Řízení rizik procesů malé obce s ohledem na novou právní úpravu ochrany osobních údajů

Svatava Wagnerová

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Svatava Wagnerová**
Osobní číslo:	**L16274**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Řízení rizik procesů malé obce s ohledem na novou právní úpravu ochrany osobních údajů**

Zásady pro vypracování:

1. **Zpracujte teoretické a metodické řízení procesů týkající se vybrané organizace v rozsahu nařízení GDPR.**
2. **Analyzujte a zhodnoťte řízení procesů vybrané organizace v rozsahu nařízení GDPR.**
3. **Navrhněte a formulujte doporučení pro zlepšení řízení procesů vybrané organizace v rozsahu nařízení GDPR.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[2] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017. Právo. ISBN 978-80-7554-097-3.

[3] Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 28.8.2017. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-24.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**Ing. Slavomíra Vargová, PhD.** Ústav krizového řízení
Datum zadání bakalářské práce:	**30. listopadu 2018**
Termín odevzdání bakalářské práce:	**15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15. 5. 2019

Jméno a příjmení studenta: Svatava Wagnerová

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá „Řízením rizik procesů malé obce s ohledem na novou právní úpravu ochrany osobních údajů“. Práce je rozdělena na teoretickou a praktickou část. Část teoretická se zabývá definicemi a pojmy v dané oblasti. Praktická část je zaměřena na analýzu formou kontrolního seznamu a následného zhodnocení rizik. Předmětem zkoumání jsou rizika v rámci jednotlivých činností přípravy a implementace GDPR v procesech realizovaných na malé obci.

Klíčová slova: Analýza, obec, proces, riziko, zákon

ABSTRACT

This bachelor's thesis deals with „Risk Management of Processes for the small village with respect to the new legal regulations for protection of personal data“. The thesis is divided into the theoretical and the practical part. The theoretical part deals with definitions and terms in the given sphere. The practical part pays particular attention to the analysis using the check list and the follow-up risk evaluation. The investigation subject consists of the risks within the framework of individual activities to prepare and implement GDPR in the processes realised in the small village.

Keywords: Analysis, village, process, risk, law

„Každý, kdo se přestane učit, je starý, ať je mu dvacet nebo osmdesát. Každý, kdo se stále učí, zůstává mladý.“ Henry Ford americký průmyslník 1863 – 1947

Poděkování,

Ráda bych poděkovala Ing. Slavomíře Vargové, PhD za odborné vedení, cenné rady, připomínky a podněty při zpracování této bakalářské práce. Dále bych chtěla poděkovat své rodině za podporu a trpělivost, kterou měli po celou dobu studia.

OBSAH

ÚVOD

Dne 25. května 2018 nastala účinnost *„Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“[3]*. V té době autorka zastávala na obci funkci starostky, a tudíž se touto otázkou velice podrobně zabývala. Z tohoto důvodu bylo zvoleno téma bakalářské práce *„ Řízení rizik procesů malé obce s ohledem na novou právní úpravu ochrany osobních údajů.“*

Ačkoliv v České republice platil zákon č. 101/2000 Sb., o ochraně osobních údajů, který tuto problematiku řešil, tak srpnu v roce 2017 začaly přicházet první metodiky z Ministerstva vnitra, kde obce měly řešit své pověřence plynoucí z povinnosti EU. Nebyly informace a starostové na svých setkáních nechápali, proč by měli zaměstnávat dalšího člověka a hledat pro něj peníze už v tak nízkém obecním rozpočtu. Jak již bylo zmíněno, informací bylo málo a přišly pozdě. Ministerstvo vnitra situaci podcenilo. Svaz měst a obcí ČR se naopak snažil obcím pomáhat.

Kromě těchto institucí se o problematiku začalo zajímat stále víc a víc firem, které viděly jen rychlý zisk. Obcím tyto firmy nabízely, že jim zpracují úplně celou agendu, ale za nemalé peníze. Nakonec obce odolaly náporu těchto firem a velké množství se jich rozhodlo spojit se Svazem měst a obcí ČR nebo s dobrovolným svazkem obcí. Toto spojení s dobrovolným svazkem obcí si zvolila i vybraná obec. Autorka byla tedy členem týmu, který vše řídil, organizoval, připravoval a na všem se podílel.

Prostory vybraného obecního úřadu nesplňovaly podmínky dle směrnice EU a musely projít rekonstrukcí od výměny podlah po nový a plně funkční nábytek. Řešilo se nové vhodnější uspořádání kanceláří. Zaváděl se kamerový systém, klíčový systém, nové smlouvy s dodavateli, aby bylo vše v souladu s novou směrnicí EU.

Hlavním cílem v teoretické části bakalářské práce bylo seznámit se světovým a evropským vývojem a současně se stavem zabezpečení ochrany osobních údajů v České republice. Následuje vysvětlení pojmů, které jsou spojené se směrnicí EU. V části praktické byly řešeny už konkrétní činnosti, analýzy formou kontrolního seznamu a tabulky, které určily pracovní postup. Cílem bylo zjistit jednotlivé agendy, určit odpovědnost, kompetence a rizika. Pokud něco bylo opomíjeno nebo špatně nastaveno v systému, bylo potřeba vše znovu nastavit tak, aby nebyly porušovány zákony.

I. TEORETICKÁ ČÁST

1 VÝVOJ OCHRANY OSOBNÍCH ÚDAJŮ

V současné době patří právo na ochranu osobních údajů mezi základní práva člověka. Toto právo je součástí práva na ochranu soukromí, které se vyvíjelo do současné podoby tak, jak se vyvíjela moderní společnost. Nastala nutnost chránit nejen soukromí jako celek, ale poskytnout zvláštní ochranu také fyzickým osobám při zpracování jejich osobních údajů. Zpracování osobních údajů začalo negativně zasahovat do soukromí člověka [3].

Rozsah zpracovávaných informací o jedinci je obsáhlejší než před několika desítkami let. Zároveň je i snadnější díky dostupnějším technologiím. Součástí našeho každodenního života se staly kamerové systémy, aplikace umožňující v několika sekundách provádět různé druhy zpracovatelských operací, které dříve zabraly dny nebo vůbec nebyly reálně možné, samozřejmostí je internet umožňujícím jedním kliknutím zaslat osobní údaje na druhý konec světa nebo je zpřístupnit. Moderní prostředky představují i velké riziko pro osobní údaje a soukromí člověka. Lidské chování je stéle více sledováno a podrobováno profilování [3].

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném zpracování těchto údajů [5] (dále jen nařízení) známé jako „GDPR“ je v platnosti s účinností od 25. května 2018 - po dvouleté periodě určené k přípravě. Nahrazuje současný zákon 101/2000 Sb., o ochraně osobních údajů [5].

Nařízení tak dává subjektům údajů mnohem větší práva, stanovuje mnohem přísnější požadavky jak správcům, tak zpracovatelům a uplatňuje výrazně vyšší sankce, než tomu bylo doposud [5].

Mezinárodní a evropské právní instrumenty zaručovaly a upravovaly právo na soukromí, respektive na ochranu osobních údajů. Tyto normy stanovující pravidla při zpracování osobních údajů, ukázaly, jaký vývoj za poslední desítky let společnost prodělala. Zjistíme, že Obecné nařízení je jen logickým vyústěním dnešní složité doby [3].

1.1 Světový a evropský vývoj

Prvním celosvětově významným mezinárodním dokumentem zaručujícím právo na soukromí byla **Všeobecná deklarace lidských práv, přijatá v San Francisku v roce 1948** Valným shromážděním Organizace spojených národů. Tato deklarace v čl. 12 stanovovala

mimo jiné zákaz vystavovat kohokoliv svévolnému zasahování do soukromého života a korespondence [3].

Obdobně jako Všeobecná deklarace lidských práv zaručovala v čl. 8 právo na respektování rodinného a soukromého života **Evropská úmluva o ochraně lidských práv a základních svobod sjednaná v roce 1950 v Římě.** Tyto dva dokumenty deklarovaly právo na ochranu soukromí obecně, ale nevěnovaly se právu na ochranu osobních údajů při jejich zpracování, které bylo v době přijetí těchto dokumentů přirozenou součástí práva na ochranu soukromí. V průběhu dalších let docházelo k rozvoji společnosti včetně rozvoje automatizovaných prostředků a aplikací, které byly stále více využívány ke zpracování osobních údajů. Tím vyvstala nutnost reagovat a začít chápat ochranu osobních údajů při jejich zpracování jako samostatnou právní oblast zasluhující zvláštní právní pozornost [3].

Dne 28. ledna 1981: *„Podpis smlouvy o ochraně osob s ohledem na automatické zpracování osobních údajů. Byla podepsána jako Úmluva Rady Evropy č. 108 a vstoupila v platnost dne 1. října 1985. Všech 47 členů Rady Evropy smlouvu ratifikovalo (podepsalo), s výjimkou Turecka* [5] .“

Úmluvou č. 108 byly položeny základy ochrany osobních údajů při jejich zpracování, na kterých stavěly další evropské dokumenty. Na počest přijetí Úmluvy č. 108, jakožto dokumentu s historickým významem, považován den **28. ledna za mezinárodní den ochrany osobních údajů** [3].

„Vývoj společnosti především té západní, se v 80. a 90. letech 20. století ubíral mílovými kroky, svět se vlivem moderních dopravních prostředků neustále „zmenšoval“, informace, včetně osobních údajů, se začaly v čím dál větším rozsahu zpracovávat automatizovaně, novými prostředky a nastalá nutnost předávat osobní údaje do třetích zemí byla jednou z projevů počínající globalizace. V evropském prostoru i s ohledem na fungování Evropské unie založené na volném pohybu osob, zboží a služeb (a s tím spojeného pohybu osobních údajů) nastala potřeba alespoň rámcově sjednotit pravidla pro zpracování osobních údajů a jejich předání do jiných států [3].“

Bylo nutné regulovat zpracování osobních údajů takovou právním normou, která by ochranu osobních údajů při jejich zpracování podrobně upravila jako celek, brala v potaz technologický vývoj od přijetí Úmluvy č. 108 a zároveň by právní úpravu v evropském prostoru alespoň částečně sjednotila.

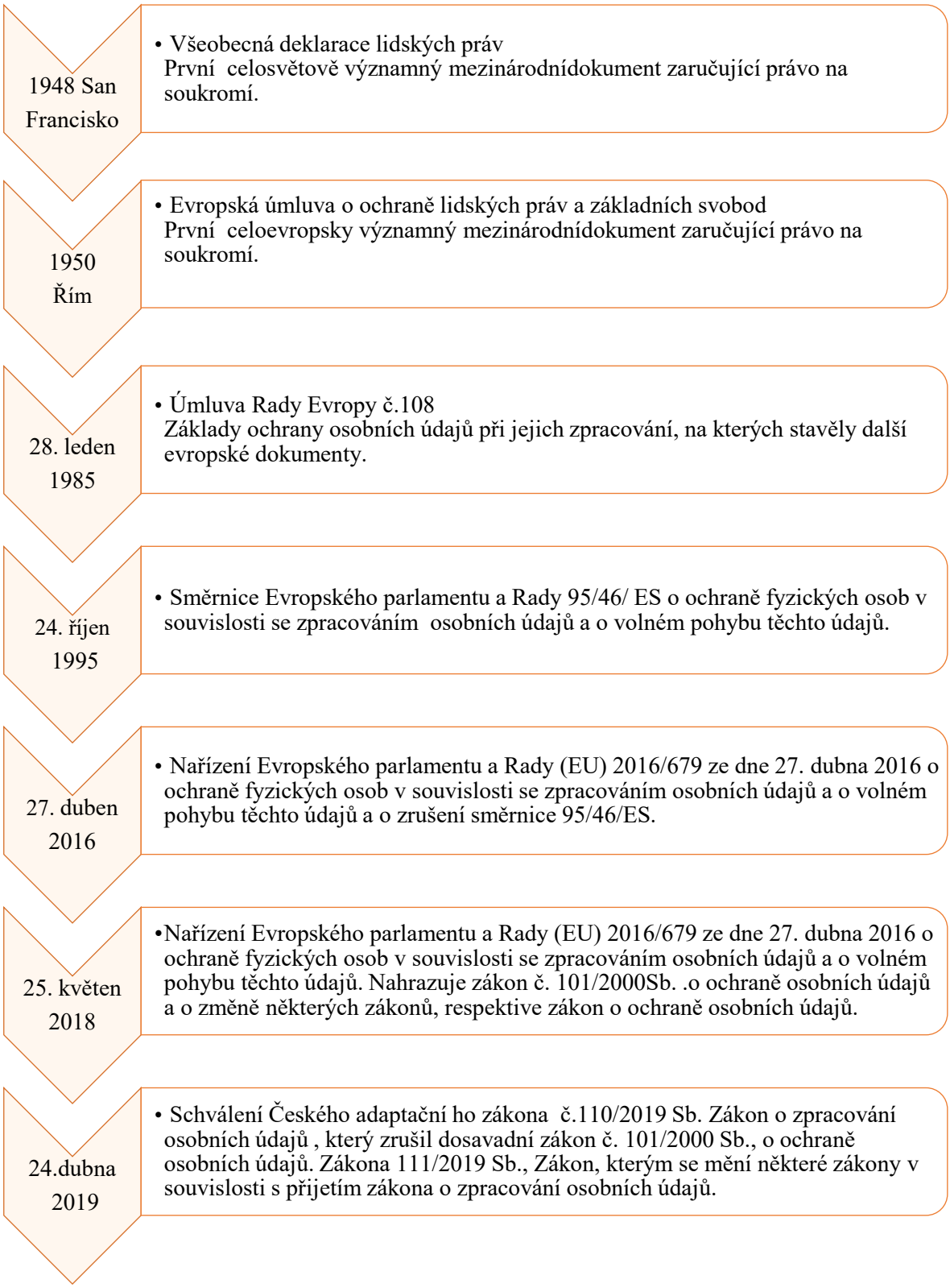
Tímto právním instrumentem se stala směrnice Evropské unie, konkrétně **Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů** (dále jen Směrnice 95/46/ES) [3].

Vlivem novel jednotlivých zákonů a dílčích právních úprav členských států se začaly jednotlivé vnitrostátní právní úpravy více lišit a požadovaná dosažená harmonizace nepřicházela. „*Zároveň v prvním desetiletí nového milénia začal rychlý rozvoj počítačové techniky, internetu a sociálních sítí, což přineslo nové obtíže při aplikaci zastaralých vnitrostátních zákonů. Vzrostl tlak na novelizaci, protože tyto zákony původně vycházející z již zastaralé Směrnice 95/46/ES, při jejímž vzniku nikdo nepředpokládal tak rapidní vývoj zpracování osobních údajů, nemohly v měnícím se světě bez jejich změny obstát. Současně musela být vzata v potaz rozšiřující se globalizace a související vzrůstající tlak na efektivní zajišťování ochrany osobních údajů při přeshraničním zpracování a vytvoření odpovídajících mechanismů ochrany fyzických osob. Muselo tak dojít k revizi celého právního rámce ochrany osobních údajů v evropském prostoru, která začala po roce 2010* [3].“

Dne 27. dubna 2016: Je v Úředním věstníku Evropské unie uveřejněno **Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů** a o zrušení směrnice 95/46/ES. Tímto momentem vstupuje GDPR v platnost [1].

Dne 25. května 2018: Nastává účinnost Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. GDPR vstupuje v účinnost [5].

Na Obr. 1. je graficky znázorněna časová osa právních norem na ochranu osobních údajů.



Obr. 1. Časová osa vlastní zpracování dle [2].

1.2 Vývoj a stav v České republice

V prostředí České republiky začala být ochrana osobních údajů při jejich zpracování samostatně řešena přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který, jak již z názvu vyplývá, upravoval pouze zpracování osobních údajů v informačních systémech [3].

„Na ochranu osobních údajů při jejich zpracování neměla Česká republika až do roku 2000 plnohodnotný zákon, který by pro zpracování osobních údajů na zákonné úrovni prováděl čl. 10 odst. 3 Listiny základních práv a svobod, jelikož zákon o ochraně osobních údajů v informačních systémech se vztahoval pouze na informační systémy a neřešil ochranu osobních údajů při jejich zpracování komplexně, tj. nevztahoval se na zpracování prostřednictvím evidence, tak jak už se vztahovala Směrnice 95/46/ES [3].“

O plnohodnotné ochraně osobních údajů v České republice lze hovořit až od 1. června 2000, kdy nabyl účinnosti zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, kterým byl zároveň zřízen Úřad pro ochranu osobních údajů jako dozorový úřad nad dodržováním povinností stanovených při zpracování osobních údajů. Aby Česká republika při vstupu do Evropské unie naplnila i podmínky v oblasti ochrany osobních údajů, byl v roce 2004 zákon o ochraně osobních údajů významněji novelizován v souvislosti s nutností transponovat (realizovat na zákonné úrovni) Směrnici 95/46/ES [3].

„Obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru, které od 25. května 2018 přímo stanovilo pravidla pro zpracovávání osobních údajů, včetně práv subjektů. V českém právním prostředí tak Obecné nařízení od 25. května 2018 nahradilo zákon č. 101/2000Sb. o ochraně osobních údajů a o změně některých zákonů, respektive zákon o ochraně osobních údajů [5].“

Dne 24. dubna 2019: Nastává účinnost Zákona č. 110/2019 Sb. Zákon o zpracování osobních údajů, který zrušil dosavadní zákon 101/2000 Sb,. O ochraně osobních údajů [17] . Dále nastává účinnost Zákona 111/2019 Sb., Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů [18].

Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie, který upřesňuje naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů [17].

1.3 Definice pojmů

Osobní údaj

Osobním údajem je informace o identifikované fyzické osobě. *Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby* [5].

Zpracování osobních údajů

„Zpracováním je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení [5].“

Zpracováním ve smyslu Obecného nařízení není jakékoli nakládání s osobním údajem. Zpracování osobních údajů je činnost, kterou správce s osobními údaji provádí za určitým účelem a systematicky. Pro nakládání s osobními údaji způsobem, který není zpracováním, poskytuje ochranu například zákon č. 89/2012 Sb., občanský zákoník. Obecným nařízením se tak správci řídí pouze subjekty, které osobní údaje zpracovávají ve smyslu definice zpracování [5].

Subjekt údajů

Subjektem údajů je fyzická osoba, které se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách [5].

Správce

„Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (například zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely, například pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob [5].“

Správcem může být jakýkoli subjekt. Správcem může být i fyzická osoba. Správce odpovídá za dodržování povinnosti kladených nařízením [5].

Každý správce by si měl udělat vlastní analýzu zpracování, které provádí, čímž zjistí, jaké eventuální povinnosti se na něj vztahují. Součástí analýzy může být i vytipování slabých míst správce, například v zabezpečení či provedení revize právních důvodů a jejich uvedení do souladu s podmínkami nařízení (například pokud správce využívá souhlas se zpracováním osobních údajů, provést zhodnocení, zdali udělené souhlasy budou použitelné i v době účinnosti nařízení) [5].

Desatero zpracování pro správce

Desatero zpracování pro správce je zestručnění základních pravidel ochrany osobních údajů, základní jednoduchý návod, jak zacházet s osobními údaji [7].

1. Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, musí být legitimní a nesmí být v rozporu s právními předpisy nebo morálkou.

2. Každé zpracování údajů musí být založeno na některém ze základních důvodů (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností nebo plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby [7].

3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr nebo účel zpracování údajů.

4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být vždy přiměřené účelu zpracování.

5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít jasný zákonný podklad, takové zpracování nelze nahradit souhlasem se zpracováním údajů [7].

6. Správce i zpracovatel osobních údajů musí osobní údaje patřičně zabezpečit a chránit organizačními a technickými opatřeními v míře odpovídající rizikovosti zpracování.

7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno férově, korektně a transparentně. Informace o zpracování poskytované subjektu údajů musí být zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci [7].

8. Zpracování nesmí nadměrně zasahovat do soukromí. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení nebo zveřejnění negativních či jinak citlivých údajů [7].

9. Po naplnění účelu zpracování je dána povinnost osobní údaje zlikvidovat. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).

10. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví nařízení. Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů [7].

Zpracovatel

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat [5].

Osobní údaje lze zpracovávat, pokud je přítomen alespoň jeden z těchto právních úkonů:

- subjekt udělil souhlas jen pro jeden nebo i více účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce nebo třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů [5].

Obecné nařízení je postaveno na těchto zásadách:

- *„zákonnost, korektnost, transparentnost správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,*
- *omezení účelu osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,*
- *minimalizace údajů musí být přiměřené a relevantní pro konkrétní účel,*
- *přesnost osobní údaje musí být přesné,*
- *omezení uložení osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektů údajů jen pro nezbytnou dobu pro dané účely, pro které jsou zpracovávány,*
- *integrita a důvěrnost, technické a organizační zabezpečení osobních údajů* [5].“

Pověřenec

Hlavním úkolem pověřence je pomoc správcům dosáhnout souladu zpracování osobních údajů a tím chránit i práva a svobody subjektu údajů u rizikovějších zpracování, protože povinnost jej jmenovat byla omezena pouze pro některé správce, v souladu s přístupem založeným na riziku. Pověřenec působí jako kontaktní místo jak pro subjekty údajů, tak i pro dozorový úřad. Roli pověřence, která je v organizaci důležitá, odpovídají i podmínkám pro jeho působení a úkoly mu svěřené [3].

„Pověřenec dle Nařízení v rámci správcovy organizace má nezávislé postavení. Musí se vyvarovat střetu zájmů, a ohledně jeho úkolů mu nesmějí být ukládány žádné pokyny. Pověřenec musí fungovat jako samostatný poradní orgán, který se nemusí řídit obchodním či jiným zájmem správce nebo zpracovatele. Naopak pokud pověřenec zjistí, že správce nebo zpracovatel postupuje v rozporu s požadavky nařízení a ochrany osobních údajů obecně, musí se vůči takovému postupu vymezit [4].“

Jmenovat pověřence nemusí každý správce a zpracovatel. Tuto povinnost mají pouze ty organizace, které naplní alespoň jednu z podmínek uvedených v čl. 37 odst. 1 nařízení. Tyto podmínky vymezují situace, které představují vyšší riziko při zpracování. Proto je nutné, aby na takové zpracování dohlížela nezávislá poradní osoba. Pověřence je dle nařízení nutné jmenovat v případě když:

- zpracování provádí orgány veřejné moci nebo jiné subjekty, s výjimkou soudů.

- činnosti správce nebo zpracovatele se uskutečňují v operacích, které vyžadují pravidelné a systematické monitorování subjektů údajů [4].

Správce nebo zpracovatel se může rozhodnout, že pověřence jmenuje dobrovolně. Dobrovolné jmenování pověřence nicméně může být pro správce nebo zpracovatele výhodné. Jmenováním pověřence získají nezávislou osobu, která dohlíží na jejich zpracování a upozorňuje na nesoulad [4].

Na Obr. 2. je graficky znázorněna činnost pověřence.

Obr. 2. Činnosti pověřence [vlastní]

1.4 Porušení zabezpečení

Stručný návod při vzniku incidentu byl vytvořen Úřadem pro oblast ohlášení porušení zabezpečení osobních údajů v souladu s nařízením [7].

Postup ohlašování

Ohlašuje se jakékoliv porušení zabezpečení osobních údajů, které může mít za následek riziko pro práva a svobody fyzických osob [8].

Může jít například o útok proti počítači, ve kterém jsou zpracovávány osobní údaje. Důsledkem je únik osobních údajů, jejich pozměnění nebo jiné zneužití. Dalším nebezpečím může být ztráta dokumentů obsahujících osobní údaje, které byly součástí manuálně vedené evidence fyzických osob nebo byly vytištěny z počítače, v němž je taková evidence vedena. Obsah těchto dokumentů zakládá riziko pro dotčené osoby. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví obecné nařízení. Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů [8].

Ohlašovat není třeba případy, u nichž je nepravděpodobné, že by porušení mělo za následek riziko pro dotčené osoby.

Může jít o momentální nemožnost dohledat listinný dokument, který byl nebo měl být součástí manuálně vedené evidence fyzických osob nebo byl vytištěn z počítače, ve kterém je taková evidence vedena, přičemž je nepravděpodobné, že se dostal do nepovolaných rukou, ale jde spíše o jeho momentální chybné založení [8].

Ohlášení musí obsahovat:

- popis povahy daného případu porušení zabezpečení osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů [8].

Pokud není možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Byl-li správcem nebo zpracovatelem jmenován pověřenec, k jehož úkolům patří spolupráce s dozorovým úřadem, může být vypracování ohlášení úkolem tohoto pověřence [8].

Kontakt pro ohlášení

Správce osobních údajů ohlašuje případ dozorovému úřadu, kterým je Úřad pro ochranu osobních údajů se sídlem Pplk. Sochora 27, Praha 7. Zpracovatel ohlašuje případ příslušnému správci [8].

Termín ohlášení

Správce i zpracovatel ohlašují případ bez zbytečného odkladu. Správce případ ohlásí Úřadu pokud možno **do 72 hodin** od okamžiku, kdy se o něm dověděl. Pokud není ohlášení Úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění [8].

Správce zasílá Úřadu ohlášení na adresu elektronické pošty, e-mail: **posta@uoou.cz** nebo do datové schránky: **qkbaa2n.**

Výjimky z povinnosti oznámit takový případ

Oznámení dotčeným osobám se nevyžaduje jestliže:

- správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování [8],
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví, vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření. Zpracovatel zasílá ohlášení správci na dohodnuté kontaktní údaje správce [8].

2 ŘÍZENÍ PROCESŮ NA OBCI

„Obec je základním územním samosprávným společenstvím občanů, které je vymezeno hranicí území obce [9].“

„Obec je samostatně spravována zastupitelstvem obce dalšími orgány obce jsou starosta, obecní úřad a zvláštní orgány obce [9].“

„Obec spravuje své záležitosti samostatně (dále jen "samostatná působnost"). Státní orgány a orgány krajů mohou do samostatné působnosti zasahovat, jen vyžaduje-li to ochrana zákona, a jen způsobem, který zákon stanoví. Rozsah samostatné působnosti může být omezen jen zákonem. Státní správu, jejíž výkon byl zákonem svěřen orgánu obce, vykonává tento orgán jako svou přenesenou působnost. Pokud zvláštní zákon upravuje působnost obcí a nestanoví, že jde o přenesenou působnost obce, platí, že jde vždy o samostatnou působnost [9].“

2.1 Organizační struktura obce XY

Organizační struktura je hierarchické uspořádání vztahů mezi jednotlivými pracovními místy v rámci organizačních útvarů a vztahů mezi útvary v rámci organizace. Zahrnuje vztahy nadřízenosti a podřízenosti a řeší vzájemné pravomoci (kompetence), vazby a odpovědnost. Je nezbytná pro řízení lidí a proto se bez organizační struktury neobejde žádná organizace, protože nastavuje komunikační pravidla a tím sjednocuje jednotlivé činnosti, procesy a lidi a formalizuje jejich vztahy za účelem dosažen společných cílů organizace [10].

- Zastupitelstvo obce XY
- Starosta obce XY
- Místostarosta obce XY
- Finanční výbor zastupitelstva obce XY

  Předseda
  Členové
- Kontrolní výbor zastupitelstva obce XY

  Předseda
  Členové

Starosta obce

Starosta obce zastupuje obec navenek. Volí jej zastupitelstvo obce, jemuž se zodpovídá za výkon své funkce. Musí být občanem ČR. Úkony, které vyžadují schválení zastupitelstvem nebo radou, splní až po tomto schválení [9].

Místostarosta obce

Místostarosta obce je volen zastupitelstvem obce a zastupuje starostu obce.

Orgány zastupitelstva obce

Zastupitelstvo obce zřizuje jako své iniciativní a kontrolní orgány výbory. Stanoviska a návrhy předkládají zastupitelstvu obce. Předsedou je vždy člen zastupitelstva obce. Zastupitelstvo obce vždy zřizuje finanční a kontrolní výbor. Výbory plní úkoly, kterými je pověřuje zastupitelstvo obce a ze své činnosti se také zastupitelstvu zodpovídají. Počet členů je vždy lichý. Schází se dle potřeby. Usnesení výboru se vyhotovuje písemně a podepisuje ho předseda výboru. Usnesení je platné, jestliže s ním vyslovila souhlas nadpoloviční většina všech členů výboru [9].

Finanční výbor

Finanční výbor provádí kontrolu hospodaření s majetkem a finančními prostředky obce a plní úkoly, jimiž jej pověřilo zastupitelstvo obce. Členy výboru nesmí být starosta, místostarosta nebo účetní. Členům finančního výboru náleží odměna [9].

Kontrolní výbor

Kontrolní výbor kontroluje plnění usnesení zastupitelstva obce a rady obce, kontroluje dodržování právních předpisů ostatními výbory a obecním úřadem na úseku samostatné působnosti a plní úkoly, jimiž jej pověřilo zastupitelstvo obce. Členům kontrolního výboru náleží odměna [9].

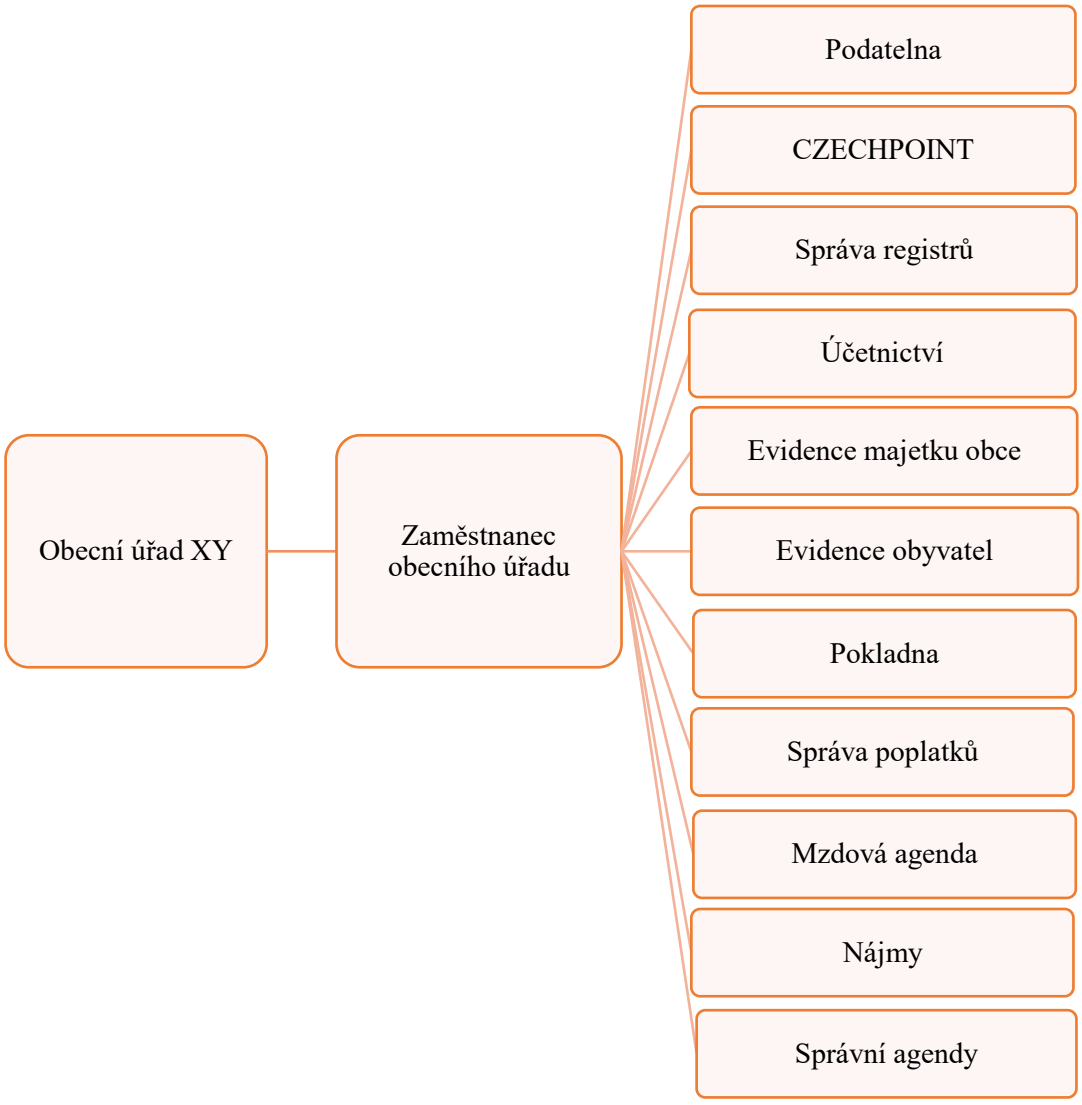
Kulturní komise

Kulturní komise aktivně se podílí na pořádání kulturních akcí Obce, navštěvuje jubilanty, účastní se občanských obřadů. Členům kulturního výboru odměna nenáleží, jejich činnost je dobrovolná [9].

Obecní úřad

Je tvořen starostou, místostarostou a zaměstnanci obce zařazených do obecního úřadu. V jeho čele je starosta. Obecní úřad plní v oblasti samostatné působnosti úkoly, které mu uložilo zastupitelstvo obce nebo rada obce a pomáhá výborům a komisím v jejich činnosti. V oblasti přenesené působnosti obce vykonává státní správu s výjimkou věcí, které patří do působnosti zastupitelstva obce, rady obce a zvláštních orgánů obce, případně i komisí [9].

Struktura úřední agendy obecního úřadu je graficky znázorněna na Obr. 3.



Obr. 3. Struktura úřední agendy [vlastní]

2.2 Správa obce

Obec své záležitosti spravuje samostatně (samostatná působnost). Státní správu, která byla svěřena orgánům obce, vykonává jako přenesenou působnost [9]. Agendy, které obec nevykonává, si musí obyvatelé vyřídit na Městském úřadě XY.

Samostatná působnost

Do samostatné působnosti patří hlavně záležitosti, které jsou v zájmu obce a jejích občanů. Obec v souladu s místními předpoklady a zvyklostmi pečuje o vytváření podmínek pro uspokojování potřeb občanů a rozvoj sociální péče. Jedná se především o potřeby informací, výchovy a vzdělávání, celkového kulturního rozvoje, ochrany a rozvoje zdraví, dopravy, spojů, bydlení a ochrany veřejného pořádku. Obec může zřizovat a zakládat právnické osoby, organizační složky obce a obecní policii. Obec může ukládat povinnosti obecně závaznou vyhláškou. Obce mohou vzájemně spolupracovat i s obcemi jiných států nebo vytvářet a vstupovat do svazku obcí [9].

Přenesená působnost

Obce, které plní úkoly v přenesené působnosti, dostávají příspěvek ze státního rozpočtu. Pokud byla orgánu obce zákonem svěřena státní správa, vykonává ji jako svou přenesenou působnost. Obec v přenesené působnosti může v souladu se zákonem vydávat nařízení obce [9].

Obce lze podle rozsahu výkonu státní správy v přenesené působnosti rozdělit na:

- **obce se základním rozsahem přenesené působnosti,**
- **obce s pověřeným obecním úřadem** - vedle přenesené působnosti vykonává přenesenou působnost určenou zvláštními zákony ve správním obvodu určeném prováděcím právním předpisem,
- **obecní úřady obcí s rozšířenou působností** - vedle přenesené působnosti vykonává přenesenou působnost určenou zvláštními zákony ve správním obvodu určeném prováděcím právním předpisem [9]

2.3 Procesy obecního úřadu

Proces je soubor činností, které přeměňují vstupy na výstupy v řízených podmínkách. Je to řada po sobě jdoucích kroků, které vedou k předem definovanému cíli [16].

Proces legislativní je typ procesu, který funguje na obecních úřadech, a jež jsou součástí jejich procesního řízení. Jedná se o procesy, které ve své každodenní praxi používají obecní úřady, procesy, které přeměňováním vstupů na výstupy generují hodnoty. Proces je chápán jako „*soubor vzájemně souvisejících nebo vzájemně působících činností, který přeměňuje vstupy na výstupy* [16].“

Ochranou osobních údajů v podobných souvislostech, které vyplývají z nového evropského nařízení, se obce stejně jako všichni další správci osobních údajů musí zabývat již téměř dvě desetiletí. Současná situace je ale vhodná k posouzení, zda nastavení systému ochrany osobních údajů v obci je dostatečné ve všech následujících oblastech:

- nastavení kompetencí ,
- zabezpečení osobních údajů,
- evidence dokumentů.

Pokud by obec porovnáním své situace s následujícími seznamy došla k závěru, že některá z oblastí není dostatečně pokryta, doporučuje se přijmout odpovídající opatření (určení odpovědné osoby, přijetí nebo doplnění vnitřního předpisu, úprava zabezpečení-uzamykatelnost prostor, nastavení hesel, úprava a evidence přístupů k dokumentům ve spisové službě atd.). Základní pravidla k ochraně osobních údajů stanovuje vnitřní předpis. Nemusí se jednat o předpis věnovaný výhradně ochraně osobních údajů, ale konkrétní pravidla bude obsahovat typicky:

- organizační řád,
- pracovní řád,
- spisový a skartační řád [13].

2.4 Nastavení kompetencí při zpracování osobních údajů

V obci musí být určena osoba, která se věnuje níže uvedeným otázkám a zodpovídá za jejich řešení. Má tedy odpovídající činnosti v popisu práce, popřípadě jí vyplývají z vnitřního předpisu nebo pokynu.

- stanovení prostředků (manuální/elektronické) zpracování osobních údajů,
- stanovení účelů zpracování (proč se údaje zpracovávají),
- posouzení, které osobní údaje je nutno shromažďovat,
- stanovení opatření, která omezí zpracování na minimální nutný rozsah. (Např. nastavení kamery, základní dobu uložení údajů atd.),

- stanovení opatření, která prakticky chrání soukromí dotčených osob. (Např. úroveň zabezpečení, rozsah sdělování příjemcům atd.).
- řízení přístupu-udělování oprávnění pracovníkům zpracovávat osobní údaje,
- poučení zaměstnanců o ochraně osobních údajů a mlčenlivosti [13].

NOVĚ:

- jmenování pověřence pro ochranu osobních údajů,
- zveřejnění kontaktních údajů pověřence a jejich sdělení Úřadu pro ochranu osobních údajů,
- plnění povinnosti hlásit porušení zabezpečení ochrany osobních údajů ÚOOÚ,
- oznamování porušení zabezpečení ochrany osobních údajů dotčeným osobám,
- projednávání připomínek a námětů pověřence,
- vnitřní kontrola dodržování pravidel ochrany osobních údajů,
- vedení záznamů o činnostech zpracování [11].

Záznamy obsahují:

- název a kontakty obce,
- jméno a kontakty pověřence,
- účel zpracování,
- kategorie dotčených osob a osobních údajů,
- kategorie příjemců,
- případné lhůty pro výmaz,
- popis technických a organizačních opatření.

- vedení evidence souhlasů se zpracováním osobních údajů,
- informační povinnost poskytování informací subjektům údajů o zpracování,

a) pokud jsou údaje získány přímo od subjektu údajů, bude poučen o:

- kontaktech na obec,
- kontaktech na pověřence,
- účelu zpracování,
- případných oprávněných zájmech, pro něž je zpracování nezbytné,
- případných příjemcích údajů mimo orgány obce.

b) pokud jsou údaje z jiných zdrojů, osoba bude zpravidla do 1 měsíce nebo při prvním zamýšleném kontaktu poučena o:

- kontaktech na obec,
- kontaktech na pověřence,
- účelu zpracování,
- typech získaných osobních údajů,
- případných příjemcích mimo orgány obce.

- vyřizování podání subjektů údajů souvisejících s uplatněním jejich práv,

Žádosti o:

- přístup ke svým osobním údajům,
- o opravu nebo doplnění osobních údajů,
- o výmaz osobních údajů,
- o omezení zpracování osobních údajů,
- o přenos osobních údajů.

Námitky dotčených osob proti zpracování.

- likvidace osobních údajů [12].

Zabezpečení osobních údajů

Obec nesmí zklamat důvěru lidí, kteří jí, ať už povinně či dobrovolně, svěřují své osobní údaje. Tyto údaje je potřeba chránit proti zneužití, což jí ukládá i obecné nařízení. Způsob zabezpečení má odpovídat stupni rizika, které by hrozilo subjektům údajů v případě ohrožení bezpečnosti údajů [12].

Fyzické zabezpečení

Je rozhodující u manuálního zpracování, má odpovídat stupni rizika.

Způsob trvalého uchovávání písemnosti a spisů.

- v uzamčené místnosti v uzamčené skříni,
- volně v uzamčené místnosti,
- v uzamčené skříni ve volně přístupné místnosti (předpoklad správy klíčů.),
- jiný způsob.

Řízení přístupu osob k písemnostem.

- jen pověření zaměstnanci,
- všichni zaměstnanci zajištění dohledu nad osobami,
- externí dodavatelé za přítomnosti zaměstnanců,
- externí dodavatelé bez přítomnosti zaměstnanců,
- veřejnost za přítomnosti zaměstnanců,
- veřejnost bez přítomnosti zaměstnanců,

Spis by neměl být ponechán volně v neuzamčené kanceláři. Před odchodem z kanceláře na konci pracovní doby je potřeba uložit spis např. do uzamčené zásuvky [12].

Zabezpečení elektronického zpracování

Elektronické zpracování odpovídá stupni rizika - evidence všech přenosných paměťových médií používaných k práci, opatření k ochraně neautorizovaného použití externích médií, např. pomocí zvláštního software, šifrování paměťových médií používaných ke zpracování osobních údajů, pracovat pouze se zaheslovanými soubory, trvalé uchování paměťových médií [12].

- v uzamčené místnosti v uzamčené skříni,
- volně v uzamčené místnosti,
- v uzamčené skříni ve volně přístupné místnosti (předpoklad správy klíčů),
- jiným způsobem.

Řízení přístupu k médiím a tiskárnám, v jejich paměti mohou být uložena data, popřípadě může být ohroženo zabezpečení údajů u sdílených tiskáren v době mezi tiskem a odebráním výtisku, čemuž lze předejít například přístupem k tiskárně pomocí kódu PIN [12].

Evidence dokumentů

- výhradně v systému spisové služby,
- i v jiných evidencích, potom musí být vyřešeno, jak budou provázány se spisovou službou.

Přiřazování skartačních znaků evidovaným dokumentům také souvisí s otázkou výmazu osobních údajů [12].

Skartační řízení

Skartační řízení Obecní úřad zajišťuje v souladu s platnými předpisy a po ukončení výběru archiválií příslušného archivu je povinna zbylé dokumenty likvidovat [12].

Způsob předávání účetních dokladů z účetní evidence do spisové služby. Doporučuje se, aby si obecní úřad udělal přehled o případných systémech, které ukládají dokumenty mimo organizaci, například v cloudu nebo úložišti na krajském úřadě a podobně [12].

Spisová služba

„Zpracováním osobních údajů je operace nebo soubor, který je prováděn pomocí nebo bez pomoci automatizovaných postupů, za určitým účelem. Zpracováním osobních údajů se považuje shromáždění, zaznamenání nebo uložení osobních údajů [6].“

Vedení spisové služby „*je činnosti obce, kde dochází ke zpracování osobních údajů ve smyslu čl. 4 odst. 2 nařízení. Obec při vedení spisové služby zpracovává osobní údaje za stanoveným účelem a povinna plnit související povinnosti stanovené v nařízení* [6].“

„Pokud obecní úřad vede správní řízení a má vlastní evidenci dokumentace obsahující osobní údaje, a to za účelem řádného uplatňování nebo bránění svých práv v tomto řízení, pak určuje nové účely a prostředky zpracování osobních údajů, osobní údaje subjektů údajů zpracovává jako správce, pak musí plnit povinnosti stanovené v nařízení. Vzniká povinnost tuto dokumentaci evidovat. Vedení spisové služby musí být prováděno v souladu s přijatým spisovým a skartačním řádem [6].“

Informační aktiva jsou celky informací, které mají pro organizaci určitelnou hodnotu. Informační aktiva mohou být uložena na jakémkoliv médiu nebo papíru, záznamovému médiu, počítači, v dokumentu, v aplikaci a podobně. Hodnota je dána využitelností pro organizaci. Jsou to nějaké ucelené kusy informací nebo dat, které mají dohromady hodnotu. Nejde tedy o jednotlivé záznamy, ale například o celou databázi, která je někde uložena a měla by být oceněna a chráněna jako cenné aktivum [6].

Informační aktivum v informační bezpečnosti. Pojem informačního aktiva je o něco širší - za aktivum mohou být považovány také samotné nosiče informací nebo celé počítače a to z toho důvodu, že mohou být předmětem ochrany z hlediska fyzické bezpečnosti [6].

V následující části bude řešena problematika mapování informací, provedení analýz a zavedení těchto nových údajů do praktického procesu řízení malé obce.

II. PRAKTICKÁ ČÁST

3 DOPADY NAŘÍZENÍ NA OBEC XY

Nařízení subjektům údajů dává možnost dotazovat se a také vznášet námitky, klade důraz na transparentnost zpracování osobních údajů a na práva subjektů údajů. Obec musí plnit povinnosti vůči subjektům údajů vyplývající z nařízení. Tato nová povinnost upravuje procesy a přijímá vhodná technická a organizační opatření za účelem uplatňování práv ze strany subjektů údajů [12].

V rámci samostatné i přenesené působnosti byly provedeny analýzy. Těmito podklady byl zjištěn způsob, jak nakládat s osobními údaji, jaké osobní údaje zpracovávat, k jakým účelům zpracování a na základě jakého právního důvodu. Byla provedena analýza činností, při kterých dochází ke zpracování osobních údajů [12].

Obec vyhodnotila rizika spojená se zpracováním osobních údajů a podle tohoto vyhodnocení přijala vhodná technická a organizační opatření. Účelem zajištění byl výstup, který zaručil, že zpracování bude prováděno v souladu s nařízením, a tuto skutečnost bude muset obec doložit [12].

3.1 Mapování agend obce XY

První etapa byla zaměřena na zmapování všech agend a informačních systémů obce na základě předpřipraveného formuláře. Tato zpracovaná tabulka je uvedena v Příloze P V: Záznamy o činnostech zpracování všech agend.

3.2 Metoda analýzy dostupné dokumentace obce XY

Cílem analýzy obce bylo identifikovat úroveň naplnění nařízení. Projektový tým si v rámci realizace místních šetření vyžádal veškerou dokumentaci, která se dotýkala problematiky nařízení. Mezi tuto dokumentaci patřily tyto dokumenty:

- Organizační řád,
- Pracovní řád,
- Směrnice pro nakládání s osobními údaji,
- Směrnice pro uživatele výpočetní techniky,
- Směrnice personální,
- Spisový a skartační řád + spisový plán.

Analýza dokumentace hodnotila problematiku ochrany osobních údajů, vazby zjišťovaných informací, účelnost a aktuálnost dokumentů. Dokumenty mapovaly aktuální situaci v

obci a pomáhaly v oblasti zajištění bezpečnosti informací. Řešily se základní zásady nařízení:

Zákonnost: pro každé zpracování doložit zákonný důvod zpracování plnění právní povinnosti, splnění úkolu ve veřejném zájmu, splnění smlouvy, jejíž stranou je subjekt údajů, souhlas.

Účelové omezení: údaje zpracovávány pro jasně stanovený účel.

Minimalizace: zpracovávány jen ty údaje, kterých je pro daný účel opravdu potřeba.

Přesnost: zpracovávány pouze údaje přesné a aktualizované.

Omezení uložení: údaje zpracovávány po nezbytně nutnou dobu, dále pak uložení podle zákonných lhůt, skartace.

Integrita a důvěrnost: důsledná ochrana osobních údajů před neoprávněným nebo protiprávním zpracováním nebo před náhodnou ztrátou, zničením, poškozením a nutnost zachování mlčenlivosti.

Zvláštní kategorie osobních údajů: vypovídající o rasovém nebo etnickém původu, politických názorech, náboženství, filozofii a podobně jsou zpracovávány v těchto případech:

- je udělen výslovný souhlas subjektem údajů,
- zpracování je nezbytné pro plnění povinností vyplývajících z pracovního práva,
- je to nutné pro ochranu životních zájmů subjektu údajů,
- zpracování se týká osobních údajů subjektem zjevně zveřejněných,
- zpracování je nezbytné pro určení, výkon, obhajobu právních nároků,
- zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo státu,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, vědecký nebo historický výzkum nebo statistické účely [10].

Informování subjektů údajů o zpracování osobních údajů, tato informace o zpravování osobních údajů musí být vyvěšena na internetových stránkách, informačních tabulích.

Byly vedeny záznamy o činnostech zpracování, které popisovaly:

- účely zpracování,
- kategorie subjektů, o nichž se osobní údaje zpracovávají a kategorie osobních

údajů, které se o těchto subjektech zpracovávají,

- příjemce, kteří s údaji pracují nebo jim byly zpřístupněny,
- zda jsou údaje předávány do třetí země, mimo EU,
- plánované lhůty uložení a následného výmazu,
- popis technických a organizačních opatření [10].

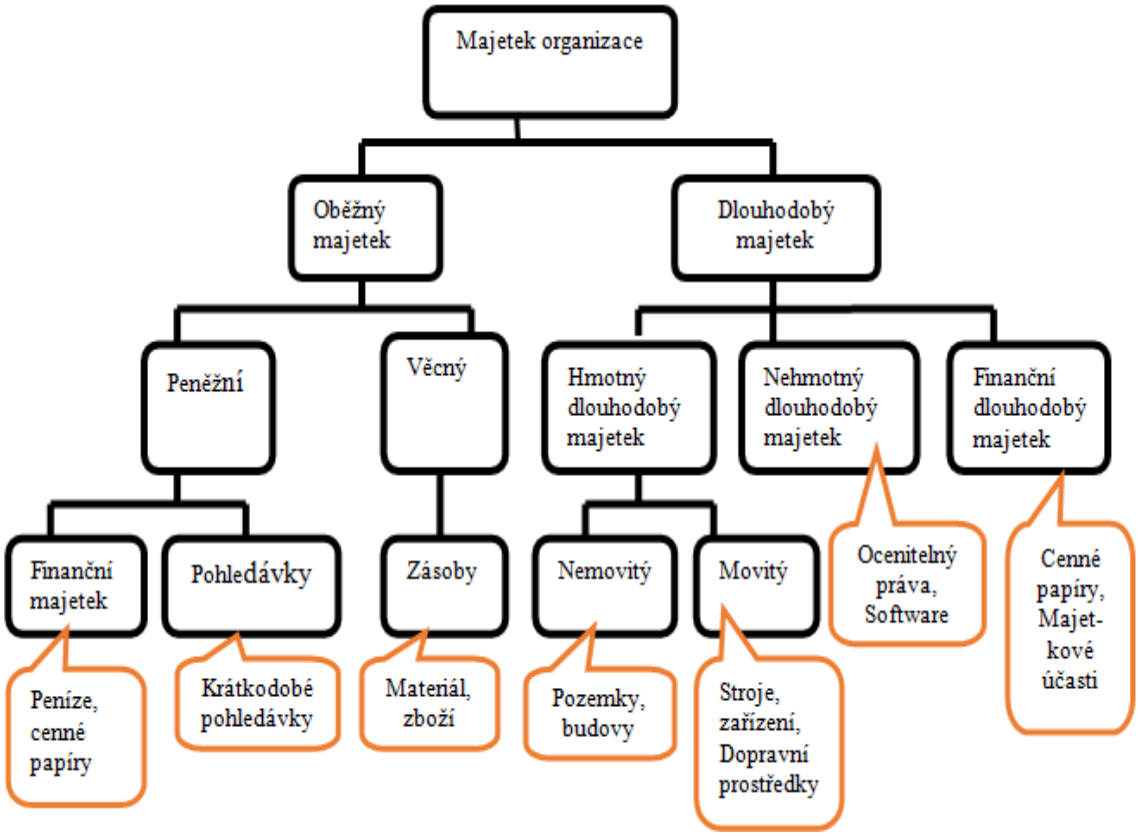
Pomoc subjektům při uplatňování jejich práv:

- právo na přístup k osobním údajům,
- právo na opravu,
- právo na výmaz (právo být zapomenut),
- právo na omezení zpracování,
- právo na přenositelnost údajů,
- právo vznést námitku a automatizované individuální rozhodování.

Právo podat stížnost u dozorového úřadu a právo na účinnou soudní ochranu, s tím související právo na náhradu újmy a odpovědnost, ale tak aby byl zajištěn soulad mezi přístupem veřejnosti k úředním dokumentům a právem na ochranu osobních údajů podle tohoto nařízení [10].

4 METODA ANALÝZY RIZIK V RÁMCI ORGANIZACE OBCE

Cílem analýzy bylo určit vhodná technická a organizační opatření, která byla nutná pro zajištění bezpečnosti osobních údajů při jejich zpracování a pro minimalizaci rizik vztahujících se ke zpracování [12]. Na Obr. 4. je znázorněná Majetková struktura vybrané organizace.



Obr. 4. Majetková struktura organizace [vlastní]

Projektovým týmem byla zvolena metoda analýzy rizik, která ze zákona o kybernetické bezpečnosti vychází. Byla doplněna o části posuzující a vyhodnocující problematiku z pohledu subjektu údajů a jeho práv [12].

Zákon o kybernetické bezpečnosti a **jeho prováděcí vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech**, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti [19].

Projektovým týmem bylo provedeno ohodnocení primárních aktiv dle jejich kritičnosti. Nařízení nepředepisuje povinný formát analýzy rizik a také neuvažuje hodnotu aktiva. Hodnota aktiv je z pohledu nařízení stejná, a předepisuje chránit osobní údaje jako celek. V **rámci normy ISO 27001: 2013 Certifikace systémů managementu bezpečnosti informací** se tím způsobem řeší, zda aktivum bude zahrnuto do analýzy rizik nebo nikoliv [20]. Projektovým týmem byla stanovena na základě dotazníkového šetření a sběru interních aktů řízení identifikovaná aktiva:

- **Listinné úložiště v rámci výkonu agend úřadu:**
  listiny související s výkonem agend úřadu,
- **Listinné úložiště v rámci vnitřního chodu úřadu**:
  listiny souvisejí s vnitřním chodem úřadu (příjem a propuštění zaměstnanců, účetnictví atd.),
- **Informační systém spisové služby,**
- **Agendové informační systémy – samostatná působnost**,
- **Agendové informační systémy – přenesená působnost,**
- **Ekonomický informační systém,**
- **Portály:** veřejné i neveřejné webové portály,
- **Ostatní elektronická úložiště**: e-mail, sdílené disky, lokální disky.

Identifikovaným aktivům jsou na Obr. 5. přiřazeny role subjektů údajů.

Hodnota aktiv:

- **běžná hodnota aktiva** – jedná se o osobní údaje zaměstnanců – bodová hodnota 1,
- **střední hodnota aktiva** – obsahuje osobní údaje občanů – bodová hodnota 3,
- **vysoká hodnota aktiva** – obsahuje citlivé osobní údaje 5 [12].

4.1 Metoda určení a ohodnocení aktiv

Aktiva byla projektovým týmem určena na základě sběru informací a jejich vyhodnocení. Aktivum jsou chápána jako objekt, který obsahuje osobní údaje.

Posouzení rizik, která primárním aktivům hrozí, je ohodnocení samotných primárních aktiv. Projektovým týmem bylo provedeno posouzení požadavků na důvěrnost, integritu a dostupnost aktiv, případně dat v aktivech obsažených a služeb aktivy poskytovaných.

Obec neměla zaveden registr aktiv, který by obsahoval skutečné hodnoty těchto aktiv. Projektovým týmem byla vytvořena následující stupnice hodnoty primárních aktiv [12].

Stupnice hodnoty primárních aktiv jsou uvedeny v Tab. 1.

Tab. 1. Stupnice hodnocení aktiv pro účely analýzy rizik [12]

STUPEŇ	HODNOTA	KRITERIUM
1	VELMI NÍZKÁ	Ztráta, poškození, narušení bezpečnosti primárního aktiva má jen nepatrný nebo žádný vliv na ochranu osobních údajů v rámci organizace. Obsahuje aktivum osobní údaje zaměstnanců obce či úřadu.
2	NÍZKÁ	Ztráta, poškození, narušení bezpečnosti primárního aktiva má nízký dopad na zákonné povinnosti v rámci ochrany osobních údajů. Nedojde k uplatnění sankcí.
3	STŘEDNÍ	Ztráta, poškození, narušení bezpečnosti primárního aktiva má střední dopad na zákonné povinnosti v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí. Porušení zákonných povinností nebude mít zásadní vliv na fungování organizace. Obsahuje aktivum osobní údaje občanů.
4	VYSOKÁ	Ztráta, poškození, narušení bezpečnosti primárního aktiva je velmi významná, může vést k neakceptovatelnému porušení zákonných požadavků v rámci ochrany osobních údajů. Narušením primárního aktiva pravděpodobně dojde k uplatnění sankcí. Porušení zákonných povinností bude mít vliv na fungování organizace.
5	VELMI VYSOKÁ	Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů. Narušením primárního aktiva dojde k uplatnění sankcí. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace. Aktivum obsahuje citlivé osobní údaje

Unikátní aktivum s dlouhodobou tradicí, které nelze jinak nahradit a na kterém se podílely předchozí generace, bude mít hodnotu větší, než aktivum, které je v elektronické nebo listinné formě a které vzniklo strojovým zpracováním dat. Jedná se např. o obecní kroniky či jiné materiály, sloužící k dokumentování kulturního či folklorního dědictví. Tyto informace je nezbytné uvést do vlastního hodnocení aktiva [12].

4.2 Hrozby a identifikace pravděpodobnosti hrozeb

Hodnocení rizik je identifikací hrozeb a zranitelností, je zpracován seznam hrozeb dle standardů a hrozeb týkajících se ochrany osobních údajů vycházejících z nařízení. Hrozba představuje aktivitu, jejímž následkem je poškození analyzovaného systému IT a jeho aktiv. Cílem je identifikace hrozeb, kterým mohly být vystaveny primární aktiva obce v její správě [12].

„Osobnostní práva subjektu údajů Dle čl. 10 Listiny základních práv a svobod má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě [15].“

Hrozby budou popsány v následující Tab. 2. kde je uvedena kategorie hrozeb a její vysvětlení.

Tab. 2. Popis hrozeb [12]

HROZBY – KATEGORIE	POPIS
Vnější útoky	Zneužití přístupuk PC nebo diskreditace OÚ
	Zneužití přístupuk poč. síti nebo diskreditace OÚ
	Krádež nebo prolomení hesla do IS nebo diskreditace OÚ
	Útok na IS s cílem diskreditace či zcizení OÚ nebo omezení funkčnosti
	Útok na web s možností zcizení nebo modifikace OU
	Cílený útok na OU s motivem jejich odcizení a cílené diskreditace organizace
	Narušení referenčních OÚ v aplikacích nebo IS
	Fyzické zcizení primámího aktiva včetně listinných evidencí s os. daty
	Průnik z vnější sítě do vnitřní sítě s cílem zcizení nebo kompromitace OÚ uložených v IS nebo aplikacích
	Kompromitace dohledových prostředků nebo prostředků ke sledování a monitorování přístupuk OÚ
	Kompromitace identity oprávněného uživatele Správce nebo Zpracovatele.
Technické chyby	Chyby zálohování
	Výpadek elektřiny
	Výpadek hardwaru koncové stanice
	Výpadek softwaru koncové stanice
	Poškození nebo ztráta dat
	Mechanické poškození listinné evidence osobních údajů
	Narušení řádné čitelnosti listinné evidence osobních údajů
	Poškození/selhání programového vybavení
	Nedostatečná ochrana vnějšího perimetru
	Nedostatečná údržba informačního systému nebo aplikace, kde jsou evidovány OÚ
	Nedostatečné postupy při identifikaci a odhalení incidentů
	Dlouhodobé přerušení podpory dodavatele SW
	Nedostatečná ochrana prostředků IS
	Technické chyby ochrany úložišť listin obsahující OÚ
Lidský	Obecná chyba uživatele

HROZBY – KATEGORIE	POPIS
faktor	Opomenutí uživatele
	Nedostatečné školení nebo povědomí o nakládání s OÚ nebo jejich ochraně OÚ
	Zkoušení prolomení zabezpečení uživatelem
	Poškození fyzické vrstvy sítě
	Zavlečení škodlivého SW
	Porušení bezpečnostní politiky uživatelem
	Zneužití oprávnění ze strany uživatelů
	Zneužití oprávnění ze strany administrátorů
	Narušení fyzické bezpečnosti – kancelář, serverovna
	Nepřítomnost/zranění/smrt administrátora informačního systému
	Nedostatečné vymezení bezpečnostních pravidel
	Nedostatečná míra nezávislé kontroly
	Nedostatečná ochrana úložišť listin obsahující OÚ
Narušení integrity oú	Neoprávněné manipulování evidencemi OÚ na úrovni IS nebo aplikací
	Neoprávněné manipulování s listinnými evidencemi obsahující OÚ
	Provedení neoprávněných činností
	Zneužití vedených osobních údaj
	Nevhodné či nesprávné nastavení přístupových oprávnění
	Fyzické narušení listiny obsahující OÚ
Neoprávněný přístup	K OÚ má přístup osoba, která k danému úkonu nemá oprávnění
	Modifikace vedených OÚ
	Nedostatečné monitorování činnosti uživatelů
	Nedostatečné monitorování činnosti administrátorů
Narušení dostupnosti	Nedostupnost osobních údajů z důvodu pochybení organizačního charakteru
	Nedostupnost osobních údajů z důvodu technického pochybení
Ztráta osobních údajů	Nevhodná manipulace s listinnou evidencí obsahující OÚ
	Technické chyby v IS uchovávající osobní údaje
	Umyslné zcizení OÚ v listinné podobě z listinné evidence
	Úmyslný export OÚ z IS nebo aplikací
	Výmaz OÚ z IS nebo aplikací
	Předání listinné evidence OÚ neautorizované osobě bez udání důvodu a bez dostatečné evidence a povinnosti navrátit předané OÚ
Narušení práv a svobod subjektu údajů	Narušení práva na soukromí
	Narušení práva na ochranu cti a důstojnosti
	Narušení práva na informační sebeurčení
	Narušení práva na život
	Narušení práva na duševní a tělesnou integritu
	Narušení práva subjektu údajů na informace a přístup k osobním údajům
	Narušení práva subjektu údajů na výmaz (právo být zapomenut)
	Narušení práva subjektu údajů na přenositelnost OÚ
	Narušení práva na ochranu osobních údajů
	Umyslná kompromitace osobních údajů třetím subjektem
	Narušení zákazu diskriminace
	Narušení ochrany identity
	Hmotné ztráty subjektu údajů
	Neoprávněné zrušení pseudonymizace

Pro každé aktivum byla posouzena pravděpodobnost výskytu hrozby. Pro analýzu budou použity kritéria pro hodnocení pravděpodobnosti hrozby v Tab. 3.

Tab. 3. Stupnice hodnocení pravděpodobnosti hrozby [12]

STUPEŇ	ČETNOST VÝSKYTU	KRITERIUM
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo žádné.
2	Nízká	Hrozba se může uplatnit méně než 1 x za rok
3	Střední	Hrozba se může uplatnit zhruba 1x za rok nebo se hrozba jednou uplatnila v průběhu kritického období.
4	Vysoká	Hrozba se může uplatnit zhruba 1x za měsíc nebo se hrozba uplatnila jednou v průběhu více než 1x v kritickém období.
5	Velmi vysoká	Hrozba se může uplatnit zhruba 1x týdně nebo se hrozba uplatnila denně v kritickém období

4.3 Identifikace zranitelnosti

Projektovým týmem byl zpracován odhad zranitelnosti aktiv, kde jsou uvedena slabá místa posuzovaných aktiv. Pro analýzu budou použita kritéria pro hodnocení zranitelnosti, které jsou uvedeny v Tab. 4.

Tab. 4. Stupnice hodnocení zranitelnosti aktiv [12]

STUPEŇ	ZRANITELNOST AKTIVA	KRITERIUM
1	Velmi nízká	Hrozba se nemůže vůči aktivu uplatnit.
2	Nízká	Aktivum je chráněno, je odolné velmi dobře proti hrozbě.
3	Střední	Aktivum je chráněno částečně, je mírně odolné proti uplatnění hrozby.
4	Vysoká	Aktivum je chráněno nedostatečně, je málo odolné proti uplatnění hrozby.
5	Velmi vysoká	Aktivum není chráněno vůbec.

4.4 Celková míra rizika

Cílem identifikace míry rizika bylo zajištění optimálního výběru opatření působících proti těmto rizikům.

Hodnota míry rizika se provádí jako kombinace (součin) tří hodnot:

- **Hodnota aktiva** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.

- **Pravděpodobnost hrozby** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.
- **Zranitelnost** na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.

Hodnota míry rizika je tak určena jako bezrozměrné číslo – rizikovým score. Bezrozměrné číslo je zvoleno, protože hodnocení je kalkulováno z hodnot, které nelze převést na stejnorodé jednotky.

Rizikové skóre se vypočítává podle níže uvedené rovnice:

Rizikové skóre = hodnota aktiva x pravděpodobnost x zranitelnost

Hranice akceptovatelného rizika

Hranice akceptovatelného rizika je manažerské rozhodnutí na straně subjektu, u kterého je analýza rizik prováděna.

Celková míra expozice je doporučena jako pořadí priorit při řešení a implementaci organizačních a technických opatření [12].

4.5 Vyhodnocení systémové analýzy

Projektovým týmem byla provedena identifikaci problému, popis a navržení opatření.

Dalším krokem byla příprava plánu implementace. Plán obsahoval postup obce pro implementaci opatření v technické, organizační a právní oblasti.

Projektovým týmem byla sloučena rizika při hodnocení do tří kategorií, a to nízká rizika, běžná a vysoká.

5 PROCES ANALÝZY RIZIK

Prvním krokem bylo zpracování analýzy pomocí kontrolního seznamu (CLA, Check List Analysis). Je to jednoduchá technika, ve které byl využit seznam položek, kroků či úkolů podle kterých byl ověřen správný postup dalších činností. Kontrolní seznam je uveden v Příloze P III. Podklady pro sestavení kontrolního seznamu byly čerpány z Přílohy P V.

Základní pojmy procesu analýzy rizik:

Hrozba – cokoliv, co může narušit důvěrnost, integritu a dostupnost aktiva,

Zranitelnost – vlastnost aktiva, logické, fyzické nebo administrativní bezpečnosti, která může být zneužita hrozbou,

Celková míra rizika – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti,

Opatření – technické nebo organizační opatření, snižující zranitelnost a ochrana aktiva před jakoukoli hrozbou.

Byla zavedena vhodná technická a organizační opatření, která byla podle potřeby

revidována, aktualizována a doložitelná:

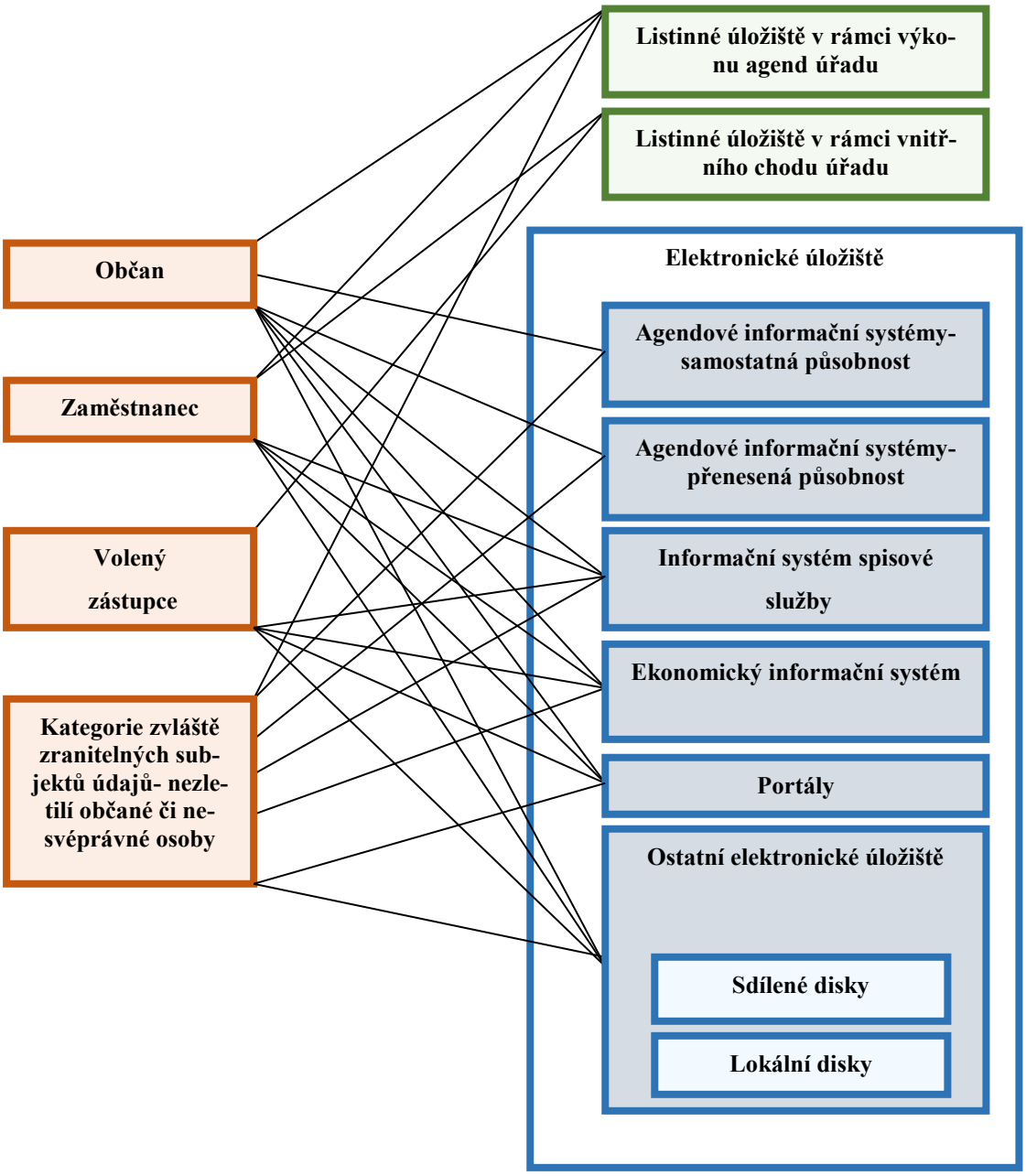
- byla provedená faktická analýza údajů:
  zda jsou data důsledně chráněna, jaké údaje, pro jaký účel, na základě jakého právního důvodu jsou zpracovávány a ukládány, zda máme jen potřebné a aktuální údaje, je dodržována doba uložení, víme, kdo s údaji pracuje a komu jsou předávány
- personální zabezpečení – s osobními údaji pracují osoby oprávněné podle vnitřních směrnic, zachovávají mlčenlivost
- postup podle vnitřních směrnic, které jsou v souladu s nařízením: ochranu osobních údajů byla ošetřena v organizačním řádu obce, byl aktualizován skartační řád, byl přijat Provozní řád informačního systému, podle kterého pracujeme s osobními údaji v automatizovaných systémech [10].
- **listinné dokumenty s osobními údaji byly uloženy do uzamykatelných skříní,** místnosti, s uloženými osobními daty, jsou v nepřítomnosti zodpovědných osob uzamčeny, byla nastavena evidenci klíčů
- osobní data v elektronických systémech:

- chráněna přístupovými hesly do počítačů, pro práci více osob na jednom počítači, každá tato osoba má nastaveno své přístupové heslo do svého profilu, ve kterém pracuje
- chráněna přístupovými hesly do programů, modulů, přístupy do centrálních informačních systémů jsou chráněny zdvojenou ochranou heslem a certifikátem
- pracujeme pouze s legálním a aktualizovaným softwarem, antivirovým programem a firewallem
- pravidelně zálohujeme informace a máme nastaven systém pro jejich obnovu
- zodpovědně pracujeme s informacemi umisťovanými na internetové stránky, zejména při umisťování fotografií a osobních dat
- nastavujeme ochranu osobních údajů do smluv se zpracovateli a poskytovateli softwaru a internetových stránek
- pro zpracování osobních údajů, na které potřebujeme souhlasy, revidujeme a nastavujeme informované souhlasy se zpracováním osobních údajů, v souladu s nařízením

Z výše uvedeného vyplývá, že byl nastaven funkční systém ochrany osobních údajů [10].

5.1 Role subjektů osobních údajů

Na základě šetření byla provedena identifikace rolí subjektů údajů a poté k nim byla přiřazena odpovídající aktiva. Tyto vazby jsou znázorněny na Obr. 5.



Obr. 5: Role subjektu osobních údajů a přiřazení aktiv [vlastní]

5.2 Rizika zpracování osobních údajů

Dle definovaných aktiv projektový tým provedl jejich ohodnocení, a to dle stupnice, která je uvedena v Tab. 5. Stupnice hodnocení aktiv pro účely analýzy rizik.

Analýza rizik byla projektovým týmem provedena z pohledu subjektu údajů dle nařízení. Hodnota aktiv a stanovení parametrů analýzy rizik byly určeny z pohledu dopadu na subjekt údajů. Toto ohodnocení aktiv je uvedeno v Tab. 5.

Tab. 5. Hodnocení aktiv pro účely analýzy rizik [12]

NÁZEV AKTIVA	STUPEŇ HODNOCENÍ	POPIS HODNOCENÍ
Listinné úložiště v rámci výkonu agend úřadu	5	Projektový tým ohodnotil aktivum na nejvyšší stupeň. Aktivum má vysokou koncentraci osobních údajů citlivých údajů včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Subjekty osobních údajů mají vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení ke vztahu subjektům osobních údajů. Vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z nařízení. Narušením primárního aktiva dojde k uplatnění sankcí v rámci nařízení. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů
Listinné úložiště v rámci vnitřního chodu úřadu	3	Projektový tým ohodnotil aktivum na střední stupeň. Aktiva, a všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nemá tolik osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. Nepředpokládá se, že v rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva by došlo k uplatnění sankcí vyplývající z nařízení. Narušení aktiva nebude mít zásadní vliv na fungování obce či úřadů.

NÁZEV AKTIVA	STUPEŇ HODNOCENÍ	POPIS HODNOCENÍ
Informační systém spisové služby	5	Projektový tým ohodnotil aktivum na nejvyšší stupeň. Aktivum má vysokou koncentraci osobních údajů citlivých údajů včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Subjekty osobních údajů mají vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení ke vztahu subjektům osobních údajů. Vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z nařízení. Narušením primárního aktiva dojde k uplatnění sankcí v rámci nařízení. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů
Agendové informační systémy – samostatná působnost	5	Projektový tým ohodnotil aktivum na nejvyšší stupeň. Aktivum má vysokou koncentraci osobních údajů citlivých údajů včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Subjekty osobních údajů mají vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení ke vztahu subjektům osobních údajů. Vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z nařízení. Narušením primárního aktiva dojde k uplatnění sankcí v rámci nařízení. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů
Agendové informační systémy – přenesená působnost	5	Projektový tým ohodnotil aktivum na nejvyšší stupeň. Aktivum má vysokou koncentraci osobních údajů citlivých údajů včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Subjekty osobních údajů mají vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení ke vztahu subjektům osobních údajů. Vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z nařízení. Narušením primárního aktiva dojde k uplatnění sankcí v rámci nařízení. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů

NÁZEV AKTIVA	STUPEŇ HODNOCENÍ	POPIS HODNOCENÍ
Ekonomický informační systém	5	Projektový tým ohodnotil aktivum na nejvyšší stupeň. Aktivum má vysokou koncentraci osobních údajů citlivých údajů včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Subjekty osobních údajů mají vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení ke vztahu subjektům osobních údajů. Vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z nařízení. Narušením primárního aktiva dojde k uplatnění sankcí v rámci nařízení. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a bude mít zásadní dopad na subjekt údajů a realizaci práv subjektu údajů
Portály	3	Projektový tým ohodnotil aktivum na střední stupeň. Aktiva, a všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. Aktivum nemá tolik osobních údajů jako v případě úložiště spojené s výkonem agend obce vůči občanům. Nepředpokládá se, že v rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva by došlo k uplatnění sankcí vyplývající z nařízení. Narušení aktiva nebude mít zásadní vliv na fungování obce či úřadů.
Ostatní elektronické úložiště	1	Projektový tým ohodnotil aktivum na nízký stupeň. Aktiva a všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí obce či úřadu. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z nařízení. Narušení aktiva nebude mít vliv na fungování obcí či úřadů

Projektovým týmem byl sestaven v Tab. 2. seznam hrozeb dle standardů, které se týkaly ochrany osobních údajů vycházející z nařízení. Projektovým týmem byly k hrozbám přiřazeny pravděpodobnosti uplatnění hrozeb. Tyto hrozby se vázaly na identifikovaná aktiva. Hodnocení aktiv je uvedeno v Tab. 4. Hrozby a identifikace pravděpodobnosti hrozeb. Projektovým týmem byla zařazena do hodnocení výše stupně pravděpodobnosti uplatnění hrozby včetně popisu zvolení dané výše pravděpodobnosti. Hodnocení pravděpodobnosti těchto hrozeb na jednotlivá aktiva uvedena v Příloze P I. Dále byla projektovým týmem na základě zjištěných informací z mapování obce určena hrozba zranitelnosti jednotlivých hrozeb, a to ke každému aktivu.

Projektovým týmem byla zařazena do hodnocení výše stupně zranitelnosti aktiv vůči hrozbám s popisem stupně zranitelnosti. Hodnocení zranitelnosti aktiv vůči hrozbám je v Příloze P II.

V Tab. 6 jsou uvedeny pravděpodobnosti uplatnění hrozeb k aktivům.

Tab. 6. Pravděpodobnost jednotlivých aktiv vůči hrozbám [12]

PRAVDĚPODOBNOST									
Aktivum	Hodnota aktiv	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod sub. údajů
Listinné úložiště v rámci výkonu agend úřadu	5	2	1	3	3	2	3	3	3
Listinné úložiště v rámci vnitřního chodu úřadu	3	2	1	3	3	2	3	3	3
Informační systém spisové služby	5	2	5	3	4	2	3	4	3
Agendové info. systémy – samostatná působnost	5	2	4	4	3	3	2	3	3
Agendové info. systémy – přenesená působnost	5	3	2	2	4	2	2	2	3
Ekonomický informační systém	5	3	2	3	1	2	4	2	3
Portály	3	3	2	2	1	4	4	2	3
Ostatní elektronické úložiště	1	3	5	4	4	4	2	3	3

Projektový tým dále určil úroveň zranitelnosti jednotlivých aktiv vůči stanoveným hrozbám, které jsou uvedeny v Tab. 7.

Tab. 7. Zranitelnost jednotlivých aktiv vůči hrozbám [12]

ZRANITELNOST									
Aktivum	Hodnota aktiv	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Zráta osobních údajů	Narušení práv a svobod subj. údajů
Listinné úložiště v rámci výkonu agend úřadu	5	3	3	4	3	3	2	4	4
Listinné úložiště v rámci vnitřního chodu úřadu	3	3	3	4	3	3	2	4	4
Informační systém spisové služby	5	2	2	2	2	2	2	3	3
Agendové info. systémy – samostatná působnost	5	2	2	2	2	3	3	3	3
Agendové info. systémy – přenesená působnost	5	2	2	2	2	3	2	3	3
Ekonomický informační systém	5	2	3	3	3	2	3	3	3
Portály	3	3	2	3	3	2	3	3	3
Ostatní elektronické úložiště	1	2	2	3	3	3	2	4	4

V Tab. 8 je uvedeno závěrečné rizikové skóre k jednotlivým aktivům.

Celková míra rizika hrozby:

Indikátor ukazuje celkové míry rizika hrozeb dle jejich výše. Je tedy patrné, které hrozby jsou pro obec nejzávažnější a mohou zde směřovat technická a organizační opatření.

Celkové míra rizika aktiva:

Indikátor ukazuje celkové míry rizika aktiv dle jejich výše. Je tedy patrné, která aktiva jsou nejnáchylnější a potřebují zvýšenou pozornost či ochranu ze strany obce.

Rizikové skóre = (Tab. 6) hodnota **aktiva x** (Tab. 6) **pravděpodobnost x** (Tab. 7) **zranitelnost**

Příklad: (5x2x3) = 30

Tab. 8. Rizikové skóre [12]

RIZIKOVÉ SKÓRE										
Rizikové skóre	Hodnota aktiv	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta osobních údajů	Narušení práv a svobod subjektu údajů	Indikátor celkové míry rizika aktiva
Listinné úložiště v rámci výkonu agend úřadu	5	30	15	60	45	30	30	60	60	330
Listinné úložiště v rámci vnitřního chodu úřadu	3	18	9	36	27	18	18	36	36	198
Informační systém spisové služby	5	20	50	30	40	20	30	60	45	295
Agendové info. systémy – samo-statná působnost	5	20	40	40	30	45	30	45	45	295
Agendové info.systémy – přene-sená působnost	5	30	20	20	40	45	20	30	45	250
Ekonomický informační systém	5	30	30	45	15	20	60	30	45	275
Portály	3	27	12	18	9	12	36	18	27	159
Ostatní elektronické úložiště	1	6	10	12	12	12	4	12	12	80
Indikátor celkové míry rizika hrozby		181	186	261	218	202	228	291	315	

Příklad:

Indikátor celkové míry rizika aktiva = ∑ všech vodorovných řádků

30+15+60+45+30+30+60+60=330

Indikátor celkové míry rizika hrozby = ∑ všech svislých řádků

30+18+20+20+30+30+27+6=181

6 ROZHODOVACÍ ANALÝZA VE VEŘEJNÉM SEKTORU

Posláním veřejného sektoru je zajišťovat produkci veřejných statků a veřejných služeb, tzn. takových společensky žádoucích produktů, jejichž poskytování je z pohledu soukromého sektoru ekonomicky neefektivní. Z toho vyplývá, že posláním veřejného sektoru není co největší ekonomický efekt, ale maximální efekt společenský. Tato pozice sebou nese následující problémy:

- velké množství různorodých potřeb a očekávání,
- charakter rozvojových aktivit (veřejné statky a služby),
- omezené zdroje (finanční, technické, personální).

Rozhodovací analýza je jedna z nejdůležitějších metod rozhodování. Zaměřuje se na formální, procedurální stránku rozhodovacího procesu, doporučuje konkrétní kroky. Cílem je najít optimální variantu použitím objektivních metod [16].

Nejdůležitějším krokem rozhodovací analýzy je identifikace problému, neboť chybně definovaný problém znamená, že bude chybné rozhodnutí. Identifikace problému by se měla zaměřit na vymezení problému, zjištění příčin problému a na zjištění dalších možných souvislostí [16].

Kromě vyjasnění příčin problému je třeba v rámci analýzy:

- specifikovat podstatné stránky a faktory problému a jejich vzájemné vazby,
- posoudit vývojové tendence problému a jeho organizačního kontextu,
- vymezit okruh zainteresovaných stran (osob, útvarů či organizací, které by mohly být určitým řešením problému dotčeny),
- stanovit cíle řešení problému.

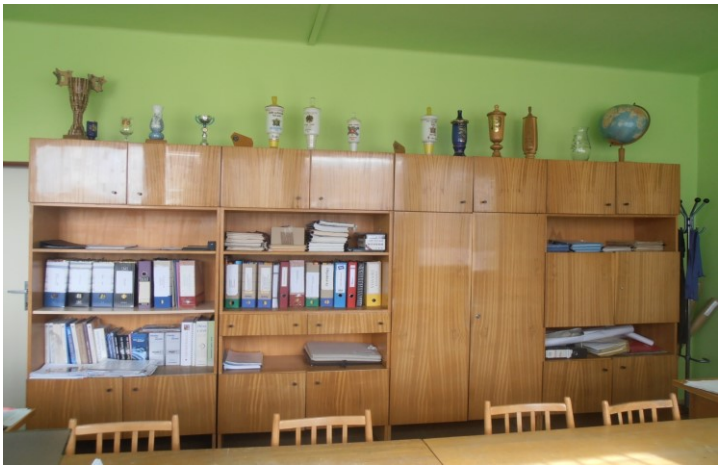
Výsledkem této fáze je vlastní formulace problému, která má pro kvalitu řešení zásadní význam:

- bližší poznání problémové situace,
- identifikace příčin,
- specifikace podstaty problému,
- posouzení vývojových tendencí problému a jeho organizačního kontextu,
- vymezení okruhu zainteresovaných stran,
- stanovení cílů problémů,

- formulace problému.

Formulace kritérií hodnocení je předpokladem správného vyhodnocení variant rozhodování a výběru varianty určené k realizaci. Kritéria hodnocení mohou být buď kvalitativní nebo kvantitativní [15].

Obr. 6 je zachycena kancelář starosty před rekonstrukcí. Obr. 7 zachycuje kanceláře starosty a účetní po rekonstrukci.



Obr. 6. Kancelář před rekonstrukcí [vlastní]

Obr. 7. Kanceláře starosty a účetní po rekonstrukci [vlastní]

7 OPATŘENÍ K ZAJIŠTĚNÍ SOULADU POSUZOVANÝCH PROCESŮ S NAŘÍZENÍM

V této kapitole je řešeno rozfázování jednotlivých činností projektového týmu. Cílem bylo všechny procesy uvést do souladu s nařízením.

1) **Sestavení projektového týmu.** Projektový tým zahrnoval starostku a účetní.
2) **Zpracování analýzy** včetně mapování aktuálního zpracování osobních údajů, tento dokument je uveden v Příloze P V Záznam o činnostech zpracování všech agend. Zajištěno zpracování mapování osobních údajů v rozsahu definovaném touto systémovou analýzou.
3) **Zpracování záznamů o činnostech zpracování.** Výstupem byly záznamy o činnostech zpracování.
4) **Nastavení interních procesů řízení rizik.** Projektovým týmem byl ustanoven interní proces řízení rizik.
5) **Vymezení aktiv**. Byla vymezena listinná úložiště v návaznosti na záznamy o činnostech zpracování. Revize práv přístupů k těmto úložištím a zhodnocení jejich stavu z pohledu fyzické a objektové bezpečnosti. Výstupem byl seznam listinných úložišt a zhodnocení jejich stavu.
6) **Vymezení listinných úložišť.** Byla vymezena listinná úložiště v návaznosti na záznamy o činnostech zpracování. Součástí byla revize práv přístupů k těmto úložištím a zhodnocení jejich stavu z pohledu fyzické a objektové bezpečnosti. Výstupem byl seznam listinných úložišt a zhodnocení jejich stavu.
7) **Vymezení nástrojů užívaných pro zpracování osobních údajů v databázi a v e-mailu, sdílených disků.** Byl zhodnocen rozsah užívaných aplikací a IS, ve kterých se zpracovávají osobní údaje. Zhodnocení úrovně a kvality poskytované legislativní podpory ze strany dodavatele ve vztahu k nařízení a provedení revizi práv a oprávnění k aplikacím a IS. Projektovým týmem byla provedena revize e-mailu a sdílených disků a odstraněno neoprávněné zpracování dat s osobními údaji. Výstupem byl seznam aplikací a IS zpracovávající OÚ a zhodnocení jejich stavu.
8) **Provedení analýzy rizik.** Byla provedena analýza rizik na základě nastavených interních procesů řízení rizik. Výstupem analýzy rizik je prioritizace oblastí, které následně projektový tým řešil organizačními a technickými opatřeními.

9) **Zpracování rozdílové analýzy.** Projektovým týmem byla vypracována rozdílová analýza s ohledem na závěry mapování a provedené analýzy rizik tak, že v rozdílové analýze byly popsány nedostatky současného stavu oproti cílovému naplnění dle nařízení. Byl určen ideální stav souladu s nařízením.
10) **Vyhodnocení přípravné fáze a určení interních projektů pro implementaci organizačních a technických opatření.** Projektovým týmem bylo provedeno vyhodnocení přípravné fáze, připraveny projekty implementace organizačních a technických opatření a zahájena jejich realizace.
11) **Ustanovení pověřence.** Výstupem je ustanovení pověřence včetně uzavření pracovně právního vztahu s pověřencem nebo jiného vztahu, na základě kterého pověřenec vykoná svoji činnost.
12) **Přijetí směrnice o ochraně osobních údajů.** Byla přijata směrnice o ochraně osobních údajů.
13) **Proškolení zaměstnance.** Proběhlo proškolení zaměstnance a zastupitelů obce v oblasti ochrany a zpracování osobních údajů a interních pravidel a postupů pro dotčenou problematiku nařízení.
14) **Implementace organizačních opatření.** Správcem byla určena organizační opatření a provedena jejich implementace v souladu s definicí projektů v přípravné fázi. Byla provedena výměna kanceláří starosty a účetní z důvodu dostupnosti archívu, trezoru a kopírky. **V obou kancelářích byl pořízen nový nábytek, který je uzamykatelný a tudíž je v souladu s nařízením.** Byla zřízena přepážka sloužící pro výběr poplatků, občané nemohou vstupovat dále do místnosti a listinná úložiště jsou chráněna. Obec používá fyzické i elektronické ukládání dat**.** V případě fyzického ukládání se jedná o **listinné dokumenty uložené v zamykatelných skříňkách**, tzv. kartotékách, které jsou umístěné v kanceláři starosty a účetní, jež s nimi pracují. Klíče od skříněk jsou během úřední doby zastrčené v zámku, po skončení úřední doby jsou uschovány a vhodně zabezpečeny.
15) **Implementace technických opatření.** Správcem byla určena technická opatření a provedena jejich implementace v souladu s definicí projektů v přípravné fázi. Dále bylo provedeno ověření technických opatření např. formou penetračních testů či jiným testováním přijatých opatření s cílem vyhodnotit kvalitu přijatých opatření. Jako ochrana objektu byl zaveden kamerový systém. Počítače mají základní ochra-

nu ve formě antivirového programu. Počítačovou síť má na starost externí správce IT. Obecní úřad má jednu síťovou tiskárnu s automatickým tiskem pro dvě kanceláře.

16) **Implementace procesů k realizaci práv subjektů údajů. Nastavení postupů zpracování žádostí subjektu údajů.** Správcem bylo provedeno nastavení postupů pro zpracování žádostí subjektů údajů např. o rozsahu zpracování, uplatnění "práva být zapomenut" a přenositelnosti, dále bylo připraveno technické a organizační zázemí pro zpracování žádostí subjektů údajů včetně přidělení odpovídajících materiálních a lidských zdrojů. Správce je povinen identifikovat úložiště informací obsahující osobní údaje a to jak ve strukturované, tak i nestrukturované formě a v elektronické a listinné podobě a zajistí výkon zpracování žádostí subjektů údajů nad těmito úložišti. Úložiště měl správce určit v provedeném mapování a při zpracování záznamů o činnostech. Správce nesmí opomenout žádné úložiště osobních údajů. Obec má Facebookové stránky, kde uveřejňuje jen hlášení rozhlasu.

17) **Implementace procesů k realizaci práv subjektů údajů. Publikace postupů a případných podmínek k uplatnění práv subjektů údajů na veřejně dostupných zdrojích.** Správce může publikovat na veřejně dostupných zdrojích pokyny k uplatnění práv subjektů údajů.

18) **Revize zpracovatelských smluv.** S ohledem na mapování a záznamy o činnostech zpracování byla provedena revize smluv se zpracovateli a zajištěna odpovídající kvalita zpracování osobních údajů včetně sankcí a dalších vhodných mechanismů. Vybraná obec využívá informační systém veřejné správy GORDIC a obecní webovou stránku. Informační systém je uložen na serverech dodavatele, obec tedy nemá žádné datové centrum.

19) **Revize souhlasů subjektů údajů.** Byla provedena revize souhlasů subjektů údajů na základě provedeného mapování a záznamů o činnostech. Pokud je to nezbytně nutné, vyžádá si informovaný souhlas subjektu údajů ke zpracovávaným osobním údajům v již používaných evidencích a agendách.

20) **Vyhodnocení implementace organizačních a technických opatření ve vztahu k rozdílové analýze.** Projektovým týmem bylo provedeno vyhodnocení implementace organizačních a technických opatření na základě výstupů přípravné fáze. Vedení vybrané obce vyhodnocení vzalo na vědomí.

21) **Úvodní posouzení stavu zpracování osobních údajů ze strany pověřence a průběžné monitorování stavu zpracování osobních údajů.** Pověřencem bylo provedeno úvodní posouzení stavu každé situace nebo činnosti, kdy dochází k nakládání s osobními údaji, a to na základě záznamů o činnostech zpracování.

22) **Pravidelné sebehodnocení Správce formou aktualizace analýzy rizik** Správce s ohledem na přijaté procesy řízení rizik provede aktualizaci analýzy rizik.

23) **Pravidelná aktualizace rozdílové analýzy (např. v ročním cyklu).** Výstupem je aktualizovaná rozdílová analýza na základě dosavadního postupu implementace organizačních a technických opatření.

24) **Aktualizace záznamů o činnostech při změnách nebo implementaci nových agend či povinností obce v porovnání se zpracovaným mapováním a zpracovaných záznamů o činnostech.** V případě, že dojde k úpravě určujícího právního předpisu, účelu nebo ke změně oprávněného zájmu při zpracování osobních údajů, provede správce neprodleně odpovídající aktualizaci.

25) **Uplatňování práv subjektů údajů.** Na webových stránkách obce jsou publikovány pokyny a vzory žádostí k uplatnění práv subjektu údajů.

26) **Vyhodnocení dosavadního průběhu interních projektů z přípravné fáze a jejich případná aktualizace a optimalizace.** Správcem bylo provedeno vyhodnocení realizace projektů definovaných v přípravné fázi zaměřených na implementaci organizačních a technických projektů. Bylo navrženo jejich ukončení, aktualizace nebo optimalizace. Toto vyhodnocení je vhodné provádět pravidelně a to alespoň jednou ročně.

27) **Pravidelné každoroční školení zaměstnanců.** Správce zajistí pravidelné školení zaměstnanců v oblasti zpracování osobních údajů a jejich ochrany a to s cílem průběžného zvyšování povědomí o předmětné problematice.

ZÁVĚR

Dílčími cíli v teoretické části bakalářské práce bylo poskytnout základní informace o tématu ochrany osobních údajů, o jeho vývojových fázích ve světě, Evropě, Evropské Unii a v České republice. Byly vysvětleny jednotlivé pojmy, které jsou spojeny s problematikou ochrany osobních údajů. Součástí práce bylo seznámení s řízením procesů obce, veřejné správy a představení organizace vybrané obce a jejich nových povinností spojených s nařízením.

Cílem bakalářské práce bylo zjistit jednotlivé agendy, jejich činnost, určit odpovědnost, určit kompetence a rizika. Projektovým týmem, jehož členkou autorka byla, bylo prováděno mapování, analýzy a na základě výsledku analýz byla ohodnocena aktiva, identifikovány hrozby, pravděpodobnosti hrozeb, identifikace zranitelnosti. Z analýzy bylo patrné, které hrozby byly pro vybranou obec nejzávažnější a mohla se učinit technická a organizační opatření. Byla určena nejnáchylnější aktiva, která potřebují zvýšenou pozornost či ochranu ze strany vybrané obce. Dále byla zjištěna celková míra rizika. V procesu analýzy rizik byly přiřazeny role subjektů údajů. Z jednotlivých analýz byl vyhodnocen návrh opatření k zajištění plného souladu posuzovaných procesů s nařízením. Vybraná obec XY byla plně připravena na nové nařízení.

V době prudkého rozvoje technologií a rozšíření internetu je to nutnost ochrany osobních dat. Existuje mnoho možností, jak se dostat k osobním údajům a jak je okamžitě ukrást a zneužít. Žádná složitost, jen několik kliknutí myší. Nevyžádaná pošta je jen lepší variantou. Naše osobní údaje volně plující po síti a vystavené na místech, kde si je mohou prohlížet milióny lidí na celém světě. Tudíž upřesnění pravidel pro zpracování osobních údajů cíleným působením na ty, kdo vaše osobní údaje zpracovávají.

Měli bychom se chovat opravdu zodpovědně. Pokud máme možnost, zkontrolovat si, co o nás která společnost ví a pro jaké účely tyto informace využívá. Pokud někomu poskytnete svůj souhlas se zpracováním osobních údajů, můžete jej následně i kdykoli odvolat.

Tato skutečnost platí v celé Evropské unii a ve všech jejích členských státech se můžete domoci svých práv.

SEZNAM POUŽITÉ LITERATURY

[1] *Nařízení Evropského parlamentu a Rady (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. In: EU: Brusel, 2016, ročník 2016.

[2] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.

[3] *Směrnice Evropského parlamentu a Rady 95/46/ES: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*. In: . ES: Brusel, 1995.

[4] NULÍČEK, Michal. GDPR-obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

[5] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[6] Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR-obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 28. 8. 2017, [2017]. Ostrava: Sagit. ÚZ. ISBN 978-80-7488-241-8.

[7] *Úřad pro ochranu osobních údajů: desatero-zpracovani-pro-spravce* [online], [cit. 2019-01-28]. Dostupné z: Https://www.uoou.cz/desatero-zpracovani-pro-spravce/ds-4821/p1=4821

[8] *Úřad pro ochranu osobních údajů: poruseni-zabezpeceni* [online], [cit. 2019-01-28]. Dostupné z: Https://www.uoou.cz/poruseni-zabezpeceni/ds-5020/archiv=0&p1=3938

[9] ČESKO. Zákon č. 128/2000 Sb.: Zákon o obcích (obecní zřízení), ve znění pozdějších předpisů. In: *Sbírka zákonů.* Praha, 2000, ročník 2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-128

[10] BRŮNA, Miroslav. *Veřejná správa: (se zaměřením na obce a kraje)*. Vyd. 2. Praha: Institut pro místní správu, 2006. Skripta (Institut pro místní správu). ISBN isbn:80-86976-09-2.

[11] KÝVALOVÁ, Pavlína. *Metodika GDPR: Informace o zpracování osobních údajů*. Rouské, 2018.

[12] *Systémová analýza obcí* [online]. Praha: Ministerstvo vnitra České republiky., 2018 [cit. 2019-01-28]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/gdpr-web-aktuality-aktuality-systemova-analyza-obci.aspx

[13] *Kontrolní seznamy (Checklisty) pro obce* [online]. Praha: Ministerstvo vnitra České republiky, 2017 [cit. 2019-01-28]. Dostupné z: Https://www.mvcr.cz/gdpr/clanek/kontrolni-seznamy-checklisty-pro-obce.aspx

[14] *K blahopřání jubilantům obcemi* [online]. Praha: Úřad pro ochranu osobních údajů, 2016 [cit. 2019-01-28]. Dostupné z: https://www.uoou.cz/k-nbsp-blahopreni-jubilantum-obcemi/d-20337/p1=2013

[15] ČESKO. Usnesení č. 2/1993 Sb.: Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky. In: *Sbírka zákonů* [online]. Praha, 1992, ročník 1993, číslo 2. Dostupné také z: https://zakonyprolidi.cz/cs/1993-2

[16] ŠEFČÍK, Vladimír a Jiří KONEČNÝ, 2013. *Procesní inženýrství: bezpečné a spolehlivé vedení procesů*. Ve Zlíně: Univerzita Tomáše Bati. ISBN 978-80-7454-280-0.

[17] ČESKO. Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. In: *Sbírka zákonů* [online]. Praha, 2019, ročník 2019, číslo 110. Dostupné také z: https://zakonyprolidi.cz/cs/2019-110

[18] ČESKO. Zákon č. 111/2019 Sb.: Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: *Sbírka zákonů* [online]. Praha, 2019, ročník 2019, číslo 111. Dostupné také z: https://zakonyprolidi.cz/cs/2019-111

[19] ČESKO. Vyhláška č. 316/2014 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka Zákonů*. Praha, 2014, ročník 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316

[20] ISO NORMA. *Certifikace systémů managementu bezpečnosti informací: ISO 27001*. Praha, 2013.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIS Agendový informační systém.

CD Compact Disc.

CLA Check List Analysis.

ČR Česká republika.

IS Informační systém.

ISO lnternational Organization for Standardization.

IT Informační technologie.

GDPR General Data Protection Regulation.

ES Evropská směrnice.

EU Evropská Unie.

MŠ Mateřská škola.

OÚ Obecní úřad.

OÚ Osobní údaj.

PIN Personal Identification Number.

SW Software.

ÚOOÚ Úřad pro ochranu osobních údajů.

ZO Zastupitelstvo obce.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: HODNOCENÍ PRAVDĚPODOBNOSTI AKTIV VŮČI HROZBÁM [VLASTNÍ ZPRACOVÁNÍ]

Název aktiva	Hrozba	Pravděpo-dobnost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci výkonu agend úřadu	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Obec nedisponuje takovým objemem osobních údajů, proto vnější útoky nejsou častým jevem
	Technické chyby	1	Dle zjištěných informací přiřadil hodnocení pravděpodobnosti hrozby na velmi nízkou úroveň. Hrozba je nepravděpodobná, jelikož obec nedisponuje technologiemi v zajištění listinných úložišť, které by byly náchylné na technické chyby, pravděpodobnost výskytu je na velmi nízké úrovni.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obce na střední úrovni, jelikož obec nedisponuje interními akty, které by upravovaly procesy nakládání s os. údaji a jejich úložišť, které by byly pro zaměstnance obcí a úřadů závazná.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obce na střední úrovni, jelikož obec nedisponuje interními akty, které by upravovaly procesy nakládání s os. údaji a jejich úložišť.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Obec má zámky, které nejsou lehce překonatelné, objektová bezpečnost je na střední úrovni. Uzamykatelné skříně jsou dřevěné, jsou nové a vykazují známky středního odporu při překonávání. Obec nedisponuje takovým objemem osobních údajů, malý výskyt neoprávněných přístupů k osobním údajům.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Narušení dostupnosti os. údajů v obci je na střední úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Ztráta os. údajů v obci je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Může dojít k narušení práv a svobod subjektu osobních údajů.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci vnitřního chodu úřadu	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Obec nedisponuje takovým objemem osobních údajů, proto vnější útoky nejsou častým jevem.
	Technické chyby	1	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na velmi nízkou úroveň. Technická opatření obce zamezují jakékoliv pravděpodobnosti vzniku tech. chyb v rámci tohoto aktiva.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Pravděpodobnost této hrozby je v rámci obce na střední úrovni, jelikož obec nedisponuje interními akty, upravující procesy nakládání s os. údaji a jejich úložišť, nejsou pro zaměstnance obce a úřadů závazná.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obce na střední úrovni, jelikož manipulaci s tímto aktivem je v pravomoci malého okruhu.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Pravděpodobnost uplatnění této hrozby je v rámci obce na nízké úrovni, jelikož manipulaci s tímto aktivem je v pravomoci malého okruhu zaměstnanců obce.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Narušení dostupnosti os. údajů v obci je na střední úrovni, a to i z důvodu menšího počtu agend spojených s interním chodem obce a jeho úřadu.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Ztráta osobních údajů v obci je na střední úrovni, a to i z důvodu menšího počtu agend.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Může dojít k narušení práv a svobod subjektu os. údajů, ale jen subjektů údajů, které jsou spojeny s vnitřním chodem úřadu (zaměstnanci, smluvní partneři atd.).

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Informační systém spisové služby	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Informační systém spisové služby u obce je většinou hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které má obec k dispozici.
	Technické chyby	5	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na velmi vysokou úroveň. Velmi vysoká úroveň pravděpodobnosti byla týmem stanovena z důvodu možného selhání technického zajištění IS spisové služby, tak i vnějších jevů jako je výpadek elektřiny apod..
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obci, kde jsou zaběhlé procesy využívání daného IS a u obce nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Narušení integrity OÚ	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. V rámci aktuálních technických a organizačních opatřeních na obci tým předpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Pravděpodobnost je na nízké hodnotě, jelikož obec nedisponuje takovými opatřeními, zamezující neoprávněný přístup k OÚ, nepředpokládá se častější výskyt dané hrozby z důvodu menší atraktivity a objemu osobních údajů u obci, které by se staly terčem neoprávněného přístupu, popřípadě zcizení.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň.
	Ztráta osobních údajů	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Ztráta os. údajů v obci je na vysoké úrovni, a to z důvodu vyspělosti IS spisové služby a úložiště IS spisové služby je hostováno u poskytovatele.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Střední úroveň je zde zapříčiněna vyspělostí IS spisové služby a jejich dlouhodobé používání.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Agendové informační systémy – samostatná působnost	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Agendový informační systém u obce je hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem os. údajů, které má obec k dispozici.
	Technické chyby	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Vysoká úroveň pravděpodobnosti byla týmem stanovena z důvodu vysoké pravděpodobnosti selhání tech. zajištění AIS – samostatná působnost a technické chyby jsou častým jevem.
	Lidský faktor	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Obec má pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. V rámci aktuálních tech. a org. opatřeních na obci tým nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Přístupy do agendových informačních systémů jsou jen v malém kruhu zaměstnanců obce či úřadu.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Ztráta osobních údajů v obci je na střední úrovni, a to z důvodu vyspělosti agendových informačních systémů a jejich úložišť
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Střední úroveň je zde zapříčiněna vyspělostí agendových IS a jejich používání jen malého okruhu zaměstnanců obcí či úřadů.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Agendové informační systémy – přenesená působnost	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Agendový informační systém u obce je hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které má obec k dispozici
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Nízká úroveň pravděpodobnosti byla týmem stanovena z důvodu nízké pravděpodobnosti selhání technického zajištění AIS. Technické chyby nejsou častým jevem.
	Lidský faktor	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Obec nemá pevně stanovené procesy prací s agendovými informačními systémy např. interními akty.
	Narušení integrity OÚ	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. V rámci aktuálních tech. a org. opatřeních na obci se základním rozsahem přenesené působnosti projekční tým předpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Přístupy do agendových informačních systémů jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň.
	Ztráta osobních údajů	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Ztráta osobních údajů v obci je na nízké úrovni, a to z důvodu vyspělosti agendových informačních systémů a jejich úložišť.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti uplatnění hrozby na střední úroveň. Střední úroveň je způsobená vyspělostí agendových IS a jejich používání jen úzkého kruhu zaměstnanců obce či úřadu.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Ekonomický informační systém	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Ekonomický informační systém u obce je hostovaný informační systém, který je dobře chráněn. Atraktivitu pro vnější útoky snižuje také menší objem osobních údajů, které má obec k dispozici.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Nízkou úroveň pravděpodobnosti byla týmem stanovena z důvodu možného selhání technického zajištění Ekonomického informačního systému, tak i vnějších jevů jako je výpadek elektřiny, technické chyby nejsou častým jevem.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Obec nemá pevně stanovené procesy prací s Ekonomickým informačním systémem např. interními akty.
	Narušení integrity OÚ	1	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na velmi nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obci se základním rozsahem přenesené působnosti tým nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Přístupy do Ekonomického informačního systému jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.
	Narušení dostupnosti	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň.
	Ztráta osobních údajů	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Ztráta osobních údajů v obci je na nízké úrovni, a to z důvodu vyspělosti Ekonomického IS a jeho úložišť.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Střední úroveň je zde zapříčiněna vyspělostí Ekonomického IS a jejich dlouhodobé používání.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Portály	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Využívané portály obcí se základním rozsahem nedisponují vyspělou ochranou a mohou se stát terčem vnějších útoků.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Technické zajištění portálů není na vysoké úrovni a může dojít k technickým chybám.
	Lidský faktor	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň. Obec nemá pevně stanovené procesy prací s Ekonomickým informačním systémem např. interními akty.
	Narušení integrity OÚ	1	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na velmi nízkou úroveň. V rámci aktuálních technických a organizačních opatřeních na obci se základním rozsahem přenesené působnosti tým nepředpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Přístupy do Ekonomického informačního systému jsou jen v úzkém kruhu zaměstnanců obcí či úřadu.
	Narušení dostupnosti	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň.
	Ztráta osobních údajů	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň.

Název aktiva	Hrozba	Pravděpodobnost	Hodnocení pravděpodobnosti
Ostatní elektronická úložiště	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Aktivum nemá tak velký rozsah osobních údajů, aby bylo terčem vnějších útoků.
	Technické chyby	5	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na velmi vysokou úroveň. Velmi vysoká úroveň pravděpodobnosti byla týmem stanovena z důvodu možného selhání technického zajištění ostatních elektronických úložišť.
	Lidský faktor	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Obec nemá pevně stanovené procesy prací s ostatními elektronickými úložišti např. interními akty.
	Narušení integrity OÚ	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. V rámci aktuálních technických a organizačních opatřeních na obci se základním rozsahem přenesené působnosti projekční tým předpokládá častější uplatnění dané hrozby.
	Neoprávněný přístup	4	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na vysokou úroveň. Přístupy do Ekonomického informačního systému jsou jen v úzkém kruhu zaměstnanců obcí či úřadu. Existuje nebezpečí kybernetického útoku.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na nízkou úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Ztráta osobních údajů v obci je na střední úrovni, a to z důvodu vyspělosti ostatních elektronických úložišť.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení pravděpodobnosti hrozby na střední úroveň. Střední úroveň je zde zapříčiněna vyspělostí ostatních elektronických úložišť a jejich dlouhodobé používání.

PŘÍLOHA P II: HODNOCENÍ ZRANITELNOSTI AKTIV VŮČI HROZBÁM [VLASTNÍ ZPRACOVÁNÍ]

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci výkonu agend úřadu	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Zabezpečení listinných úložišť je v obci na nízké úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, nepředstavují zásadní překážku pro vnější útoky.
	Technické chyby	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Ochrana před tech. chybami či vnějšími vlivy nedosahuje u obce takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obec nedisponuje zabezp. systémy obsahující tepelný detektor či kouřový detektor.
	Lidský faktor	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany os. údajů.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obec má zámky, které nejsou lehce překonatelné, objektová bezpečnost je na střední úrovni. Uzamykatelné skříně jsou nové a známky středního odporu při překonávání. Obec disponuje kamerovým systémem.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Narušení dostupnosti os. údajů v obci je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Hodnota zranitelnosti byla stanovena z důvodu absence vnitř. předpisů pro nakl. s listinami a jejich úložišť. Objektová bezpečnost je na střední úrovni. Uzamykatelné skříně jsou nové.
	Narušení práv a svobod subjektu údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla stanovena týmem z důvodu zneužití os. údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Listinné úložiště v rámci vnitřního chodu úřadu	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Zabezpečení listinných úložišť je v obci na nízké úrovni. Listiny jsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy nepředstavují zásadní překážku pro vnější útoky.
	Technické chyby	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Ochrana před technickými chybami či vnějšími vlivy nedosahuje u obce takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. Obec nedisponuje zabezpečovacími systémy obsahující např. tepelný detektor či kouřový detektor.
	Lidský faktor	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na vysokou úroveň. Vysoká hodnota zranitelnosti aktiva byla týmem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany osobních údajů.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední hodnota zranitelnosti aktiva byla týmem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Obec má zámky, které nejsou lehce překonatelné, objektová bezpečnost je na střední úrovni. Uzamykatelné skříně jsou nové, vykazuj známky středního odporu při překonávání. Obec disponuje kamerovým systémem.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Narušení dostupnosti os. údajů v obci je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na vysokou úroveň. Vysoká hodnota zranitelnosti aktiva byla týmem stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, objektová bezpečnost je na střední úrovni. Uzamykatelné skříně jsou nové, známky vykazují střední odporu při překonávání. Obec disponuje kamerovým systémem.
	Narušení práv a svobod subjektu údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou úroveň. Vysoká hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití os. údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Informační systém spisové služby	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana informačního systému spisové sl. je na vysoké úrovni a většinou jsou uložiště u poskytovatele IS spisové sl., které je dostatečně zabezpečeno.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Ochrana informačního systému spisové sl. je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele IS spisové sl., které je dostatečně zabezpečeno. IS spisové sl. jsou ochráněny před tech. chybami, které by mohly nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obci, kde jsou zaběhlé procesy využívání daného IS a nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Narušení integrity OÚ	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici IS spisových služeb na obci, kde jsou zaběhlé procesy využívání daného IS a nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na omezený počet zaměst. obce či úřadu, kteří mají přístupy do IS spisové služby a nedochází k časté fluktuaci osob mající přístupy a k neoprávněným přístupům k IS spisové sl.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Obec disponuje alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Agendové informační systémy – samostatná působnost	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chybami, které by mohly nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici AIS na obci, kde jsou zaběhlé procesy využívání daného IS a u obce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici AIS na obci, kde jsou zaběhlé procesy využívání daného IS a u obce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Obec nedisponuje ochranou před úmyslným exportem dat z AIS či výmazem dat z AIS. Zároveň disponuje obec alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití os. údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
Agendové informační systémy – přenesená působnost	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chyby, které by mohli nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici AIS na obci, kde jsou zaběhlé procesy využívání daného IS a u obce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Narušení integrity OÚ	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na již dlouhou tradici AIS na obci, kde jsou zaběhlé procesy využívání daného IS a u obce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Obec disponuje alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední hodnota zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Ekonomický informační systém	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Ochrana Ekonomického informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele Ekonomického informačního systému, které je dostatečně zabezpečeno.
	Technické chyby	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Ze zjištěných informací Ekonomický informační systém je chráněn jen základním způsobem před technickými chybami.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešili procesy užití Ekonomického IS.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiv na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešili procesy užití Ekonomického IS. Dále je to také absence politiky přístupů obce či úřadu do Ekonomického IS.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Nízká úroveň byla týmem zvolena s ohledem na omezený počet zaměstnanců obce či úřadu, který mají přístupy do Ekonomického IS a nedochází k časté fluktuaci osob mající přístupy do Ekonomického IS.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Obec nedisponuje ochranou před úmyslným exportem dat z Ekonomického IS či výmazem dat z Ekonomického IS. Zároveň disponuje obec alespoň základní ochranou před ztrátou dat.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitel-nost	Hodnocení pravděpodobnosti
Portály	Vnější útoky	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Obec nedisponuje ochranou portálů před vnějšími útoky.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Portály jsou zpravidla poskytovány externími subjekty a uloženy v rámci cloudového řešení, takže zranitelnost je na nízké úrovni.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb administrátory portálů obce.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb redaktory a administrátory portálů obce.
	Neoprávněný přístup	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Tým nepředpokládá neoprávněných přístup na portály obce.
	Narušení dostupnosti	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň.
	Ztráta osobních údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Portály disponují jen základní ochranou.
	Narušení práv a svobod subjektu údajů	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

Název aktiva	Hrozba	Zranitelnost	Hodnocení pravděpodobnosti
Ostatní elektronické úložiště	Vnější útoky	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Obec má ostatní elektronická úložiště oddělena od veřejně dostupné sítě.
	Technické chyby	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízkou úroveň. Obec provádí zálohu dat.
	Lidský faktor	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Narušení integrity OÚ	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Neoprávněný přístup	3	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na střední úroveň. Střední úroveň byla týmem zvolena s ohledem volný přístup do prostor budov obce či úřadu, kde je v těchto prostorách možnost připojení do ethernetových výstupů, a tedy přístupu do sítě.
	Narušení dostupnosti	2	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na nízká úroveň.
	Ztráta osobních údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na vysokou úroveň.
	Narušení práv a svobod subjektu údajů	4	Dle zjištěných informací tým přiřadil hodnocení zranitelnosti aktiva na vysokou úroveň. Vysoká úroveň zranitelnosti tohoto aktiva byla týmem stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

PŘÍLOHA P III: KONTROLNÍ SEZNAM CLA [VLASTNÍ ZPRACOVÁNÍ]

	CLA - Check List Analysis	Odpovědi: ANO - NE
1.	Jmenovala obec svého pověřence?	ANO
2.	Oznámila obec jmenování svého pověřence?	ANO
3.	Je obec správcem údajů	ANO
4.	Ustanovil správce projektový tým?	ANO
5.	Zajistil správce mapování osobních údajů?	ANO
6.	Vytvořil správce kvalifikované záznamy o činnostech?	ANO
7.	Stanovil správce interní proces řízení rizik?	NE
8.	Vymezil správce listinná úložiště na záznamy o činnostech zpracování?	ANO
9.	Byl vytvořen seznam listinných úložišť?	ANO
10.	Byl zhodnocen stav listinných úložišť?	ANO
11.	Byl vytvořen seznam aplikací informačního systému obecního úřadu?	ANO
12.	Byl zhodnocen stav aplikací informačního systému obecního úřadu?	ANO
13.	Provedl správce revizi e-mailu a sdílených disků?	ANO
14.	Odstranil správce neoprávněná data s osobními údaji?	NE
15.	Seznámilo se vedení obce se závěry analýzy rizik?	ANO
16.	Řídí se vedení obce závěry analýzy rizik?	ANO
17.	Byla zpracovaná rozdílová analýza?	ANO
18.	Byl stanoven ideální cílový stav v souladu s GDPR?	ANO
19.	Seznámilo se vedení obce se závěry rozdílové analýzy?	ANO
20.	Provedl správce vyhodnocení přípravné fáze?	ANO
21.	Provedl správce projekt na implementaci organizačních opatření?	ANO
22.	Provedl správce projekt na implementaci technických opatření?	ANO
23.	Zahájil správce realizaci výše uvedených opatření?	ANO
24.	Byl uzavřen pracovně právní vztah s pověřencem?	ANO
25.	Přijal správce směrnici o ochraně osobních údajů?	NE
26.	Proškolil správce své zaměstnance s problematikou GDPR?	ANO
27.	Byl vytvořen záznam o proškolení zaměstnanců?	ANO
28.	Byla vytvořena zpráva o implementaci organizačních opatření?	NE
29.	Byla vytvořena zpráva o implementaci technických opatření?	NE
30.	Provedl správce penetrační test?	ANO
31.	Má správce publikované pokyny formou životních situací na webu obce?	ANO
32.	Zrevidoval správce zpracovatelské smlouvy?	ANO
33.	Provedl správce revizi souhlasů subjektů údajů?	ANO
34.	Vyžádal si souhlas subjektu údajů ke zprac. v používaných agendách?	ANO
35.	Provedl správce vyhodnocení implementace organizačních opatření?	ANO
36.	Provedl správce vyhodnocení implementace technických opatření?	ANO
37.	Provedl pověřenec posouzení stavu každé situace či činnosti?	ANO
38.	Má správce vypracovaný organizační řád?	NE
39.	Má správce vypracovaný spisový řád?	ANO
40.	Má správce vypracovaný skartační řád	ANO
41.	Má správce kamerový systém?	ANO
42.	Je obec zpracovatelem údajů	ANO

	CLA - Check List Analysis	Odpovědi: ANO - NE
43.	Vede obec evidenci souhlasů se zpracováním osobních údajů?	ANO
44.	Vede obec evidenci v listinné podobě?	ANO
45.	Vede obec evidenci v elektronické podobě?	NE
46.	Agenda evidence obyvatel má zvláštní kategorii osobních údajů?	NE
47.	Agenda evidence obyvatel využívá spolupráce s externím příjemcem?	ANO
48.	Agenda evidence obyvatel využívá kategorii příjemců mimo EU?	NE
49.	Je vedena kontrola zpracování OÚ v agendě evidence obyvatel?	NE
50.	Je vedena evidence poplatků v elektronické podobě?	NE
51.	Je vedena evidence telefonických kontaktů se souhlasy osob?	ANO
52.	Je vedena evidence klíčů?	ANO
53.	Jsou trvale uchovávané písemnosti a spisy v uzamykatelných místnostech?	ANO
54.	Jsou trvale uchovávané písemnosti a spisy v uzamykatelných skříních?	ANO
55.	Je řízen přístup osob k písemnostem?	ANO
56.	Je při práci se spisem možnost kontaktu s cizí osobou?	ANO
57.	Na konci pracovní doby je spis uložen do uzamčené zásuvky?	ANO
58.	Jsou evidovaná přenosná paměťová média používaná k práci?	NE
59.	Je určen správce WEB stránek obce?	ANO
60.	Jsou řízena administárorská práva k přiděleným počítačům?	ANO
61.	Jsou řízeny přístupy k osobním údajům v rámci IT?	ANO
62.	Jsou využívány antivirové programy?	ANO
63.	Je využíváno šifrování?	NE
64.	Agenda volební systém má zvláštní kategorii osobních údajů?	NE
65.	Agenda volební systém využívá kategorii příjemců mimo EU?	ANO
66.	Využívá agenda volební systém spolupráci s externím příjemcem?	NE
67.	Je vedena kontrola zpracování OÚ v agendě volební systém?	NE
68.	Agenda informace dle zákona 106/1999Sb. má zvláštní kategorii osob. údajů?	NE
69.	Agenda informace dle zák.106/1999Sb. využívá kategorie příjemců mimo EU?	NE
70.	Využívá agenda informace dle zák. 106/1999Sb.spolupráci s exter. příjemcem?	NE
71.	Je vedena kontrola zprac. OÚ v agendě informace dle zákona 106/1999Sb.?	ANO
72.	Agenda Czech Point má zvláštní kategorii osobních údajů?	NE
73.	Agenda Czech Point využívá kategorii příjemců mimo EU?	NE
74.	Využívá agenda Czech Point spolupráci s externím příjemcem?	ANO
75.	Je vedena kontrola zpracování OÚ v agendě Czech Point?	NE
76.	Agenda personální a mzdová má zvláštní kategorii osobních údajů?	ANO
77.	Agenda personální a mzdová využívá kategorii příjemců mimo EU?	NE
78.	Využívá agenda personální a mzdová spolupráci s externím příjemcem?	ANO
79.	Je vedena kontrola zpracování OÚ v agendě personální a mzdové?	ANO
80.	Agenda místní poplatky má zvláštní kategorii osobních údajů?	NE

	CLA - Check List Analysis	Odpovědi: ANO - NE
81.	Agenda místní poplatky využívá kategorii příjemců mimo EU?	NE
82.	Využívá agenda místní poplatky spolupráci s externím příjemcem?	ANO
83.	Je vedena kontrola zpracování OÚ v agendě místní poplatky?	ANO
84.	Agenda smlouvy, plné moci má zvláštní kategorii osobních údajů?	NE
85.	Agenda smlouvy, plné moci využívá kategorii příjemců mimo EU?	NE
86.	Využívá agenda smlouvy, plné moci spolupráci s externím příjemcem?	NE
87.	Je vedena kontrola zpracování OÚ v agendě smlouvy, plné moci?	ANO
88.	Agenda informace občanům má zvláštní kategorii osobních údajů?	NE
89.	Agenda informace občanům využívá kategorii příjemců mimo EU?	NE
90.	Využívá agenda informace občanům spolupráci s externím příjemcem?	ANO
91.	Je vedena kontrola zpracování OÚ v agendě informace občanům?	NE
92.	Agenda účetnictví má zvláštní kategorii osobních údajů?	NE
93.	Agenda účetnictví využívá kategorii příjemců mimo EU?	NE
94.	Využívá agenda účetnictví moci spolupráci s externím příjemcem?	ANO
95.	Je vedena kontrola zpracování OÚ v agendě účetnictví?	ANO
96.	Agenda spisová služba má zvláštní kategorii osobních údajů?	NE
97.	Agenda spisová služba využívá kategorii příjemců mimo EU?	NE
98.	Využívá agenda spisová služba spolupráci s externím příjemcem?	ANO
99.	Je vedena kontrola zpracování OÚ v agendě spisová služba?	ANO
100.	Agenda správní rozhodnutí má zvláštní kategorii osobních údajů?	NE
101.	Agenda správní rozhodnutí využívá kategorii příjemců mimo EU?	NE
102.	Využívá agenda správní rozhodnutí spolupráci s externím příjemcem?	ANO
103.	Je vedena kontrola zpracování OÚ v agendě správní rozhodnutí?	ANO
104.	Agenda knihovna má zvláštní kategorii osobních údajů?	NE
105.	Agenda knihovna využívá kategorii příjemců mimo EU?	NE
106.	Využívá agenda knihovna spolupráci s externím příjemcem?	NE
107.	Je vedena kontrola zpracování OÚ v agendě knihovna?	ANO
108.	Agenda zápisy ze ZO má zvláštní kategorii osobních údajů?	NE
109.	Agenda zápisy ze ZO využívá kategorii příjemců mimo EU?	NE
110.	Využívá zápisy ze ZO spolupráci s externím příjemcem?	NE
111.	Je vedena kontrola zpracování OÚ v agendě zápisy ze ZO?	ANO
112.	Agenda střetu zájmů má zvláštní kategorii osobních údajů?	NE
113.	Agenda střetu zájmu využívá kategorii příjemců mimo EU?	NE
114.	Využívá agenda střetu zájmů spolupráci s externím příjemcem?	ANO
115.	Je vedena kontrola zpracování OÚ v agendě střetu zájmu?	NE
116.	Agenda legalizace a vidimace má zvláštní kategorii osobních údajů?	NE
117.	Agenda legalizace a vidimace využívá kategorii příjemců mimo EU?	NE
118.	Využívá agenda legalizace a vidimace spolupráci s externím příjemcem?	NE

PŘÍLOHA P IV: JEDNOTLIVÉ FÁZE ČINNOSTÍ [VLASTNÍ ZPRACOVÁNÍ]

P. č.	Fáze	Činnosti		Relevantní článek GDPR	Popis	Výstup činnosti
1	Přípravná fáze	Sestavení projektového týmu		Čl. 24	Správce ustanovil tým zahrnující nejméně starostu a účetní.	Výstupem byl zápis o sestavení týmu, určení odpovědností a stanovení kompetencí jednotlivých členů týmu.
2		Zpracování úvodní analýzy včetně mapování aktuálního zpracování osobních údajů		Čl. 5	Správce zajistil zpracování mapování osobních údajů alespoň v rozsahu definovaném touto systémovou analýzou včetně určení vztahů se zpracovateli.	Výstupem byla zpracovaná analýza popisující věrně aktuální stav.
3		Zpracování záznamů o činnostech zpracování		Čl. 6, čl. 30	Správce vytvořil kvalifikované záznamy o činnostech zpracování na základě provedeného mapování.	Výstupem byly záznamy o činnostech zpracování.
4		Nastavení interních procesů řízení rizik		Čl. 24	Správce ustanovil interní proces řízení rizik.	Výstupem byla směmice o řízení rizik.
5		Vymezení aktiv	Vymezení listinných úložišť	Čl. 5 a čl. 6	Správce detailně vymezil listinná úložiště v návaznosti na záznamy o činnostech zpracování. Součástí je revize práv přístupů k těmto úložištím a zhodnocení jejich stavu z pohledu fyzické a objektové bezpečnosti.	Výstupem byl seznam listinných úložišt a zhodnocení jejich stavu.

P. č.	Fáze	Činnosti		Relevantní článek GDPR	Popis I	Výstup činnosti
6	Přípravná fáze	Vymezení aktiv	Vymezení nástrojů užívaných pro zpracování os. údajů v databázi a v e-mailu, sdílených disků		Správce zhodnotil rozsah užívaných aplikací a IS, ve kterých zpracovává os. údaje. Zhodnotil úroveň a kvalitu poskytované legisl. podpory ze strany dodavatele ve vztahu ke GDPR a provedl revizi práv a oprávnění k aplikacím a IS. Provedl revizi e-mailu a sdílených disků a odstranil neoprávněně zpracování data s os. údaji.	Výstupem byl seznam aplikací a IS zpracovávající OÚ a zhodnocení jejich stavu.
7		Provedení analýzy rizik		Čl. 24	Správce provedl analýzu rizik na základě nastavených interních procesů řízení rizik. Výstupem analýzy rizik je prioritizace oblastí, které následně správce řešil organizačními a technickými opatřeními.	Výstupem byla analýza rizik. Správce zajistil, aby tato analýza rizik byla známa vedení obce, které je povinno se závěry řídit.
8		Zpracování rozdílové analýzy		Čl. 5	Správce zpracoval rozdílovou analýzu s ohledem na závěry mapování a provedené analýzy rizik tak, že v rozdílové analýze byly detailně popsány nedostatky současného stavu oproti cílovému stavu naplnění povinností správce dle GDPR. Správce si v rozdílové analýze určil ideální cílový stav souladu s GDPR.	Výstupem byla rozdílová analýza. Správce zajistil, aby tato rozdílová analýza byla známa vedení obce.
9		Vyhodnocení přípravné fáze a určení interních projektů pro implementaci org. a tech. opatření		Čl. 24 a čl. 25	Správce provedl vyhodnocení přípravné fáze a připravil projekty implementace organizačních a technických opatření a zahájil jejich realizaci.	Výstupem byl přehled projektů, jejich věcných garantů, detailní popis projektů včetně jejich rozpočtu.

P. č.	Fáze	Činnosti	Relevantní článek GDPR	Popis I	Výstup činnosti
10	Implementační fáze	Ustanovení pověřence	Čl. 37	Správce ustanovil pověřence a informuje o tomto kroku obec.	Výstupem je ustanovení pověřence včetně uzavření pracovně právního vztahu s pověřencem nebo jiného vztahu, na základě kterého pověřenec vykoná svoji činnost.
11		Přijetí směrnice o ochraně osobních údajů nebo kodexu	Čl. 24	Správce přijal směrnici o ochraně osobních údajů nebo kodex o jeho implementaci do organizace.	Směrnice o ochraně osobních údajů nebo kodex.
12		Proškolení zaměstnance	Čl. 24	Správce proškolil zaměstnance či jiné spolupracující osoby v oblasti ochrany a zpracování osobních údajů a interních pravidel a postupů pro dotčenou problematiku GDPR.	Výstupem bylo školení a záznam o proškolení zaměstnanců.
13		Implementace organizačních opatření	Čl. 25	Správce určil organizační opatření a provedl jejich implementaci v souladu s definicí projektů v přípravné fázi.	Výstupem byla zpráva o implementaci organizačních opatření.
14		Implementace technických opatření	Čl. 25	Správce určil technická opatření a provedl jejich implementaci v souladu s definicí projektů v přípravné fázi. Správce provedl ověření technických opatření např. formou penetračních testů či jiným testováním přijatých opatření s cílem vyhodnotit kvalitu přijatých opatření.	Výstupem byla zpráva o implementaci technických opatření.

P. č.	Fáze	Činnosti		Relevantní článek GDPR	Popis I	Výstup činnosti
15	Implementační fáze	Implementace procesů k realizaci práv subjektů údajů	Nastavení postupů zpracování žádostí subjektů údajů	Čl. 15 až čl. 22	Správce provedl nastavení postupů pro zpracování žádostí subjektů údajů např. o rozsahu zpracování, uplatnění "práva být zapomenut" a přenositelnosti. Správce připravil technické a organizační zázemí pro zpracování žádostí subjektů údajů včetně přidělení odpovídajících materiálních a lidských zdrojů. Správce je povinen identifikovat úložiště informací obsahující osobní údaje a to jak ve strukturované, tak i nestrukturované formě a v elektronické a listinné podobě a zajistí výkon zpracování žádostí subjektů údajů nad těmito úložišti. Úložiště měl správce určit v provedeném mapování a při zpracování záznamů o činnostech. Správce nesmí opomenout žádné úložiště osobních údajů (listinné archivy, kartotéky, aplikace, IS apod.).	Zpráva o testu zpracování žádostí subjektů údajů. Zdokumentované a zavedené nové procesy pro zpracování žádostí subjektů údajů.
16			Publikace postupů a případných podmínek k uplatnění práv subjektů údajů na veřejně dostupných zdrojích	Kap. 3	Správce může publikovat na veřejně dostupných zdrojích pokyny k uplatnění práv subjektů údajů.	Publikované pokyny např. formou životních situací na webových stránkách obce.
17		Revize zpracovatelských smluv, pokud existují		Čl. 28	Správce s ohledem na provedené mapování a záznamy o činnostech zpracování provede revizi smluv se zpracovateli a zajistí odpovídající kvalitu zpracování os. údajů včetně sankcí a dalších vhodných mechanismů (informační povinnost při kompromitaci zprac. os. údajů a způsobů řešení či eskalace těchto situací).	Zpráva o revizi zpracovatelských smluv.

P. č.	Fáze	Činnosti	Relevantní článek GDPR	Popis I	Výstup činnosti
18	Implementační fáze	Revize souhlasů subjektů údajů	Čl. 7	Správce provede revizi souhlasů subjektů údajů na základě provedeného mapování a záznamů o činnostech. Pokud je to nezbytně nutné, vyžádá si informovaný souhlas subjektu údajů ke zpracovávaným osobním údajům v již používaných evidencích a agendách.	Revidované informované souhlasy subjektů údajů.
19		Vyhodnocení implementace organizačních a technických opatření ve vztahu k rozdílové analýze	Čl. 24	Správce provede vyhodnocení implementace organizačních a technických opatření na základě výstupů přípravné fáze. Vedení obce vyhodnocení vezme na vědomí.	Zpráva o stavu implementace organizačních a technických opatření.

P. č.	Fáze	Činnosti	Relevantní článek GDPR	Popis I	Výstup činnosti
20	Provozní fáze	Úvodní posouzení stavu zpracování osobních údajů ze strany pověřence a průběžné monitorování stavu zpracování osobních údajů	Čl. 39	Pověřenec provede úvodní posouzení stavu každé situace či činnosti, kdy dochází k nakládání s osobními údaji a to na základě záznamů o činnostech zpracování.	Zpráva o posouzení stavu obsahující případné nálezy a postup jejich nápravy.
21		Pravidelné sebehodnocení Správce formou aktualizace analýzy rizik	Čl. 5	Správce s ohledem na přijaté procesy řízení rizik provede aktualizaci analýzy rizik.	Výstupem je aktualizace analýzy rizik.
22		Pravidelná aktualizace rozdílové analýzy (např. v ročním cyklu)	Čl. 5	Správce zajistí provádění pravidelné aktualizace rozdílové analýzy na základě postupu implementace organizačních a technických opatření zpravidla v ročním cyklu. Aktualizace rozdílové analýzy by měly správci ukázat vývoj a postup v implementaci opatření a vývoj jeho vyspělosti v oblasti zpracování osobních údajů dle požadavků GDPR.	Výstupem je aktualizovaná rozdílová analýza na základě dosavadního postupu implementace organizačních a technických opatření.
23		Aktualizace záznamů o činnostech při změnách nebo implementaci nových agend či povinností obce v porovnání se zpracovaným mapováním a zpracovaných záznamů o činnostech	Čl. 30	V případě, že dojde k úpravě určujícího právního předpisu, účelu nebo ke změně oprávněného zájmu při zpracování osobních údajů, provede správce neprodleně odpovídající aktualizaci záznamů o činnostech zpracování.	Výstupem jsou aktualizované záznamy o činnostech zpracování.

P. č.	Fáze	Činnosti	Relevantní článek GDPR	Popis I	Výstup činnosti
24	Provozní fáze	Uplatňování práv subjektů údajů	Kap. 3	Na webových stránkách obce jsou publikovány pokyny a vzory žádostí k uplatnění práv subjektu údajů.	Výstupem jsou žádosti subjektů údajů a jejich zpracování v řádných termínech a deklarované kvalitě.
25		Vyhodnocení dosavadního průběhu interních projektů z přípravné fáze a jejich případná aktualizace a optimalizace	Čl. 24 a čl. 25	Správce provede vyhodnocení realizace projektů definovaných v přípravné fázi zaměřených na implementaci organizačních a technických projektů. Následně navrhne jejich ukončení, aktualizaci nebo optimalizaci. Toto vyhodnocení je vhodné provádět pravidelně a to alespoň jednou ročně.	Výstupem je zpráva o aktuálním stavu. Tato zpráva by měla být aktualizována nejméně jednou ročně či v závislosti na implementaci organizačních a technických opatření. Zpráva by měla zhodnotit úroveň vyspělosti obce a měla by být vodítkem pro posuzování přiměřenosti implementačního opatření.
26		Pravidelné každoroční školení zaměstnanců	Čl. 24	Správce zajistí pravidelné školení zaměstnanců v oblasti zpracování osobních údajů a jejich ochrany a to s cílem průběžného zvyšování povědomí o předmětné problematice.	Výstupem je záznam o proškolení zaměstnanců.

PŘÍLOHA P V: ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ VŠECH AGEND [VLASTNÍ ZPRACOVÁNÍ]

Oblast zpracování osobních údajů	Evidence obyvatel	Volební systém (seznamy voličů, voličské průkazy)	Informace podle zákona 106/1999 Sb.
Osobní údaje	Jméno, příjmení, rodné číslo, bydliště, místo narození, omezení způsobilosti, údaje o opatrovníkovi, národnost a státní příslušnost, jména a příjmení rodičů, rodinný stav, údaje o pěst. péči - jména a příjmení, adresa pěstounů	Jméno, příjmení, datum narození, rodné číslo, státní příslušnost, omezení způsobilosti, údaje o opatrovníkovi	Jméno, příjmení, rodné číslo, bydliště, e-mail, datová schránka, podpis, údaje o vzdělání
Zvláštní kategorie osobních údajů	NE	NE	NE
Správce	Obec	Obec	Obec
Zpracovatel	Obec	Obec	Obec
Subjekt údajů = osoba, jejíž osobní údaje jsou zpracovávány	Občan - přenesená působnost, kategorie zvláště zranitelných subjektů údajů (nezletilý)	Občan - přenesená působnost	Občan - samostatná působnost
Právní základ zpracování osobních údajů	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti
Účel nakládání s osobními údaji	Zajištění agendy evidence obyvatel - Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech	Zajištění volební agendy - Zákon č. 247/1995 Sb., o volbách do Parlamentu ČR	Poskytování informací občanům - Zákon č. 106/1999 Sb., o svob. přístupu k informacím
Kategorie příjemců	Interní příjemci - účetní	Interní příjemci - účetní, starosta, místostarosta. Extemí příjemci - Členové volební komise, správce počítač..syst.	Starosta, místostarosta, účetní
Kategorie příjemců mimo EU	NE	NE	NE
Doba uložení osobních údajů pro potřeby Správce OÚ	V/5, S/50	S/5, V/5, A/5	S/5, A5
Využívání spolupráce s externím příjemcem	ANO (xxxxxxxxxxx)	ANO (xxxxxxxxxxx)	NE
Způsob kontroly zpracování OU	NE	NE	MV

Oblast zpracování osobních údajů	Czech Point	Personální a mzdová agenda	Místní poplatky - za psa, odpad, stočné
Osobní údaje	Jméno, příjmení, rodné číslo, bydliště, místo naroz. rodné příjmení, číslo dokladu totožnosti (OP + cestovní pas), národnost a státní přísl., jména a příjmení rodičů	Jméno, příjmení, RČ, bydliště, místo narození, rodné příjmení, OP, národnost, rodinný stav, státní příslušnost, e-mail, telefon, bankovní spojení, jména, příjmení, data narození dětí, zaměstnání partnerů	Jméno, příjmení, datum narození, bydliště, jména a příjmení rodičů u nezletilých, omezení způsobilosti, údaje o opatrovníkovi, jména a příjmení rodičů u nezletilých
Zvláštní kategorie osobních údajů	NE	Zdravotní stav – vstup. zdrav. prohlídky, typ důchodu, exekuce, výživné	NE
Správce	Obec	Obec	Obec
Zpracovatel	Obec	Obec	Obec
Subjekt údajů = osoba, jejíž osobní údaje jsou zpracovávány	Občan - přenesená působnost	Zaměstnanec (PS, DPP, DPČ), zastupitel	Občan, majitel rekreačních objektů - samostatná působnost
Právní základ zpracování osobních údajů	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti
Účel nakládání s osobními údaji	Plnění právní povinnosti - Zákon č. 356/2000 Sb., o informačních systémech veřejné správy, č.111/2009 Sb., o základních registrech	Zákon č. 262/2006 Sb., zákoník práce a právní předpisy upravující mzdové účetnictví	Zákon č. 565/1990 Sb., o místních poplatcích
Kategorie příjemců	Starosta, účetní	Účetní, starosta, místostarosta, externí zdrav. pojišťovny, OSSZ, FÚ, ÚP,kooperativa - zákonné, soud a exekuční úřad, celní úřad	Účetní
Kategorie příjemců mimo EU	NE	NE	NE
Doba uložení osobních údajů pro potřeby Správce OÚ	S/10	V5, S10, S45, S5, V5, V10, S50	S10, V5, S5
Využívání spolupráce s externím příjemcem	ANO	ANO	ANO
Způsob kontroly zpracování OU	NE	Kontrola třetí stranou, OSSZ, zdravotní pojišťovny, finanční úřad, ÚP, audit kraje	Kontrola třetí stranou - audit

Oblast zpracování osobních údajů	Smlouvy, plné moci	Informace občanům - sms info-kanál, IVVS - rozhlas, email	Účetnictví	Kronika	Spisová služba
Osobní údaje	Jméno, příjmení, bydliště, rodné číslo, číslo účtu	Jméno, příjmení, telefonní číslo, email	Údaje z evidence obyvatel a mzdové agendy	Jméno, příjmení, datum narození, bydliště	Jmenné, adresní, datum narození, kontaktní údaje
Zvláštní kategorie osobních údajů	NE	NE	NE	NE	NE
Správce	Obec	Obec	Obec	Obec	Obec
Zpracovatel	Obec	Obec	Obec	Obec	Obec
Subjekt údajů = osoba, jejíž osobní údaje jsou zpracovávány	Smluvní strana	Občan - samostatná působnost	Dodavatelé, odběratelé, občané	Občan, dodavatel	Odesílatel a adresát zásilek
Právní základ zpracování osobních údajů	Smlouva	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti
Účel nakládání s osobními údaji	Plnění smlouvy	Veřejná informovanost občanů	Zákon č. 563/1991 Sb., o účetnictví a prováděcí vyhláška 410/2009 Sb	Zákon č. 132/2006 Sb., o kronikách obcí	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
Kategorie příjemců	Starosta, účetní, nemovitosti - KÚ, místostarosta, audit, geodet, stavební úřad, zastupitelé	Starosta, účetní, místostarosta	Strukturované GORDIC - moduly a Spisová služba, nestrukturované PC u účetní	Kronikář	Účetní, starosta, místostarosta
Kategorie příjemců mimo EU	NE	NE	NE	NE	NE
Doba uložení osobních údajů pro potřeby Správce OÚ	A10, V5, A5	NE	S5, A10, V10, V20, S10	NE	A50, A5, V5
Využívání spolupráce s externím příjemcem	NE	ANO	ANO	NE	ANO
Způsob kontroly zprac. OÚ	Kontrola třetí stranou - audit, kontr. výbor - veřejnopr. Sml.	NE	Audit Olomouckého kraje, finanční výbor	Zastupitelstvo	Kontrola třetí stranou - státní archiv

Oblast zpracování osobních údajů	Správní rozhodnutí	Knihovna	Zápisy ze ZO a jiných veřejných projednávání a jednání výborů	Střet zájmů a majetková přiznání	Legalizace a vidimace
Osobní údaje	Jméno, příjmení, bydliště, datum narození	Jméno, příjmení, bydliště, podpis	Jméno, příjmení, bydliště, věk	Jméno, příjmení, adresa, datum narození, kontaktní údaje	Jméno, příjmení, datum narození, místo narození, č. průk. totožnosti, podpis
Zvláštní kategorie osobních údajů	NE	NE	NE	NE	NE
Správce	Obec	Obec	Obec	Obec	Obec
Zpracovatel	Obec	Obec	Obec	Obec	Obec
Subjekt údajů = osoba, jejíž os. údaje jsou zpracovávány	Občan, fyzická osoba bez trv. bydliště v obci	Občan	Účastníci jednání	Žadatelé - starosta, místostarosta	Žadatel
Právní základ zpracování osobních údajů	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti	Plnění právní povinnosti
Účel nakládání s osobními údaji	Zákon č. 500/2004 Sb., správní řád	Zákon č. 257/2001 Sb., o knihovnách	Zákon č. 128/2000 Sb., o obcích	Zákon č. 159/2006 Sb., o střetu zájmů a zákon č.106/1999 Sb., o svobodném přístupu k informacím	Zákon č. 21/2006 Sb. o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu
Kategorie příjemců	Účetní, starosta, místostarosta	Knihovnice	Starosta, místostarosta, zapisovatel, ověřovatelé	starosta, místostarosta	Účetní, starosta
Kategorie příjemců mimo EU	NE	NE	NE	NE	NE
Doba uložení osobních údajů pro potřeby Správce OÚ	Dle jednot. agend, na které dopadá spr. řízení	V5	A/10	Elektronicky neomezeně, listinně 5 let	S10
Využívání spolupráce s externím příjemcem	ANO	NE	NE	ANO	NE
Způsob kontroly zpracování OÚ	Kontrola třetí stanou - Krajský úřad	Kontrola třetí stranou - centrální knihovna	Audit OK, MV	NE	ORP , kraj

Oblast zpracování osobních údajů	Evidence čísla popisného	Vítání občánků	Jubilea	Úřední deska
Osobní údaje	Jméno, příjmení, bydliště	Jméno, příjmení, adresa rodičů, jméno, příjmení, datum narození dítěte	Jméno, příjmení, adresa, datum narození	Jméno, příjmení, bydliště, datum narození
Zvláštní kategorie osobních údajů	NE	NE	NE	NE
Správce	Obec	Obec	Obec	Obec
Zpracovatel	Obec	Obec	Obec	Obec
Subjekt údajů = osoba, jejíž osobní údaje jsou zpracovávány	Žadatel	Občan obce	Občan obce	Občan, fyzická osoba bez trvalého bydliště v obci
Právní základ zpracování osobních údajů	Plnění právní povinnosti	Plnění veřejného zájmu, souhlas	Plnění veřejného zájmu, souhlas	Plnění právní povinnost
Účel nakládání s osobními údaji	Zákon č.128/2000 Sb., o obcích, vyhláška č. 326/2000 Sb.	Zákon č.128/2000 Sb., o obcích: §36a ve spojení s §149a	Zákon č.128/2000 Sb., o obcích: §36a ve spojení s §149a	Zákon č.128/2000 Sb., o obcích, zákon č. 500/2004 Sb., správní řád
Kategorie příjemců	Účetní, starosta, místostarosta, stavební úřad	Účetní, starostka, místostarosta, předsedkyně kulturní komise	Účetní, starosta, místostarosta	Občané
Kategorie příjemců mimo EU	NE	NE	NE	NE
Doba uložení osobních údajů pro potřeby Správce OÚ	A/5	NE	NE	Podle oblasti agendy
Využívání spolupráce s externím příjemcem	NE	NE	NE	NE
Způsob kontroly zprac. OU	NE	NE	NE	Audit OK, MV