyceno protiprávní jednání vůči jeho osobě, může současně požádat správce o omezení zpracování, které zajistí, že nedojde k vymazání dotčených záběrů).
- 5) Kamerový záznam se bude poskytovat 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).
- 6) Za poskytnutí druhé a další kopie kamerových záznamů subjektu údajů bude moci správce žádat přiměřenou úhradu nákladů spojených se zpracováním poskytovaného kamerového záznamu.
- 7) Správce bude mít vypracovanou Žádost, která bude muset být vyplněna a evidována při každém vydání kamerového záznamu.

## 8.4 Práva zaznamenaných subjektů údajů

Všechna práva a jejich možnost a nemožnost uplatnění budou rozebrány v interní směrnici k provozování kamerového systému. Výčet práv subjektů údajů:

- 1) **Právo na přístup k osobním údajům** – je možnost jej uplatnit;
- 2) **Právo na opravu** - je možnost jej uplatnit;
- 3) **Právo na výmaz** - je možnost jej uplatnit;
- 4) **Právo na omezení zpracování** - je možnost jej uplatnit;

<sup>5</sup> Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů, str. 18, bod 3.3.2.1

- 5) **Právo na přenositelnost osobních údajů** – nedává smysl;
- 6) **Právo vznést námitku proti zpracování** - je možnost jej uplatnit;
- 7) **Právo nebýt předmětem automatizovaného rozhodování včetně profilování** – je u kamerového systému v případě školy bezpředmětné.

## **8.5 Provoz kamerového systému na pracovišti zaměstnanců**

V rámci zaváděného kamerového systému bude dodržován zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, který stanovuje, ve svém ustanovení § 316 odst. 2, že zaměstnavatel nesmí narušovat soukromí zaměstnanců na pracovišti tím, že by je vystavoval otevřenému nebo skrytému sledování či odposlechu, a to tehdy, pokud mu k tomu nesvědčí závažný důvod v podobě zvláštní činnosti. Kamery budou umístěny v prostorách školy a nebudou nikterak zasahovat do sboroven, kabinetů, kanceláří, toalet. Každý zaměstnanec bude v dostatečném předstihu informován o umístění kamer, bude seznámem se směrnici pro provoz kamerového systému a zaměstnavatelem bude veden seznam takto seznámených zaměstnanců s provozem kamerového systému.

## **9 Plánovaná opatření včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s obecným nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob**

Plánovaná opatření jsou podrobně rozebrána v jednotlivých článcích tohoto dokumentu. Opatření, která budou realizována:

Správce zavede seznam oprávněných osob, jímž je umožněn přístup k počítači a ke kamerovému systému. Ostatní osoby budou mít k počítači přístup zakázán. Bude povinen umožnit přístup ke kamerovému systému také Policii ČR a správním orgánům (pouze z důvodu prověření události zaznamenané kamerovým systémem, která může přispět k odhalení a objasnění protiprávního jednání po hodnověrném prokázání své příslušnosti k uvedeným orgánům). O přístupu ke kamerovému systému bude povinnost vždy učinit záznam. Závady nebo výpadky kamerového systému budou zaznamenávány pověřenou osobou a budou uloženy v ředitelně školy a dále budou nahlášeny odpovědné osobě, která zajistí neprodleně jejich opravu.

Správce provede proškolení oprávněných zaměstnanců, zavede technické a bezpečnostní zabezpečení, povede záznamy o činnostech zpracování všeobecně a také pro tuto agendu a bude plnit informační povinnosti vůči subjektům údajů. Budou proškoleni taktéž všichni zaměstnanci školy v souvislosti s ochranou osobních údajů. O všech školeních se povedou písemné záznamy. Kontrolní činnost bude provádět ředitel školy, nebo jeho statutární zástupce.

## 10 Závěrečné zhodnocení

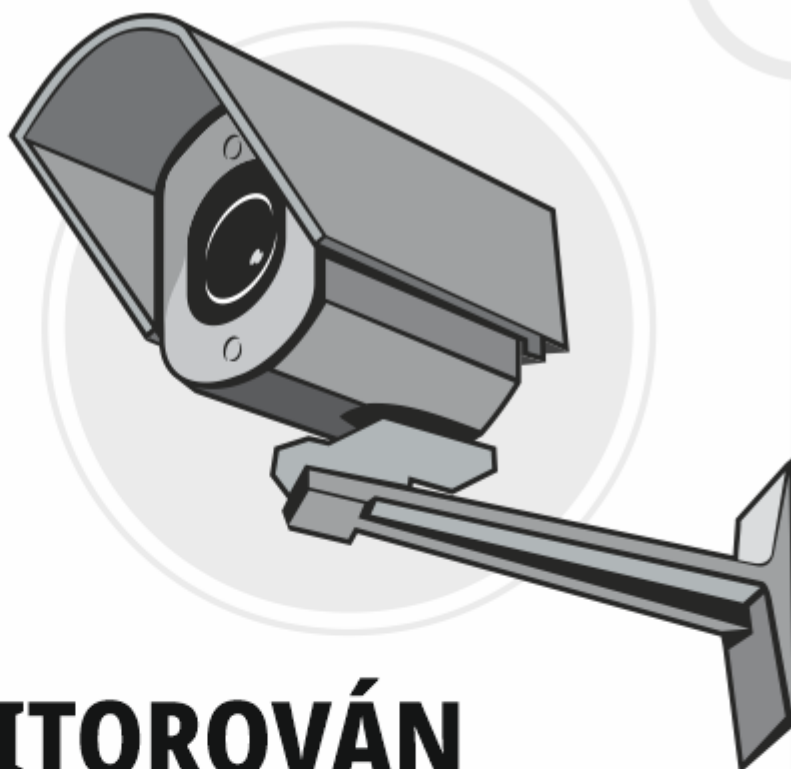
Před započítáním vypracování tohoto Dokumentu byly zjištěny nízké hodnoty rizikosti zpracování osobních údajů s dopadem na subjekt údajů v rámci zavedení provozu kamerového systému školy. Správce v tomto Dokumentu zhodnotil bezpečnostní opatření (technické a organizační zabezpečení), provedl před započítáním balanční test a přijal opatření k minimalizaci rizikosti zpracování osobních údajů zaznamenaných subjektů údajů. Kamerový systém bude provozován dle výše uvedených právních předpisů se zavedením vhodné míry technického, organizačního a bezpečnostního opatření.

V případě rozšíření kamerového systému bude nezbytné zahrnutí této skutečnosti do stávající dokumentace vztahující se ke kamerovému systému a provedení revize tohoto Dokumentu.

Zhodnocení provedl	Mgr. Markéta Maříková pověřenec pro ochranu osobních údajů
--------------------	---



**MONTEA CZ**



# **OBJEKT JE MONITOROVÁN KAMEROVÝM SYSTÉMEM SE ZÁZNAMEM**

Správce: Základní škola T.G. Masaryka a Mateřská škola Písek, Čelakovského 24  
Pověřenec pro ochranu osobních údajů: [www.mesto-pisek.cz](http://www.mesto-pisek.cz); ochrana osobních údajů  
Informace o kamerovém systému: tel. 380 425 341, [www.zstgmpisek.cz](http://www.zstgmpisek.cz)  
Účel a právní základ zpracování jsou vymezeny v Zásadách ochrany osobních údajů  
dostupných na [www.zstgmpisek.cz](http://www.zstgmpisek.cz), stejně tak, jako práva subjektu údajů,  
která lze uplatnit vůči správci.

## Příloha č. 2 – Šablony a formuláře pro případ úniku dat

Ohlášení případů porušení zabezpečení osobních údajů dozorovému úřadu do 72 hodin						
<p>Obsah ohlášení:                      Kontaktní údaje pověřence                      Kontaktní údaje správce                      Popis povahy případů                      Kategorii osobních údajů                      Kategorii subjektů údajů                      Množství dotčených záznamů osobních údajů                      Množství dotčených subjektů údajů                      Popis pravděpodobných důsledků                      Popis opatření</p>			<p>Jméno a kontaktní údaje správce:                      Základní škola T. G. Masaryka a Mateřská škola Písek                      IČ: 709 43 150                      tel.: 382 425 343                      email: info@tgmpisek.cz</p>		<p>Jméno a kontaktní údaje pověřence:                      Mgr. Markéta Maříková                      Budovcova 207/6, 39701 Písek                      tel.: 382 330 773                      email: marketa.marikova@mupisek.cz</p>	
Popis povahy případů	Kategorie osobních údajů	Kategorie subjektů údajů	Množství dotčených záznamů osobních údajů	Množství dotčených subjektů údajů	Popis pravděpodobných důsledků	Popis opatření

Oznámení případů porušení zabezpečení osobních údajů subjektu údajů do 72 hodin						
<p>Obsah ohlášení:                      Kontaktní údaje pověřence                      Kontaktní údaje správce                      Popis povahy případů                      Kategorii osobních údajů                      Kategorii subjektů údajů                      Množství dotčených záznamů osobních údajů                      Množství dotčených subjektů údajů                      Komu bylo oznámeno a jakým způsobem,                      Popis pravděpodobných důsledků                      Popis opatření</p>			<p>Jméno a kontaktní údaje správce:                      Základní škola T. G. Masaryka a Mateřská škola Písek                      IČ: 709 43 150                      tel.: 382 425 343                      email: info@tgmpisek.cz</p>		<p>Jméno a kontaktní údaje pověřence:                      Mgr. Markéta Maříková                      Budovcova 207/6, 39701 Písek                      tel.: 382 330 773                      email: marketa.marikova@mupisek.cz</p>	
Popis povahy případů	Kategorie osobních údajů	Kategorie subjektů údajů	Množství dotčených záznamů osobních údajů	Množství dotčených subjektů údajů	Popis pravděpodobných důsledků	Komu bylo oznámeno a jakým způsobem

## Formulář

pro oznámení porušení zabezpečení osobních údajů subjektům údajů  
poškozeným porušením zabezpečení

Správce:

Základní škola T. G. Masaryka a Mateřská škola Písek, Čelakovského 24  
Čelakovského 24  
397 01 Písek  
IČ: 70943150  
tel.: 382 425343  
email: info@tgmpisek.cz

Pověřenec pro ochranu osobních údajů:

Mgr. Markéta Maříková  
Budovcova 207/6  
397 01 Písek  
tel.: 382 330 773  
e-mail: [marketa.marikova@mupisek.cz](mailto:marketa.marikova@mupisek.cz)

Další subjekt zapojení do dotčeného zpracování (zpracovatel, další správce, příjemce):

Role (zpracovatel – správce – příjemce):  
Název nebo jméno a příjmení:  
Sídlo nebo bydliště – ulice, město, PSČ:  
IČO:

### I. Hlavní údaje k porušení zabezpečení

1. Členský stát, kde došlo k porušení zabezpečení:

2. Datum a čas porušení zabezpečení:

3. Datum a čas zjištění porušení zabezpečení:

4. Datum a čas ukončení porušení zabezpečení:

5. Odbor/útvár, ve kterém k porušení došlo:

6. Možná příčina porušení zabezpečení:

Škodlivý útok

interní  externí

Nehoda (selhání systému – *upřesněte níže*)

Nedbalost (lidské pochybení – *upřesněte níže*)

Jiná (prosím, upřesněte)

Podrobnější popis příčiny porušení:

7. Popis povahy případu:

8. Pokud se jednalo o škodlivý útok, co bylo příčinou porušení zabezpečení:

Trojský kůň

Malware

Zašifrování (Ransomware)

CEO-fraud

Phishing

Vydírání

Útoky DDoS, DoS

Jiné, upřesněte:

9. Pravděpodobný dopad porušení zabezpečení:

Zveřejnění osobních údajů

Porušení důvěrnosti/integrity osobních údajů

Krádež osobních údajů

Škoda na majetku, zdraví

Krádež identity nebo fraud

Přímá finanční újma

Odpovědnosti za škody třetích stran

Přerušování provozu

Poškození reputace

Porušení dostupnosti dat

Jiné, upřesněte

10. Kategorie dotčených osobních údajů:

Identifikační údaje (např. jméno, příjmení, datum narození, rodné číslo, jiné identifikátory)

Kontaktní údaje (např. e-mail, telefon, adresa)

Ekonomické a finanční údaje

Data o poloze (lokační údaje)

Jiné, upřesněte:

**11. Zvláštní kategorie osobních údajů:**

Údaje vypovídající o rasovém nebo etnickém původu

Údaje vypovídající o politických názorech a členství v odborech

Údaje vypovídající o filozofickém přesvědčení nebo náboženském vyznání

Údaje o zdravotním stavu

Údaje o sexuální orientaci nebo vyznání

Genetické nebo biologické údaje, jsou-li zpracovávány za účelem jednoznačné identifikace fyzické osoby

Údaje o trestných činech nebo trestních odsouzeních, o páčání přestupků

**12. Množství dotčených subjektů údajů:**

**13. Množství dotčených záznamů osobních údajů:**

**14. Stav zašifrování dotčených osobních údajů:**

Kompletní

Částečné

Žádné

**15. Důsledky – povaha pravděpodobného dopadu na ohrožené subjekty údajů:**

Ztráta kontroly nad osobními údaji

Data mohou být spojena s dalšími informacemi

Data mohou být využívána k jiným/nekalým účelům

- Neoprávněné obrácení pseudonymizace (zpracovávaná data již mohou být přiřazena k identifikované nebo identifikovatelné fyzické osobě)
  - Ztráta nebo změna schopnosti správce/zpracovatele poskytovat služby pro dotčené subjekty údajů
  - Krádež identity
  - Podvod
  - Omezení práv dotčených subjektů údajů
  - Diskriminace dotčených subjektů údajů
  - Finanční ztráty
  - Poškození pověsti
  - Ztráta důvěrnosti dat chráněných profesním tajemstvím
- Ostatní (upřesněte):

16. Jaký způsob IT instituce využívá?

- Interní IT tým
- Externí IT společnost

## II. Opatření přijatá před vznikem porušení zabezpečení:

17. Jakými prostředky byly ohrožené osobní údaje zpracovávány (např. SW, HW):

18. Další organizační a technická opatření přijatá před porušením zabezpečení (např. uzamykání skříněk, místností, řízené přístupy, hesla, logování...):

### III. Opatření zvolená k nápravě porušení zabezpečení

19. Technická a organizační opatření přijata ke snížení následků porušení zabezpečení:

- Obnovení dat
- Vymazání škodlivého SW
- Výměna poškozeného nosiče
- Externí testování
- Školení zaměstnanců
- Posílení bezpečnosti dat
- Jiné bezpečnostní nástroje
- Šifrování

Upřesněte:

20. Popis a doložení dalších opatření (jako příloha formuláře), přijatá k řešení/porušení zabezpečení (v čem opatření spočívá):

21. Datum a čas přijatých opatření:

22. Kolik souborů osobních údajů bylo využito/dotčeno/zcizeno

23. Komunikace s dalšími orgány (ohlášení policii, jinému úřadu...):

Ano

Ne

#### IV. Opatření do budoucna

24. Co bylo učiněno nebo naplánováno, aby oznámené porušení zabezpečení nenastalo znovu:

Vylepšení bezpečnostních opatření s ohledem na bezpečnost dat;

Audit shromažďování údajů

Audit zpracovávání osobních údajů

Audit a opětovné vyhodnocení zpracovatele

Zašifrování dat

Nebyla přijata bezpečnostní opatření

Jiná technická a organizační opatření, upřesněte:



## Formulář

pro ohlášení porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů

Správce:

Základní škola T.G. Masaryka a Mateřská škola Písek, Čelakovského 24  
Čelakovského 24  
397 01 Písek  
IČ: 70943150  
tel.: 382 425 343  
e-mail: info@tgmpisek.cz

Jméno a kontaktní údaje pověřence:

Mgr. Markéta Maříková  
Budovcova 207/6  
397 01 Písek  
telefon: +420 382 330 773  
e-mail: marketa.marikova@mupisek.cz

Další subjekt zapojení do dotčeného zpracování (zpracovatel, další správce, příjemce):

Role (zpracovatel – správce – příjemce):  
Název nebo jméno a příjmení:  
Sídlo nebo bydliště – ulice, město, PSČ:  
IČO:

### I. Typ oznámení

Prvotní ohlášení

Doplnění ohlášení

### II. Hlavní údaje k porušení zabezpečení

1. *Odvětví:*

2. *Počet zaměstnanců:*

3. *Členský stát, kde došlo k porušení zabezpečení:*

4. *Datum a čas porušení zabezpečení:*

5. Datum a čas zjištění porušení zabezpečení:

6. Datum a čas ukončení porušení zabezpečení:

7. Odbor/útvár, ve kterém k porušení došlo:

8. Pokud je incident oznamován více jak 72 hodin po jeho zjištění, uveďte důvody tohoto zpoždění:

9. Možná příčina porušení zabezpečení:

- Škodlivý útok  
 interní     externí

Nehoda (selhání systému – upřesněte níže)

Nedbalost (lidské pochybení – upřesněte níže)

Jiná (upřesněte):

Podrobnější popis příčiny porušení:

10. Popis povahy případu:

11. Pokud se jednalo o škodlivý útok, co bylo příčinou porušení zabezpečení:

Trojský kůň

Malware

Zašifrování (Ransomware)

CEO-fraud

Phishing

Vydírání

Útoky DDoS, DoS

Jiné, upřesněte:

12. Pravidelný dopad porušení zabezpečení:

- |                          |                                     |                          |  |
|--------------------------|-------------------------------------|--------------------------|--|
| <input type="checkbox"/> | Zveřejnění osobních údajů           | <input type="checkbox"/> | Porušení důvěrnosti/integrity osobních údajů |
| <input type="checkbox"/> | Krádež osobních údajů               | <input type="checkbox"/> | Škoda na majetku, zdraví                     |
| <input type="checkbox"/> | Krádež identity nebo fraud          | <input type="checkbox"/> | Přímá finanční újma                          |
| <input type="checkbox"/> | Odpovědnosti za škody třetích stran | <input type="checkbox"/> | Přerušování provozu                          |
| <input type="checkbox"/> | Poškození reputace                  | <input type="checkbox"/> | Porušení dostupnosti dat                     |
| <input type="checkbox"/> | Jiné, upřesněte:                    |                          |  |

13. Kategorie dotčených osobních údajů:

- Identifikační údaje (např. jméno, příjmení, datum narození, rodné číslo, jiné identifikátory)
- Kontaktní údaje (např. e-mail, telefon, adresa)
- Ekonomické a finanční údaje
- Data o poloze (lokační údaje)
- Údaje o trestních odsouzeních, o spáchaných přestupcích
- Jiné, upřesněte:

14. Zvláštní kategorie osobních údajů:

- Údaje vypovídající o rasovém nebo etnickém původu
- Údaje vypovídající o politických názorech a členství v odborech
- Údaje vypovídající o filozofickém přesvědčení nebo náboženském vyznání
- Údaje o zdravotním stavu
- Údaje o sexuální orientaci nebo vyznání
- Genetické nebo biologické údaje, jsou-li zpracovávány za účelem jednoznačné identifikace fyzické osoby
- Údaje o trestných činech nebo trestních odsouzeních, o páchaní přestupků

**15. Kategorie subjektů údajů:**

- Zaměstnanci nebo osoby v pracovněprávním vztahu ke správci/zpracovateli
- Uživatelé
- Občané/klienti
- Zranitelné osoby (např. děti, žáci)
- Jiné, upřesněte:

**16. Množství dotčených subjektů údajů:**

**17. Množství dotčených záznamů osobních údajů:**

**18. Stav zašifrování dotčených osobních údajů:**

- Kompletní
- Částečné
- Žádné

**19. Byly dotčené osobní údaje předmětem posouzení vlivu zpracování na ochranu osobních údajů?**

- Ano
- Ne

**20. Důsledky – povaha pravděpodobného dopadu na ohrožené subjekty údajů:**

- Ztráta kontroly nad osobními údaji
- Data mohou být spojena s dalšími informacemi
- Data mohou být využívána k jiným/nekalým účelům
- Neoprávněné obrácení pseudonymizace (zpracovávaná data již mohou být přiřazena k identifikované nebo identifikovatelné fyzické osobě)
- Ztráta nebo změna schopnosti správce/zpracovatele poskytovat služby pro dotčené subjekty údajů
- Krádež identity
- Podvod

- Omezení práv dotčených subjektů údajů
- Diskriminace dotčených subjektů údajů
- Finanční ztráty
- Poškození pověsti
- Ztráta důvěrnosti dat chráněných profesním tajemstvím
- Jiné (upřesněte):

21. Jaký způsob IT instituce využívá?

- Interní IT tým
- Externí IT společnost

### III. Opatření přijatá před vznikem porušení zabezpečení:

22. Označení a popis relevantní dokumentace, kterou je správcem řízeno zpracování osobních údajů:

- Vnitřní předpis
- Písemné pokyny zaměstnancům
- Smlouva o zpracování osobních údajů
- Závazné politiky správy a zabezpečení dat a informací
- Jiné (upřesněte):

23. Jakými prostředky byly ohrožené osobní údaje zpracovávány (např. SW, HW):

24. Další organizační a technická opatření přijatá před porušením zabezpečení (např. uzamykání skříněk, místností, řízené přístupy, hesla, logování...):

#### IV. Opatření zvolená k nápravě porušení zabezpečení

25. Technická a organizační opatření přijata ke snížení následků porušení zabezpečení:

- Obnovení dat
- Vymazání škodlivého SW
- Výměna poškozeného nosiče
- Externí testování
- Školení zaměstnanců
- Posílení bezpečnosti dat
- Jiné bezpečnostní nástroje
- Šifrování

Prosím, upřesněte:

26. Popis a doložení dalších opatření (jako příloha formuláře), přijatá k řešení/porušení zabezpečení (v čem opatření spočívá):

27. Datum a čas přijatých opatření:

28. Odhadovaná finanční škoda:

29. Kolik souborů osobních údajů bylo využito/dotčeno/zcizeno?

30. Bylo porušení zabezpečení osobních údajů oznámeno subjektům údajů:

Ano (doplnit datum, kdy a jakým způsobem, počet informovaných subjektů údajů + doložit obsah v příloze formuláře)

Ne, ale budou informováni (doplnit předpokládaný datum, kdy a jakým způsobem + následně informaci doplnit)

Ne, nebudou informováni (odůvodnit tento postup)

Porušení zabezpečení pravděpodobně nepředstavuje velké riziko pro práva a svobody dotčených fyzických osob

S ohledem na přijatá technická a bezpečnostní opatření, dotčené osobní údaje jsou nesrozumitelné pro všechny neoprávněné osoby (např. šifrování)

Správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody dotčených fyzických osob již nebude pravděpodobně naplněno

Představovalo by nepřiměřené úsilí informovat každou fyzickou osobu individuálně (+ uvést způsob učiněného veřejného oznámení)

Upřesnění odůvodnění

Zatím nebylo rozhodnuto o informování dotčené fyzické osoby (upřesnit důvod)

31. Komunikace s dalšími orgány (ohlášení policii, jinému úřadu...):

Ano

Ne

## V. Přeshraniční zpracování

32. Přeshraniční zpracování:

Ne

Ano

Upřesnění dle formuláře ÚOOÚ:

33. Ohlášení je činěno vůči Úřadu pro ochranu osobních údajů jako:

- Vedoucímu dozorovému úřadu
- Dotčenému dozorovému úřadu (označit vedoucí dozorový úřad a doplnit informace o oznámení tomuto úřadu)

34. V jakých členských státech EU mají bydliště subjekty údajů, které jsou dotčeny předmětným porušením zabezpečení:

## VI. Opatření do budoucna

35. Co bylo učiněno nebo naplánováno, aby oznámené porušení zabezpečení nenastalo znovu:

- Vylepšení bezpečnostních opatření s ohledem na bezpečnost dat
- Audit shromažďování údajů
- Audit zpracovávání osobních údajů
- Audit a opětovné vyhodnocení zpracovatele
- Zašifrování dat
- Nebyla přijata bezpečnostní opatření
- Jiná technická a organizační opatření, prosím, upřesněte:



ŽÁDOST O VYDÁNÍ ZÁZNAMU

Žadatel:.....

datum žádosti:.....

Důvod vydání záznamu ze dne:..... čas:.....

---

Žadatel:

Jméno a příjmení:.....

Instituce (organizace):.....

Upozornění: se záznamem z kamerového systému lze nakládat pouze v souladu s Nařízením (EU) 2016/679, obecné nařízení o ochraně osobních údajů GDPR a dalšími dotčenými právními předpisy.

Podpis přebírající osoby:.....

---

Záznam vydal:

Jméno a příjmení:.....

Datum vydání záznamu:.....

---

Popis záznamu:

datum:.....

čas: .....

kamera — umístění:.....

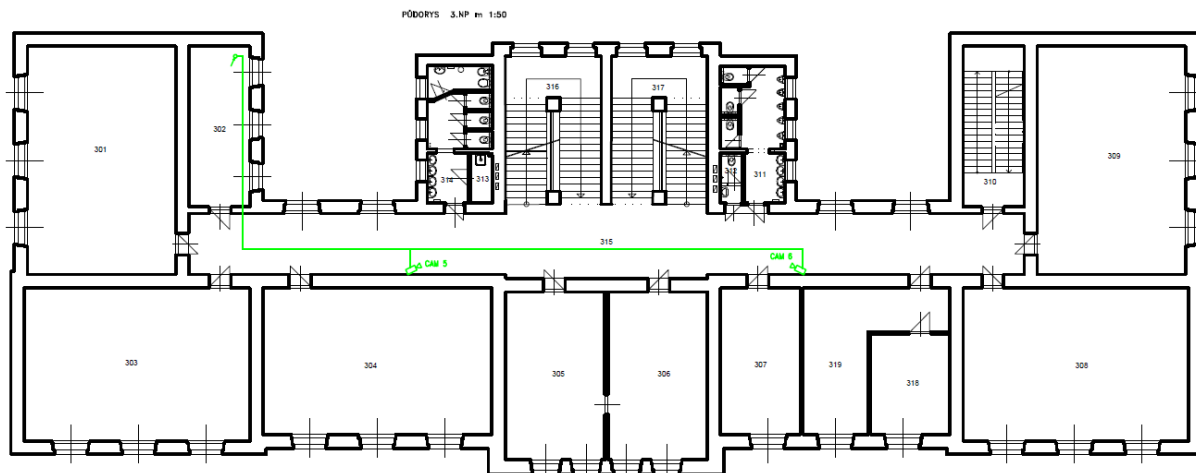
předání na mediu:.....

Podpis osoby, která záznam vydala:.....

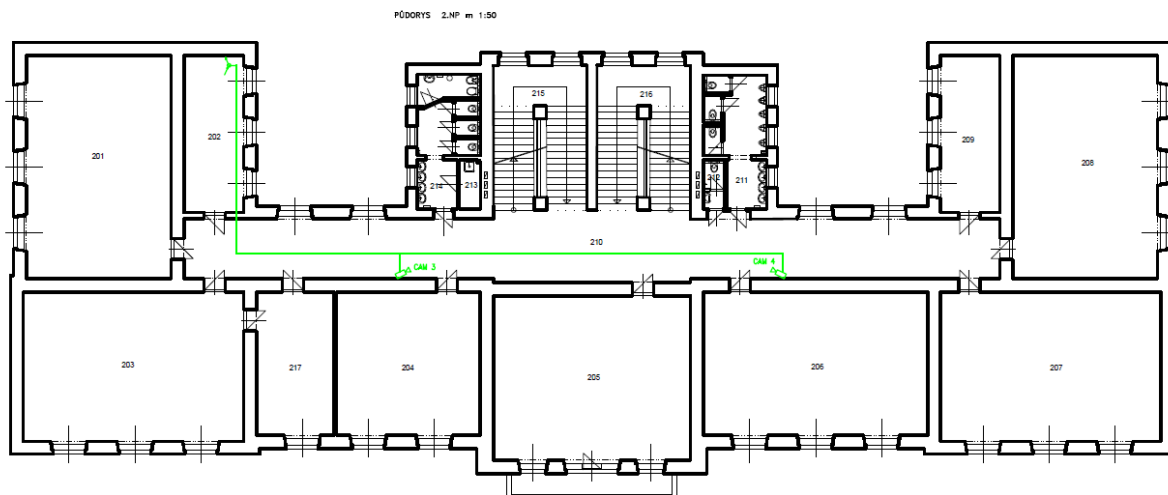
---

Příloha č. 4 – Projektová dokumentace – kamery

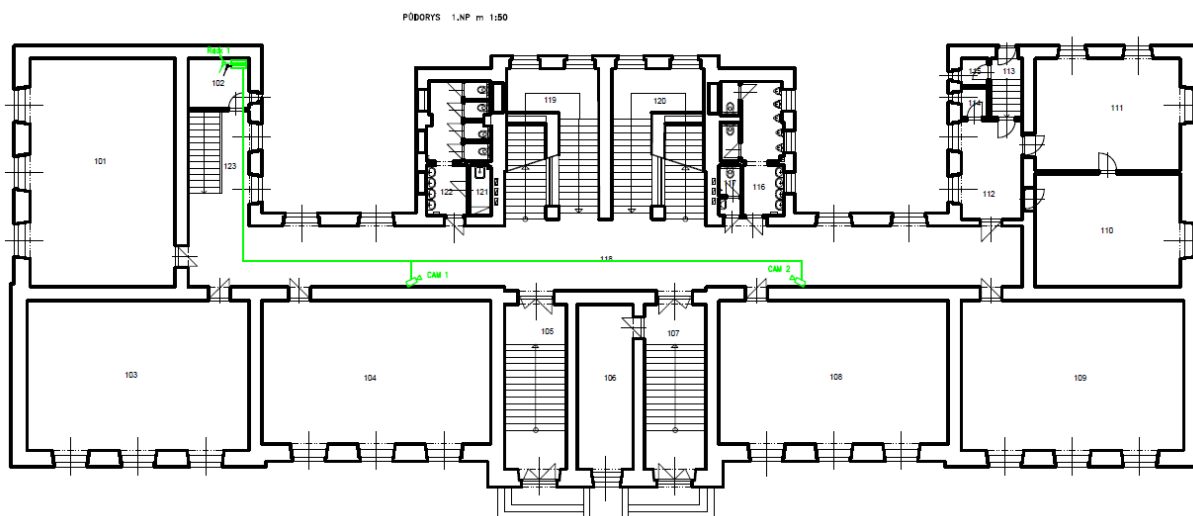
2. stupeň – 3.NP



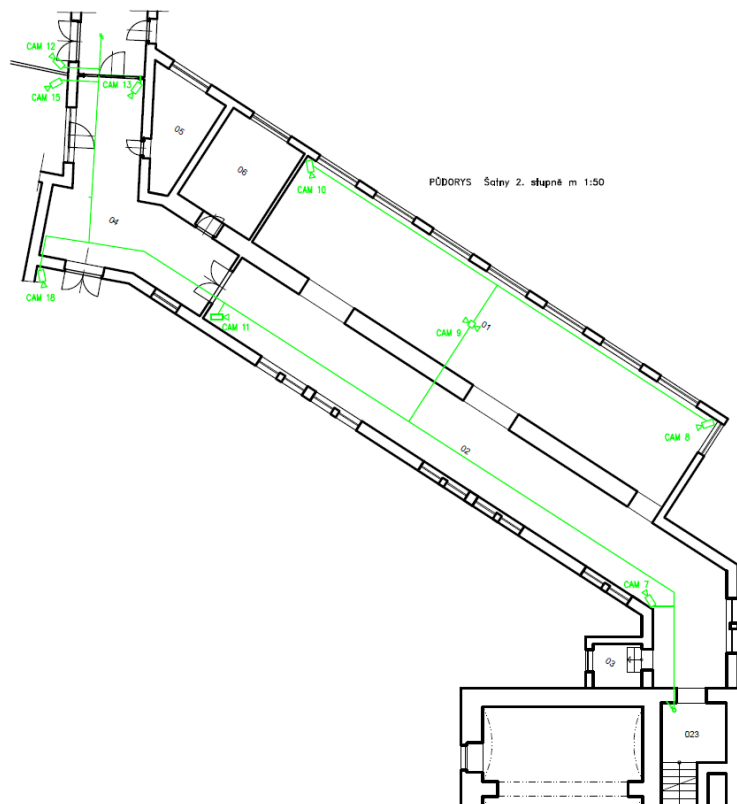
2. stupeň – 2.NP



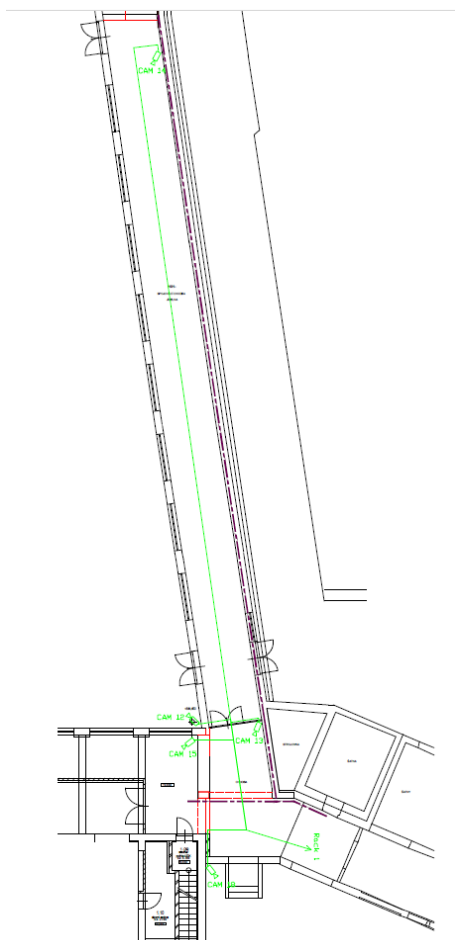
2. stupeň – 1.NP



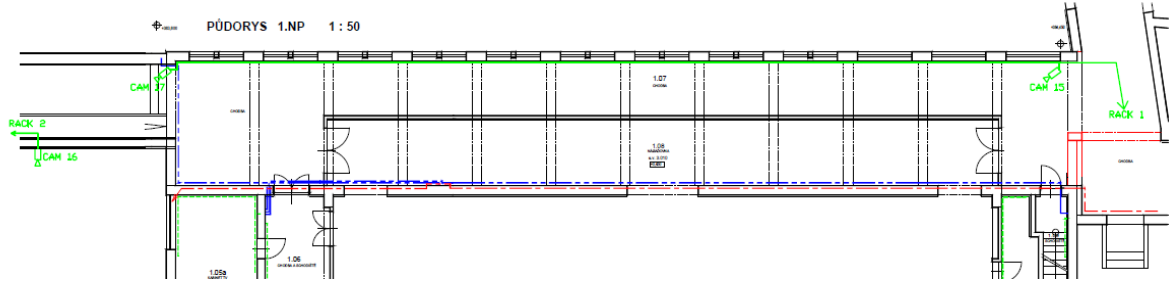
## Šatny 2. stupeň



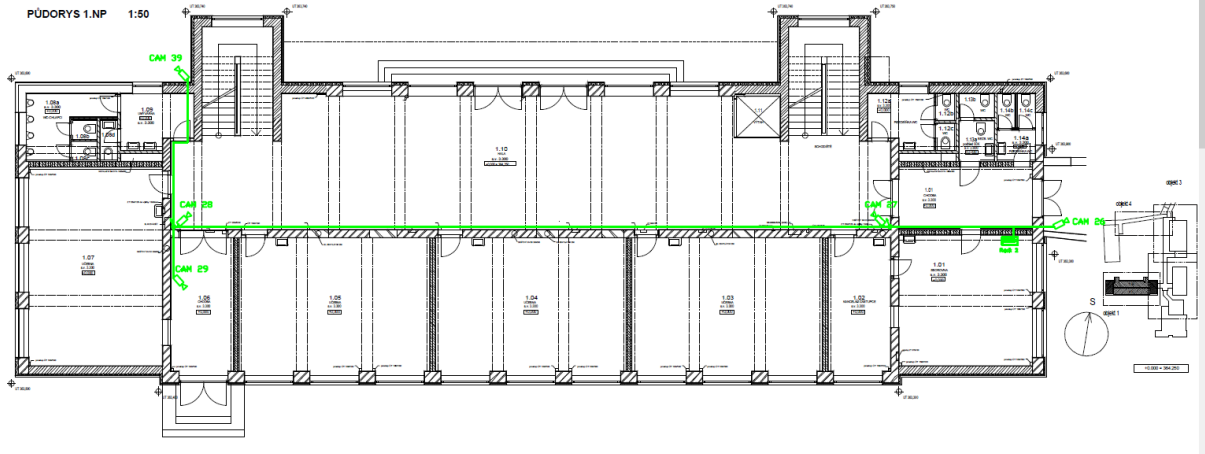
## Koridor ke školní jídelně



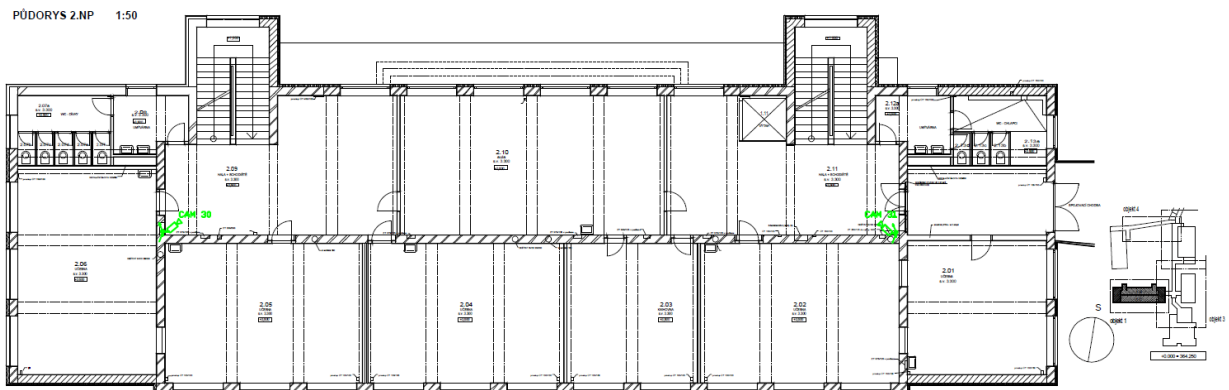
# Koridor u velké tělocvičny



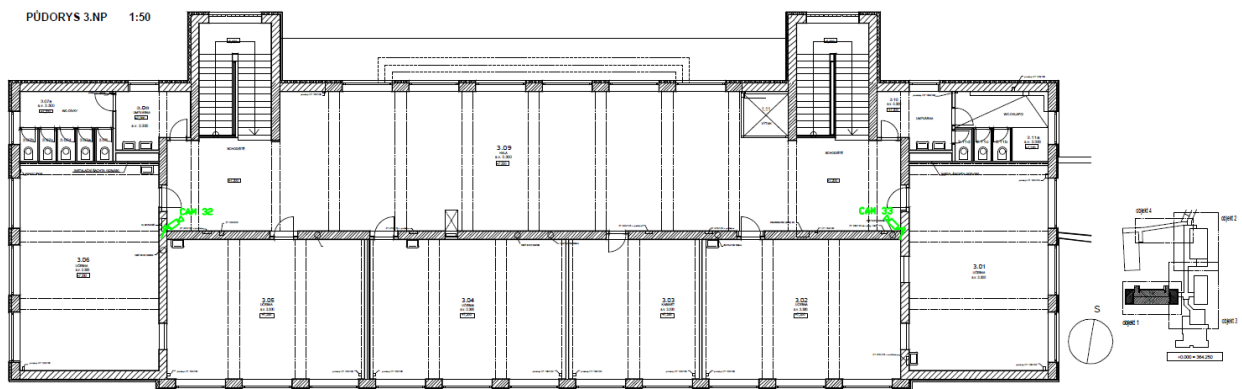
1. stupeň – 1.NP



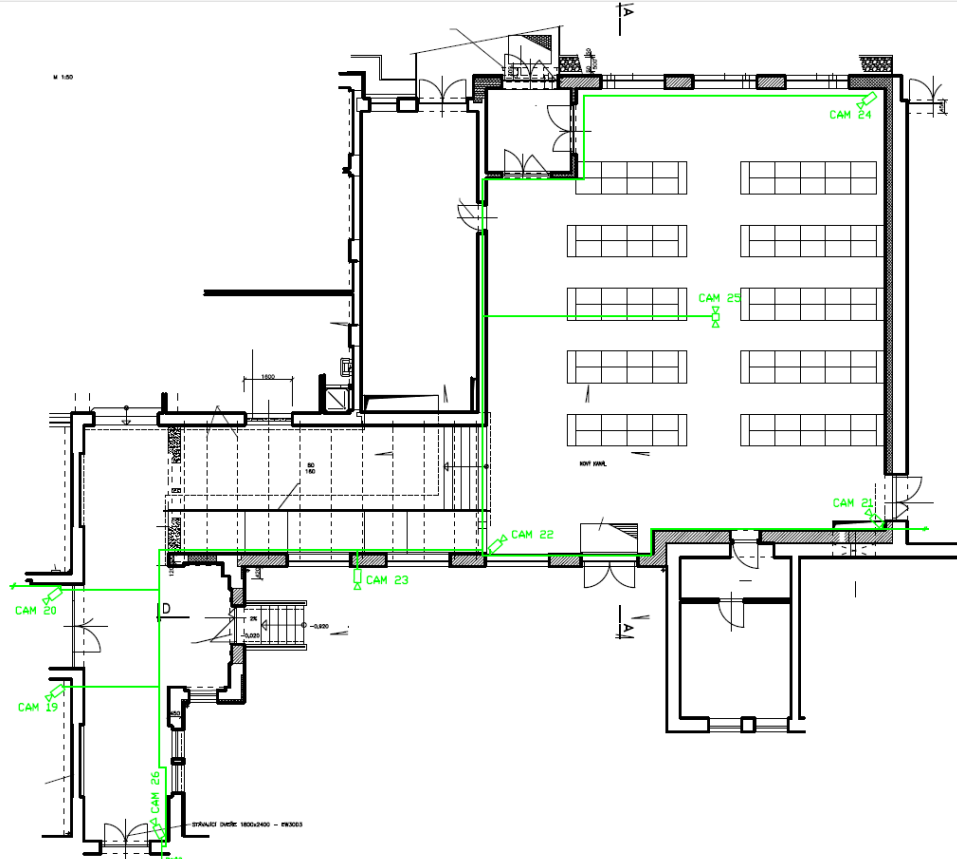
1. stupeň – 2.NP



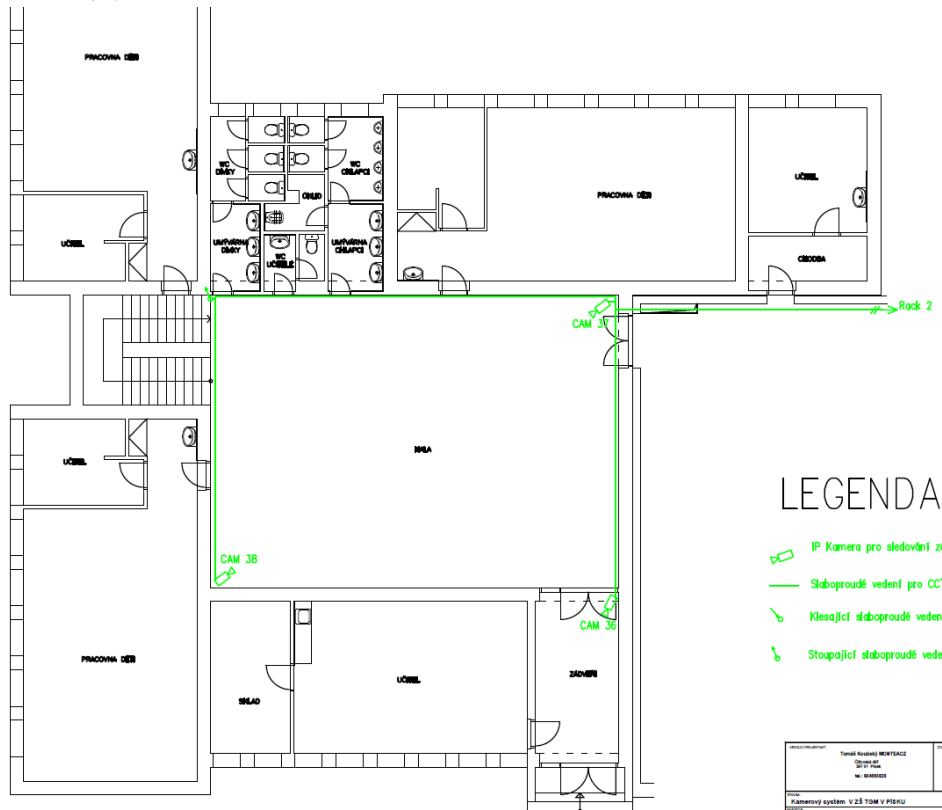
1. stupeň – 2.NP







# Šatny 1. stupeň



# Školní družina – 1.NP

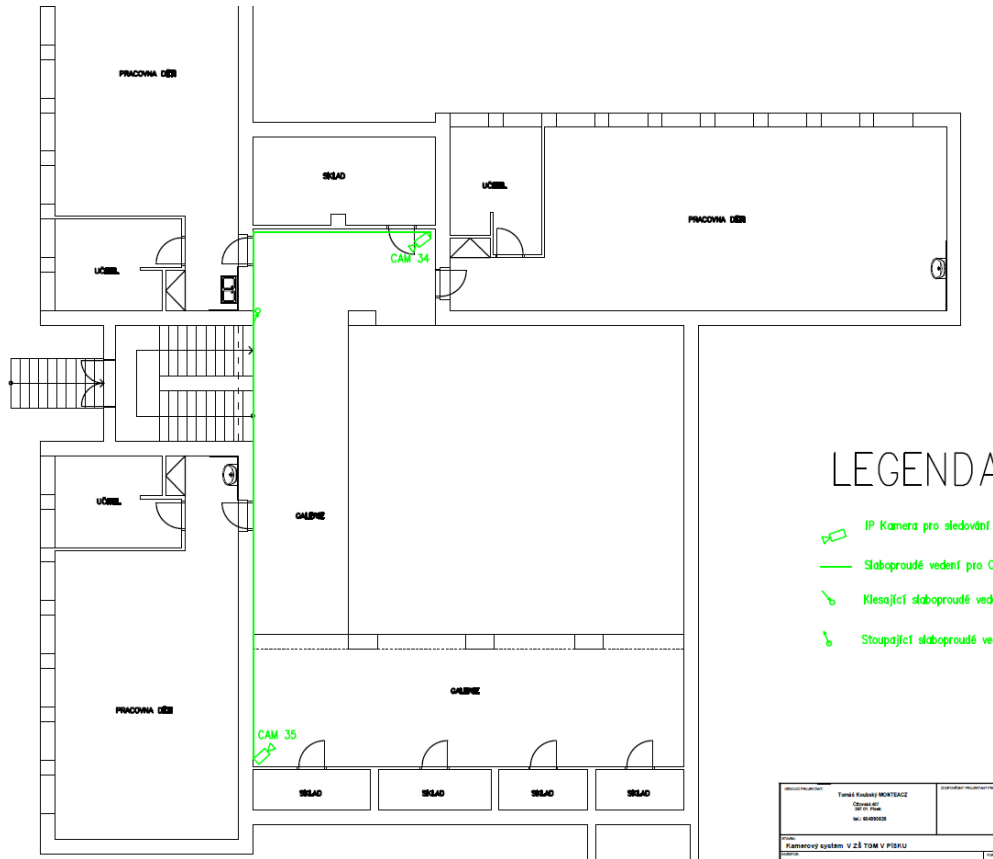


## LEGENDA:





-  IP Kamera pro sledování zón
-  Slaboproudé vedení pro CCTV
-  Klesající slaboproudé vedení
-  Stoupající slaboproudé vedení

Technická zpráva Téma: Realizace MONTÁŽE Objekt: MŠA Místnost: Kameryový systém v ZŠ TOM V PÍSKU Datum:
---

# Školní družina – 2.NP



## LEGENDA

-  IP Kamera pro sledování
-  Slaboproudé vedení pro C
-  Klesající slaboproudé vedení
-  Stoupající slaboproudé vedení

Tiskárna Tiskárna Tiskárna Tiskárna	Tiskárna Tiskárna Tiskárna Tiskárna
Komerční systém V ZŠ TGM v Písku	