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

Martina Capitová

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:	**Martina Capitová**
Osobní číslo:	**L16013**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Řízení procesů na malé obci s ohledem na novou právní úpravu ochrany osobních údajů**

Zásady pro vypracování:

1. **Zpracujte literární rešerši o řízení procesu vybrané organizace v rozsahu nařízení GDPR.**
2. **Analyzujte rizika zpracovávání osobních údajů ve vybrané organizaci veřejné správy.**
3. **Navrhněte možnosti ošetření rizik vedoucí k efektivnímu řízení procesů ve vybrané organizaci.**

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 978-80-7488-241-8.

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

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: Martina Capitová

.....
podpis studenta

ABSTRAKT

Cílem bakalářské práce je navrhnout opatření na zavedení souladu s všeobecným nařízením o ochraně osobních údajů. Práce je rozdělena na teoretickou a praktickou část. Teoretická část se zabývá podstatou legislativy GDPR. Cílem praktické části je aplikovatelnost principů GDPR v rámci organizace.

Výsledkem bakalářské práce jsou mimo implementační opatření na zavedení souladu s GDPR i směrnice organizace, která stanovuje a upravuje pravidla a principy pro všechny zaměstnance organizace tak, aby vše bylo uskutečňováno v souladu s GDPR.

Klíčová slova: GAP analýza, GDPR, ochrana osobních údajů, risk

ABSTRACT

The aim of the bachelor thesis is to propose measures to introduce compliance with the general regulation on the protection of personal data. The thesis is divided into theoretical and practical part. The theoretical part deals with the substance of GDPR legislation. The aim of the practical part is the applicability of GDPR principles within the organization.

Out of the implementation measures, the result of the bachelor thesis is the introduction of compliance with GDPR and the organization's guidelines that set and regulate rules and principles for all employees of the organization so that everything is done in accordance with the GDPR.

Keywords: GAP analysis, GDPR, protection of personal data, risks

Poděkování:
Ráda bych poděkovala paní Ing. Slavomíře Vargové, PhD., jakožto vedoucí mé bakalářské práce za cenné rady a připomínky ke struktuře a obsahu bakalářské práce a za podporu a ochotu v průběhu jejího vytváření a vypracování.
Mé velké poděkování patří také rodině za poskytnutou podporu během celého studia a pomoc s péčí o naše dva syny, abychom si s manželem mohli rozšířit své znalosti.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Na dynamický rozvoj společnosti v oblasti problematiky osobních údajů Evropská unie zareagovala Nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, kterým se zrušuje směrnice 95/46/ES.

Nařízení o ochraně osobních údajů, pojmenované jako GDPR (Generel Data Protection Regulation), je novou právní normou ochrany osobních údajů platný na celém území Evropské unie platný od 25. května 2018. Téměř 18 let platil v ČR zákon č. 101/2000 Sb., o ochraně osobních údajů. Cílem je zvýšit ochranu soukromí jednotlivce ve veřejném prostoru.

Nástup rychlého rozvoje informačních technologií a aplikací, které využívají osobní data jednotlivce vytvářejí již delší dobu fakticky nekontrolovatelné hromadění soukromých dat a informací v rukách nejen státních ale i soukromých, většinou marketingových subjektů. Osobní údaje vytvářejí ekonomickou hodnotu pro digitální trh, zejména pak pro online platformy jako vyhledávače, sociální sítě, online videa apod.

GDPR vzniklo v důsledku vzrůstajícího počtu zneužívání osobních údajů. Uživatelům byla tímto nařízením umožněna kontrola nad tím, jak jsou jejich údaje shromažďovány, ukládány a využívány. Lidé se mylně domnívají, že jejich osobní údaje zadávané online jsou v bezpečí. Citlivé údaje častokrát bez zaváhání zveřejňujeme a poskytujeme poskytovatelům služeb, aniž bychom věnovali zvýšenou pozornost tomu, jak citlivé informace o své osobě sdělujeme.

Dnešní uspěchaná je důkazem toho, že se mohou osobní údaje vymknout kontrole jakýmkoliv způsobem, aniž bychom si uvědomovali. Jejich ztrátu či zneužití začínáme řešit většinou až když se začne týkat naší osoby. Z tohoto důvodu byla nařízena Evropskou unií právní úprava na ochranu osobních údajů.

Veřejná správa osobní údaje zpracovává dnes a denně. Otázkou je, nakolik je nutné a potřebné v rámci výkonu veřejné správy osobní údaje sbírat, uchovávat, nebo je zveřejňovat.

Ochrana osobních údajů není žádnou novinkou, nicméně naléhavost problému si žádá jistá nová opatření, která zabrání jejich zneužití nesprávnými osobami.

I. TEORETICKÁ ČÁST

1 TERMINOLOGICKÝ SLOVNÍK

V následující kapitole jsou uvedeny základní pojmy, které jsou součástí nové právní normy pro ochranu osobních údajů v EU.

GDPR – (General Data Protection Regulation), *„obecné nařízení o ochraně osobních údajů, plným názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, (dále jen nařízení), představuje právní rámec ochrany osobních údajů platný na celém území Evropské unie, který hájí práva jejich občanů proti neoprávněnému zacházení s jejich daty a osobními údaji“*. [1]

Obecné nařízení – nový právní rámec ochrany osobních údajů v evropském prostoru, platný od 25. května 2018 přímo stanovující pravidla pro zpracování osobních údajů. V českém právním prostředí tak nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. [1], [9]

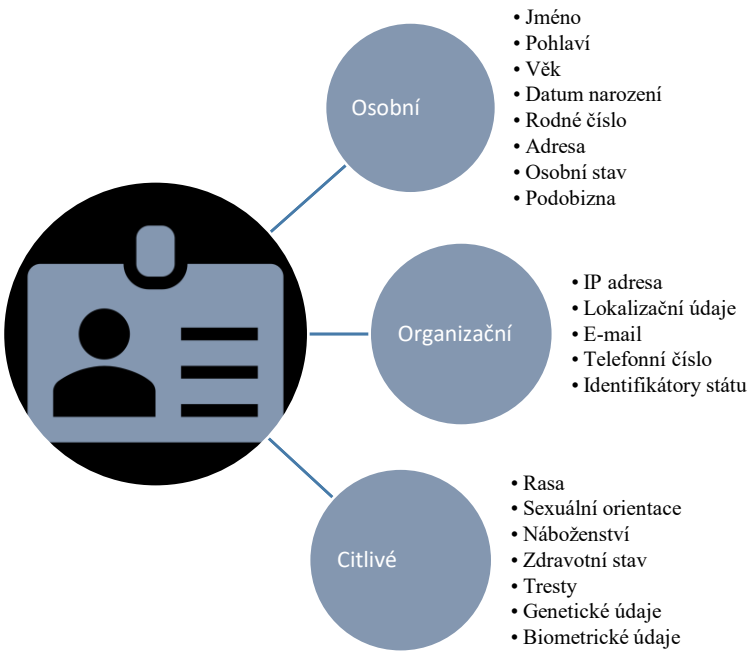
Zpracování osobních údajů – *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“*. [2]

Osobní údaj – *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určité identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*. [2]

Organizační údaj – jsou například emailová adresa, telefonní číslo, identifikační údaje vydané státem. [4]

Citlivý údaj – *„zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob“*. [2]

Na obrázku č. 1 je znázorněno rozdělení údajů.



Obrázek č. 1 Rozdělení údajů, [3]

Subjekt údajů – fyzická osoba, které se osobní údaj týká. Subjekt údajů není právnická osoba. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě. [1]

Správce – *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti, ale může je zpracovávat i pro vlastní potřebu“.* [1], [2]

Zpracovatel – *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatel je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Zpracovatel se liší od správce tím, že v rámci činnosti pro správce může provádět takové zpracovatelské operace, kterými jej správce pověří a vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen“.* [1], [2]

2 PRÁVNÍ DŮVODY PRO VZNIK PRÁVNÍ ÚPRAVY

„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 známé pod zkratkou GDPR (General Data Protection Regulation)“, upřesňuje platná pravidla pro práci s osobními údaji. [7]

2.1 Důvody pro vznik nové právní úpravy

Mezi pádné důvody, proč hledat nová opatření, která zabezpečí a zvýší ochranu soukromí jedince, se rozmohlo s rychlým rozvojem informačních technologií a aplikací, které vyžadují data jedince. Nepřeberné množství soukromých dat a informací ve státních i soukromých sférách, a hlavně u marketingových subjektů.

Je nutné si uvědomit, že ochrana osobních údajů má ve společnosti svá opodstatnění. Již od narození nás obklopují různá data, která identifikují naši osobu. Údaj, kterým je jméno a příjmení, datum narození, národnost, zdravotní stav nebo náboženské vyznání. Informace jsou tak křehké, že jejich zneužití by mohlo jedinci značně znepříjemnit život. [6]

2.2 Porovnání nové a dosavadní právní úpravy

Obecné nařízení s sebou přináší oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů změny, které mají své procesy, týkající se zpracovávání osobních údajů. Avšak z mého pohledu si myslím, že subjekty, které doposud zpracovávaly osobní údaje v souladu splatným zákonem, by s implementací neměly mít výraznější komplikace. [9]

Porovnáním Obecného nařízení o ochraně osobních údajů z roku 1995 lze zjistit následující hlavní rozdíly:

- Posílení působnosti.
- Posílení ochrany dětí.
- Posílení informačních povinností správců.
- Posílení některých práv subjektů údajů. [8]

2.3 Nově upravené a hlavní změny

Mezi nové úpravy a změny patří:

- Právo být zapomenut, dle čl. 17. [7]
- Právo na přenositelnost osobních údajů, dle čl. 20. [7]
- Podrobná úprava vztahu správce a zpracovatele.

- Posílení kontroly nad správci mimo území EU.
- Posílení řady požadavků na správce a zpracovatele, včetně hodnocení dopadů na soukromí a předběžných konzultací s dozorovým orgánem.
- Upuštění od notifikace všech nových zpracování osobních údajů dozorovanému orgánu.
- Posílení pravidel o zabezpečení dat a hlášení narušení bezpečnosti osobních dat.
- Podrobná úprava instrumentů soft law (kodexy chování, certifikace).
- Zásadní sjednocení pravomocí dozorových úřadů.
- Podrobná úprava spolupráce dozorových úřadů.
- Zcela nová a principiálně nevyzkoušená úprava společného rozhodování dozorových úřadů v různých typech přeshraničních případů.
- Zavedení rozhodovací pravomoci pro Evropský dozorový úřad v konkrétních věcech.
- Sjednocení prostředků pro soudní ochranu před rozhodnutím či nečinností dozorového úřadu a pro soudní ochranu před nezákonným zpracováním, včetně náhrady škody.
- Sjednocení a zásadní zvýšení sankcí formou 2 % nebo dokonce 4 % podílu ročního globálního obratu podnikatele nebo absolutní částkou 20 mil. eur pro všechny ostatní.
- Sektorové úpravy pro smíření práva na ochranu údajů se svobodou projevu, s přístupem k úředním dokumentům, pro národní identifikační čísla, pro zaměstnanecké vztahy. [8]

Naopak nařízení od platné směrnice v zásadě přebírá nebo jen upravuje – většinu hlavních definic (osobní údaj, citlivé údaje, správce, koncept souhlasu atd.), většinu zásad ochrany osobních údajů (principy a zákonnost zpracování), většinu práv subjektů údajů a základních povinností správců, systém opt-out z přímého marketingu, koncept bariéry u přenosů do třetích zemí s důslednými restrikcemi a požadavky na ochranu osobních údajů, zásadní prvky postavení nezávislých dozorových úřadů, koncept výjimek pro privilegovaná zpracování (archivní, statistická, vědecká, historická), koncept výjimek pro ochranu veřejných zájmů (bezpečnost, ekonomika, ochrana práv jiných atd.). [8]

Srovnání úprav mezi zákonem o ochraně osobních údajů a požadavky GDPR je uveden v následující tabulce č. 1.

Tabulka č. 1 Srovnání právní úpravy zákona o ochraně osobních údajů s GDPR, [9], [18]

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Osobní údaje – *„jakákoliv informace týkající určeného nebo určitelné fyzické osoby, jestliže ji lze přímo či nepřímo identifikovat zejména základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“.*	**Osobní údaje** – *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.*
Citlivý údaj – *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě fyzické osoby a genetický údaj fyzické osoby; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci fyzické osoby“.*	**Citlivé údaje** – *„jsou speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob“.*
Anonymní údaj – *„takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určené nebo určitelné fyzické osobě“.*	GDPR se nevztahuje na anonymní data.
Oznamovací povinnost – *„ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů před zpracováním osobních údajů“.*	Tato povinnost bude zrušena.
Likvidace osobních údajů – *„správce, nebo na základě jeho pokynu, zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti fyzické osoby“.*	**Právo být zapomenut** – *„subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se dané fyzické osoby týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat“.*
Přístup subjektu údajů k informacím – *„požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat“.*	**Právo na přístup** – *„fyzická osoba má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům“.*
Ochrana práv subjektu údajů – je-li žádost fyzické osoby shledána oprávněnou, správce nebo	**Právo na opravu** – *„fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se jí týkají. S přihlédnutím k účelům zpracování má fyzická osoba práva na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení“.*
Toto právo není v zákoně upraveno.	**Právo na přenositelnost údajů** – *„fyzická osoba má právo získat osobní údaje, které se jí týkají, jež poskytla správci ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil“.*

Tabulka č. 2 Srovnání právní úpravy zákona o ochraně osobních údajů s GDPR, (pokračování tabulky), [9], [18]

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Tato povinnost není v zákoně upravena.	**Posuzování vlivu na ochranu osobních údajů** – *„pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro právo a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení“.*
Tato povinnost není v zákoně upravena	**Pověřenec pro ochranu osobních údajů** – *„správce a zpracovatel jmenují pověřence pro ochranu osobních údajů“.*
Tento časový údaj není v zákoně uveden.	**Porušení ochrany dat** – *„jakékoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu“.*
Sankce – max. do výše 10 000 000 Kč.	**Sankce** – *„10 000 000 EUR nebo do výše 2 % celkového ročného obratu celosvětově za předchozí finanční rok, 20 000 000 EUR nebo do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok“.*

Jak již bylo uvedeno v tabulce č. 1 GDPR je postaveno na pilířích, (Obrázek č. 2)

Obrázek č. 2 Pilíře GDPR, [5]

3 PROBLEMATIKA GDPR V KONTEXTU ORGANIZACE

Postupy a mechanismy, které slouží k ochraně osobních údajů jsou postupně upravovány. Obce jsou povinny přijímat taková opatření, aby bylo s osobními údaji zacházeno v souladu s GDPR. Žádná organizace není stejná, i když se jedná o obecní či městské úřady, školy a školky. Každá organizace má své vlastní zázemí, software, hardware, dodavatele, současně s tím i obsluhující procesy, které se navzájem odlišují. Jediné, co může mít mezi sebou podobné vazby, jsou stanoveny zákonem stanovené agendy a činnosti, naprosto unikátní je samotný způsob zpracování činnosti. [11]

3.1 Zásady dodržování GDPR

Dle čl. 10 odst. 3 Listiny základních práv a svobod má *„každý právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“.* [12]

Zásady zpracování osobních údajů můžeme označit jako stavební kameny, na nichž je celé nařízení postaveno. Zásady zpracování, kterými jsou zákonnost, korektnost, transparentnost, omezení účelu, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost. Principem odpovědnosti správce je dodržení zásad při zpracování. [6]

3.1.1 Zásada zákonitosti

Je považována za nejdůležitější zásadu, protože vyjadřuje tezi, že správce osobních údajů může osobní údaje k určitému účelu zpracovávat pouze tehdy, má-li k takovému zpracování alespoň jeden právní důvod. Právní důvod představuje právním řádem předpokládané oprávnění zpracovávat osobní údaje ze strany správce za určitým legitimním účelem. Pokud u zpracování osobních údajů nastane absence právního důvodu takového zpracování, vzniká povinnost osobní údaje zlikvidovat. [6]

3.1.2 Zásada korektnosti a zásada transparentnosti

Korektností se rozumí popis zpracování, ke kterému dal souhlas subjekt údajů, a transparentností je chápáno, zda zpracování údajů odpovídá tomu, co jedinec odsouhlasil.

Zásady spravedlivého a transparentního zpracování vyžadují, aby byl subjekt informován o probíhající operaci zpracování a jejich účelech. Správce by měl poskytnout veškeré další informace potřebné pro zajištění spravedlivého a transparentního zpracování, s přihlédnutím ke kontrolním okolnostem a kontextu, v němž jsou osobní údaje zpracovávány. [1], [7]

3.1.3 Zásada omezení účelu

Osobní údaje musí být shromažďovány ve formě, která umožňuje identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje je možné uložit i po delší dobu, pokud jsou zpracovávány výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. To vše za předpokladu provedení příslušných technických a organizačních opatřeních požadovaných tímto nařízením s cílem zaručit práva a svobody subjektům údajů. [6]

3.1.4 Zásada minimalizace údajů

Zásada minimalizace údajů představuje povinnost zpracovávat osobní údaje pouze přiměřené, relevantní a omezené. Tato zásada brání správci, aby v souvislosti se stanoveným legitimním účelem požadoval po subjektu údajů více údajů, než je nezbytně nutné. Zároveň lze tuto zásadu považovat i jako bezpečnostní prvek, protože čím méně je osobních údajů zpracováno, tím hrozí subjektu údajů menší riziko v případě jejich úniku. [6]

3.1.5 Zásada přesnosti

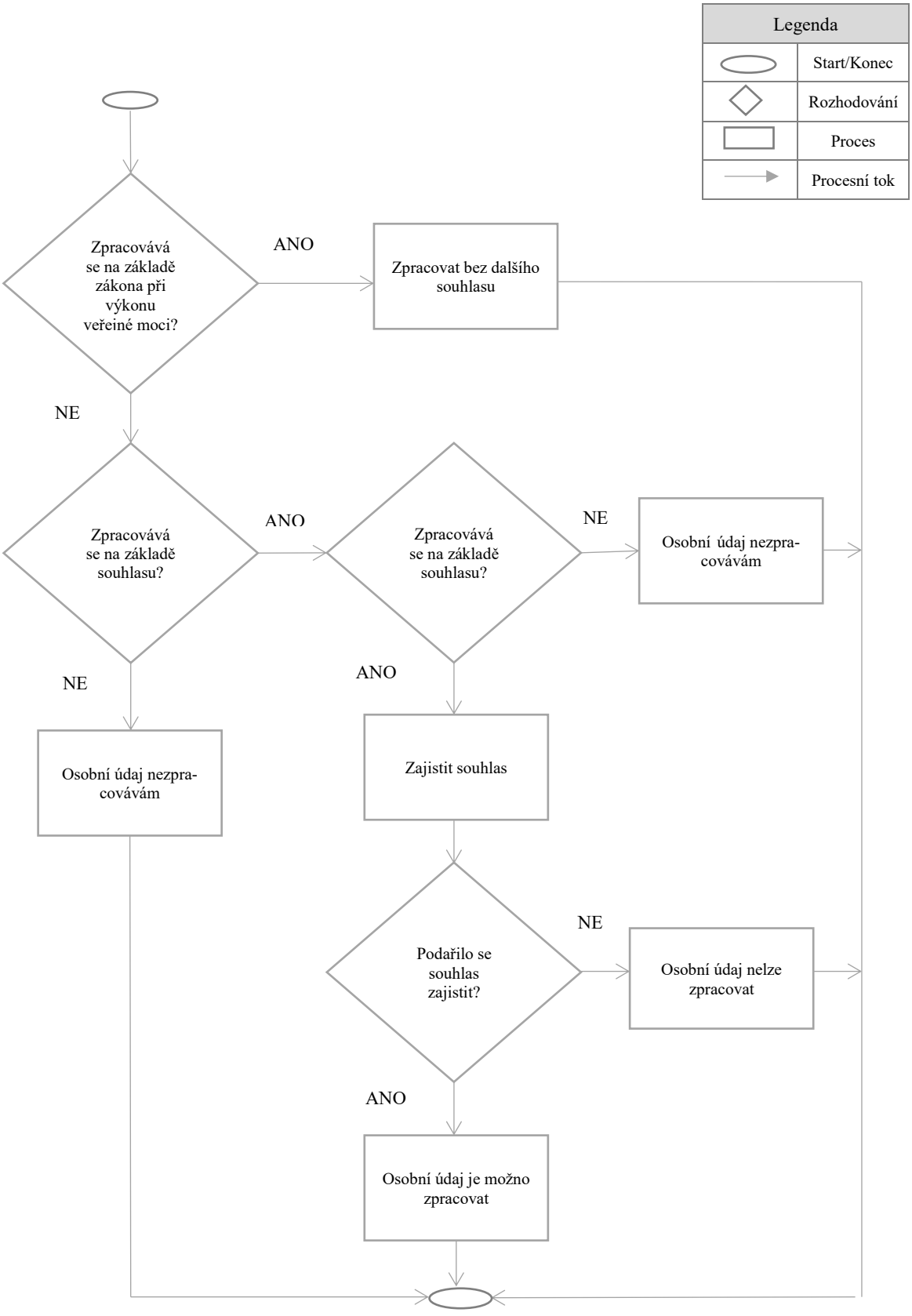
Provádí především právo na opravu a doplnění. *„Subjekt má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelu zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení“.* [7]

3.1.6 Zásada omezení uložení

„Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů po dobu delší, než je nezbytně nutné pro účely, pro které jsou zpracovávány“. Jinými slovy jde o vyjádření povinnosti zlikvidovat osobní údaje, pokud pomine účel zpracování, což je jedna ze skutečností, která podle čl. 17 odst. 1 písm. a) Obecného nařízení zakládá právo subjektu údajů, aby byly jeho osobní údaje správcem vymazány. [6], [7]

3.1.7 Zásada integrity a důvěrnosti

Zpracované osobní údaje by měly být dostatečně zabezpečeny, a to prostřednictvím vhodných technických nebo organizačních opatření chránících je před neoprávněným či protiprávním zpracováním před náhodnou ztrátou, zničením, nebo poškozením. Jedná se o vyjádření požadavku na zajištění důvěrnosti a integrity systému. Zabezpečení osobních údajů při zpracování musí odpovídat povaze, rozsahu, kontextu a účelům zpracování. [6], [7]



Obrázek č. 3 Postup při zpracování osobního údaje, [24]

3.2 Pověřenec pro ochranu osobních údajů

Hlavním úkolem pověřence je být nápomocný správcům při dosažení souladu se zpracováním osobních údajů, chránit práva a svobody subjektu údajů. Pověřenec působí jako kontaktní místo současně pro subjekt údajů tak i pro dozorový úřad. [6]

Povinnost jmenovat pověřence nemají všechny subjekty, které zpracovávají osobní údaje. Tato povinnost dle čl. 37 odst. 1 nařízení vzniká ve třech případech:

- pokud je zpracování provedeno orgánem veřejné moci či veřejným subjektem, výjimku tvoří soudy, které jednají v rozsahu svých pravomocí,
- jestliže hlavní činnosti správců nebo zpracovatelů jsou založeny na operacích zpracovávání, které vyžadují obsáhlé pravidelné a systematické monitorování subjektů údajů,
- jestliže hlavní činnosti správce a zpracovatele spočívají ve zpracování zvláštních kategorií údajů nebo osobních údajů, které se týkají rozsudků v trestních věcech a trestných činů. [7], [8]

Nařízením není stanovena přesná kvalifikace pověřence, jmenován je na základě získaných profesních kvalit, odborných znalostí z práva a praxe v oblasti ochrany osobních údajů, schopnosti plnit úkoly ze čl. 39 nařízení. [7]

Pověřenec by měl mít dobré znalosti k provádění operací zpracovávání jako i informačních systémů, bezpečnosti dat a správcových potřeb v oblasti ochrany osobních údajů. U orgánu veřejné moci nebo veřejného subjektu musí být pověřenec obeznámen s administrativními pravidly a postupy dané organizace. [8]

Postavení pověřence v organizaci musí provázet zajištění nezbytných podmínek dle požadavku obecného nařízení, jako jsou zajištění nezávislosti, zamezení střetu zájmu, zabezpečení dostatečných zdrojů pro výkon funkce. [14]

Zajištění nezávislosti znamená, že pověřenec musí mít přístup k nejvyššímu vedení obce, neměl by být mimo výkon pověřence pověřován k výkonu úkolů v jiné agendě, kde by mohl být ovlivněn účel zpracování osobních údajů. Pověřenec musí být v každém případě nezávislý a nesmí být ve střetu zájmů. Měl by mu být umožněn přístup ke všem zdrojům informací, které potřebuje pro výkon své agendy.

Zamezení střetu zájmu je zásadním požadavkem při výkonu pověřence. Pověřenec se v procesu plnění svých úkolů, které jsou mu uloženy, nesmí dostat do situace, kdy může přímo ovlivnit účel zpracování osobních údajů.

Zabezpečení dostatečných zdrojů pro výkon funkce je v povinnosti organizace, která pověřence jmenovala, ať už se týká zajištění pracovního prostředí, personálu, mzdy, dostatečná časová dotace. [14]

3.3 Úkoly pověřence

K hlavním úkolům pověřence patří:

- Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, jejichž činnost souvisí se zpracováním a povinnostmi souvisejícími s ochranou osobních údajů.
- Monitorování souladu s nařízením, s koncepcí správce a zpracovatele, včetně rozdělení odpovědnosti, zvyšování podvědomí a odborné přípravy pracovníků podílejících se na operacích zpracování a souvisejících auditů.
- Poskytování informací na požádání, jestliže se jedná o posouzení vlivu na ochranu osobních údajů a monitorování.
- Spolupráce s dozorovým úřadem, které se týkají zpracování. [7]

3.4 Práva subjektů údajů

Práva subjektů údajů jsou rozdělitelná na dvě skupiny. První skupinou jsou práva, která jsou aplikovatelná automaticky, a není nutné jejich vyžádání ze strany subjektu údajů. Druhou skupinou jsou práva, která jsou uplatnitelná pouze na žádost subjektu údajů. [14]

3.4.1 Právo automaticky uplatnitelné

Mezi uplatnitelné právo subjektů patří:

- Právo na informace o zpracování osobních údajů.
- Právo nebýt předmětem automatizovaného rozhodnutí založeného na profilování.
- Právo na výmaz.
- Právo obrátit se na pověřence.
- Právo na poskytnutí svobodného souhlasu se zpracováním osobních údajů a jeho odvolání.
- Právo na opravu nebo aktualizaci údajů. [14]

3.4.2 Právo subjektu údajů na žádost

Mezi právo na žádost subjektu patří:

- Právo získat od správce osobních údajů potvrzení o zpracování údajů.
- Právo na přístup subjektu ke svým osobním údajům.
- Právo získat kopii zpracovávaných osobních údajů.
- Právo na omezení zpracování.
- Právo na přenositelnost údajů.
- Právo vznést námitku. [14]

3.5 Povinnosti správců a zpracovatelů údajů

Mezi základní povinnosti patří:

- Povinnost vést záznamy o činnostech zpracování.
- Povinnost zajistit odpovídající zabezpečení osobních údajů.
- Povinnost ohlašovat bezpečnostní incidenty na poli ochrany osobních údajů.
- Povinnost provést posouzení vlivu na ochranu osobních údajů.
- Povinnost realizovat předchozí konzultace s dozorovým úřadem.
- Povinnost jmenovat pověřence pro ochranu osobních údajů. [14]

3.6 Sankce

Úřad pro ochranu osobních údajů zůstává nadále dozorovým orgánem. Účelem hrozby sankce je donutit adresáty chovat se podle normou stanovených pravidel. Obecné nařízení v čl. 83 stanovuje podmínky pro ukládání pokut, včetně jejich možné výše. [6]

Sankce jsou rozděleny do dvou kategorií, a to dle **výše sankce a dopadu porušení**. Přehledy výše sankcí za porušení povinností jsou uvedeny v tabulce č. 2 a 3. Společně pro obě kategorie platí, že pokud správce nebo zpracovatel u stejných nebo souvisejících operací zpracování poruší více ustanovení obecného nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení. [6]

Pokuty ukládané veřejné moci a veřejným subjektům, plynou zpravidla z veřejných rozpočtů a bylo by neúčelné ponechat pro tyto subjekty nejvyšší možnou výši pokuty. [6]

Dozorový úřad může při rozhodování, zda uložit pokutu a v jaké výši přihlédnout k následujícím okolnostem:

- povaze, závažnostem a délce trvání porušení s přihlédnutím k povaze, rozsahu nebo účelu dotčeného zpracování, jakož i k počtu dotřených subjektů údajů a míře škody, jež jim byla způsobena;
- zda k poručení došlo úmyslně nebo z nedbalosti;
- jaké byly podniknuty kroky ke zmírnění škod způsobených subjektům údajů;
- jaká je míra odpovědnosti správce či zpracovatele s přihlédnutém k technickým a organizačním opatřením;
- předchozí porušení správcem či uživatelem;
- způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel poručení oznámil;
- dodržování schválených kodexů chování. [6]

Tabulka č. 3 Sankce ve výši 10 000 000 EUR, [1]

10 000 000 EUR nebo, jde-li o podnik, 2 % celkového ročního celosvětového obratu za porušení	
Správce a tam, kde připadá v úvahu i zpracovatel	Povinnosti při zabezpečení ochrany osobních údajů.
	Podmínek pro najmutí a spolupráci se zpracovatelem.
	Povinnosti vyhotovit záznamy o činnostech zpracování.
	Povinnosti spolupráce s dozorovým úřadem.
	Povinnosti při ohlašování.
	Povinnosti týkající se jmenování a podmínek pověřence.
	Povinnosti ustanovit zástupce pro správce nebo zpracovatele usídleného mimo Evropskou unii.
	Povinnosti týkající se činnosti při získávání osvědčení.

Tabulka č. 4 Sankce ve výši 20 000 000 EUR, [1]

20 000 000 EUR nebo, jde-li o podnik, 4 % celkového ročního celosvětového obratu za porušení	
Správce tam, kde připadá v úvahu i zpracovatel	Zásad a zákonnosti zpracování.
	Podmínek vyjádření souhlasu.
	Podmínek pro zpracování zvláštní kategorie osobních údajů.
	Práv subjektu údajů.
	Podmínek pro předávání osobních údajů do třetí země.
	Povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které Obecné nařízení umožňuje upravit na vnitrostátní úrovni.
	Povinnost splnit příkaz nebo dočasné či trvalé omezení nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 Obecného nařízení nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1 Obecného nařízení.
	Nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 Obecného nařízení nebo neposkytnutí přístupu při uplatnění dozorové pravomoci.

4 OBEC

Obecní zřízení je upraveno zákonem č. 128/2000 Sb., Zákon o obcích, (dále jen zákon o obcích), který definuje obec *„jako základní územní samosprávné společenství občanů. Obec tvoří územní celek, který je vymezen hranicí území obce. Obec je veřejnou korporací, má vlastní majetek, vystupuje v právních vztazích svým jménem a nese odpovědnost z těchto vztahů vyplývající, pečuje o všestranný rozvoj svého území a o potřeby svých občanů; při plnění svých úkolů chrání taktéž veřejný zájem“.* [13]

4.1 Evidence obce

K tomu, aby obec efektivně plnila svou povinnost v samostatné i přenesené působnosti, potřebuje pro svojí každodenní činnost nezbytnou evidenci; tu tvoří například zvláštní předpisy, jako je Zákon zákoník práce, č. 89/2012 Sb., zákon. č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, Zákon občanský zákoník, č. 262/2006 Sb., Zákon o zaměstnanosti č 435/2004 Sb., Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání, č. 561/2004 Sb.

Obec nadále vykonává činnosti, při kterých dochází ke zpracování osobních údajů, nejen v přímé souvislosti s výkonem samostatné nebo přenesené působnosti, ale rovněž např. z pozice zaměstnavatele nebo účastníka smlouvy.

Obec může být jak správcem, tak zpracovatelem osobních údajů. Správcem je v případě, kdy sama určuje účely a prostředky zpracování osobních údajů, pokud jsou udávány zákonem. Zpracovatelem je v situaci, kdy provádí činnosti zpracování pro jiného správce, kdy může být definován přímo zákone. [11]

4.1.1 Uveřejňování dokumentů

Z každodenní zkušenosti s výkonem veřejné správy a ve spojitosti s tím i s ochrannou osobních údajů, lze říci, že problematika zajištění ochrany osobních údajů je každodenní rutinou. [14]

Obec při zpracování dokumentů musí některé dokumenty uveřejňovat na základě různých typů povinností. V případě, že dokumenty obsahují osobní údaje, je vždy nutné posoudit, zda se povinnost uveřejnění vztahuje také na osobní údaje, které dokument obsahuje, a to z hlediska GDPR i souvisejících právních předpisů. Jestliže obec nazná, že uveřejnění osobních údajů není možné, je důležité, aby přijala odpovídající technická opatření, která umožní uveřejnění dokumentů, aniž by docházelo k uveřejnění osobních údajů. [11]

4.1.2 Registr smluv

Obec je povinna v rámci své činnosti uveřejňovat různé dokumenty, které mohou obsahovat osobní údaje. Taková povinnost je uložena zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.
Zákonným požadavkem uveřejnění prostřednictvím registru smluv podle zákona o registru smluv je identifikace smluvních stran. Jako je jméno, příjmení a IČO fyzické osoby jako smluvní strany. [16]

4.1.3 Pořizování a zveřejňování obrazových a zvukových záznamů ze zasedání zastupitelstva obce a zápisů ze zasedání zastupitelstva

Pořízení, uchování a zveřejnění zvukového nebo audiovizuálního záznamu z jednání zastupitelstva obce lze považovat za zpracování osobních údajů tehdy, pokud obsahuje informace týkající se identifikované nebo identifikovatelné fyzické osoby. [11]

Dle stanoviska Úřadu pro ochranu osobních údajů lze identifikovat dva účely zpracování. Prvním účelem je pořízení záznamu jako podkladu pro pozdější vyhotovení zápisu ze zasedání zastupitelstva a druhým účelem je informovanost veřejnosti o činnosti obce a zastupitelstva, prostřednictvím zveřejnění na internetových stránkách obce. [17]

Obec nesmí v uveřejňovaných zvukových či audiovizuálních záznamech ze zastupitelstva ani v zápisech ze zasedání zastupitelstva uvádět osobní údaje o třetích osobách, jejichž záležitosti jsou na zasedání zastupitelstva projednávány. Tato povinnost se nevztahuje na osobní údaje členů zastupitelstva i jiných úředních osob, dále i na osobní údaje osob, které se aktivně vyjadřují na zastupitelstvech k projednávaným věcem. [11]

V souvislosti s prováděnými úkony veřejné správy je důležité nalézt a zabezpečit takové místo pro uchovávání dat, které bude schopné pojmout velké množství dat uchovaných v nejrůznějších rejstřících a databázích veřejné správy. Z hlediska uchovávání osobních údajů není podstatné, zda je nosič informací vlastnictvím správce nebo zda jej zajišťuje zpracovatel nebo osoba jiná. Dá se předpokládat, že s rozvojem cloudů, tedy sdílených datových úložišť, ve kterých si jednotlivé subjekty pouze pronajímají část prostoru pro svá data, se stále častěji budeme setkávat se situací, kdy správce bude mít osobní údaje uložené u někoho dalšího. [14]

5 PROJEKT IMPLEMENTACE GDPR DO ORGANIZACE

Prvním krokem je seznámení se s obsahem a požadavky, které GDPR na organizaci klade v oblasti ochrany osobních dat. Následným krokem je vstupní analýza, jejímž úkolem je popis aktuálního stavu ochrany osobních údajů v organizaci, který poukáže na rozdíly z běžné praxe a procesů aktuálně běžících v organizaci oproti požadavkům legislativy. [1]

5.1 GAP analýza

Cílem analýzy je nalezení nesrovnalostí mezi cíli dosažitelnými a požadovanými. Zaměřuje se také na prozkoumání a odkrytí příležitostí.

Je technika, která se používá k definování rozdílu mezi stavem současným a stavem požadovaným. Technika se zaměřuje na:

- procesy organizace, zapojená oddělení,
- využívané osobní údaje,
- aplikace technických a organizačních opatření zaměřených na ochranu informací,
- dokumentace organizace a její využívání,
- výcvik a podvědomí pracovníků. [25]

Moment, kde chceme být, jasně stanoví pravidla daná nařízením. To, kde jsme, záleží především na organizaci samotné. Organizace, které implementovaly do svých procesů požadavky zákona č. 101/2000 Sb., o ochraně osobních údajů, tak v nařízení vnímá spíše jako evoluci. [1], [9]

Cílem analýzy je zjistit:

- kde jsou v organizaci sběrné uzly osobních dat;
- jaká je jejich struktura;
- pomocí jakých nástrojů;
- zjistit formální obsah;
- způsob získání souhlasu ke zpracování osobních dat;
- kdo má přístup k datům;
- na základě jakého oprávnění;
- jak jsou data uchovávána a chráněna;
- v jakých systémech a aplikacích se s daty pracuje;
- v jakých procesech data figurují a jak probíhá jejich zpracování;
- zda jsou formy a procesy v souladu s nařízením GDPR;

- kontrola smluvních závazků týkajících se osobních dat;
- vazby a smlouvy třetích stran;
- přístup k hodnocení dopadu na soukromí;
- proces řízení incidentů a schopnost reagovat;
- návrhy a doporučení v případě nesouladu s nařízením. [1]

5.1.1 Výstup GAP analýzy

Souhrnná zpráva by měla přehledně obsahovat zjištěné nálezy a doporučení. Zpráva umožní organizaci identifikovat rizika a problémy, které vyžadují řešení. Na základě výsledků lze stanovit pořadí, v jakém bude docházet k nápravě jednotlivých požadavků na dodržení GDPR. Zpráva poukazuje na úroveň zabezpečení IT systémů, jelikož mnoho dat se nachází v digitální podobě. Organizace, které přistoupily k implementaci zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen zákon o kybernetické bezpečnosti) nebo ISO normy 27001 - Systém řízení bezpečnosti informací, která definuje požadavky na systém managementu bezpečnosti informací, měly situaci ulehčenou. [1], [28]

5.1.2 Postup při GAP analýze

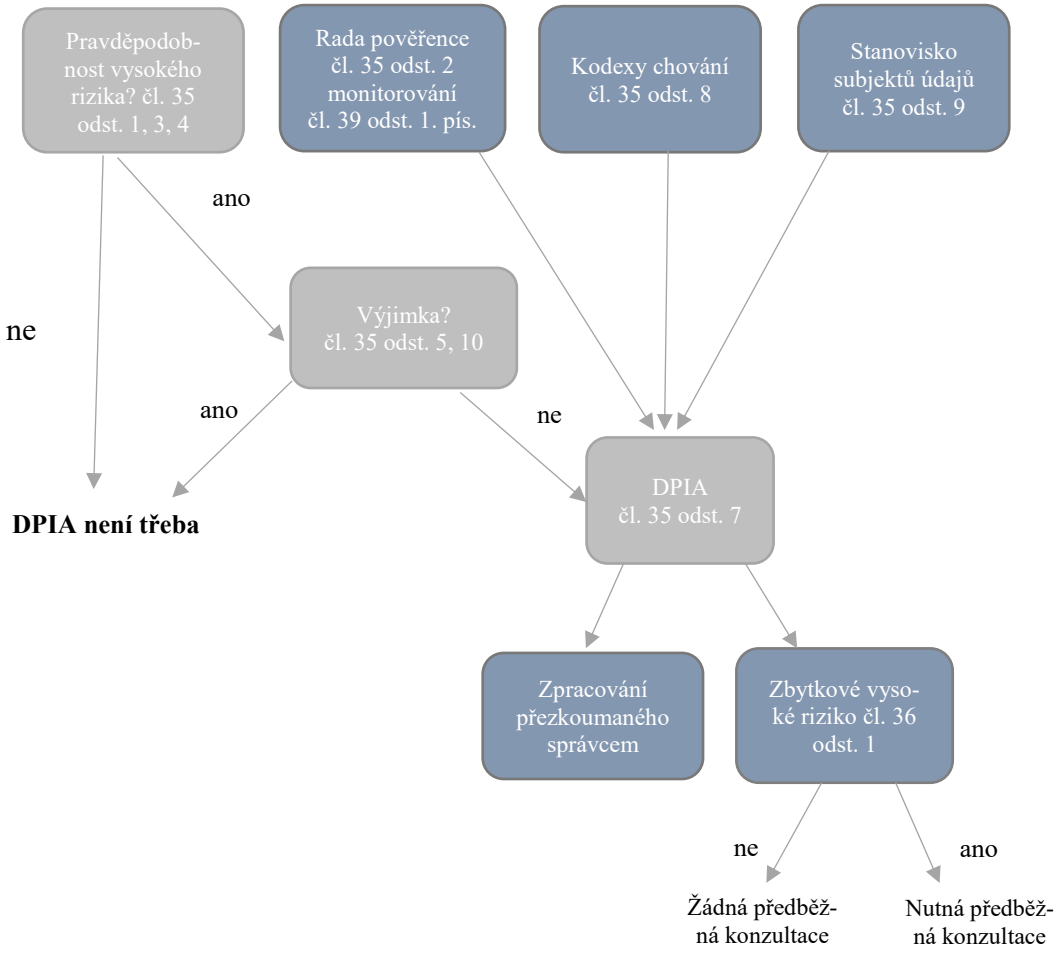
Prvním krokem je zajistit angažovanost vedení organizace, bez které by bylo nemožné dosáhnout relevantních výsledků analýzy. Druhým krokem je získat data o jednotlivých uzlech zpracování osobních údajů, jedná se tedy o místa, kde jsou osobní data shromažďována a vstupují do organizace. Takovým místem může být online formulář na webu, vyplnění dotazníku u personalisty, podaná žádost na svoz komunálního odpadu. Pokud jsou v organizaci identifikovány uzly sběru osobních údajů, je nutné vytvořit jejich přehledný seznam, včetně odpovědných osob. Následně je provedena identifikace jednotlivých zpracování, formulář je uveden jako příloha práce P I. Třetím krokem je popsání bezpečnosti dat v organizaci, jak v listinné, tak v digitální podobě. V souvislosti s analýzou směrnic vztahujících se ke skartaci, nakládání s osobními a citlivými údaji, směrnice o archivaci, směrnice na vyřizování dotazů zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Následným krokem je provedení analýzy o posouzení vlivu na ochranu osobních údajů (DPIA). [1]

5.2 Posouzení vlivu na ochranu osobních údajů (DPIA)

DPIA (Data Protection Impact Assessment) je proces, jehož cílem je popsat zpracování, posoudit nezbytnost a přiměřenost zpracování a napomoci zvládnutí rizik pro práva a svobody fyzických osob vyplývající ze zpracování osobních údajů. [1]

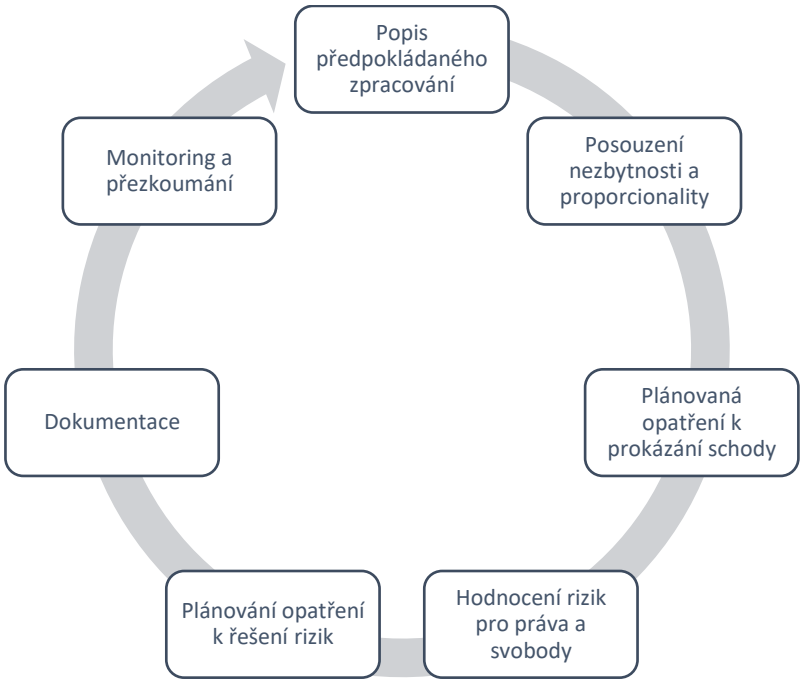
Organizace na základě sestavení DPIA identifikuje a zhodnocuje rizika a hrozby plynoucí ze zpracování osobních údajů pro subjekty. Ustanovení souvisí s požadavkem GDPR na minimalizaci zpracovaných dat, během analýzy DPIA se může ukázat, že některá data jsou pro účel zpracování zbytečná. [1]

Za zmínění stojí, že analýzu není nutné provádět ve všech případech. Je povinná pouze v případech, že existuje pravděpodobnost, že zpracování přinese vysoké riziko a ohrozí tím práva a svobody fyzických osob. Obecné nařízení klade důraz zejména na situace, kdy se zavádí v organizaci nové technologie nebo nový způsob zpracování dat. O tom, jestli organizace použije nebo nepoužije DPIA analýzu, může rozhodnout následující obrázek č. 1. [1]



Obrázek č. 4 Posouzení vlivu na ochranu osobních údajů (DPIA), [1]

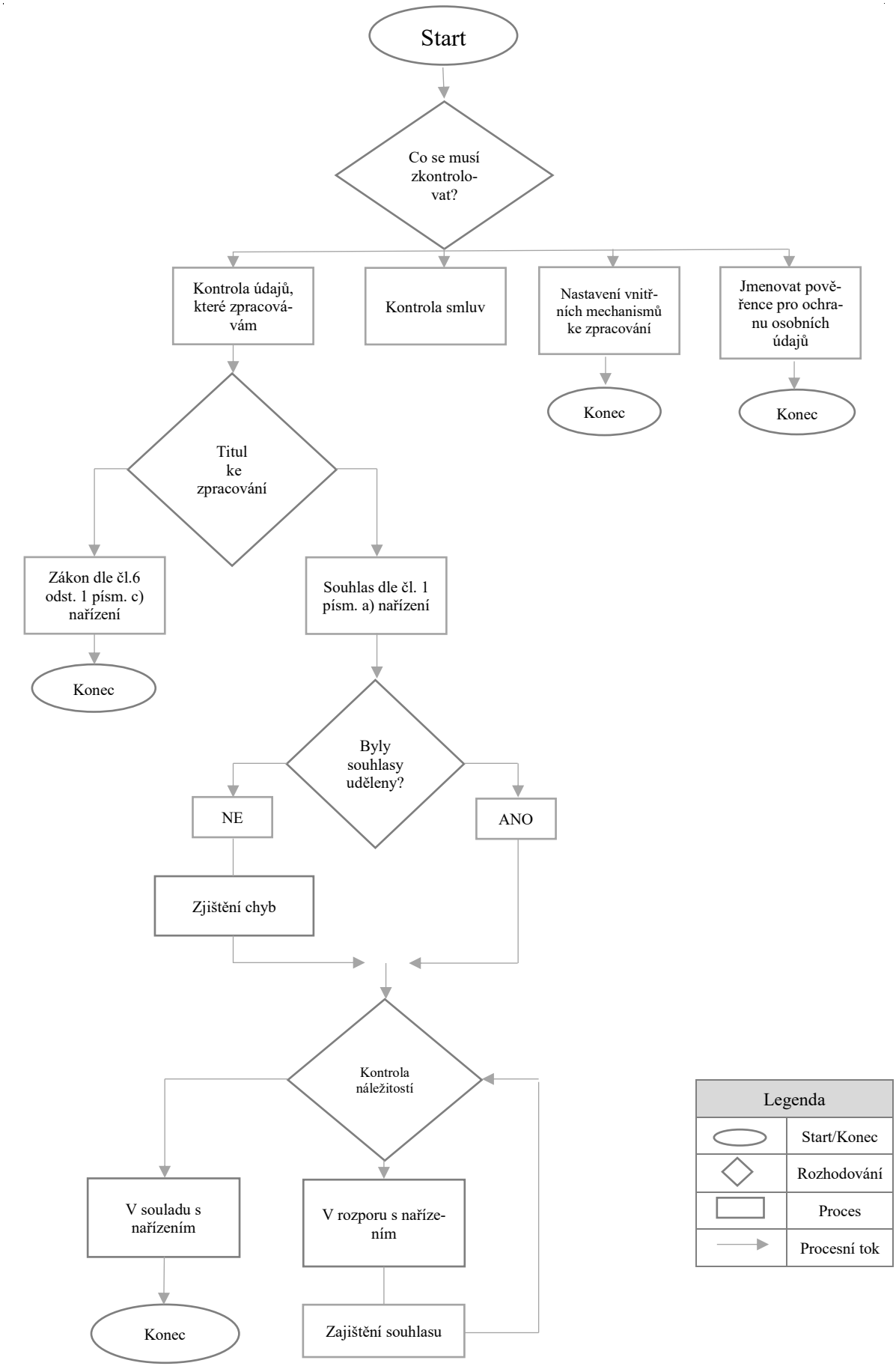
Postup provedení posouzení vlivu popisuje následující obrázek z výkladových stanovisek WP29.



Obrázek č. 5 Opakovací proces provádění DPIA, [1]

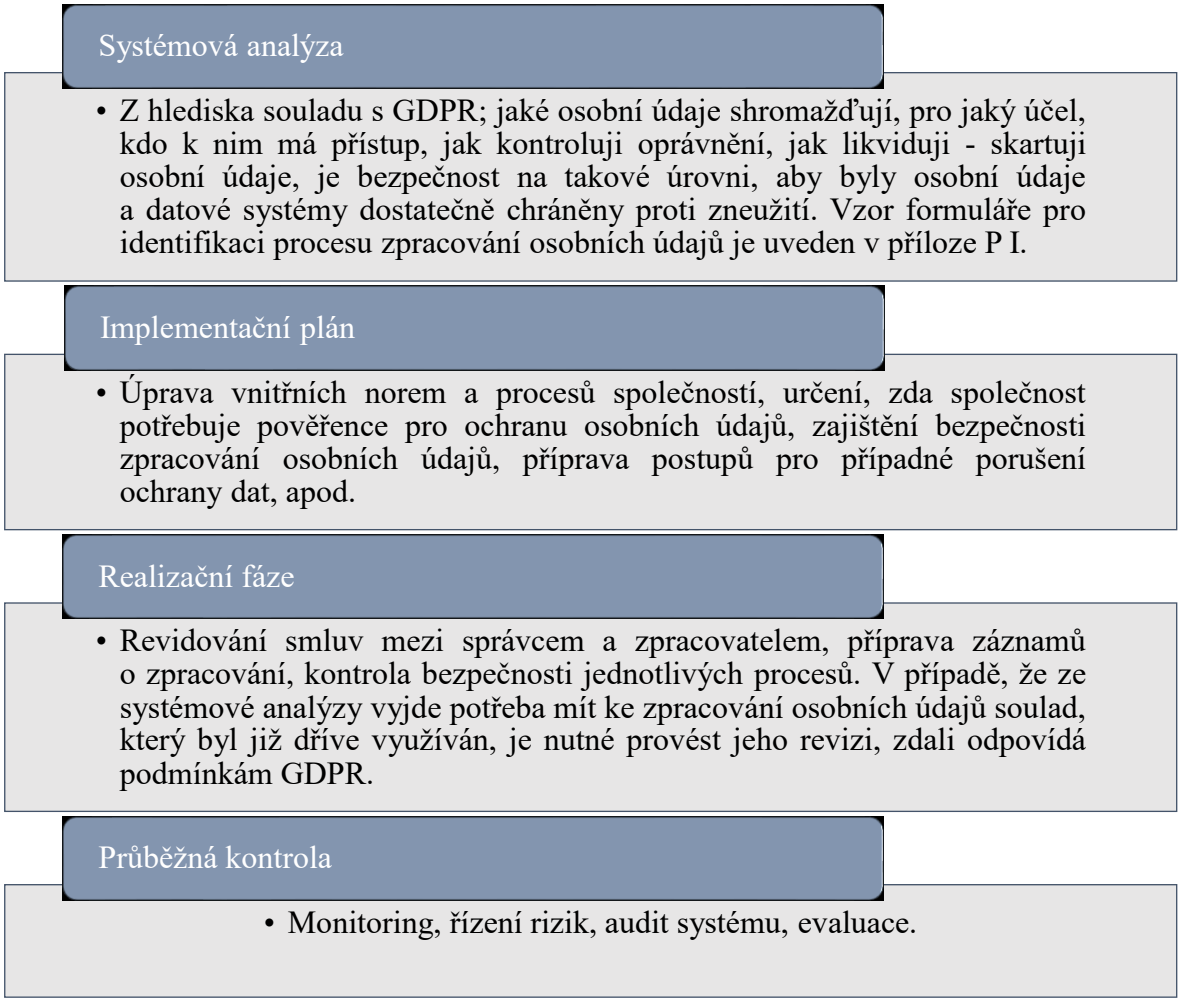
WP29 je pracovní skupina složená z vedoucích zástupců dozorových úřadů členských zemí EU. Mezi její činnosti, které patří mimo jiné posuzování otázek týkajících se uplatňování vnitrostátních předpisů přijatých k provedení směrnice 95/46/ES. Pracovní skupina WP29 může z vlastního podnětu podat doporučení k jakékoliv otázce týkající se ochrany osob v souvislosti se zpracováním osobních údajů. Výstupem veřejnosti jsou stanoviska a doporučení této pracovní skupiny, která obsahují postupy pro správce a zpracovatele. [1]

Následují obrázek č. 6 v rámci implementace GDPR do organizace poukazuje na náležitosti, kterým je nutné věnovat pozornost.



Obrázek č. 6 Čemu je nutné věnovat pozornost, [24]

Každá organizace musí ochraňovat osobní údaje, které zpracovává, proto je přípravu na GDPR rozdělit na několik etap. Přehlednější popis implementace je uveden na obrázku č. 7.



Obrázek č. 7 Etapy GDPR, [26]

Jak vyplývá z obrázku č. 7 etapy pro přípravu na GDPR lze rozdělit do čtyř fází – systémové analýzy, implementačního plánu, realizační fáze a průběžné kontroly v rámci, které se provádí řízení a kontrola rizika.

Řízení rizik je popsáno v následující kapitole.

6 MANAGEMENT RIZIK

Management rizik je soustavná a opakující se činnost zaměřená na analýzu a snížení rizika, pomocí různých metod a technik, jehož cílem je řídit potenciální rizika, omezit tak pravděpodobnost jejich výskytu nebo snížit jeho dopad na organizaci a její cíle. Tato kapitola je zaměřena na riziko a seznámení se s procesem managementu rizik. [19]

6.1 Definice rizika

Riziko je nejistá událost nebo podmínka, která pokud nastane, má negativní vliv na dosažení cíle projektu a ostatní aktiva. Je nutné ho chápat jako konkrétní událost v krizovém scénáři a vždy se posuzuje v celém kontextu. Samotná spouštěcí událost, která pokud by nastala, způsobí popsaný nechtěný nebo vynucený děj s popsanými dopady na cíl projektu a další aktiva, způsobující danou škodu. Pojetí rizika prošlo určitým vývojem, nejčastěji převažovalo chápání rizika jako určitého nebezpečí. [21], [22]

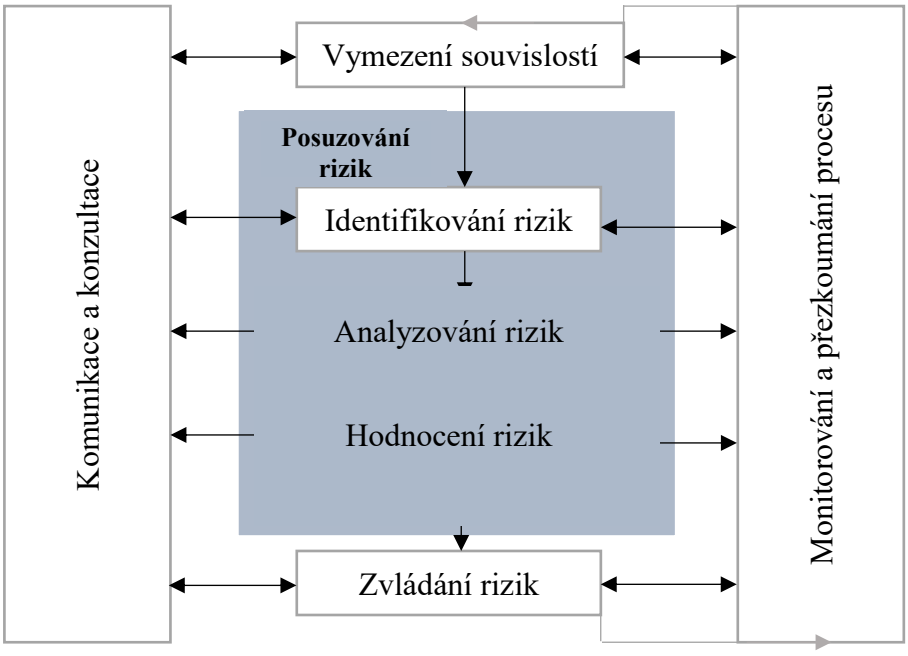
Rizika členíme následně podle jejich věcné náplně:

- **Technicko-technologická** – spojená s aplikací výsledků vědecko-technického rozvoje vedoucí k neúspěchu vývoje nových výrobků a technologií, nezvládnutí technologického procesu. [20], [21]
- **Výrobní** – mající často charakter omezenosti, případně nedostatku zdrojů různé povahy (suroviny, materiál, energie, pracovní síly, kvalifikace). [20], [21]
- **Ekonomická** – zahrnují širokou škálu nákladových rizik, jsou vyvolány růstem cen surovin, materiálu, energií, služeb. Tato rizika mohou zapříčinit překročení plánované výše nákladů. [20], [21]
- **Tržní** – jsou spojena s úspěšností výrobku nebo služeb na domácím i zahraničním trhu. Mají převážně podobu rizika prodejního ve vztahu k velikosti prodeje a rizika cenového z hlediska dosahovaných prodejních cen. [20], [21]
- **Finanční** – jsou závislá na způsobu financování, s dostupností zdrojů financování a schopnosti dostát svým závazkům, s výší úrokových sazeb a změnami měnových kurzů. [20], [21]
- **Legislativní** – jsou rizika vyvolané hospodářskou a legislativní vládou. Např. změny daňových zákonů, zákonů o ochraně životního prostředí, změny celní politiky, změny rozpočtové a investiční politiky aj. [20], [21]

- **Politická** – zahrnuje stávky, rasové a národnostní nepokoje, války, teroristické útoky aj. Uvedené příklady jsou zdrojem politické nestability a změn politického systému. [20], [21]
- **Environmentální** – mohou mít podobu nákladů na odstranění škod na životním prostředí, nákladů spojených se zpřísněným opatřením na ochranu životního prostředí, daní spojených s využíváním neobnovitelných zdrojů aj. [20], [21]
- **Rizika spojení s lidským činitelem** – jedná se především o rizika managementu, která je jedním z rozhodujících faktorů úspěšnosti organizace. Další rizikový faktor ze zmíněné kategorie je ztráta klíčového pracovníka, podvodné či nezákonné jednání zaměstnanců, stávky, sabotáže. [20], [21]
- **Informační** – týkají se informačních systémů a dat. Jejich nedostatečné zabezpečení může být zneužito interními či externími subjekty. [20], [21]
- **Zásahy vyšších mocí** – spojené s riziky havárií výrobních zařízení a nebezpečných živelných pohrom různého druhu, např. požáry, zemětřesení, výbuchy, sopečné výbuchy, rizika teroristických útoků aj. [20], [21]

6.2 Proces managementu rizik

Rámec managementu je souborem prvků poskytující základy a organizační uspořádání pro navrhování, implementování, monitorování, přezkoumání a neustálé zlepšování managementu rizik v celé organizaci. [23]



Obrázek č. 7 Proces managementu rizik, [23]

6.3 Stanovení kontextu

Při stanovení kontextu se vymezí základní parametry pro řízení rizika a nastaví se rozsah platnosti a kritéria pro zbytek procesu. V úvahu jsou brány vnitřní a vnější parametry, které se týkají organizace jako celku a stejně jako podklady k posuzovaným rizikům. [23]

Postup stanovení kontextu:

- stanovení vnějšího kontextu,
- stanovení vnitřního kontextu,
- stanovení kontextu procesu managementu rizik,
- vymezení kritérií rizika. [23]

6.4 Posuzování rizik

Posuzování rizik slouží k pochopení rizik, jejich příčin, následků a pravděpodobností. Posuzování rizik zahrnuje identifikace, analýzu a hodnocení rizik. [23]

6.4.1 Identifikace rizik

Identifikace je proces nalezení, rozpoznání a zaznamenávání rizik. Účelem je zjistit, co by se mohlo stát nebo jaké by mohly nastat situace a zda by mohly mít dopad na dosažení cílů organizace. [23]

6.4.2 Analýza rizik

Analýza rizik se týká rozvíjení a chápání rizika. Poskytuje vstup do hodnocení rizik a rozhodnutí o tom, zda je rizika třeba ošetřit a o tom, které strategie a metody ošetření jsou nejvhodnější. [23]

Do analýzy rizik patří určení následků a jejich pravděpodobnostní pro identifikované události rizika. Následky a jejich pravděpodobnost jsou potom zkombinovány za účelem stanovení úrovně rizika. [23]

6.4.3 Hodnocení rizik

Do procesu hodnocení rizik je zahrnuto srovnání odhadovaných úrovní rizika s kritérii stanovenými při stanovení kontextu. Využívá se pochopení rizika získaného během analýzy rizik za účelem rozhodnutí o budoucích zásazích na ošetření tohoto rizika. [23]

6.4.4 Volba technik posuzování rizik

Posuzování rizik používá nejrůznější metody pro identifikaci, analýzu a hodnocení rizik. Realizace posouzení rizik je možná na různém stupni hloubky a podrobností a za použití jedné nebo mnoha metod. Volbu přístupu k posuzování rizik ovlivňují faktory jako dostupnost zdrojů, povaha a stupeň nejistoty a složitost aplikace. [23]

6.5 Ošetření rizika

Po skončení fáze posuzování rizik přichází na řadu fáze ošetření rizik. V této fázi dochází k zahrnutí volby a odsouhlasení jedné nebo více variant, jak by se dalo změnit pravděpodobnost výskytu a důsledku rizik. Po ošetření rizika nastupuje opakující se proces posuzování nové úrovně rizika. [23]

6.6 Monitorování a přezkoumávání

Monitorování rizik a přezkoumání rizik zahrnuje audity stavu rizik, které slouží k včasné detekci chyb zpracování procesu řízení rizik a pro včasnou identifikaci nezvládání rizik.

Účelem procesu monitorování a přezkoumávání je:

- sledování interních a externích změn, které mají dopad na projekt,
- identifikace nových rizik,
- ověření, že řízení rizik je účinné a efektivní,
- zvýšení úrovně řízení rizik využitím informací z průběhu projektu,
- poučení se z událostí, změn, trendů, úspěchu a chyb na projektu. [22]

6.7 Komunikace a konzultace

Komunikace a konzultace se všemi zainteresovanými stranami na projektu ať již s vnitřními nebo vnějšími probíhá v průběhu celého procesu řízení rizik a má být plánovaná a řízená.

Účelem procesu komunikace je:

- zajištění včasných, přesných a nezkreslených informací o rizicích na projektu,
- sjednocení pohledu na rizika a nastavení spolupráce mezi zainteresovanými stranami,
- minimalizace scénáře, kdy bude projekt negativně ovlivněn neidentifikovatelnými riziky některé ze zainteresovaných stran. [22]

„Řízení rizik je prováděno s cílem určit vhodná technická a organizační opatření, která je nezbytné zavést pro zajištění bezpečnosti osobních údajů při jejich zpracování a pro zmírnění nebo eliminaci rizik. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob“. [7]

Management organizace může vnímat hodnocení rizika jako obtěžující a zbytečné, pouze z pocitu splnění povinnosti dochází k nevhodně zhodnocenému riziku. Zodpovědně provedená analýza rizik může posloužit jako stavební kámen bezpečnosti. Podcenění a neuváženost při zhodnocení rizik může organizaci přivodit značné problémy. [1]

7 CÍL A METODY ZPRACOVÁNÍ BAKALÁŘSKÉ PRÁCE

Hlavním cílem této práce je identifikace a analýza rizik v souladu doporučeními GDPR.
V rámci teoretické části byla sumarizována problematika GDPR na obecné právní úrovni. Tento teoretický základ je vstupem pro zpracování praktické části. Na základě výsledků analýzy rizik byly stanoveny problematické oblasti z hlediska organizačního a technického opatření. [11]

Pro účely bakalářské práce byly stanoveny následující tři cíle:

- Zpracovat literární rešerši o řízení procesu vybrané organizace v rozsahu nařízení GDPR.
- Analyzovat rizika zpracování osobních údajů ve vybrané organizaci veřejné správy.
- Navrhnout možnosti ošetření rizik vedoucí k efektivnímu řízení procesů ve vybrané organizaci.

Při zpracování bakalářské práce je využito zejména vícezdrojového sběru informací z odborné literatury a webových stránek.
Dále jsou v práci využity metody identifikace, analýza, vyhodnocení a aplikace. Pro identifikaci rizik ohrožující interní a externí prostředí organizace jsou prostřednictvím GAP analýzy identifikovány potenciální hrozby a pro analyzování jednotlivých rizik, je zvolena „Jednoduchá bodová kvantitativní metoda PZH“.

II. PRAKTICKÁ ČÁST

8 CHARAKTERISTIKA VYBRANÉ OBCE S OHLEDEM NA GDPR

Následující kapitola pojednává o analyzované obci. Je zde uveden popis a charakteristika posuzovaného objektu.

8.1 Představení a historie obce

Obec jejíž analýzou současného stavu se práce bude se nachází v okrese Vyškov v nadmořské výšce 260 m n.m.

První písemné zmínění o obci pochází z roku 1497. Rozloha katastrálního území je 1802 ha. V katastrálním území se nachází zaniklá středověká obec. Jedná se o naleziště viditelných zbytků základů 22 domů středověké vesnice s kostelem a tvrzí, ve které byla nalezena pec na pálení výrobků z hlíny. V současné době je v obci přihlášeno 830 obyvatel.

V posledních letech zaznamenala obec opětovný nárůst obyvatel.

8.2 Charakteristika posuzovaného subjektu – obecní úřad

Struktura úřadu a personální zajištění

- Pracovníci zařazení do obecního úřadu.
- Pracovníci obce, kteří v rámci své činnosti zpracovávají osobní údaje.

Organizační složky zřizované obcí

Obec je zřizovatelem Mateřská škola a Základní škola, pečovatelské služby, místní knihovny a jednotky sboru dobrovolných hasičů.

Technické zabezpečení úřadu

Obecní úřad je dvoupodlažní budova v řadové zástavbě se dvěma vchody, které jsou zabezpečeny dveřmi s běžným zámkem FAB. Kromě kanceláří obecního úřadu se v 1. NP nachází prostory kulturního domu, do kterých je přístup umožněn samostatným vchodem.

Jednotlivé kanceláře obecního úřadu jsou zabezpečeny elektronickým zabezpečovacím systémem v rámci jedné zóny. Informace o poplachu jsou odesílány prostřednictvím SMS zprávy na mobilní telefon starosty a místostarosty. Dodavatelem systému, jsou prováděny pravidelné revize. Zaměstnanci obecního úřadu mají k dispozici vlastní přístupové kódy k elektronickému zabezpečovacímu systému. Vede se jednoduchá evidence přístupových kódů a jejich uživatelů.

Každému zaměstnanci obecního úřadu je přidělen osobní svazek klíčů, který obsahuje klíč od vstupu do budovy a vstup do vlastní kanceláře. Klíče od zbývajících prostor jsou jednotlivě označeny a uloženy v uzamčené skříňce v kanceláři podatelny.

8.3 Vnitřní předpis

Vnitřní předpis je prvním dokumentem organizace, který upravuje tvorbu, zpracování a nakládání s daty a stejně tak i s uchováním dokumentů. Předpis slouží pro uchování informací a dokumentů a týká se jak organizace, tak i zaměstnanců.

Součástí vnitřního předpisu je definice základních pojmů, jako jsou data, dokumenty, jaký je postup zpracování, jaký dokument je považován za písemnost, co je spisová služba, postup ukládání dokumentu do systému spisové služby.

Další část se věnuje obecným zásadám tvorby, zpracování dat a dokumentů a nakládání s nimi.

8.4 Směrnice pro zpracování osobních údajů dle GDPR

Součástí směrnice je legislativní vymezení pravidel k ochraně osobních údajů. Směrnice slouží ke správné aplikaci ochrany fyzických osob a jejich soukromí v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů v naší organizaci. A následně bylo dosaženo požadované ochrany údajů fyzických osob (zaměstnanců, žáků, uchazečů o zaměstnání, současných i budoucích obchodních partnerů a dalších osob), jejichž údaje získává naše organizace při své činnosti. Následuje soupis základních pojmů a zásad zpracování údajů a zákonnost zpracování, zpracování zvláštních kategorií osobních údajů, evidenci a způsob zpracování, a přijetí technických, organizačních a procesních opatření.

Listinná uložiště obsahující osobní údaje

Obec nedisponuje pokročilou technologií zabezpečení listinných úložišť, jako jsou bezpečnostní dveře, interní kamerové systémy, docházkové systémy pro sledování do budovy s listinným úložištěm. Listinná uložiště jsou umístěna v uzamykatelných místnostech nebo skříních.

Interní akty řízení a dokumentace

- Pracovní řád.
- Spisový a skartační řád.
- Směrnice k ochraně osobních údajů.
- Organizační řád.
- Směrnice upravující povinnost zaměstnanců uchovávat mlčenlivost.

Pracovní smlouvy jsou vytvářeny účetní obce v ekonomickém systému KEO (Alis spol. s.r.o). Počítač je stejně jako přístup do systému Kompletní evidence obce (dále jen KEO) je chráněn přístupovým heslem. V listinné podobě jsou pracovní smlouvy uloženy pod zámkem v kanceláři účetní. Dokumenty personální agendy podepisuje starosta obce.

Elektronická úložiště

V prostorách obecního úřadu se nachází tři osobní počítače. Počítače jsou propojeny přes místní datovou síť, data jsou ukládána na vlastní disky počítačů. Zálohy programu provádí technik společnosti KEO minimálně jednou za čtvrtletí. Přístup do každého počítače je možný pouze po zadání přístupového hesla. Počítač starosty je navíc zabezpečen dalším přístupovým kódem. Počítače jsou chráněny antivirovým programem NODE 32.

Připojení k internetu je zajištěno poskytovatelem O_2 Czech Republic a.s. Služby IT jsou zajišťovány externě. Zároveň je využívaná technická podpora společnosti ALIS spol. s.r.o. Místní knihovna využívá vlastní informační systém pro evidenci knih – ARL klient. Notebook v knihovně je zabezpečen přístupovým heslem. Evidence čtenářů je zpracována pouze v papírové formě, a to v nezbytném rozsahu. Evidence je uschován a uzamčena v pracovním stole knihovnice.

Informační systémy a portály

Obec jejíž analýzou se zabývám disponuje těmito informačními systémy.

Tabulka č. 5 Informační systém spisové služby, [vlastní]

Název IS	FLEXI
Dodavatel	VERA, spol. s.r.o.
Umístění	Server OR, dálkový přístup – starosta, referentka
Úložiště	Datové uložiště na HW technologického centra, správce OPR
Zabezpečení	Ochrana přístupu uživatelským heslem, automatické odhlášení při nečinnosti.

Tabulka č. 6 Agendové informační systémy, [vlastní]

Název IS	KEO X Evidence obyvatel, Evidence hřbitovů
Dodavatel	ALIS spol. s.r.o.
Umístění	Osobní počítač účetní a referentka
Úložiště	Disk osobního počítače
Zabezpečení	Ochrana přístupu uživatelským heslem.

Tabulka č. 7 Ekonomický informační systém, [vlastní]

Název IS	KEO4 Účetnictví, Poplatky, Mzdy, Majetek
Dodavatel	ALIS spol. s.r.o.
Umístění	Osobní počítač účetní
Úložiště	Disk osobního počítače
Zabezpečení	Ochrana přístupu uživatelským heslem.

Tabulka č. 8 Geografický informační systém, [vlastní]

Název IS	G-view
Dodavatel	Ing. Svatopluk Sedláček
Umístění	Osobní počítač starosty
Úložiště	Disk osobního počítače
Zabezpečení	Přístup do systému není chráněn přístupovým heslem.

8.5 Pravidla práce s výpočetní technikou

Při práci s výpočetní technikou je nutné, aby uživatel dodržoval stanovené zásady práce s počítačovým vybavením. Jejichž hlavním cílem je ochrana uživatelů, počítačového vybavení, hardwaru i softwaru. V organizaci musí být pravidla zacházení s vybavením jasně dána a všichni uživatelé s nimi musí být řádně seznámeni.

Zřízení přístupových oprávnění

Uživatele počítačové sítě v rámci organizace jsou rozděleny s ohledem na své pracovní zařazení, pracovní náplň a také na zastávanou pozici v organizační struktuře. Na základě jednotlivého rozčlenění získávají uživatelé přístup do jednotlivých informačních systémů a příslušných pracovních adresářů na síťových discích. Správu uživatelských přístupů

o informačních systémech a mapování složek ukládání dokumentů zastává technik organizace. Povinností každého uživatele je mazat takové soubory, které vytvořil, ale již je nepotřebuje ke své činnosti a nadále je již nebude používat. Uživatel má povinnost ukládat soubory obsahující osobní údaje pouze do složek k tomuto účelu jsou zřízeny technikem.

Pravidla pro uživatelská jména a přístupová hesla

Všichni uživatelé mají přiděleno jedinečné uživatelské jméno a musí dodržovat následující pravidla pro uživatelské heslo:

- Nesdělovat žádné osobě své heslo a udržovat jej v maximální tajnosti.
- Heslo nezaznamenávat na žádné médium tak, aby se k němu mohla dostat jiná osoba.
- Měnit jej kdykoliv pokud dojde k jeho odtajnění nebo k podezření, že je s heslem obeznámena jiná osoba.
- Nesmí být založeno na skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních údajů.
- Heslo nedoplňovat v jakýchkoliv automatizovaných přihlášení.
- Po počtu dní, které je uvedeno ve směrnici pravidelně měnit heslo za nové.
- Nepoužívat uživatelské heslo v blízkosti jiné osoby tak, aby bylo možné odezírat toto heslo touto osobou.
- Pracoviště v kanceláři navrženo tak, aby nebylo možné nahlížet na zpracované informace cizím osobám, které nejsou oprávněny tyto informace vidět.

Administrátorský účet

Administrátorský účet nesmí být používán pro běžnou pracovní činnost. Názvy hlavních administrátorských účtů jsou spolu s hesly sepsány a uloženy u odpovědné osoby. V případě nutného zásahu na serveru v nepřítomnosti odpovědné osoby, může po schválení provést pomocí příslušného názvu administrátorského účtu a hesla pověřená osoba. O této skutečnosti musí být sepsán záznam.

8.6 Přístupová práva k souborům a adresářům na síťových discích

Jednotlivá pracoviště naší organizace mají svá vlastní přístupová oprávnění.

8.6.1 Zřízení přístupových oprávnění

Přístup je zřizován vždy pro konkrétního pracovníka s ohledem na jeho pracovní zařazení a pozici v organizační struktuře. Vedoucí pracovník zodpovídá za to, aby byl rozsah poskytnutého oprávnění v souladu s pracovním zařazením konkrétního zaměstnance.

8.6.2 Odebrání přístupových práv

Při změně pracovního zařazení, ukončení pracovního poměru či nástupu na mateřskou dovolenou apod. jsou všechna přístupová oprávnění a uživatelské účty zablokovány. Při zablokování účtu z důvodu ukončení pracovního poměru jsou účty zachovány pouze po dobu nezbytně nutnou, následně jsou zodpovědnou osobou zcela odstraněny.

9 POSOUZENÍ PROCESU NA MALÉ OBCI

Za pomocí GAP analýzy, byla ve spolupráci se zaměstnanci organizace vypracována na základě současného stavu identifikace potenciálních rizik.

Při analýze bylo prostředí organizace rozděleno na dvě základní oblasti:

- **interní prostředí**
- **externí prostředí**

V obou případech bylo snahou popsat co nejpravděpodobnější postupy a návyku při práci zaměstnanců. Na základě toho bylo možné identifikovat typy a zdroje osobních údajů, ke kterým mají přístupy zaměstnanci a zároveň identifikovat potenciální rizika, při kterých může dojít k jejich narušení.

9.1 GAP analýza

Základní zdroje a typy osobních údajů podle GAP analýzy jsou:

- Osobní údaje zaměstnanců;
- Osobní údaje uchazečů a zaměstnání;
- Multicash – bankovní údaje;
- Lokální server – sdílené dokumentů mezi zaměstnanci, které by mohly obsahovat ki osobní údaje osob cizích i jejich vlastních;
- Údaje o klientech v informačním systému;
- Adresát konkrétních údajů na osoby, se kterými zaměstnanci primárně komunikují.

Ke zhodnocení všech primárních rizik byly vybrány dvě kritéria, která se budou hodnotit:

- **Pravděpodobnost**
- **Následky**

Metoda, která bude použita k identifikaci rizik je z oblasti Risk managementu, známá jako řízení rizik. Identifikovaná rizika jsou umístěna na stupnici od 1 po 5, přičemž nejnižší pravděpodobnost výskytu rizika bude 5 – velmi vysoká, 4 – vysoká, 3 – střední, 2 – nízká, 1 – velmi nízká. Systém identifikace rizik bude shodný i pro následky. Výsledné hodnoty budou zaznamenány do matice rizik.

Závěr analýzy je znázorněný pomocí Matice řízení rizik, tak aby bylo čtenáři umožněno rychleji a jednoduše pochopit závěr analýzy. Matice rizik může mít různé podoby.

Identifikovaná rizika jsme umístili na stupnici od 1 do 5, přičemž v potaz se braly dvě základní kritéria a to pravděpodobnost, že riziko nastane a následky, které můžeme očekávat v případě, že riziko opravdu nastane. Nejnižší pravděpodobnost výskytu rizika byla 5 – velmi vysoká, 4 – vysoká, 3 – střední, 2 – nízká, 1 – velmi nízká. Stejným systémem byly znázorněny i následky.

9.1.1 Interní prostředí organizace – identifikovaná rizika

V rámci interního prostředí organizace byly zanalyzované následující oblasti následovného potenciálního rizika.

RIZIKO_1

Oblast: prostory/kanceláře

Riziko: neoprávněný vstup do prostoru a následné odcizení fyzických dokumentů, nacházejících se v prostoru kanceláře.

Opatření: umístění dokumentů v uzamykatelných skříních.

Pravděpodobnost: 2

Následky: 3

RIZIKO_2

Oblast: technické vybavení a jeho zabezpečení.

Riziko: krádež/ztráta/poškození notebooku

Opatření: zajištění nejvyššího zabezpečení ze strany zaměstnanců na základě vlastního vědomí a svědomí (např. uložením do uzamykatelného prostoru), zaměstnanec musí kontrolovat, zda má dostatečné přístupové zabezpečení.

Pravděpodobnost: 3

Následky: 2

RIZIKO_3

Oblast: technické vybavení a jeho zabezpečení.

Riziko: krádež/ztráta/poškození mobilních telefonů

Opatření: zajištění nejvyššího zabezpečení ze strany zaměstnanců na základě vlastního vědomí a svědomí (např. uložením do uzamykatelného prostoru), zaměstnanec musí kontrolovat, zda má dostatečné přístupové zabezpečení.

Pravděpodobnost: 3

Následky: 2

RIZIKO_4

Oblast: technické vybavení a jeho zabezpečení.

Riziko: krádež/ztráta/poškození lokálního disku.

Opatření: zajištění nejvyššího zabezpečení ze strany zaměstnanců na základě vlastního vědomí a svědomí (např. uložením do uzamykatelného prostoru), zaměstnanec musí kontrolovat, zda má dostatečné přístupové zabezpečení. Klíček od lokálního disku uchovávat mimo disk samotný a předáním zodpovědné osobě.

Pravděpodobnost: 2

Následky: 4

RIZIKO_5

Oblast: IT zabezpečení rámci interní komunikace.

Riziko: napadení PC virusem při nesprávném zacházení s internetem, externími disky apod.

Opatření: ujistit se, že všichni zaměstnanci mají nainstalovaný a aktualizovaný antivirový program. V případě, že tento není k dispozici, je nutné zajištění jeho koupě.

Další možné zásady lze navrhnout ve směrnici organizace.

Pravděpodobnost: 3

Následky: 2

RIZIKO_6

Oblast: nový zaměstnanec

Riziko: porušení bezpečnosti ochrany osobních údajů, a to z důvodu, porušení povinnosti zaměstnance zachovávat mlčenlivost.

Opatření: zabezpečit zodpovědnou osobou, aby byli nový pracovníci poučení v rámci směrnice upravující povinnost zaměstnance uchovávat mlčenlivost.

Pravděpodobnost: 3

Následky: 4

RIZIKO_7

Oblast: výběrové řízení

Riziko: riziko zneužití, ztráty či krádeže osobních údajů uchazeče.

Opatření: zavedení pokynu do směrnice jakým způsobem se s údaji nakládají ze strany zaměstnavatele. Podepsání souhlasu na ochranu osobních údajů, který obsahuje přesný účel zpracování a dobu po, kterou budou zpracovány a uchovávány.

Pravděpodobnost: 3

Následky: 3

RIZIKO_8

Oblast: přístup zaměstnanců na lokální disk.

Riziko: přístup neoprávněného zaměstnance do evidence, která není potřebná pro výkon náplně práce daného zaměstnance. Například jejich výmaz, kopírování, zablokování. Neoprávněny vstup správce lokálního disku.

Opatření: nastavení logistiky přístupů tak, aby každý zaměstnanec měl přístup jen k údajům potřebným na vykonávání pracovní činnosti. Úprava smluvního vztahu se správcem lokálního disku, úprava bude v souladu GDPR.

Pravděpodobnost: 2

Následky: 3

9.1.2 Externí prostředí organizace – identifikovaná rizika

V rámci externího prostředí organizace a zanalyzování oblasti jsme zjistili následující potenciální rizika:

RIZIKO_1

Oblast: mzdy a účetnictví.

Riziko: únik osobních údajů v elektronické a fyzické podobě.

Opatření: výplatnice jsou při přeposílání zaheslovány. Při předání fyzických dokumentů, podpis tisku obsahující datum, čas, odevzdávající osoba, přebírající osoba. Úprava smluvního vztahu, bude v souladu s GDPR.

Pravděpodobnost: 2

Následky: 4

RIZIKO_2

Oblast: bezpečnost IT systému

Riziko: porušení bezpečnosti z hlediska provozovatele, například zneužitím údajů, poškození dat, nebo odcizení dat.

Opatření: úprava smluvního vztahu s firmou, které zabezpečuje IT bezpečnost, to vše v souladu s GDPR.

Pravděpodobnost: 2

Následky: 4

RIZIKO_3

Oblast: bezpečnost IT systému

Riziko: porušení bezpečnosti osobních údajů klientů organizace, ke kterým mají přístup.

Opatření: úprava smluvního vztahu s firmou, která zabezpečuje IT bezpečnost, to vše v souladu s GDPR.

Pravděpodobnost: 2

Následky: 5

Závěr analýzy

Rizika, která s sebou nesou vysokou míru pravděpodobnosti, anebo následků jsou umístěna za tzv. toleranční hranici risku, která je vyznačena červeně. Takovým rizikům je nutné věnovat zvýšenou pozornost a zabezpečení. Pro přehlednější orientaci jsou rizika v interním prostředí označena modrou barvou a rizika v externím prostředí oranžovou barvou.

Tabulka č. 9 Matice řízení rizik, [vlastní]

Velmi vysoká					
Vysoká					
Střední		2, 3, 5	7	6	
Nízká			1, 8	4, 1, 2	3
Velmi nízká					
Pravděpodobnost / Následek	Velmi nízký	Nízký	Střední	Vysoký	Velmi vysoký

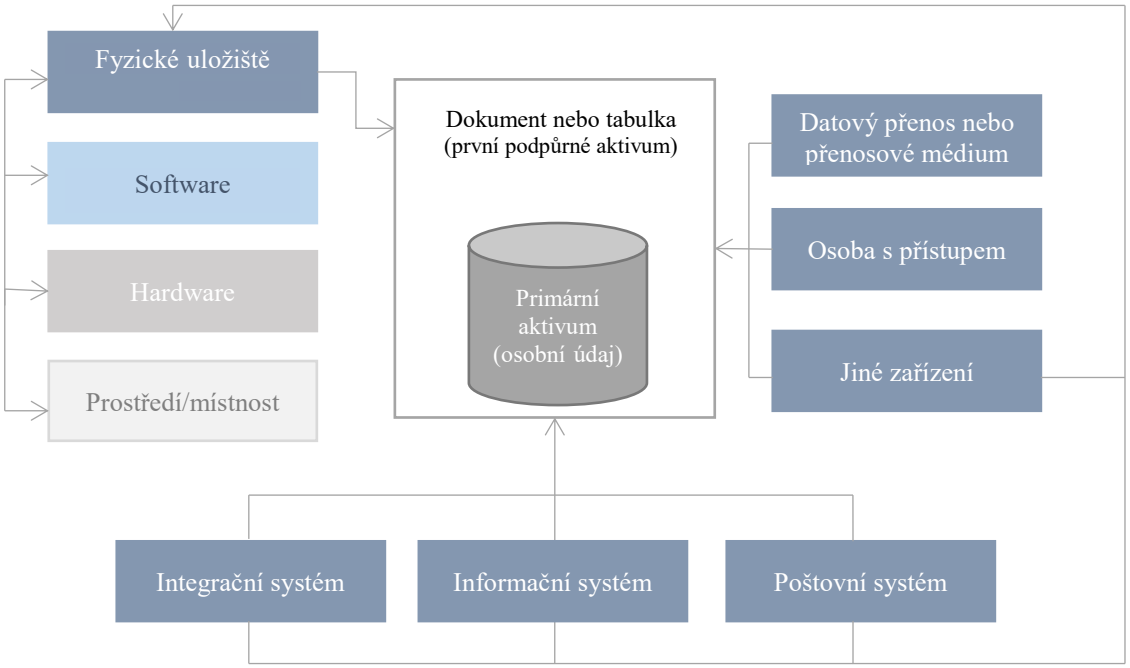
Posouzení vlivu na ochranu osobních údajů (DPIA), tedy není nutné zpracovávat, protože v rámci identifikovaných rizik z interního a externího prostředí nevzešlo žádné velmi vysoké riziko, které by bylo umístěno za toleranční hranicí risku.

10 METODA HODNOCENÍ AKTIV

Aktivum je chápáno jako objekt (aplikace, informační systém, kartotéka, spisovna, portál, evidence či jiné elektronické uložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR. [11]

Klíčovým krokem posouzení rizik, která primárně hrozí aktivům, je ohodnocení aktiv samotných. To je provedeno posouzením požadavků na integritu, důvěrnost a dostupnost aktiv, případně dat v aktivech obsažených.

Do hodnocení aktiv lze promítnout povahu a charakter posuzovaného aktiva z celospolečenského pohledu. Aktivum s dlouhodobou tradicí, které nelze jinak nahradit a na kterém se podílely předchozí generace, bude mít větší hodnotu, oproti aktivu, které je reprezentováno elektronickou a listinnou formou, a vzniklo strojovým zpracováním dat. [11]



Legenda
První podpůrné aktivum
Druhé podpůrné aktivum
Třetí podpůrné aktivum
Čtvrté podpůrné aktivum
Páté podpůrné aktivum

Obrázek č. 8 Hodnocení aktiv, [27]

11 VYHODNOCENÍ RIZIK

Jedna z metod, kterou lze použít při hodnocení rizik pro subjekty údajů, je jednoduchá kvantitativní metoda „PZH". Pomocí metody vyhodnocujeme příslušné riziko ve třech složkách, a to s ohledem na pravděpodobnost vzniku (P), zranitelnost (Z) a hodnotu aktiva (H). [1]

11.1 Aplikace jednoduché bodové kvantitativní metody – „PZH" k vyhodnocení rizika

Pomocí této metody vyhodnocujeme riziko ve třech jeho složkách s ohledem na:

- **pravděpodobnost uplatnění hrozby (P)**, odhad pravděpodobnosti, se kterou může nebezpečí opravdu nastat, je stanoven dle stupnice odhadu pravděpodobnosti vzestupně číslem od 1 do 5 kde je zahrnuta míra, úroveň a kritéria jednotlivých ohrožení (Tabulka č. 10),
- **zranitelnost aktiv vůči hrozbám (Z)**, odhad pravděpodobnosti následků závažnosti nebezpečí, je taktéž stanoven číslem od 1 do 5 (Tabulka č. 11),
- **hodnota aktiva (H),** zde se zohledňuje míra závažnosti ohrožení, počet ohrožených osob, čas působení ohrožení, stáří a technický stav technologického zařízení objektu apod. (Tabulka č. 12). [1]

Pravděpodobnost vzniku a existence nebezpečí s uvedenými hodnotami jsou uvedeny v tabulce č. 10, Zranitelnost aktiv vůči hrozbám znázorňuje tabulka č. 11 a hodnota aktiva je uvedena v tabulce č. 12.

Tabulka č. 10 P – pravděpodobnost uplatnění hrozby, [1]

Pravděpodobnost	Stupnice
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Tabulka č. 11 Z – zranitelnost aktiv vůči hrozbám [1]

Zranitelnost	Stupnice
Poškození údajů bez následků na subjekty údajů	1
Poškození s minimálními následky pro subjekty údajů	2
Poškození dat bez trvalých následků pro subjekty údajů	3
Poškození dat se závažnými následky pro subjekty údajů	4
Poškození dat s fatálními následky ohrožujícími život subjektů	5

Tabulka č. 12 H – hodnota aktiva, [1]

Hodnota aktiva	Stupnice
Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Pro posouzení a vyhodnocení zdrojů rizik je použito následující specifikace, která se zaznamenává do sloupců „P“, „Z“, „H“, v tabulce č. 14, 15, 16.

Celkové hodnocení rizika lze pak následovně po stanovení jednotlivých činitelů získat součinem, jehož výsledkem je ukazatel míry rizika „R“. [1]

Vzorec celkového rizika $\mathbf{R = P \times Z \times H}$

Tabulka č. 13 Rizikové stupně, [1]

Rizikový stupeň	**R**	**Míra rizika**
I.	≥ 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	≤ 3	Bezvýznamné riziko

Bodové rozpětí v tabulce č. 13 vyjadřuje naléhavost úkolů přijetí opatření ke snížení rizika a prioritu bezpečnostních opatření, který by měl být obsažen v plánu zvýšení úrovně bezpečnosti, jenž by měl být součást vyhodnocení a dokumentace rizik.

11.2 Míra rizik

Při stanovení kategorie závažnosti vyhodnocených rizik je možné rozdělení do pěti rizikových stupňů (I. až V.) a celkové hodnocení míry rizika (R) je pak následující:

I. *Nepřijatelné riziko s katastrofickými důsledky*, vyžadující okamžité zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik. Práce nesmí být zahájena, nebo v ní nesmí být pokračováno, dokud se riziko nesníží.

II. *Nežádoucí riziko*, vyžadující urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnou úroveň, na snížení rizika se musí přidělit potřebné zdroje.

III. *Mírné riziko*, i když není nutnost opatření tak závažná rizika jako u rizik kategorie II. Bezpečnostní opatření nutno zpravidla realizovat dle zpracovaného plánu podle rozhodnutí vedení podniku. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období. Je-li toto riziko spojeno se značnými nebezpečnými následky, musí se provést další zhodnocení, aby se přesněji stanovila pravděpodobnost vzniku úrazu, jako podklad pro stanovení potřeby dosažení a snížení rizika.

IV. *Akceptovatelné riziko*, riziko přijatelné se souhlasem vedení. Je nutno zvážit náklady na případné řešení nebo zlepšení, v případě, že se nepodaří provést technická bezpečnostní opatření ke snížení rizika, je třeba zavést vhodná opatření organizační. Většinou postačuje školení obsluhy, běžný dozor apod.

V. *Bezvýznamné riziko*, není vyžadováno žádné zvláštní opatření. Nejedná se však o stoprocentní bezpečnost, proto je nutno na existující riziko upozornit a uvést např. jaká organizační a výchovná opatření je třeba realizovat. [1]

Tabulka č. 14 Souhrnná analýza rizik, [11]

Aktivum	Hodnota aktiva dle systémové analýzy	Pravděpodobnost uplatnění hrozby								Zranitelnost jednotlivých aktivit vůči hrozbám								Rizikové skóre								Indikátor celkové míry rizika aktiva
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	
Listinné úložiště v rámci výkonu agend úřadu (L)	5	2	2	3	3	3	2	2	3	3	3	4	3	3	2	4	4	**30**	**30**	**60**	**45**	**45**	**20**	**40**	**60**	**330**
Listinné úložiště v rámci vnitřního chodu úřadu (L)	3	2	1	3	2	2	2	2	2	3	3	4	3	3	2	4	4	**18**	**9**	**36**	**18**	**18**	**12**	**24**	**24**	**159**
Informační systém spisové služby (E)	5	2	3	2	2	3	3	2	2	2	2	2	2	2	3	3	3	**20**	**30**	**20**	**20**	**30**	**45**	**30**	**30**	**225**

Tabulka č. 15 Souhrnná analýza rizik, (pokračování tabulky), [11]

Aktivum	Hodnota aktiva dle systémové analýzy	Pravděpodobnost uplatnění hrozby								Zranitelnost jednotlivých aktivit vůči hrozbám								Rizikové skóre								Indikátor celkové míry rizika aktiva
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	
Agendové informační systémy – samostatná působnost (E)	5	2	2	3	2	2	3	2	2	2	2	2	2	3	3	3	3	**20**	**20**	**30**	**20**	**30**	**45**	**30**	**30**	**225**
Agendové informační systémy – přenesená působnost (E)	5	2	2	3	2	2	3	2	2	2	2	2	2	3	3	3	3	**20**	**20**	**30**	**20**	**30**	**45**	**30**	**30**	**225**
Ekonomický informační systém (E)	5	2	3	3	2	2	3	2	2	2	3	3	3	3	3	3	3	**20**	**45**	**45**	**30**	**30**	**45**	**30**	**30**	**275**

Tabulka č. 16 Souhrnná analýza rizik, (pokračování tabulky), [11]

Aktivum	Hodnota aktiva dle systémové analýzy	Pravděpodobnost uplatnění hrozby								Zranitelnost jednotlivých aktivit vůči hrozbám								Rizikové skóre								Indikátor celkové míry rizika aktiva
		Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	Vnější útoky	Technické chyby	Lidský faktor	Narušení integrity OÚ	Neoprávněný přístup	Narušení dostupnosti	Ztráta OÚ	Narušení práv a svobod subjektu	
Portály – veřejné i neveřejné webové portály (E)	3	4	3	3	2	2	3	2	2	3	2	3	3	2	3	3	3	**36**	**18**	**27**	**18**	**12**	**27**	**18**	**18**	**174**
Ostatní elektronická úložiště (E)	1	1	2	3	2	4	2	3	3	2	2	3	3	3	2	4	4	**2**	**4**	**9**	**6**	**12**	**4**	**12**	**12**	**61**
										Indikátor celkové míry rizika hrozby *								**166**	**176**	**257**	**177**	**207**	**243**	**214**	**234**	

* Indikátor celkové míry rizika je sumář pro všechna aktiva.

Celková míra rizika hrozby – identifikátorem jsou znázorněny celkové míry hrozeb dle jejich výše. Z výše identifikátoru je patrné, které hrozby jsou pro obec nejzávažnější a mohou zde směřovat technická a organizační opatření. [11]

Celková míra rizika aktiva – identifikátorem jsou znázorněny celkové míry rizika aktiv dle jejich výše. Z výše identifikátoru je patrné, která aktiva jsou náchylnější a potřebují zvýšenou pozornost nebo pozornost ze strany obce. [11]

Tabulka č. 17 Stupnice hodnocení aktiv, [11]

Název aktiva	Stupeň hodnocení	Popis hodnocení
Listinné úložiště v rámci výkonu agend úřadu	5	Aktiva ohodnocena zhotovitelem na nejvyšší stupeň, v tomto aktivu je soustředěno velké množství osobních údajů i citlivých, které se vztahují ke kategorii zvláště zranitelných subjektů údajů. Ztráta, poškození nebo narušení primárního aktiva je katastrofická a vede k porušení zákonných zákonitostí vyplvajících z GDPR. Při narušení primárního aktiva dochází k uplatnění sankcí v rámci Obecného nařízení. Porušení zákonných povinností má zásadní vliv na fungování celé organizace.
Listinné úložiště v rámci vnitřního chodu úřadu	3	Aktivum ohodnocené zhotovitelem na střední stupeň, osobní údaje vedené v tomto aktivu závisí na rozhodnutí obce. Nepředpokládá se, že ztrátou, poškozením a narušením bezpečnosti takového aktiva by mělo dojít k uplatnění sankcí vyplývajících z Obecného nařízení. Narušené aktivum nebude mít vliv na chod obce.
Informační systém spisové služby	5	Aktiva ohodnocena zhotovitelem na nejvyšší stupeň, v tomto aktivu je soustředěno velké množství osobních údajů i citlivých, které se vztahují ke kategorii zvláště zranitelných subjektů údajů. Ztráta, poškození nebo narušení primárního aktiva je katastrofická a vede k porušení zákonných zákonitostí vyplvajících z GDPR. Při narušení primárního aktiva dochází k uplatnění sankcí v rámci Obecného nařízení. Porušením zákonných povinností bude zásadně ovlivněno fungování organizace jako celku.

Tabulka č. 18 Stupnice hodnocení aktiv, (pokračování tabulky), [11]

Název aktiva	Stupeň hodnocení	Popis hodnocení
Agendové informační systémy - Přenesená působnost	5	Aktiva ohodnocena zhotovitelem na nejvyšší stupeň, v tomto aktivu je soustředěno velké množství osobních údajů i citlivých, které se vztahují ke kategorii zvláště zranitelných subjektů údajů. Ztráta, poškození nebo narušení primárního aktiva je katastrofická a vede k porušení zákonných zákonitostí vyplvajících z GDPR. Při narušení primárního aktiva dochází k uplatnění sankcí v rámci Obecného nařízení. Porušení zákonných povinností má zásadní vliv na fungování celé organizace.
Ekonomický informační systém	5	Aktiva ohodnocena zhotovitelem na nejvyšší stupeň, v tomto aktivu je soustředěno velké množství osobních údajů i citlivých, které se vztahují ke kategorii zvláště zranitelných subjektů údajů. Ztráta, poškození nebo narušení primárního aktiva je katastrofická a vede k porušení zákonných zákonitostí vyplvajících z GDPR. Při narušení primárního aktiva dochází k uplatnění sankcí v rámci Obecného nařízení. Porušení zákonných povinností má zásadní vliv na fungování celé organizace.
Portály	3	Aktivum ohodnocené zhotovitelem na střední stupeň, osobní údaje vedené v tomto aktivu závisí na rozhodnutí obce. Nepředpokládá se, že ztrátou, poškozením a narušením bezpečnosti takového aktiva by mělo dojít k uplatnění sankcí vyplývajících z Obecného nařízení. Narušené aktivum nebude mít vliv na chod obce.
Ostatní elektronické úložiště	1	Aktivum ohodnocené zhodnotitelem na nízký stupeň, obsah tohoto aktiva osobní údaje vedené v tomto aktivu závisí na rozhodnutí obce. Nepředpokládá se, že ztrátou, poškozením a narušením bezpečnosti takového aktiva by mělo dojít k uplatnění sankcí vyplývajících z Obecného nařízení. Narušené aktivum nebude mít vliv na chod obce.

Analýza je provedena z pohledu daného subjektu údajů dle GDPR. Hodnota aktiv a stanovení kritérií analýzy rizik je stanoveno z pohledu dopadu na subjekt údajů nebo informace, které obsahují osobní údaje. Rizika zpracování vzhledem k rozsahu, kontextu, povaze a účelům osobních údajů. Na základě definovaných aktiv bylo provedeno jejich ohodnocení a podle stupnic, které jsou definovány tabulkami č. 10, 11, 12. [1], [11]

11.3 Návrh opatření k zajištění souladu posuzovaných procesů s GDPR

Cílem bakalářské práce byla implementace Obecního nařízení o ochraně osobních údajů na malé obci, bylo tedy nutné provést postupnou implementaci v rámci obce tak, aby se zabránilo případným sankcím. Příprava a následná implementace se sebou přinesla i určitá rizika a vynaložení finančních prostředků.
Byly posouzeny rizika, které mohou vzniknout v interním a externím prostředí organizace. Cílem výstupu analýzy bylo navrhnout opatření pro minimalizaci rizik a tyto informace zahrnout do zvláštního ustanovení, které by bylo vhodné zapracovat.

V následujícím textu jsou popsány návrhy opatření pro navrhované rizika.

11.4 Fyzická bezpečnost osobních údajů a dat v prostorách kanceláře

V rámci uvedené oblasti je vhodné využít následující opatření:

- Zaměstnanec je zodpovědný za klíče od kancelářských prostor, které mu byly přiděleny v den nástupu do pracovního poměru. V případě jejich ztráty nebo zcizení je zaměstnanec povinný bezodkladně nahlásit tuto skutečnost nadřízenému nebo zodpovědné osobě. Zaměstnanec si je vědom, že ztrátou klíčů od prostor kanceláře může dojít k úniku citlivých informací a ohrozit tak organizaci.
- Zaměstnanec je povinný při odchodu z práce, pokud odchází jako poslední zkontrolovat a zabezpečit: uzavření oken, vypnutí všech světel, zakódování alarmu, uzamčení vchodu od kanceláře, uzamčení hlavních dveří do budovy.
- Zaměstnanec je povinný dodržet zásadu „čistého stolu“ jejímž cílem je zabezpečit bezpečnost citlivých informací, se kterými zaměstnanec přichází během vykonávání své činnosti do styku. Politika čistého stolu znamená, že dokument, obsahující osobní údaje fyzických osob, se kterými zrovna zaměstnanec nepracuje se nemají nacházet na pracovním stole.
- Povinností zaměstnance je při skončení scanování nebo tisku dokumentů neponechávat dokumenty v kopírovacím zařízení. Ponecháním dokumentů v kopírovacím zařízení by mohlo dojít k úniku citlivých informací.
- Veškeré dokumenty v tištěné podobě, které už nejsou potřebné pro výkon práce zaměstnance, je nutné skartovat.
- V případě, že zaměstnanec neví jak, respektive kde uschovat dokumenty obsahující osobní údaje, zeptá se zodpovědné osoby.

11.5 Fyzická bezpečnost osobních údajů a dat v elektronických zařízeních

V rámci uvedené oblasti je vhodné využít následující opatření:

- Zaměstnanec má hmotnou odpovědnost za elektronická zařízení, která mu byla přidělena při nástupu do pracovního poměru. Mimo škodu za ztrátu fyzického zařízení může samotná ztráta způsobit organizaci škody většího rozsahu než případná ztráta zneužití citlivých údajů, která byla v zařízení uložena. V případě ztráty je zaměstnanec povinen ohlásit odcizení zodpovědné osobě. Zaměstnanec si je vědom, že zcizením nebo ztrátou jakéhokoliv zařízení může dojít k úniku citlivých informací.
- Zaměstnanec je povinen zabezpečit dostatečnou fyzickou ochranu svých elektronických zařízení, aby předešlo ke zcizení nebo krádeži.

11.6 Softwarové zabezpečení elektronických zařízení

V rámci uvedené oblasti je vhodné využít následující opatření:

- Zaměstnanec je povinný zkontrolovat, zda elektronické zařízení, které převzal obsahuje nejnovější verzi antivirového programu. V případě, že elektronické zařízení neobsahuje nejnovější verzi antivirového programu je tato skutečnost oznámena zodpovědné osobě, aby tuto skutečnost neprodleně vyřešila.
- Zaměstnanec je povinný nastavit co nejvyšší úroveň zabezpečení elektronického zařízení, rozumí se tím nastavení maximálního počtu hesel.
- Zaměstnanec je povinný vytvořit si takové heslo, v rámci všech přístupů, které bude obsahovat: maximálně 8 znaků, minimálně jedno velké písmeno, minimálně jeden z tzv. speciálních znaků, například - # ! < > & % * +.
- Zaměstnanec si je vědom, že by přeposíláním si dokumentů z pracovního emailu na soukromý email, mohlo dojít k úniku citlivých informací.
- Zaměstnanec si je vědom, že firemní notebook neslouží pro soukromé účely.
- Zaměstnanec si je vědom, že vstupem na nebezpečné internetové stránky může ohrozit bezpečnost elektronického zařízení. Přístup na nebezpečné internetové stránky jsou ze strany zaměstnavatele přísně zakázány. Pod nebezpečnými internetovými stránkami se rozumí například: stránky s hazardními hrami, internetové stránky, které slouží ke stahování souborů.

ZÁVĚR

Ochrana soukromí a osobních údajů je v dnešní uspěchané době velmi důležitým tématem, už jen proto že nás provázejí po celý život. V online prostředí, ve kterém se většina z nás pohybuje bez nadsázky denně, mnozí sdílí nejrůznější informace o své osobě, aniž by si uvědomovali mnohé nástrahy internetu.

Po vstupu GDPR v platnost, dostaly jednotlivé členské státy EU možnost její části zpřesnit nebo upravit v rámci domácích zvyklostí. Poslanecká sněmovna ČR nestihla schválit zákon o zpracování osobních údajů včas. Při tvorbě bakalářské práce tedy nebyl v platnosti žádný právní předpis pro Českou republiku.

V teoretické části se bakalářská práce zabývala právními normami a Nařízením Evropského Parlamentu a Rady (EU). Byly porovnány dosavadní a nově vzniklé právní úpravy ochrany osobních údajů fyzických osob. Nařízení se mimo jiné dotýká také oblasti veřejné správy. Proto jsou obce povinny přijmout taková opatření, aby bylo s osobními údaji zacházeno v souladu s GDPR. Musí dodržovat zásady, na kterých je celé nařízení postaveno. V postupu implementace GDPR do organizace je nejdůležitějším krokem provedení vstupní analýzy, jejímž úkolem je porovnání aktuálního stavu se stavem požadovaným.

Praktická část se zabývá implementací nařízení GDPR v prostředí malé obce. Nejdříve byla rozebrána charakteristika organizace, struktura, personální zajištění a technické zabezpečení úřadu. Dále jsou uvedeny informační systémy a elektronická uložiště. Následně jsou zapracovány příklady možných interních a externích hrozeb, které mohou v organizaci vyvstat. Byla zpracována GAP analýza, pomocí které byly identifikovány potenciální rizika v interním a externím prostředí. Těsně pod toleranční křivkou se ocitly z interního prostředí riziko č. 4 – technické vybavení a jeho zabezpečení a riziko č. 6 – přijetí nového zaměstnance do pracovního poměru. Z externího prostředí riziko č. 1 – mzdy a účetnictví, riziko č. 2 – bezpečnost IT systému z hlediska provozovatele a riziko č. 3 – bezpečnost IT systému z hlediska bezpečnosti osobních údajů klientů organizace. V závěru byly navrženy opatření ve třech hlavních oblastech – Fyzická bezpečnost osobních údajů a dat v prostorách kanceláře, Fyzická bezpečnost osobních údajů a dat v elektronických zařízeních a Softwarové zabezpečení elektronických zařízení.

Na základě definovaných aktiv bylo provedeno hodnocení s využitím metody PZH z pohledu dopadu na subjekt údajů. Analýza byla provedena z pohledu daného subjektu údajů.

Poslanecká sněmovna vyslovila dne 5. prosince 2018 souhlas s vládním návrhem zákona, o zpracování osobních údajů, který navazuje na stávající zákon o ochraně osobních údajů. Nově přijatá pravidla navazují na ochranu osobních údajů stanovených evropským nařízením GDPR. Dne 24. dubna 2019 vstoupil v platnost zákon č. 110/2019, o zpracování osobních údajů.

Zákon byl vytvořený Ministerstvem vnitra ve spolupráci s Úřadem pro ochranu osobních údajů v souvislosti s obecným nařízením o ochraně osobních údajů, které nastavilo stejné podmínky ochrany osobních údajů v celé EU.

SEZNAM POUŽITÉ LITERATURY

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

[2] *ČESKO, 2017, 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, ÚZ. ISBN 978-80-7488-241-8.

[3] Co to je osobní údaj? In: *www.k-net.cz* [online]. [cit. 2018-12-28]. Dostupné z: https://www.k-net.cz/gdpr-narizeni-o-ochrane-osobnich-udaju

[4] Co považuje GDPR za osobní údaje, [online]. [cit. 2019-04-13]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

[5] Pilíře GDPR: GDPR směrnice a nařízení. In: *Neofema blog* [online]. [cit. 2018-12-06]. Dostupné z: http://blog.neofema.cz/novinky/gdpr-smernice-a-narizeni/

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

[7] *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 (obecné nařízení o ochraně osobních údajů)*. Dostupné také z: https://www.codexisonline.cz/

[8] Stručný popis obsahu nového Obecného nařízení o ochraně osobních údajů. In: *Ministerstvo vnitra ČR* [online]. 2016 [cit. 2018-10-07]. Dostupné z: https://www.google.cz/search?q=Stru%C4%8Dn%C3%BD+popis+obsahu+nov%C3%A9ho+Obecn%C3%A9ho+na%C5%99%C3%ADzen%C3%AD+o+ochran%C4%9B+osobn%C3%ADch+%C3%BAdaj%C5%AF&oq=Stru%C4%8Dn%C3%BD+popis+obsahu+nov%C3%A9ho+Obecn%C3%A9ho+na%C5%99%C3%ADz aqs=chrome..69i57.6425j0j7&sourceid=chrome&ie=UTF-8

[9] ČESKO, 2000, Zákon č. 101/2000Sb., ze dne 4. dubna 2000, Zákon o ochraně osobních údajů. In: *Sbírka zákonů ČR*. 2000, ročník 2000, částka 32. Dostupné také z: https://www.codexisonline.cz

[10] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

[11] Systémová analýza působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů. In: *Ministerstvo vnitra ČR* [online]. 2018 [cit. 2018-10-07]. Dostupné z:https://cse.google.com/cse?cx=015489265366623571386%3Aizzrwg3bmqm&q=Syst%C3%A9mov%C3%A1+anal%C3%BDza+p%C5%AFsobnosti+obc%C3%AD+z+hlediska+obecn%C3%A9ho+na%C5%99%C3%ADzen%C3%AD+o+ochran%C4%9B+osobn%C3%ADch+%C3%BAdaj%C5%AF&ok.x=11&ok.y=6

[12] ČESKO, 1993, Zákon č. 2/1993 Sb., zde dne 16. prosince 1992 Listina základních práv a svobod, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*, částka 1, str. 17-23.

[13] ČESKO, 2000, Zákon č. 128/2000 Sb., ze dne 15. května 2000, Zákon o obcích (obecní zřízení), ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. ročník 2000, částka 38. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=128/2000&typeLaw=zakon&what=Cislo_zakona_smlouvy

[14] ČESKO, 2018, Průvodce pro přípravu obcí na požadavky GDPR. In: *Ministerstvo vnitra ČR* [online]. [cit. 2018-10-13]. Dostupné z: https://cse.google.com/cse?cx=015489265366623571386%3Aizzrwg3bmqm&q=Pr%C5%AFvodce+pro+p%C5%99%C3%ADpravu+obc%C3%AD+na+po%C5%BEadavky+GDPR&ok.x=0&ok.y=0

[15] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Nakladatelství Leges, 2018. ISBN 9788075022752.

[16] ČESKO, Zákon č. 340/2015 Sb., ze dne 14. prosince 2015, o zvláštních podmínkách účinnosti některých smluv. In: *Sbírka zákonů ČR*. 2015, částka 144. Dostupné také z: https://www.codexisonline.cz/

[17] Pořizování obrazových a zvukových záznamů z jednání zastupitelstva. *www.uoou.cz* [online]. Praha, červen 2013 [cit. 2018-10-28]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=22535

[18] Česko*, 2017, Nová pravidla ochrany osobních údajů,* In: *Hospodářská komora České republiky:* [online]. 2017, listopad 2017, stran 19 [cit. 2018-11-19]. Dostupné z: https://www.komora.cz/files/uploads/2017/06/2017_11_16Příručka-GDPR_final2.pdf

[19] Řízení rizik (Risk Management) [online]. [cit. 2018-11-19]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[20] HNILICA, Jiří a Jiří FOTR. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. Praha: Grada, 2009. Expert (Grada). ISBN 978-802-4725-604.

[21] FOTR, Jiří a Jiří HNILICA. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. Expert (Grada). ISBN 978-802-4751-047.

[22] Česko, 2013, *Doporučená praxe Společnosti pro projektové řízení, oblast Řízení rizik* [online]. Duben 2013,stran 31, [cit. 2018- 04-12]. Dostupné z: https://www.ipma.cz/media/1283/dobra_praxe_rizeni_rizik.pdf

[23] ČSN EN 31010 (01 0352) Management rizik – Techniky posuzování rizik, Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011, 79 s.

[24] Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství [online]. [cit. 2018-12-06].: Metodika GDPR. In: *Ministerstvo školství, mládeže a tělovýchovy* [online]. 7.11.2017 [cit. 2018-12-06]. Dostupné z: http://www.msmt.cz/file/44569/

[25] GAP analýza požadavků nařízení 2016/679/ UE: Srovnání požadavků GDPR se stavem posuzované organizace, w*ww.tud-sud.cz* [online]. 2017 [cit. 2018-12-09]. Dostupné z: https://www.tuv-sud.cz/uploads/images/151367586515212270164 2/gap-analyza.pdf

[26] Etapy GDPR In: www.czechinvest.org [online]. [cit. 2018-12-28] Dostupné z: https://www.czechinvest.org/cz/Sluzby-pro-male-a-stredni-podnikatele/GDPR

[27] GDPR snadno a srozumitelně. *www.kpcs.cz* [online]. [cit. 2019-03-14]. Dostupné z: https://www.kpcs.cz/gdpr/uz-dost-bylo-reci-o-gdpr-pojdme-konecne-neco-delat.html

[28] ČESKO, 2014, Zákon č. 181/2014., ze dne 23. července 2014, Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů, (zákon o kybernetické bezpečnosti) In: *Sbírka zákonů ČR*. 2014, ročník 2014, částka 75. Dostupné také z: https://www.codexisonline.cz.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

aj.	a jiné
apod.	a podobně
ČR	Česká republika
Čl.	Článek
DPIA	Posouzení vlivu na ochranu osobních údajů
DPO	Pověřenec pro ochranu osobních údajů
EU	Evropská unie
GAP	Analýza zaměřená na zjištění nedostatku
GDPR	Obecné nařízení o ochraně osobních údajů
ha	Hektarů
HW	Hardware
IČO	Identifikační číslo organizace
IP adresa	Identifikace síťového rozhraní v počítačové síti
IT	Informační technologie
KEO	Kompletní evidence obce
m n.m.	Metrů nad mořem
MVČR	Ministerstvo vnitra České republiky
NP	Nad podlaží
ORP	Obec s rozšířenou působností
PZH	Jednoduchá polokvantitativní metoda
Sb.	Sbírka zákonů
SMS	Služba krátkých textových zpráv
Tzv.	Takzvaně
ÚOOÚ	Úřad pro ochranu osobních údajů
WP29	Pracovní skupina zřízená podle článku 29 směrnice 95/46/ES

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VZOR FORMULÁŘE PRO IDENTIFIKACI PROCESU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Název zpracování:		**Počet zaměstnanců organizace:**	
Vymezení vztahu organizace ke zpracování:			
▪ Správce	ANO/NE	Je využíván zpracovatel: ANO/NE /v případě, že Ano, uvést zpracovatele/	
▪ Zpracovatel - Jsou využívání další zpracovatelé	ANO/NE	/v případě, že Ano, uvést kdo je správce/	
Subjekty údajů:			
▪ Zaměstnanci			
▪ Klienti			
▪ Jiné osoby			
▪ Osoby do 13 let			
Právní základ zpracování:			
Osobní údaje:	ANO/NE	Zvláštní kategorie osobních údajů:	ANO/NE
▪ Souhlas		▪ Výslovný souhlas	
▪ Plnění smlouvy		▪ Plnění povinností a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany.	
▪ Plnění právních povinností		▪ Zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas.	
▪ Ochrana životně důležitých zájmů		▪ Zpracování provádí v rámci svých oprávnění činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt u svých členů …	
▪ Plnění úkolu ve veřejném zájmu		▪ Zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů.	
▪ Oprávněné zájmy		▪ Zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků.	
		▪ Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu.	
		▪ Zpracování je nezbytné pro účely preventivního nebo pracovního lékařství	
		▪ Zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví.	
		▪ Zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.	
Rozsah zpracování:			
Systematické zpracování:			
/uvést, zda je zpracování systematické/			
Identifikátory:			

/uvést, které z identifikátorů jsou shromažďovány/	
▪ Jméno, příjmení	
▪ Titul	
▪ Rodné číslo / datum narození	
▪ Pohlaví	
▪ Rodinný stav	
▪ Vzdělání	
▪ Lokalita	
▪ Síťový identifikátor	
▪ Telefon	
▪ Podobizna	
▪ Podpis	
Zvláštní kategorie osobních údajů:	
/uvést, zda v případě, že ano, které ze zvláštních kategorií osobních údajů jsou shromažďovány/	
▪ Rasový / etnický původ	
▪ Politické názory	
▪ Náboženské vyznání	
▪ Filozofické přesvědčení	
▪ Členství v odborech	
▪ Genetické údaje	
▪ Biometrické údaje	
▪ Zdravotní stav	
▪ Sexuální život / orientace	

Informování subjektu údajů:	**Informace je povinná:**	**Informace byla podána**
/uvést, zda je pro zpracování povinné provést informaci subjektu údajů, a je-li povinné, zda bylo provedeno/	ANO/NE	ANO/ NE
Řízení incidentů:	Incident je řízen:	Incident by měl být řízen
/uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/	ANO/NE	ANO/NE
Uvést, zda je v rámci zpracování prováděno:		
▪ Profilování	ANO/NE	
▪ Generalizace	ANO/NE	
▪ Odvozování	ANO/NE	
Použitá technická a organizační opatření:		
/uvést, zda jsou využita některá z níže uvedených technických a organizačních opatření/		
▪ Pseudonymizace	ANO/NE	
▪ Anonymizace	ANO/NE	
▪ Šifrování	ANO/NE	
Uložení osobních údajů:		
/uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/		
▪ Manuální	ANO/NE	
▪ IS	ANO/NE	
Doba zpracování:		
/uvést, po jakou dobu je potřebné osobní údaje shromažďovat/		
Interní odpovědnost za zpracování:		
/uvést interní odpovědnost za toto zpracování/		
Organizační útvar(y), který(é) se seznamují s osobními údaji:		
/uvést organizační útvary, jejichž pracovníci se seznamují s osobními údaji v rámci tohoto zpracování/		
▪		