ANALÝZA ZHODNOCENÍ SOUČASNÉHO STAVU OSOBNÍCH ÚDAJŮ A NÁVRH IMPLEMENTACE GDPR PRO OBEC VLTAVICE

# Charakteristika posuzovaného subjektu

Obec Vltavice má 7 členů zastupitelstva, 201 obyvatel. Obec má zároveň příspěvkovou organizaci Mateřskou školku.

Tato analýza se týká výlučně obce Vltavice.

## Struktura obecního úřadu

Obecní úřad tvoří starosta, místostarosta, případně zaměstnanci obce zařazení do obecního úřadu. Úřední hodiny obecního úřad v obci Vltavice jsou:

Pondělí: 13:30 – 15:30

Středa: 15:00 – 18:00

Pátek: 17:00 – 19:00

# Obecná struktura uchovávání osobních údajů v obci (současný popis)

## Obec Vltavice a Úřad pro ochranu osobních údajů.

V současné době má obec Vltavice na Úřadu pro ochranu osobních údajů hlášeno provozování kamerového systému, který snímá dvůr, kopie listiny je přílohou číslo 1 této analýzy.

## Technické a organizační opatření obce Vltavice

V současné době obec Vltavice provádí novelizaci technických a organizačních opatření v takové formě, aby bylo v souladu s GDPR.

Obec má zpracované následující předpisy:

* organizační řád,
* spisový a skartační řád schválený věcně a místně příslušným archivem,
* vnitřní organizační směrnice o vedení účetnictví,
* směrnice pro poskytování a účtování cestovních náhrad

## Jaké jsou na obecním úřadě elektronické zdroje?

Za zajištění jednotlivých informačních systémů odpovídá správce informačního systému. V obci Vltavice jsou tyto elektronické zdroje/evidence:

1. Systém ÚĆTO

Účetní systém, který tvoří základ pro agendu daňových dokladů a faktur, nyní se připravuje realizace opatření, která uvede systém do souladu s GDPR. Je v něm vedena spisová služba, evidence obyvatel, Czech Point a případná konverze dokumentů.

1. Systém KN

Jde o speciální software, který umožňuje nahlížení do stavebních pozemků

1. Veřejné zakázky a výběrová řízení

Evidence je vedena v tabulce EXCEL

Případně další.

1. Evidence obyvatel
2. Evidence včelařů

**Další různé agendy, je to velmi individuální a záleží na jednotlivé obci!**

## Jaké jsou na obecním úřadě listinné zdroje?

Listiny jsou uloženy ve skříni v kanceláři starosty, včetně pracovních smluv. Pracovním smlouvám je věnována samostatná kapitola této analýzy. Zdroje osobních údajů jsou rozloženy dle jednotlivých agend a jsou v šanonu ve skříni. Na základě rozdělení skříně budou poté očíslovány.

# Návrh implementace

## Vytvoření přehledů a seznamů

Na základě návrhu implementace a dosažení souladu s GDPR byly vytvořeny tyto následující seznamy. Jde o seznam agend, který obsahuje veškeré poznatky o jednotlivých agendách, agendy dále navazují na agendové listy. Na základě tohoto seznamu je zhodnocen soulad s GDPR v jednotlivých agendách v této analýze. V případě, že došlo ke zhodnocení nesouladu, analýza navrhuje patřičná opatření případně konzultaci s dozorovým úřadem.

Tato analýza tvoří ucelený řetězec společně s přílohami a evidencemi.

## Doplnění vnitřních předpisů

Na obecním úřadu

* + Organizační řád (vydat, pokud nebyl vydán)
  + Spisový a skartační řád (např. revize skartačních dob)
  + Provozní řád informačního systému
  + Seznam evidencí a dokumentů
  + Seznam osob, které mají přístup k osobním údajům ze ZR obyvatel s popisem opatření, dle kterých lze určit, komu byly a jsou tyto údaje předávány.
  + Seznam osob, které mají přístup k Czech Pointu s popisem opatření, dle kterých lze určit, komu byly a jsou tyto údaje předávány.
  + Seznam klíčů k budově a komu byly přiděleny
  + Pravidla pro přijímání petic a vyřizování stížností
  + Seznam informačních systémů a programů s popisem certifikací a bezpečnostního systému
  + Směrnice na ochranu osobních údajů
  + Seznam razítek

## Seznam rizikových zpracování

Jelikož obec Vltavice je obcí 1. typu, lze předpokládat, že většinu zpracování osobních údajů bude provádět na základě čl. 6.odst. 1 písm. c), tedy plnění zákonné povinnosti obce, případně písm. e), kdy bude docházet ke zpracování na základě veřejného zájmu nebo písm. b) na základě plnění smlouvy.

Na základě pečlivého studia dokumentů v rámci ochrany osobních údajů byly zjištěny některé agendy, které vykazují vyšší míru rizika incidentních hrozeb.

## Dodavatelé IT softwarů a programů

Pro elektronické zdroje se zajistí dokumentace všech IT programů, které obecní úřad používá a postupnými kroky se zároveň bude chystat systémová příručka. V systémové příručce obce Vltavice budou následující body:

1. Popis implementovaného systému nebo programu (nutné podmínky pro instalaci a následný provoz
2. Licenční podmínky
3. Popis podpory uživatele (hot-line, helpdesk)
4. Bezpečnostní podmínky (jak je systém zabezpečen – přístupy, šifrování, zálohování a bezpečnostní kopie).
5. Popisy systémem vytvářených logů – systémových a transakčních
6. Zprávy a výsledky testů a certifikací, které informační systém nebo program získal
7. Případně cloudové služby

V současné době obec Vltavice nevyužívá cloudové služby a nemá to ani v plánu. Pokud ale po změně vedení, případně jiného vedení, obec Vltavice tyto služby začne používat, obec Vltavice si vyžádá informace o tom, kde se úložiště nachází a že úložiště je zabezpečeno podle GDPR.

Evidence, které spadají pod písm. 2 c) jsou evidovány v pdf souborech, případně excelových souborech. V takové fázi lze doporučit, aby došlo k šifrování takových souborů, v případě předávání k 3. osobám lze doporučit, aby byly individuálně smluvně upraveny.

## Smluvní vztahy s dodavateli softwaru

Obec Vltavice v rámci svých elektronických zdrojů a informačních systémů se písemně dotáže dodavatelů IS programů, zda jeho systém budou včas na GDPR připraven a že smluvní strany jsou připraveny spolupracovat s pověřencem pro ochranu osobních údajů, včetně kooperace s případnými kontrolami Takové prohlášení bude v písemné formě v dodatku jednotlivé smlouvy se zpracovatelem.

Zároveň obec Vltavice bude písemně po dodavateli IT softwaru požadovat:

* Závazek spolupracovat s pověřencem pro ochranu osobních údajů
* Subjekt údajů bude mít dobrou dostupnost pro informace o zpracování svých údajů
* Možnost realizovat právo subjektu na opravu nebo výmaz údajů s tím, že se uvede v jaké formě, nejlépe v písemné formě, protože písemná forma umožňuje lepší prokazatelnost
* Možnost realizovat právo na omezení zpracování
* Možnost subjektu poskytnout kopii zpracovávaných osobních údajů
* Právo na přenositelnost údajů (subjekt má právo získat osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu).
* Podpora logování v čitelné formě a s takovým rozsahem, že bude možné jednoznačně prokázat denní činnosti IS (nebo programu) s vazbou na uživatele a jeho činnosti v souvislosti s technickým a organizačním opatřením, s tím, že bude upraveno, co se stane s daty po ukončení smlouvy

Dále obec Vltavice zreviduje smlouvy, které obsahují osobní údaje následujícím způsobem:

* Zajištění mlčenlivosti osob, které přijdou do styku s osobními údaji (u externích dodavatelů, případně tam, kde není zákonná povinnost)
* Zajištění a nastavení podmínek pro zapojení dalšího zpracovatele dle nařízení GDPR
* Zajistit práva subjektu údajů (informace o vedených údajích apod., dle GDPR)
* Zajistit podporu pověřence pro ochranu osobních údajů
* Zajistit ujednání o náhradě škody, včetně regresních nároků (s pozorností na smluvní pokuty, aby nevylučovaly náhradu škody).
* Zajistit po ukončení smlouvy odstranění kopií, zničení kopií, případně předání osobních údajů.

Do příslušných dokumentací, vnitřních předpisů a nařízení by v souladu s technickým stavem věcí měly být postupně zaznamenány následující činnosti:

- pseudonymizace a šifrování osobních údajů – zajistit, aby popis byly součástí systémové příručky

- zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování (zajistit, aby popis byl součástí systémové příručky, případně i řádu informačních systémů)

- schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických a technických incidentů

Zároveň je vhodné také zajistit pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. Tento proces ideálně také sepsat do systémové příručky, a aby kontrola a realizace procesu byla součástí provozního testování, posuzování a hodnocení účinnosti zavedených opatření.

## Ŕešení zabezpečení v jednotlivých agendách:

### Daňové doklady,faktury.

Současný stav:

V současné době jsou tyto údaje v uzamykatelné místnosti a v uzamykatelné skříni v kanceláři starosty.

Návrh opatření:

V souladu s GDPR.

### Smlouvy

Současný stav:

V současné době jsou v papírové formě tyto evidence v uzamykatelné místnosti a v uzamykatelné skříni v kanceláři starosty. V elektronické formě jsou tyto evidence v pdf/excelových souborech.

Návrh opatření:

Pro papírovou formou lze konstatovat, že evidence jsou v souladu s GDPR. V elektronické formě půjde o uspořádání formátů dokumentů a zároveň zašifrování souboru, např. pouze pomocí zipovaného souboru. Zároveň také pokud v rámci zákonných důvodů obec Vltavice bude předávat osobní údaje elektronickou cestou, doporučuje se použít datovou schránku, nedoporučuje se používat e-maily, kde je riziko ztráty osobních údajů.

### Žádosti

Současný stav:

V současné době jsou v papírové formě tyto evidence v uzamykatelné místnosti a v uzamykatelné skříni v kanceláři starosty. V elektronické formě jsou tyto evidence v pdf /excelových souborech, případně jsou uloženy ve speciálních souborech, které vyžadují projektovou dokumentaci.

Návrh opatření:

Pro papírovou formu lze konstatovat soulad s GDPR. V elektronické formě půjde o uspořádání formátů dokumentů a zároveň zašifrování souboru, např. pouze pomocí zipovaného souboru. Zároveň také pokud v rámci zákonných důvodů obec Vltavice bude předávat osobní údaje elektronickou cestou, doporučuje se použít datovou schránku, zároveň není vhodné používat e-maily, kde hrozí riziko ztráty osobních údajů. GDPR

### Povolení

Současný stav:

V současné době jsou v papírové formě tyto evidence v uzamykatelné místnosti a v uzamykatelné skříni v kanceláři starosty. V elektronické formě jsou tyto evidence v pdf /excelových souborech.

Návrh opatření:

Pro papírovou formu lze konstatovat soulad s GDPR. V elektronické formě půjde o uspořádání formátů dokumentů a zároveň zašifrování souboru, např. pouze pomocí zipovaného souboru. Zároveň také pokud v rámci zákonných důvodů obec Vltavice bude předávat osobní údaje elektronickou cestou, doporučuje se použít datovou schránku, zároveň není vhodné v rámci GDPR používat pouze ty e-maily, které můžou nést rizko ztráty osobních údajů GDPR..

### Dary

Současný stav:

V současné době jsou v papírové formě tyto evidence v uzamykatelné místnosti a v uzamykatelné skříni v kanceláři starosty. V elektronické formě jsou tyto evidence v pdf /excelových souborech.

Návrh opatření:

Pro papírovou formu lze konstatovat soulad s GDPR. V elektronické formě půjde o uspořádání formátů dokumentů a zároveň zašifrování souboru, např. pouze pomocí zipovaného souboru. Zároveň také pokud v rámci zákonných důvodů obec Vltavice bude předávat osobní údaje elektronickou cestou, doporučuje se použít datovou schránku, zároveň není vhodné v rámci GDPR používat pouze ty e-maily, kde nehrozí riziko ztráty osobních údajů.

## Pracovní smlouvy obce Vltavice

Obecně pro většinu zpracovávaných dat na pracovišti nemůže a neměl by být právním důvodem souhlas zaměstnance, to z důvodu nadřízenosti a podřízenosti. Zpracování může být nezbytné pro plnění ze smlouvy, zároveň je také jasné, že zaměstnanecké poměry souvisí se spoustou zákonných povinností veřejného práva. Zároveň operace zpracování musí také být ve shodě s požadavky transparentnosti a zaměstnanci musí být jasně a plně informování o zpracování svých údajů, včetně přítomnosti jakéhokoliv sledování. Pokud stejně zaměstnavatel souhlas opatří, nemůže ho podmiňovat např. trváním pracovního poměru, případně nějakou jinou povinností, v tom případě by souhlas nebyl svobodný a byl by protiprávní.

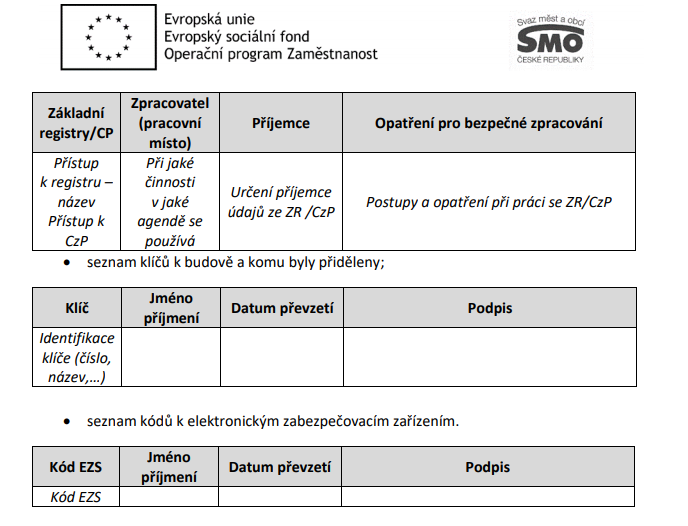
Použití oprávněného zájmu naráží právě na to, že obce jsou tzv. „orgánem veřejné moci“, orgány, které rozhodují o právech a povinnostech, OVM mohou využívat pouze v určitých případech.

Pracovní smlouvy se zabezpečí v uzamykatelné skříni v kanceláři starosty, kde bude mít přístup pouze starosta, případně další oprávněné osoby, které potřebují s osobními údaji pracovat. Zároveň se provede revize souladu s GDPR a to nejméně v takovém rozsahu:

* Určí se závazek (nejlépe vnitřním předpisem) spolupracovat s pověřencem pro ochranu osobních údajů
* Pokud osoba pracuje s osobními údaji, vytvoří se dodatek mlčenlivosti a zákazu předání 3. Osob s výjimkou, kdy je předání nezbytné, v tom případě se upraví práva a povinnosti předáním právě dodatkem smlouvy, pokud osoba činnost vykonává externě, případně není právní povinností.

V Praze dne 11. 4. 2018

Přílohy:



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dokument/seznam/doklad** | **Účel zpracování** | **Údaje** | **Příjemce** | **Zákon** | **Komentář** | **Rizikový** |
| Daňové doklady, faktury | Ekonomické agendy | Jméno, příjmení, adresa | Dodavatel  Odběratel | Zákon č. 563/1991 Sb., o účetnictví | Vytváří se na PC a tisknou se, zakládají | NE |
| Smlouvy | Evidence smluv | jméno, příjmení, adresa, datum narození | Smluvní strana | Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník | o dílo, pronájmy, … Vytváří se na PC a tisknou se, zakládají | NE |
| Žádosti | Správní rozhodování obce, potvrzení | jméno, příjmení, adresa | Žadatel, referent úřadu | Zákon č. 114/1992 Sb., o ochraně přírody a krajiny (dřeviny); zákon č. 183/2006 Sb., stavební zákon (souhlas se stavbou a napojením RD na inž. sítě)  Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech | kácení stromů, souhlas se stavbou a napojením RD na inž. sítě, rušení údaje o místu trvalého pobytu, evidence obyvatel | NE |
| Stížnosti |  | jméno, příjmení, adresa | Starosta | Zákon č. 500/2004 Sb., správní řád |  | NE |
| Povolení | Správní rozhodování obce | jméno, příjmení, adresa | Žadatel o  rozhodnutí | Zákon č. 114/1992 Sb., o ochraně přírody a krajiny (dřeviny) a zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech | kácení stromů, rušení údaje o místu trvalého pobytu | NE |
| Dary | Evidence žádosti a poskytnutých darů | jméno, příjmení, adresa | Žadatel o dar | Zákon č. 89/2012 Sb., občanský zákoník a s tím související zákon č. 128/2000 Sb., o obcích (obecní zřízení) – upravuje některé podmínky poskytnutí daru |  | NE |
| Dotace | Evidence žádostí o dotaci | jméno, příjmení, adresa | Žadatel o dotaci | Zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, zákon č. 500/2004 Sb., správní řád, zákon č.89/2012 Sb., občanský zákoník, zákon č.128/2000 Sb., o obcích |  | NE |
| Včelaři | Evidence včelařů v obci | jméno, příjmení, adresa | Referent úřadu | Zákon č. 326/2004 Sb., o rostlinolékařské péči a související  Vyhláška č. 327/2012 Sb. o ochraně včel, zvěře, vodních organismů a dalších necílových organismů při použití přípravků na ochranu rostlin |  | NE |
| Kódy k EZS | Zabezpečení prostor OÚ  Kulturního domu, Fary | kód, jméno, příjmení | Starosta | Organizačně technické opatření | Kódy přidělené pracovníků, seznam u starosty | NE |
| Klíče | Zabezpečení prostor OÚ, KD , Fara , Vodojemy Malenice,Zlešice a komunikace s bezp. službou. | kód klíče, jméno, příjmení | Starosta | Organizačně technické opatření | Seznam klíčů a osob. | NE |
| Razítka | Evidence dle spisového řádu | číslo razítko, jméno, příjmení | Referent úřadu, | Zákon č. 97/1974 o archivnictví |  | NE |

**Agendový list OÚ**   
1. Šablona s popisem   
2. Prázdná šablona

**Jde pouze o vzor, skutečnosti, které jsou v agentových listech, reálně neexistují!!!!!**

**Agendové listy jsou doplňkem seznamu evidencí, tedy společně tvoří ucelený řetězec.**

|  |  |
| --- | --- |
|  | **AGENDOVÝ LIST OÚ - Obecní úřad** |
| **Pořadové číslo katalogového listu** | *Pořadové číslo listu (může obsahovat i identifikátor např.*  *EK-ekonomika, EV-evidence, SP-správní činnost atd)* |
| **Pracovní místo** | *Pracovní místo kde dochází ke zpracování OÚ* |
| **Účel zpracování** | ***Název při kterém dochází ke zpracování OÚ*** |
| **Osobní údaje** | *Vyjmenování zpracováním dotčených osobních údajů* |
| **Souhlas subjektu údajů/ano/ne** | *Pokud existuje souhlas subjektu se zpracováním OÚ.* |
| **Subjekt údajů** | *Subjekt dotčený zpracováním OÚ* |
| **Zdroje osobních údajů** | *Zdroj který uvedl a poskytl osobní údaje* |
| **Příjemce osobních** | *Kdo (fyzická osoba, organizace) OÚ přijímá (bude k nim mít přístup)* |
| **Předání do zahraničí/ano/ne** | *Jsou OÚ předávány do zahraničí (seznamy pro zájezdy, družební obce a následná komunikace, smluvní vztahy, fakturace a finanční operace,…)* |
| **Druh zpracování** | *Jaký druh zpracování se bude s OÚ provádět*  *Shromažďování , Zaznamenávání , Uspořádání , Strukturování , Uložení , Přizpůsobení nebo pozměnění dat, Vyhledávání , Nahlédnutí, Použití , Zpřístupnění, Výmaz nebo zničení* |
| **Způsob zpracování** | *Manuální – práce s papírovými dokumenty, automatizované – evidence a zpracování na PC (v sw prostředku) a uvést zda zpracování bude na úřadě nebo bude v cloudu (cloudových službách)* |
| **Databáze (např. Excel)**  **Informační systém** | *Pokud budou OÚ zaznamenány a zpracovávány v informačním systému obce nebo mohou být uloženy v nějaké lokální databázi např. Excel nebo jiné používané databázi.* |
| **Popis opatření k zajištění požadované ochrany osobních údajů** | *Jedná se o zabezpečení budovy, kanceláře, skříně (= EZS, zámky skříní, zámky kanceláří, bezpečností dveře,…) a i o bezpečnost při zpracování na PC (hesla, antivirová ochrana + pravidla bezpečnosti VT uvedená ve směrnici úřadu)* |
| **Adresa zpracování, je li odlišná od sídla úřadu** | *Pokud zpracování OÚ probíhá v jiné budově než-li je budova úřadu uvede se adresa.* |
| **Informace získány (kdy)** | *Kdy byly OÚ zdrojem poskytnuty* |
| **Doba uchování dle Spisového a skartačního řádu** |  |
| **Přístupová oprávnění** | *Kdo má oprávnění (na úřadě) s OÚ pracovat (účetní starosta, správce, ..)* |

Použité zkratky :  
OÚ – osobní údaje  
EZS – elektronický zabezpečovací systém  
IS - informační systém  
SW - software

|  |  |
| --- | --- |
|  | **AGENDOVÝ LIST OÚ - Obecní úřad** |
| **Pořadové číslo katalogového listu** | VČ |
| **Pracovní místo** | Vltavice |
| **Účel zpracování** | Evidence včelařů v obci (z. 326/2004 o rostlinolékařské péče) |
| **Osobní údaje** | Jméno, příjmení, adresa |
| **Souhlas subjektu údajů/ano/ne** | Ne |
| **Subjekt údajů** | Majitelé včelstva |
| **Zdroje osobních údajů** | Majitel včelstva na základě zákonné povinnosti |
| **Příjemce osobních** | Obecní úřad Vltavice |
| **Předání do zahraničí/ano/ne** | Ne |
| **Druh zpracování** | Shromažďování, zaznamenávání, nahlédnutí, uložení |
| **Způsob zpracování** | Manuální |
| **Databáze (např. Excel)**  **Informační systém** | Desky v šanonu |
| **Popis opatření k zajištění požadované ochrany osobních.** | Evidence včel bude v uzamykatelné skříni, kde bude mít přístup pouze starosta. Zároveň klíč ke skříni bude v uzamykatelném trezoru. |
| **Adresa zpracování, je li odlišná od sídla úřadu** | Ne |
| **Informace získány (kdy)** | Např. 1. 1. 2015 |
| **Doba uchování dle Spisového a skartačního řádu** | Např. 5 let |
| **Přístupová oprávnění** | Starosta |

|  |  |
| --- | --- |
|  | **AGENDOVÝ LIST OÚ - Obecní úřad** |
| **Pořadové číslo katalogového listu** | DA |
| **Pracovní místo** | Vltavice |
| **Účel zpracování** | Evidence faktur (z. 89/2012 Sb. Občanský zákoník, z. 563/1991 Sb., o účetnictví) |
| **Osobní údaje** | Jméno, příjmení, adresa |
| **Souhlas subjektu údajů/ano/ne** | Ne |
| **Subjekt údajů** | Dodavatel, odběratel |
| **Zdroje osobních údajů** | Daňové doklady, faktury |
| **Příjemce osobních** | Obecní úřad Vltavice |
| **Předání do zahraničí/ano/ne** | Ne |
| **Druh zpracování** | Zaznamenávání, nahlédnutí, uložení, plnění |
| **Způsob zpracování** | Manuální/elektronické |
| **Databáze (např. Excel)**  **Informační systém** | Systém KEO |
| **Popis opatření k zajištění požadované ochrany osobních.** | Evidence dodavatelů a odběratelů, bude uložena v uzamykatelné skříni, kam bude mít přístup pouze starosta. Zároveň klíč ke skříni bude v uzamykatelném trezoru. Riziko je nízké. |
| **Adresa zpracování, je li odlišná od sídla úřadu** | Ne |
| **Informace získány (kdy)** | Např. 1. 1. 2018 |
| **Doba uchování dle Spisového a skartačního řádu** | Doplnit dle řádu |
| **Přístupová oprávnění** | Účetní/starosta |