
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# GDPR VE VEŘEJNÉ SPRÁVĚ
GDPR IN PUBLIC ADMINISTRATION

**BAKALÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — **Kateřina Kopcová**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR


**BRNO 2018**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání bakalářské práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Studentka: | **Kateřina Kopcová** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Manažerská informatika |
| Vedoucí práce: | **Ing. Viktor Ondrák, Ph.D.** |
| Akademický rok: | 2017/18 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

## GDPR ve veřejné správě

**Charakteristika problematiky úkolu:**

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Navrhnout systém ochrany osobních údajů.

**Základní literární prameny:**

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

KUČEROVÁ, A. a F. NONNEMANN. Ochrana osobních údajů v otázkách a odpovědích. Praha: Bova Polygon, 2010. 152 s. ISBN 978-80-7273-163-3.

NOVÁK, D. Zákon o ochraně osobních údajů a předpisy související: komentář. Praha: Wolters Kluwer, 2014. 484 s. ISBN 978-80-7478-665-5.

POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>ředitel | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

**Abstrakt**

Bakalářská práce je zaměřena na analýzu připravenosti obce Dolní Dobrouč na Obecné nařízení o ochraně osobních údajů, známé jako GDPR. První část obsahuje teoretické informace o oblastech veřejné správy a Obecného nařízení o ochraně osobních údajů. Ve druhé části je analýza současného stavu v obci. V poslední části je zhodnocení analýzy a vlastní návrhy řešení.

**Abstract**

This bachelor thesis focuses on an analysis of readiness of the Dolní Dobrouč village in relation to the General Data Protection Regulation implementation, which is known as GDPR. First part includes theoretical information about the areas of public administration and General Data Protection Regulation. The second part contains the analysis of current situation in the village. The last part covers the overall evaluation of analysis and my own proposal of solutions.

**Klíčová slova**

veřejná správa, GDPR, osobní údaje, Dolní Dobrouč, řízení rizik

**Key words**

public administration, GDPR, personal data, Dolní Dobrouč, risk management

**Bibliografická citace**

KOPCOVÁ, K. *GDPR ve veřejné správě*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 92 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

**Čestné prohlášení**

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 17. května 2018 .....

Kateřina Kopcová

**Poděkování**

Ráda bych poděkovala svému vedoucímu práce panu Ing. Viktoru Ondrákovi, Ph.D. za pomoc s vypracováním a panu starostovi obce Dolní Dobrouč Pavlu Šislerovi za umožnění zpracování bakalářské práce a poskytování informací a cenných rad o fungování obce.

# OBSAH

# ÚVOD

Otázka osobních údajů a jejich ochrany je v poslední době velice sledované téma. Může za to hlavně Evropské nařízení o ochraně osobních údajů, zkráceně Obecné nařízení nebo GDPR z anglického názvu General Data Protection Regulation, které vstupuje v platnost 25. května 2018. Nařízení se dotkne všech, kdo uchovává nebo zpracovává osobní údaje občanů Evropské unie. Toto nařízení se nevyhýbá ani veřejné správně.

Veřejná správa se v České republice dělí na státní správu a samosprávu. Samospráva se dále dělí na obce, kterých je u nás 6 258 a kraje, kterých máme 14. Obce se ještě dále člení na obce, městyse, města a statutární města.

V bakalářské práci představím obec Dolní Dobrouč, která se nachází v pardubickém kraji v blízkosti Ústí nad Orlicí. Původní název obce znamená „Ves v líbezném údolí“, který ji skvěle vystihuje.

Bakalářská práce je členěna do několika celků. Nejdříve představím cíle práce a použité metody. Jako další je teoretická část, která pomůže s pochopením daného tématu, především veřejné správy, GDPR a novinek, které toto nařízení přináší.

Třetí částí je část analytická, kde nejprve obec Dolní Dobrouč představím a dále provedu analýzu současného stavu z hlediska Obecného nařízení, a to hlavně jaké zpracovává osobní údaje, jak je uchovává a jak jsou zabezpečeny.

V poslední části představím své návrhy řešení, které je potřeba implementovat pro soulad s Obecným nařízením a zajištění práv a svobod subjektů a provedu ekonomické zhodnocení. Podkladem pro analýzu jsou informace zjištěné ze stránek obce, vlastní návštěvy a informace od zaměstnanců obce.

# CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Hlavním cílem mé bakalářské práce je na základě analýzy představit návrhy na zlepšení, kterými obec vyhoví Obecnému nařízení. Tyto návrhy budou moci být využity i ostatními obcemi malého rozsahu.

Práce obsahuje několik dílčích cílů:

- poskytnout informace související s tímto tématem,
- představit obec Dolní Dobrouč,
- analyzovat současný stav,
- na základě analýzy představit návrhy na zlepšení.

V práci využívám metodu analýzy rizik, která mi pomůže odhalit slabá místa, na která je potřeba se zaměřit.

# 1 TEORETICKÁ VÝCHODISKA PRÁCE

V této části budu psát o teoretických informacích, které využiji pro zpracování bakalářské práce, mimo jiné zde vypíši pojmy z oblasti informační bezpečnosti a ochrany osobních údajů.

## 1.1 Základní pojmy

**Informace** – existuje více možností popisu informace, v informatice se jedná o fyzicky interpretovaná data [1].

**Data** – jsou informace, které jsou opakovatelně interpretovatelné ve formalizované podobě pro komunikaci, vyhodnocování nebo zpracování [1].

**Osobní údaj** – je „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů*“. [2, s. 10]

**Subjekt údajů** – jakákoli fyzická osoba určená nebo určitelná dle osobních údajů [2].

**GDPR** – General Data Protection Regulation – Obecné nařízení na ochranu osobních údajů a zacházení s nimi vstupující v platnost 25. května 2018 [3].

**ISMS** – Information Security Management System – Systém řízení informační bezpečnosti – část celkového systému řízení organizace, která se věnuje řízení bezpečnosti informací [1].

**IS** – Informační systém – lze chápat jako systém informací a procesů, které pracují s informacemi [1].

**ICT –** Information and Communication Technology – informační a komunikační technologie [1].

**Bezpečnost informací** – je ve vzájemném vztahu s bezpečností organizace a IS/ICT, řeší ochranu a dostupnost informací [1].

**Důvěrnost** – zajištění, že k daným datům bude mít přístup pouze oprávněný uživatel [1].

**Dostupnost** – zajištění dostupnosti v momentě kdy uživatel informace potřebuje [1].

**Integrita** – zajištění správnosti a úplnosti informací [1].

**Aktiva** – jsou veškerý hmotný i nehmotný majetek [1].

## 1.2 GDPR

General Data Protection Regulation neboli Obecné nařízení na ochranu osobních údajů (dále jen GDPR) je nejucelenějším souborem na ochranu dat na světě. GDPR se dotkne každého kdo zpracovává nebo i jen shromažďuje osobní údaje evropských občanů, a to i společností a institucí mimo EU, které zde působí [3].

Nařízení míří na všechny – jednotlivce, firmy i instituce, které zacházejí s osobními údaji svých zaměstnanců, zákazníků, klientů nebo dodavatelů. Dotkne se i těch, kteří sledují a analyzují chování uživatelů na internetu, v aplikacích nebo jiných chytrých technologiích. GDPR si klade za cíl chránit osobní údaje subjektů v digitálním světě [3].

GDPR vstoupí v účinnost dne 25. května 2018 a to jednotně v celé Evropské unii. V Česku nahradí současnou právní ochranu osobních údajů v podobě směrnice 95/46/ES a souvisejícího zákona č. 101/2000 Sb., o ochraně osobních údajů. Ten bude po novele upravovat pouze body, které nejsou Obecným nařízením stanoveny nebo je možné upravovat je na vnitrostátní úrovni [3].

Období od schválení GDPR v dubnu 2016 do května 2018, kdy vstoupí v účinnost, je vyhrazeno přípravě, během které musí všichni, jichž se nařízení týká, analyzovat svůj informační systém a způsoby, jak nakládají s osobními údaji. Během této doby by měli jednotlivé státy přijmout prováděcí zákon, který upřesní některé body, svěřené do jejich pravomoci [3].

### 1.2.1 Osobní údaje

Dle § 4 písm. a) zákona č. 101/2000 Sb. se *„osobním údajem rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, pokud lze subjekt údajů přímo nebo nepřímo identifikovat na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“*. [4, § 4 písm. a)] [4]

Subjektem údajů je ale myšlena pouze fyzická osoba. Z předešlé definice je patrné, že osobním údajem může být jakákoli informace. Zákon č. 101/2000 Sb. o ochraně osobních

údajů (dále jen ZoOÚ) informace nijak neomezuje, znamená to, že mohou být i nepravdivé a k tomu dává ZoOÚ nástroje, jak se s takovou situací vyrovnat [2].

**Citlivé osobní údaje**

Dle § 4 písm. b) zákona o ochraně osobních údajů se *„citlivými osobními údaji rozumí 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 subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“*. [4, § 4 písm. b)]

Jedná se o podskupinu osobních údajů, jejichž zpracováním, zvláště neoprávněným je možno velmi významně zasáhnout do osobní a osobnostní sféry člověka. Zpracování těchto údajů má přísnější pravidla, ta jednoznačně stanovuje § 9 ZoOÚ, navíc mohou být zpracovány pouze se souhlasem subjektu údajů [2].

V Obecném nařízení se označují pojmem osobní údaje zvláštní kategorie a z jejich výčtu je odstraněn údaj o odsouzení za trestný čin, který se nově zpracovává ve zvláštním režimu dle článku 10 Obecného nařízení, který stanovuje možnost zpracování takových údajů pouze pod dozorem orgánu veřejné moci nebo pokud je takové zpracování oprávněné dle práva členského státu nebo Unie [5], [6].

### 1.2.2 Souhlas se zpracováním osobních údajů

Získáním souhlasu může správce vyřešit omezení zpracování údajů. Souhlas subjektu musí být informovaný, jednoznačný, konkrétní a svobodný. Subjekt musí mít možnost, a být na ni upozorněn, souhlas neudělit bez negativních důsledků. Organizace, a především orgány veřejné správy, které to nemohou zajistit musí najít právní oporu pro zpracování osobních údajů. Obecné nařízení také zavádí pojem zjevné potvrzení. Jedná se o aktivní činnost subjektu, nelze tedy využít možnosti, že pokud subjekt nic neudělá tak souhlasí a zaškrtávací políčko kterým by souhlas zrušil [5].

**Odvolání souhlasu**

Subjekt údajů má právo kdykoli svůj souhlas odvolat. Pokud tak učiní je správce povinen přestat jeho údaje zpracovávat, pokud neprokáže oprávněné zákonné důvody zpracování. Obecné nařízení nově staví odvolání souhlasu na stejnou úroveň jako jeho udělení, to znamená že musí být stejně jednoduché [5].

**Souhlas dítěte**

Pokud se jedná o souhlas se zpracováním údajů pro potřeby nabídky služeb informační společnosti, je u osob mladších 16 let vyžadován souhlas rodičů. Jednotlivé státy mohou tuto věkovou hranici snížit až na 13 let [5].

### 1.2.3 Role a odpovědnosti

Správce osobních údajů byl definován již v předchozí právní úpravě. Obecné nařízení nově klade důraz na povinnosti zpracovatele a na odpovědnost správce a zpracovatele vůči subjektu údajů [5].

**Správce osobních údajů**

*„Správcem se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;“* [6, čl. 4 odst. 7]

Správce má odpovědnost za zákonné korektní zpracování osobních údajů. Osoba správce určuje činnosti, které jsou spojené se zpracováním, to znamená, že rozhoduje o tom:

- jaké osobní údaje budou shromažďovány,
- zda je zapotřebí souhlas subjektu,
- po jakou dobu budou údaje uchovávány,
- kdo bude data shromažďovat,
- jaký bude účel zpracování,

- jak budou data zabezpečena,
- jaká je míra rizika pro subjekt údajů,
- o informovanosti subjektu [5].

Může nastat situace kdy bude více společných správců, v tom případě je potřeba jasně stanovit vzájemnou odpovědnost a povinnosti. Správce má povinnost ujistit se o serióznosti svých dodavatelů a zjistit, zda poskytují dostatečné záruky zavedení potřebných opatření tak aby bylo vyhověno GDPR a zároveň byla zajištěna ochrana práv subjektů. To lze přiblížit příkladem kdy správce přes webové stránky nabízí formulář k vyřízení žádosti a stránky mu spravuje třetí osoba. Tím se z ní stává zpracovatel osobních údajů a musí minimalizovat rizika pro subjekt údajů. Správce je povinen zdokumentovat použitá opatření, sledovat je a kontrolovat jejich efektivitu. Zavedení kontrol, jejich opakování a vyhodnocování je jedna z povinností správce. Nelze tedy implementovat požadavky GDPR a tím považovat práci za hotovou. Jedná se o stálý proces, který je nutné pravidelně dokazovat a určité činnosti opakovat [5].

### Zpracovatel osobních údajů

Zpracovatelé jsou osoby, které mají přístup k osobním údajům, které shromáždil správce nebo je zpracovávají. Zpracovatelem může být i společnost, která osobní údaje nijak nezpracovává, ale jsou uloženy na jejích serverech. Mezi správcem a zpracovatelem musí být smluvní vztah, který musí splňovat specifické požadavky Obecného nařízení. Zpracovatel nese odpovědnost za bezpečné a spolehlivé zpracování osobních údajů. Zpracovatel nesmí bez vědomí správce přizvat dalšího zpracovatele do procesu. To znamená, že by nikdy neměla nastat situace, že by správce nevěděl, kdo nebo jak údaje zpracovává [5].

### Pracovní skupina WP29

Do začátku účinnosti Obecného nařízení byla dle ustanovení zřízena Pracovní skupina WP29, ta se skládá z jednoho zástupce dozorového úřadu každé členské země a jednoho zástupce Evropského inspektora ochrany údajů a Evropské komise. Ke dni účinnosti Obecného nařízení – 25. května 2018 – se Pracovní skupina změní na Evropský sbor pro ochranu osobních údajů (zkráceně Sbor) [7].

Pracovní skupina WP29 v návaznosti na případ zneužití dat desítek miliónů uživatelů sociální sítě Facebook vytvoří pracovní skupinu pro sociální média (SMWG – Social Media Working Group), protože se dá předpokládat, že se jedná pouze o jeden z mnoha případů zneužití dat ze sociálních médií [8].

### 1.2.4 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů (**Data Protection Officer = DPO**) je zaměstnanec nebo externí pracovník, který působí jako ochránce osobních údajů klientů, pacientů, zákazníků, zaměstnanců apod. Obecné nařízení stanoví povinnost jmenovat pověřence všem podnikům, které nabízejí služby nebo zboží zákazníkům z některého ze členských států Evropské unie a zpracovávají jejich osobní údaje. Pověřence musí jmenovat veškeré veřejné orgány, každý, kdo jako svou hlavní činnost pravidelně a systematicky monitoruje údaje subjektů ve velkém rozsahu nebo zpracovává osobní údaje zvláštní kategorie jako je rasa, náboženské přesvědčení nebo etnická příslušnost [5].

#### Povinnosti pověřence

Pověřenec by měl správci a zpracovateli osobních údajů poskytovat informace a poradenství. Pověřenec bude také dohlížet na soulad zpracování s Obecným nařízením. Pověřenec bude poskytovat poradenství v oblasti posouzení vlivu na ochranu osobních údajů (DPIA). Neposledním úkolem bude jeho spolupráce s dozorovým úřadem a fungování jako kontaktní místo. Pověřenec bude také komunikovat se subjekty a realizovat jejich práva, a to především právo být zapomenut, právo na informace a jejich stížnosti. Práce pověřence musí být nezávislá a vhledem k přístupu k citlivým údajům také důvěrná [5].

#### Kvalifikace pověřence

V Obecném nařízení je stanoveno, že:

*„Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39“* [6, čl. 37 odst. 5].

Konkrétní úroveň znalostí a odbornosti není stanovena, ale organizace musí vzít v potaz množství, složitost a citlivost dat, které zpracovává. Bylo by přinejmenším vhodné, aby jmenovaný pověřenec měl znalosti ochrany osobních údajů a GDPR a také odvětví ve kterém organizace působí [5].

**Možnosti jmenování pověřence**

Organizace, které mají dle Obecného nařízení povinnost jmenovat pověřence na ochranu osobních údajů mají několik možností:

- pověřenec z řad zaměstnanců,
- outsourcing pověřence,
- společný pověřenec pro veřejné subjekty [5].

První možností je jmenovat pověřence z řad svých zaměstnanců, je ale důležité dodržet požadavek na kvalifikaci pověřence a jeho nezávislost. U některých pozic navíc může docházet ke střetu zájmu, jedná se především o tajemníka, ředitele finančního odboru a vedoucí IT oddělení. Jejich prací je maximalizovat zisk a minimalizovat náklady, proto se dá předpokládat, že by nerozhodovali v souladu s Obecným nařízením [7].

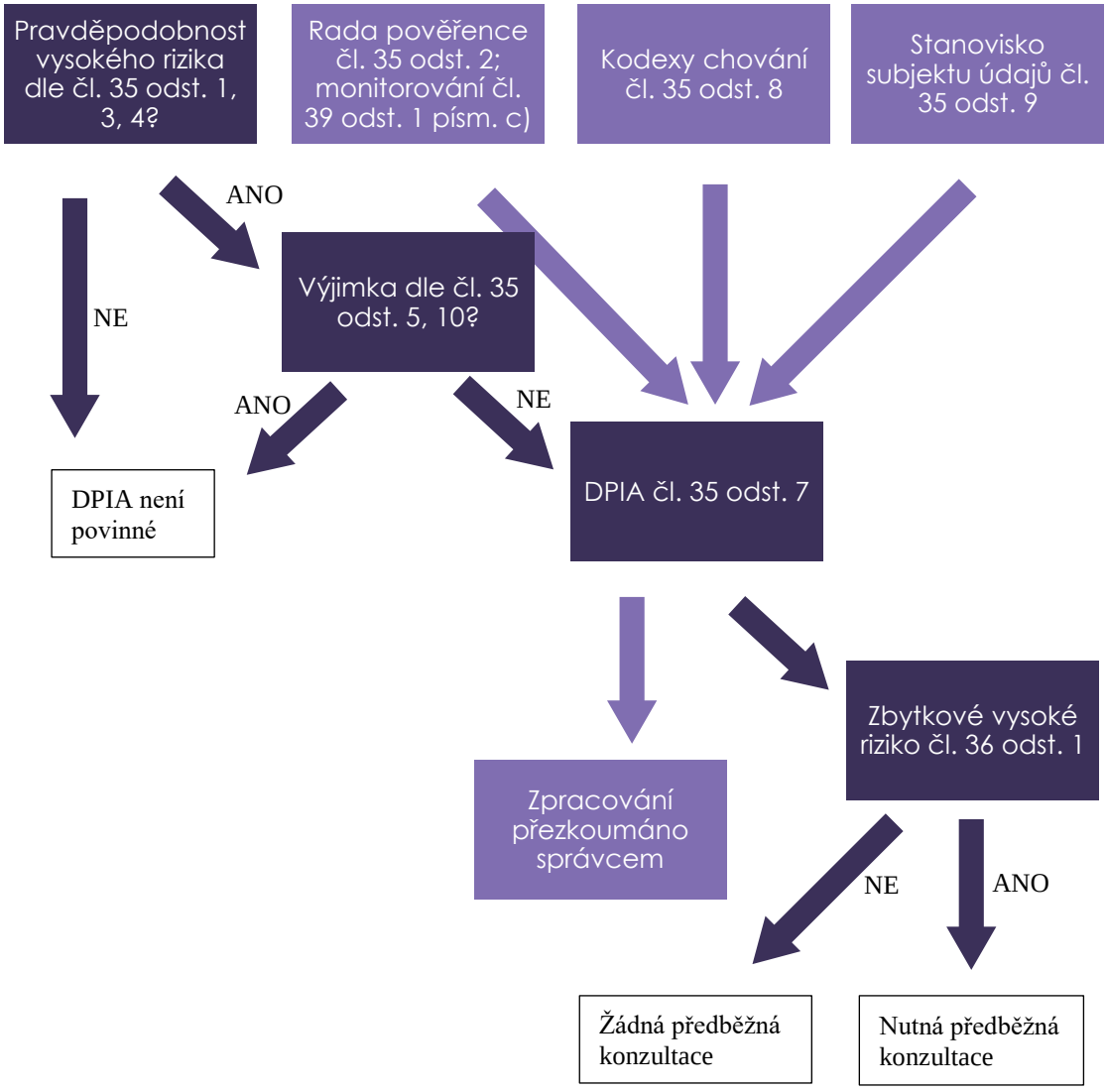
Druhou možností je najmutí pověřence od konzultační firmy nebo advokátní kanceláře. Ti budou mít lepší právní kvalifikaci, více zkušeností a pravděpodobně i pojištění pro případ způsobení škody. Smlouva s externím pověřencem může být po implementaci uzavřena úkolově, protože je možné, že služeb pověřence nebude potřeba každý den a tím může dojít ke snížení nákladů [5].

Orgány veřejné moci a veřejné subjekty mohou jmenovat společného pověřence na ochranu osobních údajů na základě vyššího správního celku nebo po dohodě několika správců, např. ve svazku obcí. Tím se náklady sníží na minimum [5]. V tomto případě se dle metodiky, kterou vydalo ministerstvo vnitra, pověřencem stává svazek obcí, přestože činnosti pověřence bude vykonávat jiná osoba. Smlouvu o poskytování služeb s pověřencem uzavře svazek v rámci svých stanov a jednotlivé obce již smlouvu uzavírat nemusejí [9].

### 1.2.5 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů (DPIA = Data Protection Impact Assessment) je proces, který slouží k doložení souladu s nařízením. Pokud je více zpracování osobních údajů velmi podobných, může být zpracováno jedno posouzení vlivu na ochranu osobních údajů pro tyto zpracování [5].

Posouzení vlivu je povinné, pokud *„je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob.“* [6, čl. 35 odst. 1]




**Obrázek 1: Diagram povinnosti DPIA** (Zdroj: Vlastní zpracování dle: 5, s. 101)

Pokud by nebylo jasné zda má organizace povinnost zpracovat posouzení vlivu Pracovní skupina WP29 doporučuje aby bylo provedeno [5].

### 1.2.6 Zásady zpracování osobních údajů

Tyto zásady můžeme považovat za základní stavební kameny ochrany osobních údajů. Tyto zásady nejsou revoluční, ve své podstatě existovali již v původní právní úpravě zákonu č. 101/2000 Sb., novinkou je jejich jasné vyjmenování, stanovení odpovědnosti a povinnosti dokládání souladu. Z nařízení vyplívají ještě další zásady:

- odpovědnost správce,
- povinnost prokazování,
- bezpečnost dat,
- mezinárodní transfery [5], [7].

**Zásada zákonnosti**

Jedná se o nejdůležitější zásadu, protože říká, že správce může osobní údaje zpracovávat či je mít pouze má-li k tomu alespoň jeden právní důvod. Pokud žádný právní důvod nemá nebo zanikne a zároveň neuplatní jiný právní důvod má povinnost osobní údaje zlikvidovat. Pokud uplatní jiný právní důvod pouze na část údajů, musí údaje, jejichž zpracování není pokryto tímto právním důvodem zlikvidovat [7].

Podle článku 6 Obecného nařízení je *„zpracování zákonné, pokud…:*

*a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*

*b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*

*c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*

*d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*

e) *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*

f) *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“* [6, čl. 6 odst. 1 písm. a) až f)]

**Zásada korektnosti a transparentnosti**

Správce nesmí zatajovat účel, pro který jsou osobní údaje zpracovávány, a zároveň by měl poskytovat informace o tom kdo, v jakém rozsahu a jak osobní údaje zpracovává a případně komu jsou předávány. Tato zásada dále požaduje, aby informace, které subjekt od správce dostává byly snadno přístupné a srozumitelné. Zásada transparentnosti bude také využita v případě porušení zabezpečení ochrany osobních údajů [7].

**Zásada omezení účelu**

V Obecném nařízení nazváno účelové omezení, to znamená, že osobní údaje musí být shromažďovány pro výslovně vyjádřené účely a nesmějí být zpracovávány způsobem neslučitelným s těmito účely. Od účelu zpracování se odvíjí právní důvody zpracování osobních údajů a další povinnosti. S touto zásadou dále souvisí čl. 25 odst. 2 Obecného nařízení, který ukládá správci povinnost zavést vhodná opatření k zajištění zpracovávání pouze takových osobních údajů, které jsou pro daný účel nezbytné [7].

**Zásada minimalizace údajů**

Tato zásada úzce souvisí se zásadou omezení účelu. Správce má povinnost zpracovávat osobní údaje pouze relevantní a v nezbytném rozsahu vztahující se ke stanovenému účelu zpracování [7].

**Zásada přesnosti**

Osobní údaje musí být v případě potřeby aktualizované, protože pouze přesné zpracování má cenu. Správce nemusí aktivně vyhledávat neaktuální a nepřesné údaje, ale měl by se opakovaně obracet na subjekt údajů s požadavkem na kontrolu a případnou aktualizaci

údajů. Správce také musí takovouto změnu umožňovat, případně nepřesné údaje vymazat [7].

**Zásada omezení uložení**

Vzhledem k tomu, že zpracování osobních údajů s sebou nese i bezpečnostní riziko je důležitou zásadou omezení uložení, která stanovuje, že by osobní údaje měli být zpětně identifikovatelné a uložené po dobu ne delší než stanovuje účel jejich zpracování. Likvidace osobních údajů může být provedena také anonymizací [7].

**Zásada integrity a důvěrnosti**

Osobní údaje by měly být zabezpečeny využitím vhodných technických nebo organizačních opatření na ochranu před neoprávněným či protiprávním zpracování nebo před náhodnou ztrátou, poškozením nebo zničením. Zabezpečení musí odpovídat povaze, rozsahu, kontextu a účelu zpracování [7].

### 1.2.7 Práva subjektu údajů

Práva subjektu údajů vyvažují vztah mezi správcem a subjektem údajů, který bývá nevyrovnaný, protože subjekt údajů často nemá možnost volby. Obecné nařízení ve srovnání se zákonem č. 101/2000 Sb. upravuje práva subjektu údajů mnohem podrobněji, to byl také jeden z důvodů vytvoření nového právního rámce. Nezbytnou podmínkou pro soulad zpracování osobních údajů je zajištění řádného výkonu práv subjektů údajů. Jmenování pověřence pro ochranu osobních údajů je významný článek pro zajištění souladu zpracování [5], [7].

Subjekt údajů má následující práva:

- právo být informován,
- právo přístupu,
- právo na opravu,
- právo být zapomenut (někdy také právo výmazu),
- právo zamezit zpracování,
- právo přenositelnosti dat,

- právo na stížnost,
- práva související s automatizovaným rozhodováním a profilováním [5].

### Právo na informace

Základním právem naplňujícím zásadu transparentnosti je právo na informace, které zaručuje informovanost subjektu o zpracování jeho osobních údajů. Obecné nařízení rozlišuje, zda jsou osobní údaje získané přímo od subjektu údajů či nikoli [7].

Informace poskytované v rámci tohoto práva musí být:

- srozumitelné, stručné, jasně napsané a snadno dostupné,
- zdarma a bez poplatků [5].

Následující tabulka shrnuje, jaké informace a kdy by měli správci poskytovat [5].

**Tabulka 1: Právo být informován** (Zdroj: 5, s. 84-85)

| Jaké informace musí být sdělovány? | Údaje získané přímo od subjektu údajů | Údaje nejsou získané přímo od subjektu údajů |
|---|---|---|
| Identifikační údaje a kontaktní údaje na správce a pověřence pro ochranu údajů | X | X |
| Účel zpracování a zákonné oprávnění pro zpracování | X | X |
| Oprávněné zájmy správce nebo případně třetí strany | | X |
| Kategorie osobních údajů | | X |
| Každý příjemce nebo kategorie příjemců osobních údajů | X | X |
| Podrobnosti o přesunech dat do třetích zemí a poskytnutých zárukách | X | X |
| Doba uchování nebo kritéria používaná k určení doby uchovávání | X | X |
| Existence jednotlivých práv subjektu údajů | X | X |

| Jaké informace musí být sdělovány? | Údaje získané přímo od subjektu údajů | Údaje nejsou získané přímo od subjektu údajů |
|---|---|---|
| Právo na odstoupení od smlouvy kdykoli, je-li to relevantní | X | X |
| Právo podat stížnost dozorovému orgánu | X | X |
| Zdroj, od kterého pocházejí osobní údaje a zda pochází z veřejně přístupných zdrojů | | X |
| Zda je poskytování osobních údajů součástí zákonného nebo smluvního závazku nebo požadavku a možné důsledky neposkytnutí osobních údajů | X | |
| Informace o existenci automatizovaného rozhodování, včetně profilování a informace o procesu rozhodování, jeho význam a možné důsledky | X | X |

Pokud správce získává osobní údaje přímo od subjektu údajů, je povinen informace poskytnout v tom okamžiku [5].

Pokud informace nezískal přímo od subjektu údajů, je povinen informace poskytnout:

- v přiměřené lhůtě, nejpozději však do 1 měsíce od získání údajů,
- pokud mají osobní údaje sloužit pro účely komunikace, tak nejpozději v okamžiku této komunikace,
- pokud mají být osobní údaje poskytnuty jinému příjemci, tak nejpozději předtím, než jsou poskytnuty [7].

**Právo na přístup k osobním údajům**

Podle Obecného nařízení má subjekt právo:

- získat potvrzení o tom, zda jsou jeho osobní údaje zpracovávány,
- získat přístup ke svým osobním údajům,
- nebo získat další informace [5].

Důvodem práva na přístup je možnost subjektu ověřit si zákonnost zpracování a získat informace o tom, že jsou jeho údaje zpracovávány. Správce je povinen první kopii poskytnout subjektu bezplatně. Pokud by se žádosti o přístup nepřiměřeně opakovaly, byly nepředmětné nebo nepřiměřené může správce za takovou žádost účtovat přiměřený poplatek, který musí odpovídat jeho nákladům [5].

**Právo na opravu a doplnění**

Pokud jsou osobní údaje neúplné nebo nepřesné subjekt údajů má právo na jejich opravu. Pokud byly osobní údaje předány třetím stranám má správce povinnost informovat je o změně. Správce musí žádosti o opravu vyhovět do jednoho měsíce od obdržení takové žádosti. Pokud by byla oprava složitá nebo obtížně splnitelná, může tuto lhůtu o dva měsíce prodloužit, pokud o tom informuje subjekt údajů. Pokud by žádosti nevyhověl, má subjekt právo podat stížnost dozorovému úřadu [5].

**Právo být zapomenut (právo na výmaz)**

Subjekt údajů má právo požádat správce, aby byly jeho údaje bez zbytečného odkladu vymazány, nezávisle na tom, zda existuje přesvědčivý důvod pro další zpracování. Toto právo však není absolutní, subjekt může požádat o vymazání, pokud je splněna jedna z těchto podmínek:

- osobní údaje již nadále nejsou potřebné, ani pro účely, pro které byly zpracovávány nebo shromážděny,
- pokud subjekt údajů odvolá svůj souhlas a neexistuje jiný právní důvod pro zpracování údajů,
- subjekt údajů vznese námitku proti zpracování údajů a zároveň neexistují žádné převažující právní důvody zpracování,
- osobní údaje subjektu byly zpracovány protiprávně,
- osobní údaje dítěte byly zpracovány bez souhlasu rodiče,
- osobní údaje musí být vymazány, aby byla splněna právní povinnost, která se vztahuje na správce [5], [7].

V těchto případech má subjekt právo na likvidaci údajů a zároveň správce má povinnost osobní údaje zlikvidovat. Podle předchozí směrnice, je právo na likvidaci údajů omezeno pouze na zpracování neodůvodněné nebo takové, které způsobuje škodu a újmu. Podle Obecného nařízení se nemusí jednat o takové zpracování, ale pokud ano, je potřeba výmazu ještě silnější [5].

Z následujících důvodů je možné právo na výmaz odmítnout:

- při uplatnění práva na informace a svobodu projevu,
- pro potřeby zákonné povinnosti nebo splnění úkolu ve veřejném zájmu nebo pro výkon veřejné moci,
- pro účely veřejného zájmu v oblasti veřejného zdraví,
- pro účely archivace, pokud se jedná o veřejný zájem, pro účely historického nebo vědeckého výzkumu nebo pro statistické účely,
- z důvodu výkonu nebo obhajoby právních nároků [5].

V případě, že správce osobní údaje zveřejňuje a vznikne mu povinnost údaje zlikvidovat, musí s ohledem na náklady a dostupnost technologie přijmout kroky a informovat další správce, kteří mohou nadále údaje zpracovávat, o žádosti subjektu na likvidaci údajů, jejich kopií i replikací. Toto ustanovení posiluje právo být zapomenut na internetu [7].

**Právo na omezení zpracování**

Podle zákona o ochraně osobních údajů bylo také možné pozastavit zpracování osobních údajů. Pokud dojde k omezení zpracování má správce možnost osobní údaje ukládat, ale nesmí je nijak zpracovávat [5].

Subjekt údajů má právo požadovat pozastavení zpracování osobních údajů a správce k tomu musí přistoupit, pokud:

- subjekt zpochybní přesnost osobních údajů, a to po dobu potřebnou k tomu, aby správce ověřil přesnost osobních údajů,
- subjekt údajů vznese námitku proti zpracování, musí být ověřeno, zda převažují oprávněné důvody správce či subjektu,
- zpracování údajů je protiprávní, ale subjekt odmítá jejich výmaz,

- správce údaje nadále nepotřebuje, ale subjekt osobních údajů je požaduje z důvodu určení, výkonu nebo obhajoby právních nároků [7].

Stejně jako u předchozího práva, pokud správce osobní údaje zpřístupnil třetím stranám, musí jim oznámit omezení zpracování těchto údajů [5].

**Právo na přenositelnost údajů**

GDPR nově zavádí právo přenositelnosti údajů, které umožňuje, aby subjekt získal své osobní údaje, které poskytl správci, ve strukturovaném, strojově čitelném a běžně používaném formátu a zároveň je předat jinému správci. K tomu může využít původního správce, který tomu nesmí bránit. Podmínkou je automatizované zpracování osobních údajů na základě smlouvy nebo souhlasu subjektu údajů [7].

„*Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl 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.*“ [5, s. 89]

Právo přenositelnosti údajů lze využít například při změně telefonního operátora, kdy si nový operátor vyžádá informace od stávajícího operátora [5].

Data poskytnutá správci údajů nejsou pouze ta data, která subjekt poskytl vědomě, ale také data získaná automaticky sledováním činnosti subjektu. Jedná se například o cookies, záznamy činností, historie vyhledávání nebo historie navštívených stránek. Dále se jedná o data, která subjekt aktivně poskytuje například uživatelské jméno, email, věk atd., nebo data získaná používáním aplikace, zařízení nebo internetové služby [5].

**Právo vznést námitku**

Subjekt má právo vznést námitku, pokud neměl možnost uplatnit některé ze svých práv. Subjekt musí být na možnost vznést námitku vždy upozorněn. Subjekt má právo vznést námitku proti:

- zpracování za účelem historického nebo vědeckého výzkumu a statistiky,
- zpracování pro účely direct marketingu,

- zpracování pro výkon veřejné moci nebo plnění úkolu ve veřejném zájmu nebo založené na oprávněných důvodech [5].

Pokud subjekt vznese námitku proti zpracování osobních údajů, správce jeho údaje nesmí nadále zpracovávat, dokud neprokáže, že jeho oprávněné důvody zpracování převyšují zájmy, práva a svobody subjektu nebo pro vznik, výkon nebo obranu právních nároků. Pokud subjekt vznese námitku proti zpracovávání osobních údajů pro účely přímého marketingu, správce má povinnost přestat údaje zpracovávat [7].

Správce nemusí pozastavit zpracování osobních údajů, pokud:

- prokáže přesvědčivé oprávněné důvody zpracování údajů, které převažují nad zájmy, právy a svobodami subjektu,
- zpracování slouží k určení, výkonu nebo obhajobě právních nároků [5].

**Právo nebýt předmětem automatizovaného individuálního rozhodování**

Toto právo je součástí jak zákona o ochraně osobních údajů, tak i směrnice 95/46/ES. Subjekt osobních údajů má právo nebýt předmětem rozhodnutí založených na automatizovaném zpracování a profilování [7].

Z následujících důvodů může být automatizované rozhodování využito:

- rozhodnutí je nezbytné k plnění nebo uzavření smlouvy mezi správcem a subjektem údajů,
- rozhodnutí je povoleno právem členského státu nebo Unie, které se na správce vztahuje a zároveň stanovuje vhodná opatření k ochraně oprávněných zájmů subjektu, jeho práv a svobod,
- subjekt údajů dal k rozhodnutí výslovný souhlas [5].

Subjekt by měl být při udělování souhlasu se zpracováním osobních údajů informován o možném profilování a o tom, zda údaje musí poskytnout a o následcích v případě jejich neposkytnutí [5].

**Profilování**

Jedná se o formu automatizovaného zpracování údajů, ty jsou použity k hodnocení subjektu jeho ekonomické situace, osobních preferencí, pracovního výkonu, spolehlivosti, pohybu nebo zdravotního stavu. Současný zákon o ochraně osobních údajů ani GDPR profilování nezakazuje, ale určuje pravidla a případy kdy může být využito. Běžný příklad profilování je banka, která hodnotí (profiluje) klienta, jeho spolehlivost a schopnost splácet [5].

### 1.2.8 Omezení práv a zásad zpracování

Práva a zásady mohou být podle návrhu zákona o zpracování osobních údajů omezeny či odloženy v případě nebo k předejití vážného ohrožení obrany státu, vyšetřování trestných činů, nezávislosti soudnictví nebo jiných veřejných zájmů Unie nebo členského státu [7].

### 1.2.9 Dozorový úřad

Dozorovým úřadem je v České republice Úřad pro ochranu osobních údajů (zkráceně ÚOOÚ). Dozorový úřad bude provádět kontroly, některé evropské dozorové úřady již zveřejnily metodiku kontrol, pro jejich snadný průběh [5].

**Sankce a pokuty**

Správní pokuty by měly být přiměřené, účinné a odrazující. Jejich výše je stanovena na základě každého případu. Znamená to tedy, že ne vždy musí být udělena pokuta. Správce může dostat upozornění nebo napomenutí, že jeho zpracování není v souladu s Obecným nařízením nebo mu dozorový úřad může nařídit uvedení zpracování do souladu s nařízením [5].

Maximální výše pokut je rozdělena do dvou kategorií na základě dopadu, který bude porušení povinností mít na práva subjektu údajů. Do nižší kategorie spadá např. *„porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů“* [5, s. 44]. Maximální výše pokuty je 10 miliónů EUR nebo až 2 % celkového ročního obratu. Do vyšší kategorie spadá *„porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva*

*subjektu údajů"* [5, s. 44]. Maximální výše pokuty je stanovena na 20 miliónů EUR nebo 4 % celkového ročního obratu [5].

V článku 83 Obecného nařízení jsou vyjmenovány okolnosti, které mohou být polehčující nebo přitěžující pro určení výše pokuty. Jedná se například o to, zda bylo porušení úmyslné či z nedbalosti, jak dlouho porušení trvalo, jeho závažnost, počet dotčených subjektů, kroky, jaké správce podnikl nebo jeho spolupráce s ÚOOÚ [5].

**Hlášení incidentu**

Správce má povinnost nahlásit dozorovému úřadu každý incident bez zbytečného odkladu nebo do 72 hodin od doby kdy ho zjistil. Pokud navíc existuje vysoké riziko ohrožení práv a svobod subjektu, má správce povinnost informovat i jej. Existují i výjimky kdy správce nemusí o incidentu subjekt informovat:

- správce používá pro ochranu OÚ šifrování nebo jiné ochranné opatření,
- správce zajistil, aby se vysoké riziko již neprojevilo,
- pokud by musel vynaložit nepřiměřené úsilí, v tom případě může subjekt informovat například pomocí veřejného oznámení [5].

Hlášení subjektu by měl správce provést ve spolupráci s dozorovým úřadem, mělo by být jasné a srozumitelné a obsahovat základní informace o:

- pověřenci na ochranu osobních údajů, především jméno a kontaktní údaje,
- jaké důsledky bude incident pravděpodobně pro subjekt mít,
- popis opatření, která správce přijal v návaznosti na incident [5].

Vzorové hlášení incidentu subjektu údajů viz příloha 3.

V hlášení dozorovému úřadu musí navíc být uveden popis porušení bezpečnosti osobních údajů, odhadovaný počet ohrožených subjektů, kategorií osobních údajů a počet ohrožených záznamů osobních údajů (vzor viz příloha 4). Zpracovatel osobních údajů má povinnost incident bezodkladně hlásit správci, aby mohl přistoupit k jeho řešení [5].

#### Záznamy zpracování

Organizace mají povinnost vést záznamy o zpracování, které prokazují soulad s Obecným nařízením. Mezi takové dokumenty patří například směrnice pro práci s osobními údaji, potvrzení o informování subjektu o zpracování jeho osobních údajů, potvrzení o souhlasu získaném od subjektu údajů nebo zpráva o posouzení vlivu, mezi další dokumenty patří důkaz o aplikaci těchto zásad, např. záznam o školení. V případě kontroly dozorovým orgánem je organizace povinna tyto dokumenty předložit [5].

Organizace, které mají méně než 250 zaměstnanců nemají povinnost vést záznamy o činnostech zpracování. Tuto výjimku ztrácí pokud jejich zpracování není příležitostné, zpracování je vysoce rizikové pro subjekty údajů, zpracovávají osobní údaje zvláštní kategorie nebo osobní údaje, které se týkají trestných činů. Správce osobních údajů má povinnost vést záznamy o činnostech zpracování v případě, že osobní údaje zpracovává třetí strana. Zpracovatel má povinnost vést tyto záznamy v případě, že osobní údaje zpracovává jménem správce [5].

### 1.2.10 Zabezpečení osobních údajů

Zabezpečení osobních údajů pomocí šifrování nebo pseudonymizace není povinné, je však doporučené. V případě bezpečnostního incidentu a využívání jedné z těchto metod zabezpečení, se na správce nemusí vztahovat oznamovací povinnost, je však důležité posoudit každý případ individuálně [5].

#### Anonymizace

Anonymizace je proces zpracování osobních údajů, tak že již nelze identifikovat subjekt údajů, ale většina údajů zůstane zachována, většinou se jedná o nahrazení jména, příjmení a adresy číselným kódem, tak aby ostatní údaje mohly být nadále využity. Anonymizace je povinná u zpracování pro vědecké, statistické nebo archivní účely [4].

#### Pseudonymizace

Pseudonymizace je proces při kterém jsou osobní údaje zpracovávány takovým způsobem, že již nemohou zpětně identifikovat subjekt údajů, bez využití dalších

informací. V databázi jsou osobní údaje doplněny jedním nebo více umělými identifikátory (pseudonymy) a podle nich rozděleny do více tabulek [5].

**Tabulka 2: Data bez pseudonymizace** (Zdroj: Vlastní zpracování dle: 5, s. 115)

| ID | Jméno | Příjmení | Věk | Navštěvovaná škola |
|---|---|---|---|---|
| 1 | Karel | Nový | 24 | VUT v Brně |

**Tabulka 3: Pseudonymizovaná data** (Zdroj: Vlastní zpracování dle: 5, s. 116)

| ID | Jméno | Příjmení |
|---|---|---|
| 1 | Karel | Nový |

| ID | Věk | Navštěvovaná škola |
|---|---|---|
| 1 | 24 | VUT v Brně |

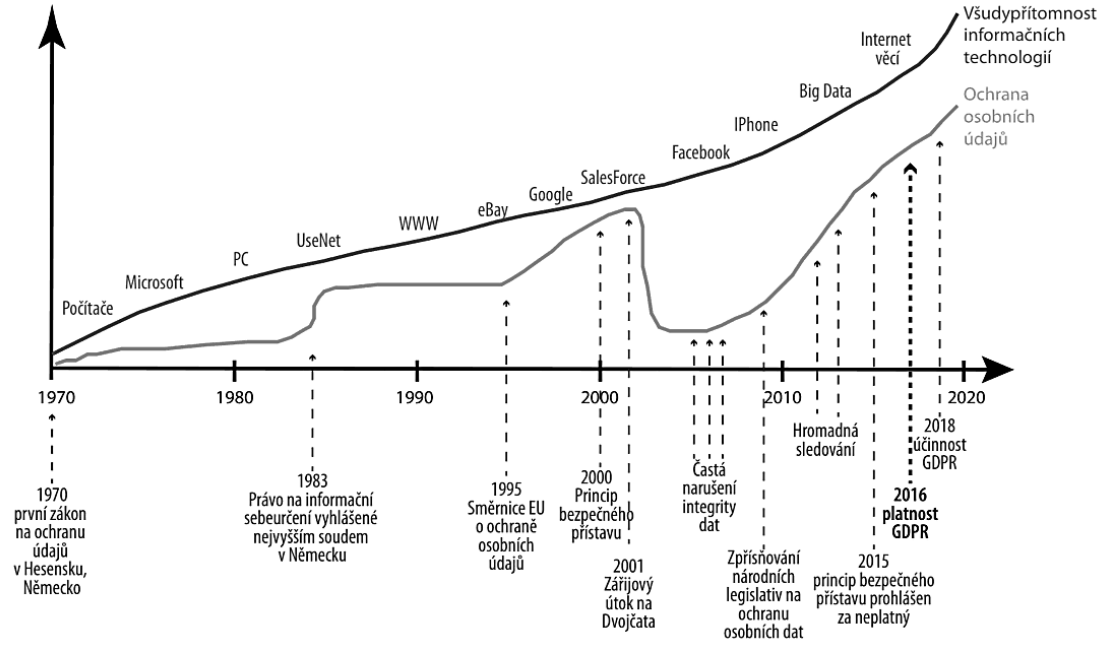
### Šifrování

Šifrování je převádění dat do číselné podoby, která se bez znalosti klíče nedá převést zpět. Šifrování dat je vhodná ochrana osobních údajů. Šifrovat lze na několika úrovních:

- šifrování celého disku zařízení,
- šifrování dat při sdílení,
- šifrování dat v databázi [5].

## 1.2.11 Historie GDPR

Technologie se vždy vyvíjejí rychleji než legislativa. Důležitá je doba reakce právních norem na technologické změny. Níže je stručně popsána historie ochrany osobních údajů [5].




**Obrázek 2: Vývoj legislativy v porovnání s vývojem technologií** (Zdroj: 5, s. 15)

**28. leden 1981** – Evropská rada přijala úmluvu o ochraně osob s ohledem na automatické zpracování osobních údajů

**4. říjen 1995** – Vytvořena evropská směrnice 95/46/ES o ochraně osobních údajů

**4. duben 2000** – Česká republika přijímá zákon č. 101/2000 Sb. o ochraně osobních údajů

**1. prosinec 2009** – Vznik Pracovní skupiny WP29

**25. leden 2012** – Evropská komise navrhuje kompletní reformu ochrany osobních údajů v EU

**12. březen 2014** – Evropský parlament odhlasoval GDPR

**27. duben 2016** – GDPR vstupuje v platnost

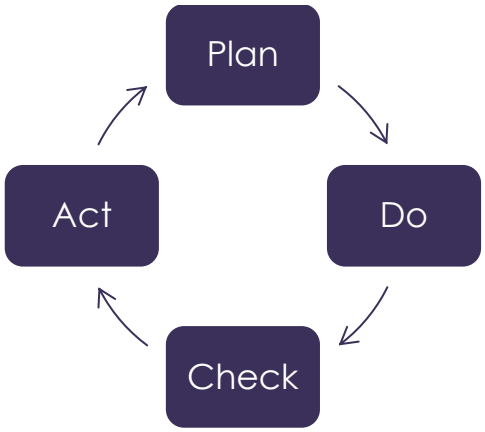
**25. květen 2018** – GDPR vstupuje v účinnost

## 1.3 ISMS

Název Information Security Management System znamená Systém řízení informační bezpečnosti. Z toho se dá vyvodit, že se jedná o řízení bezpečnosti informací. ISMS je součástí řízení organizace a zakládá se na Demingově modelu:

- plan – plánuj – analýza a návrh ISMS,

- do – dělej – implementace systému,
- check – kontroluj – sledování a zpětná vazba,
- act – jednej – zapracování změn [1].




**Obrázek 3: Demingův model** (Zdroj: Vlastní zpracování dle: 1, s. 25)

### 1.3.1 Historie ISMS

V začátcích se ochrana informací zabývala hlavně důvěrností, s rozvojem techniky bylo zapotřebí zaměřit se na ochranu elektronických dat, proto vznikl obor zabývající se ochranou dat [1].

**Knihovna ITIL** – byla publikována v letech 1989 až 1995, v letech 2000 až 2004 byla publikována druhá verze. Původní verze obsahovala 31 souvisejících svazků, ta byla poté zrevidována a nahrazena sedmi těsněji souvisejícími a konzistentními svazky – ITIL V2. Ta začala být v mnoha zemích akceptována jako základna pro efektivní poskytování služeb IT. V roce 2007 vyšla třetí verze, která obsahuje pět klíčových svazků obsahujících životní cyklus služeb [1].

**Metodika COBIT** – první verze byla publikována v roce 1996, v roce 1998 vyšla druhá verze rozšířená o „Management guidelines“, další verze následovaly v letech 2000, 2005 a od jara 2012 je dostupná verze COBIT 5 [1].

**Metodika CRAMM** – vznikla ve Velké Británii v roce 1985, postupným vývojem vznikaly nové verze. Aktuální verze CRAMM 5.2 obsahuje nejnovější verze normy ISO/IEC 27001:2005 [1].

**CC – Common Criteria** – CC vznikla sjednocením dříve existujících standardů ITSEC, CTCPEC a TCSEC [1].

**Asociace ISACA** – V České republice působí od roku 1997 jako ISACA Czech Republic Chapter, která sdružuje odborníky z oblastí kontroly, řízení, auditu a informační bezpečnosti [1].

### 1.3.2 Hodnocení rizik

Aby bylo možné ohodnotit rizika je nutné nejdříve ohodnotit aktiva. K ohodnocení aktiv je zapotřebí aktiva nejprve identifikovat. Při identifikaci aktiv se doporučuje veškerá aktiva, která k sobě logicky patří, seskupit do jedné skupiny a následně určit vlastníka každého aktiva. Poté je zapotřebí stanovit stupnici a hodnotící kritéria, která budeme používat k přiřazení ohodnocení jednotlivých aktiv. Pro větší přehlednost se využívá barev [1].

**Tabulka 4: Hodnocení aktiv** (Zdroj: 1, s. 82)

| | | | |
|---|---|---|---|
| 1 | | Žádný dopad na organizaci | Bezvýznamné riziko |
| 2 | | Zanedbatelný dopad na organizaci | Akceptovatelné riziko |
| 3 | | Potíže či finanční ztráty | Nízké riziko |
| 4 | | Vážné potíže či podstatné finanční ztráty | Nežádoucí riziko |
| 5 | | Existenční potíže | Nepřijatelné riziko |

#### Výpočet hodnoty aktiva

Existuje mnoho postupů pro výpočet ohodnocení aktiva. Nejpoužívanějším a zároveň nejjednodušším způsobem je tzv. součtový algoritmus:

$$\frac{Dostupnost + Důvěrnost + Integrita}{3}$$

Takto vypočítaná hodnota aktiva nám značí, jaký dopad pro společnost bude mít poničení nebo zničení daného aktiva [1].

### Bezpečnostní hrozby

Bezpečnostní hrozba může způsobit incident, který může poškodit organizaci, její systém nebo aktiva. Hrozby se dělí podle původu na přírodní (povodeň, požár, pád stromu) nebo způsobené lidským faktorem (chyba uživatele, odposlech). Dále můžeme hrozby rozlišovat podle úmyslu na náhodné (vymazání dat) nebo úmyslné (odcizení, poškození). Nakonec se dělí na podle zdroje na vnitřní a vnější a podle dopadu, který na systém mají, na aktivní a pasivní [1].

### Analýza rizik

Analýza rizik pomáhá zjistit jaké hrozby na aktiva působí a jak jsou pravděpodobné. Také díky ní lze zjistit, jaká je míra rizika. Ta se dá vypočítat součinem hodnocení aktiva, pravděpodobnosti hrozby a zranitelnosti aktiva [5].

**Tabulka 5: Pravděpodobnost hrozby a zranitelnost aktiva** (Zdroj: Vlastní zpracování dle: 5, s. 126)

| Pravděpodobnost hrozby | | Zranitelnost aktiva | |
|---|---|---|---|
| 1 | Nahodilá | 1 | Bezvýznamné riziko |
| 2 | Nepravděpodobná | 2 | Akceptovatelné riziko |
| 3 | Pravděpodobná | 3 | Nízké riziko |
| 4 | Velmi pravděpodobná | 4 | Nežádoucí riziko |
| 5 | Trvalá | 5 | Nepřijatelné riziko |

**Tabulka 6: Míra rizika** (Zdroj: 5, s. 127)

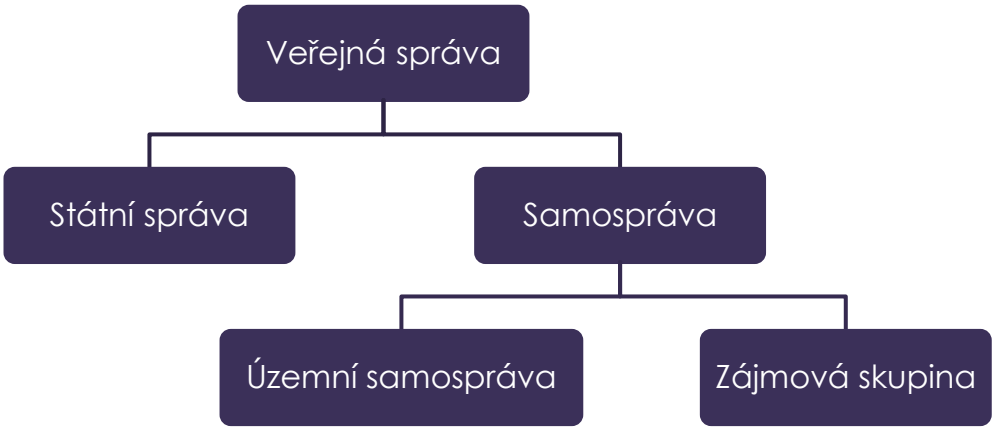
| Míra rizika | | |
|---|---|---|
| 1 | > 3 | Bezvýznamné riziko |
| 2 | 3–10 | Akceptovatelné riziko |
| 3 | 11–50 | Mírné riziko |
| 4 | 51–100 | Nežádoucí riziko |
| 5 | < 100 | Nepřijatelné riziko |

## 1.4 Veřejná správa

Veřejnou správu lze rozdělit ze dvou hledisek:

1. z hlediska toho, zda ji stát vykonává svými orgány, či přenechává část záležitostí na nestátní veřejnoprávní korporace, aby je samospravovaly,
2. z geografického hlediska [10].

Dle prvního kritéria lze státní správu chápat jako systém, který je tvořen dvěma částmi: státní správa a veřejná samospráva. Státní správu vykonává sám stát prostřednictvím institucí přímo nebo zprostředkovaně (územní samosprávou). Veřejná samospráva může mít podobu územní nebo zájmové samosprávy [10].




**Obrázek 4: Schéma veřejné zprávy dle prvního hlediska** (Zdroj: Vlastní zpracování dle: 10, s. 12)

Podle druhého kritéria je územní veřejnou správou označována veřejná správa vykonávána rámci příslušných územně administrativních jednotek, na které se stát dělí. Na této úrovni je nutné rozlišovat, zda se jedná o územní orgány veřejné správy se všeobecnou působností, omezenou působností nebo orgány samosprávy a státní správy. Někdy se můžeme setkat i s pojmem místní správa, který označuje nejnižší stupeň územní veřejné správy [10].

### 1.4.1 Státní správa

Státní správa je přímo či zprostředkovaně řízena vládou, která je orgánem se všeobecnou působností a v oblasti správy sjednocuje, koordinuje a kontroluje činnost ministerstev a dalších ústředních orgánů státní správy. V České republice existuje na úrovni územní veřejné správy smíšený model. Na úrovni obcí i krajů, je státní správa a územní samospráva vykonávána v rámci jedné jednotky. Státní správu mohou také vykonávat orgány samosprávy, v tom případě mluvíme o přenesené státní správě [10].

V České republice máme dvoustupňový systém územní státní správy:

1. obecní úřady – anebo pověřené obecní úřady a úřady s rozšířenou působností,
2. krajské úřady – ty vznikly na základě zákona č. 347/1997 Sb., ústavní zákon vymezil jednotlivé kraje a jejich území na základě stávajících okresů.

Jak obce, tak i kraje vykonávají státní správu v přenesené působnosti. V roce 2002 došlo v druhé fázi reformy územní veřejné správy k ukončení činnosti okresních úřadů a jejich působnost byla přenesena na krajské a obecní úřady s rozšířenou působností [10].

### 1.4.2 Samospráva

Samospráva se v České republice také dělí na dvoustupňový systém:

1. stupněm je obec – někdy se také používá výraz místní samospráva,
2. stupněm je kraj.

Územní samospráva nemá hierarchickou strukturu, každý územní samosprávný celek má své kompetence a nesmí zasahovat do jiných území [10].


**Obrázek 5: Členění krajů a krajská města ČR** (Zdroj: 11)

## 1.5 Obec

Obec je základní územní celek státu, který tvoří obyvatelé a je vymezen hranicí území obce. Je vymezena jako veřejnoprávní korporace, která má vlastní finanční prostředky a majetek a sestavuje vlastní rozpočet. Obec pečuje o rozvoj a potřeby svých obyvatel. Obec může být označena jako město, pokud splní stanovená kritéria. Existuje pět druhů obcí:

1. obec,
2. město,
3. městys,
4. statutární město,
5. Praha [12].

### 1.5.1 Orgány obce

Hlavním orgánem obce je zastupitelstvo, které obec samostatně spravuje. Mezi další orgány obce patří rada obce, starosta, obecní úřad a zvláštní orgány obce [12].

### Zastupitelstvo obce

Počet členů zastupitelstva je stanoven s ohledem na počet obyvatel a velikost území obce v souladu se zákonem č. 128/2000 Sb. a je vyhlášen nejpozději do 85 dnů před volbami [12].

**Tabulka 7: Počet členů zastupitelstva** (Zdroj: Vlastní zpracování dle: 12, § 68)

| Počet obyvatel obce | Počet členů zastupitelstva |
|---|---|
| Do 500 | 5 až 15 |
| 500 až 3000 | 7 až 15 |
| 3000 až 10000 | 11 až 25 |
| 10000 až 50000 | 15 až 35 |
| 50000 až 150000 | 25 až 45 |
| Nad 150000 | 35 až 55 |

Zastupitelstvo zřizuje výbory jako své pomocné orgány, ze zákona musí zřídit kontrolní a finanční výbor [12].

### Rada obce

Obecní rada je tvořena starostou, místostarostou a členy z řad zastupitelstva. Počet členů obecní rady je lichý a nesmí být vyšší než jedna třetina počtu zastupitelů, minimálně má 5 a maximálně 11 členů. V obci kde je méně jak 15 členů zastupitelstva se rada nevolí a její funkci zastává starosta. Rada obce je oprávněna zřídit jako své iniciativní a poradní orgány komise [12].

### Starosta

Starosta navenek zastupuje obec. V případě nepřítomnosti ho zastupuje místostarosta. Společně s místostarostou je volen členy zastupitelstva ze členů zastupitelstva, kterým odpovídá za svou činnost. Starosta podepisuje právní předpisy obce a se souhlasem ředitele krajského úřadu jmenuje a odvolává tajemníka obecního úřadu [12].

**Obecní úřad**

Obecní úřad tvoří starosta, který je v jeho čele, místostarosta či místostarostové, tajemník obecního úřadu, pokud je tato funkce zřízena, a zaměstnanci. Tajemník odpovídá za plnění úkolů starostovi [12].

### 1.5.2 Správa obce

Obec své záležitosti spravuje samostatně (samostatná působnost). Státní správu, která byla svěřena orgánům obce vykonává jako přenesenou působnost [12].

**Samostatná působnost**

Do samostatné působnosti patří hlavně záležitosti, které jsou v zájmu obce a jejích občanů. Obec v souladu s místními předpoklady a zvyklostmi pečuje o vytváření podmínek pro uspokojování potřeb občanů a rozvoj sociální péče. Jedná se o potřeby informací, výchovy a vzdělávání, celkového kulturního rozvoje, ochrany a rozvoje zdraví, dopravy, spojů, bydlení a ochrany veřejného pořádku. Obec může zřizovat a zakládat právnické osoby, organizační složky obce a obecní policii. Obec může ukládat povinnosti obecně závaznou vyhláškou. Obce mohou vzájemně spolupracovat, i s obcemi jiných států, nebo vytvářet a vstupovat do svazku obcí [12].

**Přenesená působnost**

Obce, které plní úkoly v přenesené působnosti dostávají příspěvek ze státního rozpočtu. Pokud byla orgánu obce zákonem svěřena státní správa, vykonává ji jako svou přenesenou působnost. Obec v přenesené působnosti může v souladu se zákonem vydávat nařízení obce [12].

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

- **obce se základním rozsahem přenesené působnosti**,
- **obce s pověřeným obecním úřadem** – vedle přenesené působnosti vykonává přenesenou působnost určenou zvláštními zákony ve správním obvodu určeném prováděcím právním předpisem,

- **obecní úřady obcí s rozšířenou působností** – vedle přenesené působnosti vykonává přenesenou působnost určenou zvláštními zákony ve správním obvodu určeném prováděcím právním předpisem [12].

### 1.5.3 Spisový a skartační řád

Doba uložení veškerých dokumentů ve veřejné správě se řídí spisovým a skartačním řádem. Ten je definován především zákonem č. 499/2004 Sb. o archivnictví a spisové službě a vyhláškou č. 259/2012 Sb. o podrobnostech výkonu spisové služby. Do výkonu spisové služby také vstupuje zákon č. 101/1999 Sb. o ochraně osobních údajů a nově také Obecné nařízení. Na stránkách Ministerstva vnitra ČR je k dispozici vzorový skartační řád, který většina organizací využívá [9].

Skartační lhůta je upravena jednotlivými zákony a standardně trvá 5 nebo 10 let, výjimku z pohledu obcí tvoří evidence obyvatel, kde je lhůta 75 let od úmrtí nebo pozbytí občanství, dále matrika, kde je lhůta 100 let pro knihu narození a 75 let pro knihy manželství, úmrtí a partnerství a evidence cestovních a občanských průkazů kde je lhůta 15 let od pozbytí platnosti dokladu [13].

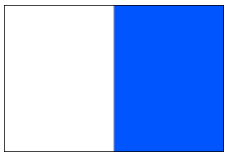
# 2 ANALÝZA SOUČASNÉHO STAVU

V této části představím obec Dolní Dobrouč, poté provedu analýzu fungování obce a připravenosti na GDPR. Údaje o obci jsou získané z jejích internetových stránek.

## 2.1 Základní údaje o obci

| | |
|---|---|
| **Kraj:** | Pardubický |
| **Okres:** | Ústí nad Orlicí |
| **Statut:** | Městys |
| **Starosta:** | Pavel Šisler |
| **Místostarosta:** | Ing. Vladimír Hovad |
| **Počet obyvatel:** | 2593 (k 1. 1. 2017) |
| **Počet zastupitelů:** | 15 |
| **Počet členů rady obce:** | 5 |

**Obrázek 6: Obecní znak**



**Obrázek 7: Obecní vlajka**

Obec Dolní Dobrouč se nachází v pardubickém kraji a leží asi 8 km severovýchodně od okresního města Ústí nad Orlicí. Vine se údolím podél potoka Dobroučka v délce přibližně 4 km. Původní německý název *„Libenthal“* znamená „ves v milém údolí“.

Dolní Dobrouč dále pokračuje místní částí Horní Dobrouč, původně nazývané *„Dittersbach“*, která je taktéž úzká a táhne se podél Dětřichova potoka.

Třetí místní částí Dolní Dobrouče je Lanšperk, který se rozléhá na návrší pod stejnojmennou zříceninou hradu asi 3 km jihozápadně od Dolní Dobrouče.

### 2.1.1 Historie obce

**1292** – První písemná zmínka o obci

**1429** – obléhání hradu Lanšperk husity

**1467** – poprvé doložen český název obce Nider Dobrucz

**1723** – nejstarší doložená obecní pečeť

**1765** – obnovena fara Dolní Dobrouč

**1873** – Dobrouč povýšena na městys

**1976** – Horní Dobrouč a Lanšperk připojeny k Dolní Dobrouči

**1977** – Dolní Dobrouč získává obecní znak (na obrázku výše)

**1978** – osada Václavov oddělena od katastrálního území Lanšperk

**1982** – Dolní Dobrouč se stává střediskovou obcí

**1999** – Dolní Dobrouč se stává členem svazku obcí *Region Orlicko – Třebovsko*

**1999** – Dolní Dobrouč uzavírá dohodu o přátelství s italským městem Roverto

**2004** – Dolní Dobrouč získává obecní vlajku (na obrázku výše)

## 2.2 Činnosti obce

Dolní Dobrouč je obec se základní rozšířenou působností. Agendy, které obec nevykonává si musí obyvatelé vyřídit v okresním městě Ústí nad Orlicí.

Poskytovaná agenda:

- agenda spojená s chodem obce a úřadu (účetnictví, personalistika, veřejné zakázky),
- evidence obyvatel,
- spisová služba,
- vedení matriky,
- vedení obecní kroniky,
- volby a jejich agenda,
- Czechpoint,
- místní poplatky,
- poskytování informací dle zákona č. 106/1999 Sb. o svobodném přístupu k informacím.

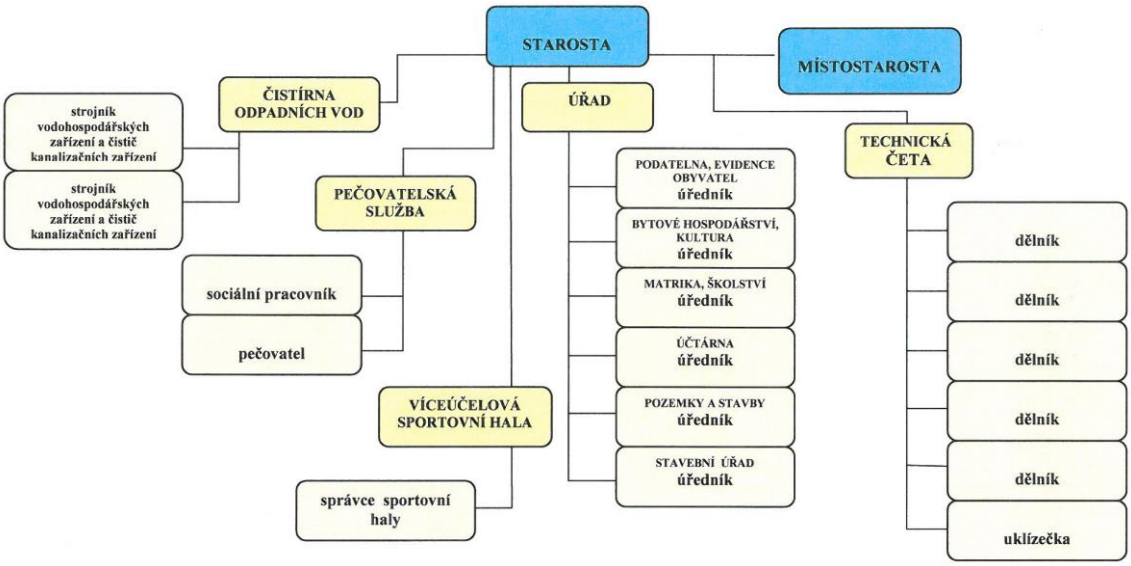
Obec využívá informační systém veřejné správy Munis a obecní webovou stránku. Informační systém je uložen na serverech dodavatele, obec tedy nemá žádné datové

centrum. Obec má Facebookové stránky, kde ale neuveřejňuje žádný obsah, veškeré příspěvky jsou od veřejnosti.

Obec používá fyzické i elektronické ukládání dat. V případě fyzického ukládání se jedná o listinné dokumenty uložené v zamykatelných skřínkách, tzv. kartotékách, které jsou umístěné v kanceláři jednotlivých úředníků, kteří s nimi pracují. Klíče od skřínek jsou během úřední doby zastrčené v zámku, po skončení úřední doby jsou uschovány v šuplíku pracovního stolu. Nejsou tedy nijak vhodně zabezpečeny.

Počítače, které úředníci využívají jsou průměrně 5 let staré, výkonově již nestačí, a proto je práce s nimi pomalá. Počítače mají základní ochranu ve formě antivirového programu. Počítačovou síť má na starost externí správce IT. Obecní úřad má jednu síťovou tiskárnu s automatickým tiskem pro dvě patra kanceláří. To je z hlediska GDPR nepřijatelné, protože než úředník patro sejde, může do dokumentů kdokoli nahlížet nebo je záměrně či omylem odnést nebo zničit. Tiskárna také disponuje funkcí opakovaného tisku, kdy po stisknutí tlačítka automaticky vytiskne poslední úlohu.

Obecní úřad má včetně starosty a místostarosty 8 zaměstnanců. Nikdo ze zaměstnanců není kvalifikovaný správce IT, a proto obec využívá externích služeb. Starosta i místostarosta řídí ještě několik dalších lidí, to lze vidět na obrázku níže.




**Obrázek 8: Organizační struktura obce Dolní Dobrouč**

### 2.2.1 Kontrolní seznam sebehodnocení

Autor knižní publikace *GDPR Praktický průvodce implementací* Luděk Nezmar [5] vytvořil kontrolní seznam sebehodnocení, který zkoumá situaci v organizaci před zavedením GDPR dle platné legislativy, tzn. před začátkem účinnosti Obecného nařízení. Otázky jsou položeny tak, aby odpovědi na ně pomohli identifikovat oblasti, které je potřeba změnit k dosažení souladu s Obecným nařízením.

Pokud bude na všechny následující otázky odpovězeno ANO, je organizace připravena na Obecné nařízení. V opačném případě kontrolní seznam napoví, které oblasti je potřeba zlepšit.

**Spravedlivé získání souhlasu se zpracováním osobních údajů:**

- V době, kdy jsou informace o subjektech údajů shromažďovány, jsou informovány o jejich použití? NE
- Jsou subjekty údajů informovány o zveřejnění nebo předání údajů třetím stranám? NE
- Získali jsme souhlas subjektu údajů s jakýmkoli druhotným zpracováním osobních údajů, protože jim to nemusí být zřejmé? NE
- Můžeme popsat postupy shromažďování údajů jako zákonné, transparentní, korektní a spravedlivé? ANO

**Specifikace účelu:**

- Je účel nebo účely, pro které jsou údaje uchovávány dostatečně jasný a zřejmý? ANO
- Jsou osoby, které již osobní údaje poskytly také srozuměny s tímto účelem? ANO
- Pokud se organizace musí zaregistrovat na Úřadu pro ochranu osobních údajů, obsahuje její záznam řádné a komplexní prohlášení o účelu zpracování? X
- Byla nějakému zaměstnanci přidělena odpovědnost za udržování přehledu všech souborů dat a účelu, který je s nimi spojen? X

**Používání a zveřejňování informací:**

- Existují definovaná pravidla týkající se používání a zveřejňování informací? ANO

- Znají všichni zaměstnanci tato pravidla? ANO
- Jsou si subjekty údajů vědomy použití a zveřejnění svých osobních údajů? Byly by překvapeny, kdyby se o nich dozvěděly? ANO, NE
- Pokud se organizace musí zaregistrovat na Úřadu pro ochranu osobních údajů, obsahuje její záznam seznam osob, kterým může organizace údaje zveřejnit? X

**Bezpečnost:**

- Existuje seznam bezpečnostních opatření pro každý soubor dat nebo databázi? NE
- Je někdo zodpovědný za implementaci a přezkum těchto ustanovení? NE
- Jsou tato opatření dostatečně vhodná pro citlivost osobníc údajů, které uchováváme? NE
- Jsou naše počítače a naše databáze chráněny hesly a šifrovány, pokud je to vhodné? NE
- Jsou naše počítače, servery a soubory bezpečně uzamčeny před neoprávněnými osobami? ANO

**Přiměřenost, relevantnost a nezbytný rozsah:**

- Shromažďujeme pouze informace, které nezbytně potřebujeme, a získáváme je spravedlivým a komplexním způsobem? ANO
- Zkontrolovali jsme, zda všechny informace, které shromažďujeme, jsou relevantní a pouze nezbytného rozsahu po náš oprávněný účel? ANO
- Pokud by nás někdo požádal, abychom mu poskytli všechny informace, které o něm uchováváme, mohli bychom tak učinit? ANO
- Existují politiky, zásady a procesy uchovávání, odmazávání, přístupu a pozastavení zpracovávání dat? NE

**Přesnost a aktuálnost:**

- Kontrolujeme námi uchovávané údaje z hlediska přesnosti? NE
- Víme, kolik z našich osobních údajů je časově citlivých, tj. pravděpodobně časem nepřesných, pokud nebudou aktualizovány? NE

- Máme zajištěnou stálou aktualizaci našich databází? NE

**Doba uchovávání:**

- Existují jasná pravidla o tom, jaké informace a jak dlouho mají být uchovány? ANO
- Jsme si jasně vědomi všech právních požadavků na uchovávání údajů po určitou dobu? Například zákon o archivnictví, účetnictví apod. ANO
- Pravidelně odmazáváme data z našich databází, která již nepotřebujeme, jako jsou údaje týkající se bývalých zákazníků nebo zaměstnanců? ANO
- Máme politiku a zásady pro mazání osobních údajů, jakmile je účel, pro který jsme údaje získali, dokončen? NE

**Právo na přístup:**

- Byla určena osoba odpovědná za zpracování žádostí o přístup? NE
- Existují jasné postupy pro řešení těchto žádostí? NE
- Zaručují tyto postupy dodržování požadavků nařízení? NE

**Registrace:**

- Máme jasno v tom, zda potřebujeme být zaregistrováni u Úřadu pro ochranu osobních údajů? ANO
- Je-li registrace požadována, je aktuální? Zaznamenává přesně naše postupy pro zpracování osobních údajů? Nezapomeňte, že pokud vaše postupy zpracování dat nejsou v souladu s údaji uvedenými v záznamu registru, můžete se dopustit vážného přestupku. X
- Byla určena osoba zodpovědná za splnění našich registračních požadavků? NE

**Školení a vzdělávání:**

- Znáte úroveň povědomí o ochraně osobních údajů ve své organizaci? NE
- Jsou si zaměstnanci vědomi svých odpovědností v oblasti ochrany osobních údajů – včetně požadavků důvěrnosti? NE

- Je součástí vzdělávacího programu pro naše zaměstnance i oblast ochrany osobních údajů? NE

**Koordinace a shoda:**

- Byl jmenován pověřenec pro ochranu osobních údajů a osoba odpovědná za dodržování předpisů v této oblasti? NE
- Jsou si všichni zaměstnanci vědomi své role? ANO
- Existují mechanismy pro formální kontrolu aktivit pověřence pro ochranu osobních údajů v rámci naší organizace? NE

Kontrolní seznam sebehodnocení ukázal nejdůležitější části, které je nutné pro soulad s Obecným nařízením zlepšit. Jedná se hlavně o povinnost jmenovat pověřence, informovat subjekt o zpracování osobních údajů, kybernetickou bezpečnost a bezpečnost celkově a školení zaměstnanců.

### 2.2.2 Identifikace zpracování

Dolní Dobrouč je správcem osobních údajů. Subjektem údajů jsou obyvatelé obce, zaměstnanci úřadu a dodavatelé. Obec má právní základ pro zpracování osobních údajů. Rozsah zpracování je do 3000 subjektů, toto číslo zahrnuje obyvatele obce, zaměstnance, smluvní partnery a dodavatele. Obec zpracovává osobní údaje zranitelných subjektů i osobní údaje zvláštní kategorie. Při zpracování osobních údajů nedochází k profilování a osobní údaje nejsou nijak šifrované, anonymizované nebo pseudonymizované. Doba zpracování se řídí skartační lhůtou dle jednotlivých zákonů, to je podrobněji popsáno v kategorii 1.5.3. Za zpracování osobních údajů a nakládání s nimi není v současnosti nikdo odpovědný. Osobní údaje uchovává v listinné i elektronické formě. Obec nevyužívá kamerový systém.

Pomocí následují tabulky můžeme zjistit, zda je zpracovávání osobních údajů pro subjekt vysoce rizikové.

**Tabulka 8: Posouzení rizik pro práva subjektů**

| | |
|---|---|
| Automatizované, systematické vyhodnocování osobních aspektů týkající se fyzických osob včetně profilování s následným rozhodováním s právním nebo obdobně významným účinkem | NE |
| Rozsáhlé systematické monitorování veřejně přístupných prostorů | NE |
| Zpracování OÚ zvláštní kategorie | NE |
| Zpracování je rozsáhlé | NE |
| Soubory dat, které byly porovnány nebo zkombinovány | NE |
| Zahrnutí údajů týkajících se zranitelných subjektů údajů | ANO |
| Inovativní používání nebo uplatňování technologických nebo organizačních řešení (např. biometrika) | NE |
| Přesun dat přes hranice mimo Evropskou unii | NE |
| Pokud samotné zpracování zabraňuje subjektům údajů vykonávat právo nebo využívat službu nebo smlouvu | NE |
| **Jedná se o zpracování s vysokým rizikem pro práva a svobody osob:** | **NE** |

Posouzení vlivu je povinné v případě vysokého rizika pro práva a svobody osob, existuje ale několik výjimek kdy i přes vysoké riziko není povinné DPIA provádět, ty jsou uvedené v čl. 35 odst. 5, 10 Obecného nařízení. O zpracování s vysokým rizikem se dle metodiky Pracovní skupiny WP29 jedná pokud platí alespoň dvě výše uvedené podmínky.

## 2.3 Analýza rizik

Pro analýzu rizik je nutné nejdříve ohodnotit aktiva, poté identifikovat hrozby a určit jejich pravděpodobnost a určit zranitelnost aktiva vůči této hrozbě. Díky tomu získám míru rizika (rizikové skóre), které napoví, jaké je potřeba provést změny.

### 2.3.1 Hodnocení aktiv

Ohodnocení aktiv je provedeno s ohledem na GDPR a osobní údaje, které jednotlivá aktiva obsahují. Pokud obsahují osobní údaje občanů mají nejvyšší hodnocení, protože v případě incidentu budou ohrožena práva a svobody velkého množství subjektů, střední hodnocení mají aktiva s osobními údaji zaměstnanců a nízké hodnocení ostatní aktiva.

**Tabulka 9: Hodnocení aktiv**

| Název aktiva | Stupeň hodnocení |
|---|---|
| Kartotéka | 5 – Velmi vysoké |
| Informační systém IS Munis | 5 – Velmi vysoké |
| Elektronické uložiště | 1 – Velmi nízké |
| Webová stránka | 3 – Střední |
| Tiskárny | 5 – Velmi vysoké |
| Dokumenty v rámci vnitřního chodu úřadu | 3 - Střední |

Kartotéka má nejvyšší hodnocení, protože obsahuje velké množství osobních údajů, včetně zvláště zranitelných subjektů. Stejně tak je ohodnocen informační systém, kde jsou tato data uložena elektronicky a tiskárna kde dochází k tisku těchto údajů. Dokumenty v rámci vnitřního chodu úřadu jsou ohodnoceny stupněm 3, protože obsahují menší množství údajů, jedná se hlavně o pracovní smlouvy, účetnictví apod. Stejně tak webová stránka, kde jsou zveřejněny pouze základní kontaktní údaje. Elektronické uložiště má nejnižší ohodnocení, jedná se o disky v počítačích, sdílené disky nebo e-maily.

### 2.3.2 Obvyklé hrozby

V následující tabulce jsou vypsané obvyklé hrozby, které se týkají osobních údajů.

**Tabulka 10: Obvyklé hrozby vzhledem k OÚ**

| Kategorie hrozeb | Příklady |
|---|---|
| Vnější útok | Zneužití slabin sítě k přístupu |
| | Krádež nebo prolomení hesla |

| Kategorie hrozeb | Příklady |
|---|---|
| | Útok na web |
| | Útok na informační systém |
| Technická chyba | Výpadek elektřiny |
| | Poškození nebo ztráta dat |
| | Chyba programu |
| | Chyba zálohy |
| | Výpadek koncového zařízení |
| Lidský faktor | Chyba uživatele |
| | Zavlečení škodlivého softwaru (viru) |
| | Zneužití práv |
| | Porušení bezpečnosti |
| Narušení integrity OÚ | Neoprávněné manipulování s OÚ |
| | Zneužití OÚ |
| | Narušení listin |
| Neoprávněný přístup | Špatně nastavené přístupy k IS |
| | Nedostatečné zabezpečení (PC, místnosti) |
| Narušení dostupnosti | Nedostupnost z organizačních důvodů |
| | Nedostupnost z technických důvodů |
| Narušení práv a svobod subjektu | Narušení práv subjektu |
| | Vyzrazení údajů třetím osobám |
| | Diskriminace |
| Ztráta OÚ | Úmyslné zcizení |
| | Vymazání z IS |
| | Zničení listin |
| | Předání listin neautorizované osobě |
| | Technická chyba při ukládání |

### 2.3.3 Hodnocení pravděpodobnosti a zranitelnosti hrozeb

V následujících tabulkách jsou uvedeny pravděpodobnosti hrozeb a zranitelnost daného aktiva k těmto hrozbám.

**Tabulka 11: Hodnocení pravděpodobnosti hrozby a zranitelnosti kartotéky vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Kartotéka | Vnější útok | 2 | 3 |
| | Technická chyba | 2 | 3 |
| | Lidský faktor | 3 | 4 |
| | Narušení integrity OÚ | 3 | 3 |
| | Neoprávněný přístup | 4 | 3 |
| | Narušení dostupnosti | 2 | 2 |
| | Narušení práv a svobod subjektu | 3 | 3 |
| | Ztráta OÚ | 2 | 4 |

Nejvyšší pravděpodobnost hrozby v případě kartotéky je neoprávněný přístup, protože kartotéky nejsou umístěné ve zvláštní uzamykatelné místnosti, a přestože jsou uzamykatelné, klíče jsou během úřední doby zastrčené v zámcích a poté jsou uschovány v šuplíku pracovního stolu úředníka. Na střední úroveň je ohodnocena pravděpodobnost lidského faktoru a narušení integrity OÚ, protože neexistují interní směrnice a metodiky na práci s listinami.

**Tabulka 12: Hodnocení pravděpodobnosti hrozby a zranitelnosti IS vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Informační systém IS Munis | Vnější útok | 2 | 2 |
| | Technická chyba | 3 | 2 |
| | Lidský faktor | 3 | 3 |
| | Narušení integrity OÚ | 2 | 2 |

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| | Neoprávněný přístup | 2 | 3 |
| | Narušení dostupnosti | 3 | 3 |
| | Narušení práv a svobod subjektu | 2 | 3 |
| | Ztráta OÚ | 2 | 3 |

Informační systém je hostovaný od společnosti Triada, a je dobře chráněn. Vnější útok také není moc pravděpodobný vhledem k rozsahu dat, jaké malá obec má. K informačnímu systému má přístup jen pár úředníků, proto ani ostatní hrozby nejsou příliš pravděpodobné.

**Tabulka 13: Hodnocení pravděpodobnosti hrozby a zranitelnosti el. úložiště vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Elektronické uložiště | Vnější útok | 1 | 2 |
| | Technická chyba | 2 | 2 |
| | Lidský faktor | 3 | 3 |
| | Narušení integrity OÚ | 2 | 3 |
| | Neoprávněný přístup | 3 | 3 |
| | Narušení dostupnosti | 2 | 2 |
| | Narušení práv a svobod subjektu | 3 | 4 |
| | Ztráta OÚ | 3 | 4 |

Na počítačové a sdílené disky se dokumenty obsahující osobní údaje ve většině případů neukládají, proto je nepravděpodobné, že by došlo k vnějšímu útoku. Největší pravděpodobnost má lidský faktor – uživatelé nejsou příliš školeni pro práci s počítači a neoprávněný přístup – do kanceláří není těžké se dostat, nejsou nijak důkladně zabezpečeny. Také může dojít k narušení práv a svobod subjektu anebo ztrátě osobních údajů.

**Tabulka 14: Hodnocení pravděpodobnosti hrozby a zranitelnosti webové stránky vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Webová stránka | Vnější útok | 4 | 3 |
| | Technická chyba | 3 | 2 |
| | Lidský faktor | 3 | 3 |
| | Narušení integrity OÚ | 2 | 3 |
| | Neoprávněný přístup | 2 | 2 |
| | Narušení dostupnosti | 3 | 3 |
| | Narušení práv a svobod subjektu | 2 | 3 |
| | Ztráta OÚ | 2 | 3 |

Vysoká pravděpodobnost vnějšího útoku na webové stránky obce je proto, že nejsou dostatečně chráněné. Obec nevyužívá nejlepší dostupný hosting, a proto je narušení dostupnosti a technická chyba na střední úrovni pravděpodobnosti. Stejně tak je na střední úroveň ohodnocen lidský faktor, protože neexistují postupy pro práci s webem.

**Tabulka 15: Hodnocení pravděpodobnosti hrozby a zranitelnosti tiskárny vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Tiskárna | Vnější útok | 3 | 4 |
| | Technická chyba | 2 | 3 |
| | Lidský faktor | 3 | 4 |
| | Narušení integrity OÚ | 2 | 3 |
| | Neoprávněný přístup | 4 | 4 |
| | Narušení dostupnosti | 2 | 2 |
| | Narušení práv a svobod subjektu | 3 | 4 |
| | Ztráta OÚ | 3 | 4 |

Neoprávněný přístup je hodnocen vysokou pravděpodobností. Situace kdy zaměstnanec odnese více dokumentů, než si vytiskl není vůbec ojedinělá. Dalším problémem je, že si dokumenty může po vytisknutí kdokoli přečíst, okopírovat nebo naskenovat a získat tak přístup k citlivým datům. Z toho vychází i střední ohodnocení lidského faktoru, ztráty osobních údajů a narušení práv a svobod subjektu. Jelikož se jedná o síťovou tiskárnu a síť není zabezpečena všemi dostupnými prostředky, je i vnější útok na tiskárnu středně pravděpodobný.

**Tabulka 16: Hodnocení pravděpodobnosti hrozby a zranitelnosti dokumentů vnitřního chodu úřadu vůči hrozbám**

| Název aktiva | Hrozba | Pravděpodobnost | Zranitelnost |
|---|---|---|---|
| Dokumenty v rámci vnitřního chodu úřadu | Vnější útok | 2 | 3 |
| | Technická chyba | 1 | 3 |
| | Lidský faktor | 3 | 4 |
| | Narušení integrity OÚ | 2 | 3 |
| | Neoprávněný přístup | 2 | 3 |
| | Narušení dostupnosti | 2 | 2 |
| | Narušení práv a svobod subjektu | 2 | 4 |
| | Ztráta OÚ | 2 | 4 |

Středním stupněm pravděpodobnosti je ohodnocen lidský faktor, protože neexistují směrnice a metodiky pro práci s dokumenty. Ostatní hrozby jsou ohodnoceny nízkým rizikem, protože dokumenty v rámci chodu úřadu neobsahují takové množství osobních údajů a přijde s nimi do styku pouze pár osob.

### 2.3.4 Pravděpodobnost uplatnění hrozeb vůči aktivům

V následující tabulce jsou shrnuty pravděpodobnosti hrozeb vůči aktivům.

**Tabulka 17: Pravděpodobnost hrozeb**

| Aktivum | Hodnota aktiva | Pravděpodobnost | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Vnější útok | Technická chyba | Lidský faktor | Narušení integrity OÚ | Neoprávněný přístup | Narušení dostupnosti | Narušení práv a svobod sub. | Ztráta OÚ |
| Kartotéka | 5 | 2 | 2 | 3 | 3 | 4 | 2 | 3 | 2 |
| Informační systém | 5 | 2 | 3 | 3 | 2 | 2 | 3 | 2 | 2 |
| Elektronické uložiště | 1 | 1 | 2 | 3 | 2 | 3 | 2 | 3 | 3 |
| Webová stránka | 3 | 4 | 3 | 3 | 2 | 2 | 3 | 2 | 2 |
| Tiskárna | 5 | 3 | 2 | 3 | 2 | 4 | 2 | 3 | 3 |
| Dokumenty v rámci vnitřního chodu úřadu | 3 | 2 | 1 | 3 | 2 | 2 | 2 | 2 | 2 |

### 2.3.5 Zranitelnost aktiv vůči hrozbám

V následující tabulce jsou shrnuty zranitelnosti aktiv vůči hrozbám.

**Tabulka 18: Zranitelnost aktiv vůči hrozbám**

| Aktivum | Hodnota aktiva | Zranitelnost | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Vnější útok | Technická chyba | Lidský faktor | Narušení integrity OÚ | Neoprávněný přístup | Narušení dostupnosti | Narušení práv a svobod subj. | Ztráta OÚ |
| Kartotéka | 5 | 3 | 3 | 4 | 3 | 3 | 2 | 3 | 4 |
| Informační systém | 5 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 3 |
| Elektronické uložiště | 1 | 2 | 2 | 3 | 3 | 3 | 2 | 4 | 4 |
| Webová stránka | 3 | 3 | 2 | 3 | 3 | 2 | 3 | 3 | 3 |
| Tiskárna | 5 | 4 | 3 | 4 | 3 | 4 | 2 | 4 | 4 |
| Dokumenty v rámci vnitřního chodu úřadu | 3 | 3 | 3 | 4 | 3 | 3 | 2 | 4 | 4 |

### 2.3.6 Rizikové skóre

Na další stránce se nachází tabulka výsledného rizikového skóre, která obsahuje také dva důležité ukazatele:

- celková míra rizika hrozby – nejvyšší hodnota nám říká, které hrozby jsou pro obec nejzávažnější a je tedy potřeba se na ně zaměřit,
- celková míra rizika aktiva – nejvyšší hodnota ukazuje, které aktivum je k hrozbám nejnáchylnější a je tedy potřeba se zaměřit na jeho ochranu.

**Tabulka 19: Rizikové skóre**

| Aktivum | Hodnota aktiva | Rizikové skóre | | | | | | | | Celková míra rizika aktiva |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Vnější útok | Technická chyba | Lidský faktor | Narušení integrity OÚ | Neoprávněný přístup | Narušení dostupnosti | Narušení práv a svobod subjektů | Ztráta OÚ | |
| Kartotéka | 5 | 30 | 30 | 60 | 45 | 60 | 20 | 45 | 40 | 330 |
| Informační systém | 5 | 20 | 30 | 45 | 20 | 30 | 45 | 30 | 30 | 250 |
| Elektronické uložiště | 1 | 2 | 3 | 9 | 6 | 12 | 4 | 12 | 12 | 60 |
| Webová stránka | 3 | 36 | 18 | 27 | 18 | 12 | 27 | 18 | 18 | 174 |
| Tiskárna | 5 | 60 | 30 | 60 | 30 | 80 | 20 | 60 | 60 | 400 |
| Dokumenty v rámci vnitřního chodu úřadu | 3 | 18 | 9 | 36 | 18 | 18 | 12 | 24 | 24 | 159 |
| **Celková míra rizika hrozby** | | 166 | 120 | 237 | 137 | 212 | 128 | 189 | 184 | |

Mezi nejrizikovější aktiva patří tiskárna, kartotéka a informační systém. Tiskárna je pro celou obec jedna, se síťovým automatickým tiskem bez dalšího zabezpečení, proto než si úředník pro dokumenty dojde, může si někdo dokument vzít, zkopírovat nebo oskenovat. Kartotéka není dostatečně zabezpečena, jak je již zmíněno výše v kapitole 2.2. Informační systém je náchylný k hrozbě lidského faktoru, narušení dostupnosti a neoprávněnému přístupu.

Největší hrozby jsou lidský faktor, protože neexistují vnitřní směrnice upravující pracovní postupy a neoprávněný přístup, to je dáno tím, že neexistuje dostatečné zabezpečení jak listinných dokumentů (lepší kartotéky, kvalitní zámky, přístup na kartu) tak i elektronických dat (volně přístupné kanceláře, nedostatečné zabezpečení PC, nedostatečně řešená práva přístupu).

Na základě výsledků této analýzy v kapitole 3 Vlastní návrh řešení doporučím opatření, která by měla obec zavést.

## 2.4 Přehled poskytované agendy

Obec má pro většinu zpracování osobních údajů zákonné důvody, výjimku tvoří pořizování záznamu na veřejné akci, kde by bylo zapotřebí souhlasu subjektu, pouze pokud by byla zaznamenána přímo jeho podoba (portrét), nebo by byl jinak ztotožněn (titulkem se jménem), jinak není záznam veřejné akce považován za zpracování OÚ. Obec Dolní Dobrouč nemá povinnost zpracovávat posouzení vlivu, ale Ministerstvo vnitra to v rámci svých metodik doporučuje. Obec tak získá přehled o tom, jaké údaje zpracovává a tím snáze zjistí, zda jsou dostatečně zabezpečeny.

**Tabulka 20: Poskytovaná agenda, správce OÚ, zákonnost, účel a rozsah zpracování**

| Agenda | Správce | Zákonnost zpracování | Účel zpracování | Rozsah zpracování |
|---|---|---|---|---|
| Smlouvy | Obec | c) b) | Smlouvy se zaměstnanci, dodavateli… | Jméno, příjmení, datum a místo narození, rodné číslo, tel., e-mail, číslo účtu, podpis, státní příslušnost, ZP, banka… |

| Agenda | Správce | Zákonnost zpracování | Účel zpracování | Rozsah zpracování |
|---|---|---|---|---|
| Žádosti | Obec | c) e) | Různé žádosti obyvatel dle zákona | Jméno, příjmení, adresa, datum narození, případně další údaje dle typu žádosti |
| Stížnosti a petice | Obec | c) e) | Dle zákona | Jméno, příjmení, adresa, datum narození, podpis |
| Povolení | Obec | c) e) | Dle zákona | Jméno, příjmení, adresa, datum narození |
| Vedení kroniky | Obec | a) c) e) | Dle zákona | Jméno, příjmení, adresa, datum narození |
| Evidence obyvatel | Obec | c) e) | Dle zákona | Jméno, příjmení, adresa, rodné číslo, datum a místo narození, trvalé bydliště, doručovací adresa, předchozí pobyt, číslo OP, omezení způsobilosti, údaje o opatrovníkovi |
| Katastr nemovitostí | Obec | c) | Dle zákona | Jméno, příjmení, adresa, datum narození, rodné číslo |
| Legalizace a vidimace | Obec | c) | Ověřování podpisů a kopií dokumentů | Jméno, příjmení, adresa, datum narození, průkaz totožnosti, podpis |
| Volby a jejich agenda | Obec | c) | Dle zákona o volbách | Jméno, příjmení, adresa, datum narození, číslo OP, podpis, údaje o zdravotním stavu, údaje o svéprávnosti |
| Czechpoint | Obec | c) e) | Ověřování kopií, výpis | Jméno, příjmení, adresa, datum a místo narození, |

| Agenda | Správce | Zákonnost zpracování | Účel zpracování | Rozsah zpracování |
|---|---|---|---|---|
| | | | z veřejných rejstříků | rodné číslo, rodné příjmení číslo OP, podpis |
| Evidence klíčů | Obec | c) | Organizační opatření | Jméno, příjmení, číslo klíče |

Zpracování je dle čl. 6 odst. 1 Obecného nařízení „*zákonné, pokud…:*

*a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*
*b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
*c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
*d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*
*e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
*f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“* [6, čl. 6 odst. 1 písm. a) až f)]

# 3 VLASTNÍ NÁVRH ŘEŠENÍ

V této části přestavím návrhy na zlepšení dle výsledku analýzy rizik, nejprve dle celkové míry rizika aktiv, poté dle celkové míry rizika hrozeb, a nakonec představím další návrhy.

## 3.1 Návrh na zlepšení dle míry rizik aktiv

Zde představím návrhy na zlepšení dle celkové míry rizika aktiv.

### 3.1.1 Tiskárna

Tiskárna je kritické zařízení, k ohrožení bezpečnosti osobních údajů může dojít několika způsoby. Ve většině organizací došlo k centralizaci tisku, vytvoření tzv. tiskových koutků nebo místností, jedná se o síťovou tiskárnu umístěnou v samostatné místnosti nebo na chodbě, kde dochází k velkému pohybu osob. Situace kdy zaměstnanec odnese více dokumentů, než si vytiskl není vůbec ojedinělá. Dalším problémem je, že si dokumenty může po vytisknutí kdokoli přečíst, okopírovat nebo naskenovat a získat tak přístup k citlivým datům. To je z hlediska GDPR nepřijatelná praktika.

Zamezit takovýmto rizikům se dá docela snadno a nemusí to být ani příliš nákladné, protože většina výrobců tiskáren nabízí tzv. soukromý tisk, kdy se dokument z počítače odešle do tiskové fronty tiskárny, ale vytištěn bude až v momentě, kdy je osoba přítomna u tiskárny, a potvrdí tisk zadáním hesla, pinu nebo přiložením přístupové karty.

Dalším rizikem je zachycení dokumentu při odeslání do tiskové fronty. Většinou jsou dokumenty posílány nešifrované a není tedy problém je po odchycení přečíst. Programy na odposlouchávání sítě jsou volně ke stažení na internetu. I takovému riziku se dá snadno bránit, protože výše zmíněné funkce soukromého tisku nabízí i šifrovaný přenos a většina zařízení umožňuje komunikaci pomocí šifrovaných protokolů.

Řešením pro obec je přidat tiskárny, tak aby byly minimálně na každé patro jedna. To by ale jen usnadnilo a urychlilo práci úředníkům, protože by pro vytištěné dokumenty nemuseli scházet poschodí. Pořídit více tiskáren, např. aby měl každý úředník vlastní by bylo neekonomické a tiskárny by ani nebyly tolik využívané. Obec Dolní Dobrouč tedy musí i tak přistoupit k dalšímu zabezpečení dokumentů při tisku, a to buď tiskem po

zadání hesla, pinu nebo pořízením přístupových karet, které by mohly být využity i při dalším zabezpečení.

### 3.1.2 Kartotéka a ostatní dokumenty

Kartotéka a tím i listiny nejsou dostatečně chráněny, to je detailně popsáno v předchozí části u tabulky číslo 8. Nejjednodušší zlepšení je nenechávat klíče v kartotékách a po skončení úřední doby je uschovat do uzamykatelné skříňky. Kartotéky ale mají pouze jednoduchý zámek, který lze snadno překonat. Lepším řešením by bylo pořídit nové kartotéky s kvalitnějším zámkem a nejlepším řešením by bylo uchovávat listinné dokumenty ve zvláštní místnosti. To ale není v této době v obci Dolní Dobrouč možné, na obecním úřadě se nenachází žádná volná místnost. Řešením by byla stavební úprava, ale to by bylo vzhledem k riziku příliš nákladné. Pokud by k tomu v budoucnu došlo, mohlo by být i zde využito přístupových karet doporučených v předchozí kapitole.

Obec by také měla zavést klasifikaci dokumentů. Tím se zajistí správné zacházení s dokumenty obsahujícími osobní údaje.

### 3.1.3 Informační systém

Do informačního systému je potřeba přidat nové funkce, aby byl v souladu s Obecným nařízením. Jedná se především o právo na informace, právo na výmaz, právo na přenositelnost a pozastavení zpracování. Jelikož je informační systém dodáván společností Triada, s.r.o. nejsou tyto úpravy v kompetenci obce. Informační systém je uložen na serverech společnosti Triada, s.r.o., ta díky tomu má přístup k informacím na serveru uloženém, který není smluvně ošetřen. Je tedy zapotřebí smlouvu zrevidovat, aby byla v souladu s Obecným nařízením, jasně stanovit odpovědnost v případě ohrožení práv a svobod subjektů (např. v případě útoku na servery společnosti Triada, s.r.o.). Dále by bylo vhodné evidovat přístup a provedené změny.

Obec si však sama řídí uživatelské účty a jejich práva, je tedy zapotřebí zrevidovat tyto účty, zda do systému nemají přístup bývalý zaměstnanci obce nebo zda stávající uživatelé nemají více práv, než k výkonu své činnosti potřebují.

### 3.1.4 Webová stránka

Webové stránky obsahují kontaktní formulář, kam návštěvníci stránek zadají osobní údaje (jméno, příjmení, e-mail) a odešlou je. Odesílání neprobíhá přes zabezpečený protokol a tím jsou osobní údaje ohroženy. Řešením je převést stránky na zabezpečený protokol HTTPS, upravit kontaktní formulář, aby se do něj zadávalo co nejméně osobních údajů nebo je při odeslání dále šifrovat. K formuláři je také potřeba přidat políčko na zaškrtnutí souhlasu se zpracováním OÚ a informace o tom, jak jsou osobní údaje zpracovávány. Tyto souhlasy je potřeba evidovat, pro případ odvolání souhlasu, nejlépe v databázi, kterou využívají webové stránky.

Obec by se také měla vyvarovat zveřejňování osobních údajů zaměstnanců, pokud to není nutné nebo je alespoň omezit na nejnutnější minimum jako je jméno, příjmení a pracovní e-mail a pokud lze předpokládat kontakt úředníka s veřejností tak i pracovní telefonní číslo. Obec by neměla zveřejňovat fotografie úředníků nebo jejich soukromá čísla, pokud by se k tomu i přes to obec rozhodla, potřebuje jejich souhlas.

Obec na své sociální sítě neuveřejňuje žádný obsah, proto není nutné nic měnit. Pokud by se ale do budoucna rozhodla obsah přidávat, bylo by vhodné, aby zavedla metodiku chování na sociálních sítích, kde by bylo jasně určeno, jaký obsah smí být zveřejňován.

Kromě webových stránek a sociálních sítí Dolní Dobrouč také vydává *Dobroučské noviny*, které vycházejí čtvrtletně. V novinách jsou uveřejněné informace ze zasedání zastupitelstva, výsledky hlasování, informace o konaných akcích nebo ohlédnutí za akcemi, které již proběhly. Mimo to se v novinách nachází část, ve které obec blahopřeje k životním jubileím, narození dětí nebo informuje o úmrtí. Základní osobní údaje jako je jméno a příjmení může uveřejňovat na základě tzv. zpravodajské licence dle občanského zákoníku. Zveřejnění dalších osobních údajů jako je věk nebo fotografie narozeních dětí lze jedině s jejich souhlasem, resp. souhlasem zákonných zástupců. V takových situacích si ale již nyní obec předem obstarává souhlas dotčených subjektů, proto v tomto ohledu nemusí nic měnit.

Na webových stránkách by také měl být uveřejněn kontakt na pověřence na ochranu osobních údajů, práva subjektu údajů, především právo být zapomenut, právo na informace a právo vznést námitku a zásady zpracování osobních údajů, účelu zpracování osobních údajů a případné příjemce osobních údajů.

### 3.1.5 Elektronické uložiště, počítače a síť

Obec disponuje staršími počítači, které již úplně nedostačují svým výkonem, bylo by tedy vhodné zakoupit nové. Počítače by měli být vhodně zabezpečeny fyzicky (přepěťová ochrana, zámek proti neoprávněnému přístupu k HW) i softwarově (antivirus, přihlašování pomocí hesla, aktuálnost softwaru).

Obec také využívá sdíleného disku, ten je velmi náchylný k hrozbám (lidský faktor, vnější útok), také není možné sledovat kdo kdy na disk přistoupil a jaké akce tam provedl. Doporučeným zabezpečením je rozdělit disk na několik částí, aby bylo možné nastavit přístupy uživatelům pouze k datům, které potřebují. Přesto není z hlediska GDPR vhodné sdílené disky využívat.

Používání paměťových médií by mělo být úplně zakázáno, může dojít k zavlečení škodlivého softwaru nebo úniku dat v případě jejich ztráty. Pokud je to pro práci nutné, měli by být paměťová média šifrovaná.

V kancelářích se nachází nevyužité ethernetové zásuvky, do kterých je možno zapojit libovolné zařízení a mohlo by tak dojít k ohrožení bezpečnosti nebo by toho mohl někdo využít k útoku. Je proto vhodné nevyužívané zásuvky zaslepit nebo odpojit. Stále ale hrozí riziko, že někdo odpojí kabel ze síťové tiskárny a připojí se tak do sítě. Z toho důvodu je vhodné využívat řízení přístupu, např. pomocí MAC adres, a tím zamezit neautorizovaným zařízením přístup do sítě.

Úředníci mohou během pracovní doby navštěvovat libovolné webové stránky, může se dostat i na stránky se škodlivým obsahem, tím je ohrožena bezpečnost jeho počítače i celé sítě. Dalším problémem je, že zaměstnanci úřadu mohou stahovat libovolné soubory, tím zase mohou zavléct do svého počítače nebo i sítě škodlivý program nebo počítačový virus. Řešením je omezit možnost navštěvovaných stránek a omezit možnost stahování souborů např. podle typu souboru.

Pracovní e-maily mohou zaměstnanci využívat i pro soukromé účely a tím ohrozit bezpečnost, např. otevřením spamu nebo stažením nakažené přílohy. Pracovní e-mailové schránky by tedy měly být určené pouze pro pracovní účely, aby se toto riziko minimalizovalo. Dále je nutné přistupovat k těmto e-mailům pouze ze zabezpečených zařízení, jinak vzniká riziko rozšíření viru, pokud bylo zařízení nějakým způsobem

nakaženo. Obec by se měla vyvarovat posílání osobních údajů v těle e-mailu, a vždy je přikládat jako přílohu. Ještě většího zabezpečení je možno dosáhnout šifrováním přílohy.

Obec Dolní Dobrouč využívá externích služeb IT společnosti, která má díky tomu přístup do jejich sítě a k počítačům úředníků. Proto je potřeba v rámci GDPR upravit smlouvu o poskytování služeb. Dále je vhodné zaznamenávat aktivity externího správce, pro případy kontrol, zda nedochází k neoprávněným akcím.

Stejně jako IT služby i e-mailové služby jsou hostované, je tedy zapotřebí také zrevidovat smlouvu o poskytování služeb a uvést ji do souladu s GDPR.

## 3.2 Návrhy na zlepšení dle míry rizik hrozeb

Zde představím návrhy na zlepšení dle celkové míry rizika hrozeb.

### 3.2.1 Lidský faktor

Lidský faktor je největší hrozba, je to dáno hlavně tím, že neexistují žádné interní dokumenty, směrnice nebo metodiky, které by jasně stanovily pracovní postupy. Řešením je vytvořit interní dokumenty pro práci s listinami, informačním systémem, webovými stránkami, sociálními sítěmi a interní dokument o bezpečnosti. Důležitým následným krokem je zaměstnance pravidelně školit. Další častou praktikou je umisťování rostlin na vršek kartotéky, při jejím přelití může dojít k zatečení vody a tím k zničení dokumentů.

### 3.2.2 Neoprávněný přístup

Druhá největší hrozba je neoprávněný přístup, jak je již zmíněno v kapitole 3.1.1 obecní úřad a kartotéky nejsou dostatečně zabezpečené. Toto riziko se ale týká i elektronických dat. Je důležité nastavit dostatečná hesla, řídit uživatelské účty a zabezpečit síť před možnými útoky. Stejně jako u předchozího rizika k tomu mohou sloužit interní dokumenty.

### 3.2.3 Narušení práv a svobod subjektu

Proti porušování práv subjektu může působit dohoda o mlčenlivosti, nemůže tak docházet k porušení práva na soukromí nebo k hmotným ztrátám. Důležité pro ochranu práv a

svobod subjektu je zacházení s osobními údaji, které by mělo být jasně určené interními dokumenty v souladu s GDPR.

### 3.2.4 Ztráta OÚ

Ke ztrátě může dojít několika způsoby, ztracení dokumentu po tisku, špatné založení, nevhodné zacházení s IS nebo při výpadku elektřiny. Většině těchto případů se dá stejně jako v předchozích případech vyvarovat vytvořením interních dokumentů upravujících pracovní postupy. Ztrátě dat při výpadku elektřiny se dá předejít pořízením UPS jednotky.

### 3.2.5 Vnější útok

Vnější útok není velmi pravděpodobný vzhledem k rozsahu a povaze dat jaké Dolní Dobrouč zpracovává. Přesto je lepší útok předcházet. Útok může probíhat z vnější přes síť nebo osobně prolomením hesla počítače nebo IS. Doporučením je zabezpečit síť, upozornit uživatele na výběr hesel (stejně jako v předchozích krocích interním dokumentem) a doporučit jim pokaždé když opouští svůj počítač uzamknout ho.

### 3.2.6 Narušení integrity OÚ

Ochrana před neoprávněným zneužitím osobních údajů je uzavřít se zaměstnanci dohodu o mlčenlivosti. Dalším možným řešením je monitorovat přístupy. V rámci IS je to jednoduché, v rámci úřadu by bylo potřeba zavést přístupové karty nebo kamery.

### 3.2.7 Narušení dostupnosti

Zabránit nedostupnosti se dá různými způsoby. Nedostupnost listinných dokumentů může být způsobena jejich ztrátou, špatným založením nebo například vyhořením. Jak zabránit těmto událostem je popsáno u ostatních hrozeb. Nedostupnost informačního systému se nedá ovlivnit, jelikož je hostovaný na serverech dodavatele. Informační systém může být pro uživatele nedostupný z důvodu přerušení dodávky elektřiny v místě úřadu nebo proto že mu nefunguje počítač. Tyto případy jsou také popsány u ostatních hrozeb.

### 3.2.8 Technická chyba

Technická chyba může nastat často. Následkům výpadku elektřiny se dá zabránit pořízením UPS jednotky, ta navíc chrání i proti přepětí. Prováděním pravidelných záloh se minimalizuje riziko ztráty dat. Technické chyby mohou taky vniknout používáním zastaralého softwaru, je proto důležité udržovat systém a aplikace aktualizované. Technické chyby mohou ale působit i na listinné dokumenty. Ty je potřeba chránit proti případnému požáru, pořízením detektorů kouře nebo tepelnými čidly.

## 3.3 Další doporučení

Zde představím další návrhy na zlepšení, které nejsou uvedené v předchozích kapitolách.

### 3.3.1 Kronika

Podle GDPR by kronika obce neměla být zveřejněna a být pouze k nahlédnutí na obecním úřadě, jak je tomu i teď. Dolní Dobrouč má navíc zdigitalizovanou pamětní knihu z let 1923–1991, kterou ale neuveřejnila. Pamětní kniha je zveřejněna na stránkách východočeského archivu. V kronice by se také neměly objevit žádné osobní údaje, což ošetřuje již zákon č. 101/1999 Sb. o ochraně osobních údajů, pokud se nejedná o osoby vykonávající veřejnou činnost nebo pokud je získán souhlas subjektu.

### 3.3.2 Mobilní telefony

Chytré mobilní telefony již mají stejnou funkčnost jako počítače, umožňují posílání a přijímání e-mailů, prohlížení webových stránek i stahování souborů. Navíc obsahují osobní údaje ve formě kontaktů nebo kalendáře ve kterém jsou zaznamenané schůzky. Je tedy důležité zabezpečit i tyto zařízení. Minimálním zabezpečením je zámek obrazovky pomocí hesla, pinu nebo obdobné technologie a jeho automatické uzamykání. Samozřejmostí by mělo být zabezpečení SIM karty pinem. Dalším doporučeným zabezpečením je šifrování obsahu telefonu. V případě pracovních telefonů s tím není problém, ale není možné nutit zaměstnance k takovému kroku v případě, že používají soukromé telefony. Řešením je zamezit nešifrovaným mobilním zařízením přístup ke kontaktům a e-mailům.

### 3.3.3 Interní dokumenty

Obce mají povinnost vytvořit nebo upravit interní dokumenty, tak aby byly v souladu s GDPR.

#### Organizační řád

Organizační řád musí obec doplnit o funkci pověřence, informační povinnost a případně další části pro dodržení souladu s Obecným nařízením.

#### Pracovní řád

Do pracovního řádu musí být přidáno ustanovení o odpovědnost při práci s osobními údaji, odpovědnosti v případě incidentu a dohoda o mlčenlivosti, která je povinná pro všechny zaměstnance, kteří mají přístup k osobním údajům.

#### Spisový a skartační řád

Spisový a skartační řád musí být upraven tak aby odpovídal požadavkům GDPR, především na ochranu osobních údajů, práva subjektů a požadavku na likvidaci osobních údajů, pokud již dále nejsou potřeba. Svaz měst a obcí České republiky vydal vzorový Spisový a skartační řád v souladu s nařízením, který je ke stažení na jejich stránkách. Ministerstvo vnitra navíc vydalo metodiku pro určování skartačních lhůt.

#### Provozní řád výpočetní techniky

Provozní řád výpočetní techniky musí být upraven pro zajištění souladu především v ohledu ochrany osobních údajů a to správným zabezpečením a využívám sítě, výpočetní techniky a softwaru.

#### Systémová příručka k IS

Obec využívá informačního systému Munis od společnosti Triada, s.r.o., která systém dodává včetně příručky pro práci se systémem a rozšířenou podporou. Obec proto tento dokument nemusí vytvářet.

**Záznamy o činnosti zpracování**

Obec nemá dle Obecného nařízení povinnost vést záznamy o činnosti zpracování, protože nezaměstnává více než 250 lidí. Výjimku tvoří volební agenda, kterou zpracovávají členové komise a kontrolní orgány. Vzorový formulář viz příloha 1.

**Popis a definice postupu při narušení zabezpečení osobních údajů**

Obec by měla vytvořit dokument, který stanoví kroky, které následují po zjištění narušení bezpečnosti. Tento dokument by měl určit odpovědnou osobu, pravidla pro oznamování dozorovému úřadu či subjektu a případně vzorové formuláře viz příloha 3: Hlášení incidentu subjektu údajů a příloha 4: Hlášení incidentu dozorovému úřadu. Povinnost hlášení incidentu je detailněji popsána v kategorii 1.2.8 Hlášení incidentu.

**Směrnice pro práci s osobními údaji**

Tato směrnice by měla stanovit pravidla pro práci s osobními údaji a jejich zabezpečení v souladu s GDPR a hlavně s nimi seznámit všechny zaměstnance.

Ministerstvo vnitra vydalo dokument „*Základní pravidla postupů souvisejících se zpracováním osobních údajů*“ (viz příloha 2), který může sloužit malým obcím, jako je obec Dolní Dobrouč, jako vzorový text, který může využít jako interní předpis na ochranu osobních údajů nebo ho mohou dále využít pro vytvoření vlastních předpisů nebo pro upravení smluv s dodavateli.

Svaz měst a obcí České republiky vydal podrobnější dokument pro práci s osobními údaji, především pro malé obce, který je ke stažení na jejich stránkách.

**Rozšířená evidence**

Obec by měla vytvořit evidenci udělených přístupů do informačního systému, přiřazených klíčů, přenosných paměťových médií, výpočetní techniky a jiného vybavení. V případě pochybení je pak snazší zjistit kdo pochybil a kdo je odpovědný.

**Nakládání s listinnými dokumenty**

Tento dokument by měl stanovit pravidla pro práci s listinnými dokumenty, především nenechávat dokumenty volně odložené (na stole, v tiskárně, …), dbát na správné uložení

do kartotéky nebo v případě dočasného odchodu dokumenty vhodně zabezpečit, například uschováním do uzamykatelného šuplíku nebo uzamčením kanceláře, aby se předešlo neoprávněnému přístupu k datům nebo jeho zničení. Dále by měl dokument zavést pravidla pro práci s dokumenty, které předejdou situacím, kdy by mohlo dojít k polití dokumentů nebo jinému znehodnocení. Tyto pravidla mohou být stanovena v rámci Pracovního řádu nebo kybernetické bezpečnosti.

**Kybernetická bezpečnost**

Obec by měla zvážit vytvoření interního dokumentu o kybernetické bezpečnosti, který určuje pravidla zabezpečení výpočetní techniky a pravidla pro její užívání. Jedná se hlavně o zásadu volby správného hesla, neotevírání podezřelých e-mailů, nestahování podezřelých souborů, zákaz navštěvování stránek s nevhodným obsahem, zákaz využívání pracovní e-mailové schránky pro osobní účely apod.

**Vystupování na sociálních sítích**

Pokud by se obec rozhodla začít využívat svůj profil na sociálních sítích ke své propagaci, nebo pro zveřejňování informací o konaných a plánovaných akcích, bylo by vhodné, aby vytvořila alespoň základní pravidla pro chování na sociálních sítích. Ty by měly obsahovat zásady veřejného vystupování, prezentování obce a netikety.

**Smlouvy s dodavateli a externími pracovníky**

Smlouvy by měli být doplněny o jasné stanovení odpovědnosti a doložku o mlčenlivosti v případě, že má dodavatel nebo externí pracovník přístup k datům.

**Informovaný souhlas**

Obec by měla vytvořit vzorový dokument Informovaný souhlas, který je potřeba pokud správce nemá zákonný důvod pro zpracování osobních údajů a potřebuje souhlas od subjektu. Takovýto dokument by měl obsahovat informace o tom jaké údaje budou zpracovávány, o účelu zpracování, době zpracování, možnosti souhlas odvolat, možnosti vznést námitku, informace o správci a případných zpracovatelích a informaci o právech na informace, opravu nebo výmaz.

**Souhlasy získané v minulosti**

Obec by měla prověřit zda souhlasy se zpracováním osobních údajů získané v minulosti jsou stále platné, především zda dále trvá zákonný důvod zpracování. Obec bude muset souhlasy kontrolovat a aktualizovat i v budoucnu pokud dojde ke změně účelu nebo způsobu zpracování osobních údajů.

### 3.3.4 Školení

Školení by mělo navazovat na vytvoření interní dokumentace a probíhat pravidelně, minimálně jednou za rok nebo v případě přijetí nového zaměstnance. Dříve bylo školení v rámci ochrany osobních údajů doporučené, zavedením GDPR se ale stává povinné. Obec musí taková školení zaznamenávat, aby byla schopna je doložit.

Školení by mělo probíhat i v ostatních oblastech. Je vhodné následně kontrolovat do jaké míry zaměstnanci interním dokumentům porozuměli.

## 3.4 Jmenování pověřence

Na obce se vztahuje povinnost jmenovat pověřence. Každý správce má povinnost zveřejnit informace o pověřenci, jeho jméno a kontakt. Obec by měla tyto údaje zveřejnit na svých webových stránkách a vyvěsit na úřední desku a dále je musí předat dozorovému orgánu.

Pro malou obec jako je Dolní Dobrouč je možnost najmutí společného pověřence nejvhodnější, vzhledem k rozsahu zpracování a jelikož je již dlouhodobě členem svazku obcí *Region Orlicko – Třebovsko*. Náklady na pověřence se rozdělí mezi celý svazek. Obce se však musí ujistit, že takto jmenovaný pověřenec bude plně zvládat svou práci pro všechny členy svazku.

## 3.5 Ekonomické zhodnocení

V této části provedu ekonomické zhodnocení navrhovaných řešení.

### Tiskárna

Pro obec doporučuji přikoupit druhou tiskárnu a software pro řešení bezpečného tisku. Pro malou obec by mohlo být dostačující bezplatné řešení od společnosti MyQ, které navíc nabízí vytváření reportů a sledování využití jednotlivými uživateli. Druhé nabízené řešení je YSoft SafeQ pro tisk zabezpečený kartami, které navíc nabízí funkci follow-me, která umožňuje tisknout na jakékoli tiskárně v síti po identifikaci, a možnost tisknout zadáním pinu, v případě, že u sebe uživatel nemá kartu.

Náklady: 6 000 Kč nová tiskárna, MyQ Free SW 0 Kč, YSoft SafeQ SW 23 000 Kč (+ náklady na čipové karty)

### Kartotéky

Pro lepší zabezpečení listinných dokumentů doporučuji pořídit nové kartotéky, které mají kvalitnější zámek, dalším vhodným opatřením by bylo pořízení nových dveří do kanceláří. Kartotéky, popř. místnosti ve kterých se kartotéky nachází je potřeba ochránit proti požáru instalováním detektorů kouře.

Náklady: nové kartotéky 50 000 Kč, nové dveře 49 000 Kč, detektory kouře 4 000 Kč, detektory kouře a tepla 7 500 Kč

### Webové stránky

Webové stránky je nutné převést na zabezpečený protokol HTTPS, případně upravit kontaktní formulář a zabezpečit posílaná data. K tomu je nutný certifikát, díky kterému se v adresním řádku zobrazí zelený zámek (certifikát Let's Encrypt – zdarma) nebo v případě placeného certifikátu (Thawte) zámek a název společnosti pro kterou byl certifikát vydán. Pořízení certifikátu nestačí, stránky je nutné ještě plně na HTTPS převést, proto je započítaná práce správce stránek. Certifikát je nutné každý rok obnovovat.

Náklady: Let's Encrypt 3 000 Kč, Thawte 3 000 Kč + 3 000 Kč

**Hardware a software**

Zakoupení nových počítačů pro úředníky, starostu a místostarostu a nové licence MS Office. Pořízení UPS jednotek, které navíc fungují jako prodlužovací kabely a ochrana proti přepětí.

Náklady: All-in-One 8 × 10 000 Kč, Licence Office 8 × 12 × 250 Kč, UPS 8 × 2 500 Kč

**Interní dokumenty**

Obec by měla zpracovat interní dokumenty pro práci s informačním systémem, vystupování na sociálních sítích, kybernetickou bezpečnost a práci s listinnými dokumenty. Také by měla revidovat organizační a pracovní řád. Dá se předpokládat, že tím bude pověřený některý ze zaměstnanců obce a tuto činnost bude provádět v rámci své pracovní doby.

Náklady: 100–200 hodin, 10 000 – 20 000 Kč

**Pověřenec**

Náklady na pověřence se rozdělí mezi členy svazku *Region Orlicko – Třebovsko*. Náklady na pověřence nejsou veřejné, ale dá se předpokládat, že se se vzhledem k počtu obcí ve svazku bude jednat o částku 1 000 až 2 000 Kč měsíčně/obec.

Náklady: 12 × 1 000 Kč

V následující tabulce porovnám náklady obce, pokud využije pouze základní zabezpečení a pokud využije všech dostupných zabezpečení.

### 3.5.1 Srovnání nákladů

**Tabulka 21: Porovnání nákladů**

| Levné řešení – základní zabezpečení | | Dražší řešení – důkladnější zabezpečení | |
|---|---|---|---|
| Tiskárna + SW | 6 000 Kč | Tiskárna + SW | 29 000 Kč |
| Kartotéky | 50 000 Kč | Kartotéky | 50 000 Kč |
| Detektory kouře | 4 000 Kč | Dveře | 49 000 Kč |

| **Levné řešení – základní zabezpečení** | | **Dražší řešení – důkladnější zabezpečení** | |
|---|---|---|---|
| HTTPS Let’s Encrypt | 3 000 Kč | Detektory tepla a kouře | 7 500 Kč |
| HW + SW | 124 000 Kč | HTTPS Thawte | 6 000 Kč |
| Interní dokumenty | 10 000 Kč | HW + SW | 124 000 Kč |
| Pověřenec | 12 000 Kč | Interní dokumenty | 20 000 Kč |
| | | Pověřenec | 24 000 Kč |
| **Celkem** | **209 000 Kč** | **Celkem** | **309 500 Kč** |

# ZÁVĚR

Cílem bakalářské práce bylo představit obec Dolní Dobrouč, provést analýzu a na základě výsledku analýzy představit návrhy na zlepšení současného stavu v obci tak aby vyhovoval GDPR.

Dílčími cíli bakalářské práce bylo poskytnout základní informace o tématu ochrany osobních údajů a veřejné správě, představit obec Dolní Dobrouč, analyzovat současný stav a na základě analýzy představit návrhy na zlepšení.

V první části jsem přestavila teoretická východiska, která s tímto tématem souvisí, jedná se o veřejnou správu, obce a činnosti obcí a hlavně GDPR, vymezení pojmů subjekt údajů, osobní údaje, práva subjektů a zásady zpracování osobních údajů, a hlavně představení novinky, kterou Obecné nařízení zavádí, a to pověřence na ochranu osobních údajů a jeho povinností.

Ve druhé části jsem představila obec Dolní Dobrouč, její stručnou historii a provedla její analýzu. Z analýzy vyplynulo, že obec není plně připravena na Obecné nařízení, hlavně co se týče zabezpečení listinných dokumentů a zamezení přístupu neoprávněných osob. Analýza odhalila i několik dalších problémů.

Ve třetí části jsem v návaznosti na výsledky analýzy navrhla řešení, které spočívá v lepším zabezpečení listinných dokumentů, vytvoření interních dokumentů, které budou upravovat pracovní postupy, jmenování pověřence a další změny, které jsou nutné pro zajištění souladu s Obecným nařízením, a nakonec jsem provedla ekonomické zhodnocení. Většinu návrhů jsem zpracovala ve dvou variantách, levná se základním zabezpečením a dražší, která poskytuje větší míru zabezpečení, proto má i celkové ekonomické zhodnocení dvě varianty.

# SEZNAM POUŽITÝCH ZDROJŮ


[1] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013, 377 s. : il, grafy, tab. ISBN 9788072048724.

[2] BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací*. 1. vyd. Olomouc: ANAG, 2013, 199 s. ISBN 9788072638116.

[3] *GDPR.cz* [online]. Praha: Škorničková, b.r. [cit. 2017-12-10]. Dostupné z: https://www.gdpr.cz/

[4] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 6. října 2016. In: *Úřad pro ochranu osobních údajů*. 2000, ročník 2000, číslo 101. Dostupné také z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=21409

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

[6] *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)*. In: . Brusel: EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE, 2016, ročník 2016, číslo 679. OJ L 119. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[7] ŽŮREK, Jiří. *Praktický průvodce GDPR*. 1. vydání. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3.

[8] *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2013 [cit. 2018-05-02]. Dostupné z: https://www.uoou.cz

[9] *Ministerstvo vnitra České republiky* [online]. Praha, 2018 [cit. 2018-04-29]. Dostupné z: http://www.mvcr.cz/

[10] PROVAZNÍKOVÁ, Romana. *Financování měst, obcí a regionů: teorie a praxe*. 3. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2015. Finance (Grada). ISBN 978-80-247-5608-0.

[11] *Cenová mapa* [online]. Praha: Verlag Dashöfer, 1997-2018 [cit. 2018-04-14]. Dostupné z: http://www.cenovamapacr.cz/

[12] *Zákon č. 128/2000 Sb. ze dne 12. dubna 2000 o obcích (obecní zřízení)*. b.r., s. 1737-1764. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3426

[13] Přehled právních předpisů stanovujících povinnost ukládat vybrané typy dokumentů. In: *Ministerstvo vnitra České republiky* [online]. b.r. [cit. 2018-04-29]. Dostupné z: http://www.mvcr.cz/gdpr/soubor/logo-mv1ef4ba13-pdf.aspx

# SEZNAM POUŽITÝCH OBRÁZKŮ

# SEZNAM POUŽITÝCH TABULEK

# SEZNAM POUŽITÝCH GRAFŮ

# SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

DPIA – Data Protection Impact Assessment – Posouzení vlivu na ochranu osobních údajů

DPO – Data Protection Officer – Pověřenec pro ochranu osobních údajů

EU – Evropská unie

GDPR – General Data Protection Regulation – Obecné nařízení o ochraně OÚ

HW – Hardware

ISMS – Information Security Management System – Systém řízení informační bezpečnosti

Netiketa – Soubor pravidel chování na internetu

OP – Občanský průkaz

OÚ – Osobní údaje

SW – Software

ÚOOÚ – Úřad pro ochranu osobních údajů

ZoOÚ – Zákon o ochraně osobních údajů č. 101/2000 Sb.

ZP – Zdravotní pojišťovna

# SEZNAM PŘÍLOH

Příloha 1: Záznam o činnostech zpracování – VOLBY [9]

| **Záznam o činnostech zpracování – VOLBY**<br>**Čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)**<br><br>**Správce:** *… (název, adresa, datová schránka) …*<br>**Zástupce správce:** *… (jméno, příjmení, funkční zařazení osoby odpovědné za agendu)* …<br>**Pověřenec pro ochranu osobních údajů:** *… (jméno, příjmení, e-mail) …* |
|---|
| **I. Účely zpracování** |
| **ZAJIŠTĚNÍ AGEND OBCE PODLE VOLEBNÍCH ZÁKONŮ** |
| **Čl. 6 odst. 1 písm. c) GDPR – zpracování nezbytné pro plnění právní povinnosti:**<br>zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů,<br>zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů,<br>zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů,<br>zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů,<br>zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky),<br>prováděcí právní předpisy k volebním zákonům. |
| **II. Kategorie subjektů údajů** |
| Občan obce – volič. Člen okrskové volební komise. Kandidát. Zmocněnec. Petent. |
| **III. Kategorie osobních údajů** |
| Základní identifikační údaje, státní občanství, volební právo a jeho případné omezení, číslo dokladu totožnosti, účast při hlasování; v případě členů okrskových volebních komisí údaje nezbytné pro výkon činnosti člena komise a pro jeho odměňování; v případě kandidátů a zmocněnců identifikační údaje dle kandidátní listiny a čestného prohlášení kandidáta; v případě petentů u nezávislých kandidátů identifikační údaje dle náležitostí petice. |
| **IV. Kategorie příjemců** |
| Členové okrskových volebních komisí pro účely plnění jejich povinností podle volebních zákonů. Kontrolní orgány (krajský úřad, Státní volební komise). |
| **V. Plánované lhůty pro výmaz kategorií osobních údajů** |
| Platí skartační lhůty stanovené vyhláškami k volebním zákonům: ve vztahu ke kandidátním listinám a souvisejícím dokumentům – A10, pro ostatní volební dokumentaci – V5. |
| **VI. Obecný popis technických a organizačních bezpečnostních opatření** |
| Listinná vyhotovení volební dokumentace jsou ukládána v uzamčených prostorách a v průběhu voleb se pečetí.<br>Přístup k elektronickým datovým souborům je zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy obce. |

Příloha 2: Základní pravidla postupů souvisejících se zpracováním osobních údajů [9]

Příloha usnesení zastupitelstva obce XY č. ../2018

Obec XY

Základní pravidla postupů souvisejících se zpracováním osobních údajů

Čl. 1

(1) Zastupitelstvo obce *XY* usnesením *č. .../2018 ze dne…* vzalo na vědomí pravidla postupů souvisejících se zpracováním osobních údajů v samostatné a přenesené působnosti obce v souladu s nařízením 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) – GDPR.

(2) Zastupitelstvo obce *XY* ukládá jednotlivým členům zastupitelstva obce, aby při plnění svých úkolů zajišťovali dodržování těchto pravidel. Starostovi obce ukládá zajistit dodržování těchto pravidel při zpracování osobních údajů obecním úřadem a při plnění smluv, jejichž předmětem je zpracování osobních údajů.

Čl. 2

(1) Obec zpracovává osobní údaje výhradně v souladu s právními důvody stanovenými v čl. 6 GDPR, pouze v nezbytném rozsahu a po nezbytnou dobu. Účely zpracování osobních údajů a dobu jejich zpracování eviduje obec pro jednotlivé agendy v záznamech o činnostech zpracování podle čl. 30 GDPR.

(2) K osobním údajům mají přístup pouze osoby, které s nimi potřebují nakládat při plnění svých úkolů a povinností pro obec. Tyto osoby zachovávají o osobních údajích, s nimiž se seznamují, mlčenlivost.

(3) V případech, kdy obec hodlá v souladu s GDPR zveřejnit osobní údaje, například ve zpravodaji obce nebo na internetových stránkách, vždy předem posoudí vhodnost a rozsah tohoto zveřejnění.

Čl. 3

(1) Obec přijímá opatření k zabezpečení osobních údajů, a to zejména:

a) zajištění přítomnosti osoby uvedené v čl. 2 odst. 2 v prostorách, kde jsou zpracovávány osobní údaje, po dobu, kdy jsou tyto prostory přístupné jiným osobám, popřípadě uzamykání listin s osobními údaji, pokud osoba uvedená v čl. 2 odst. 2 není v této době přítomna,

b) uzamykání prostor, v nichž jsou uchovávány osobní údaje,

c) ochrana přístupu k výpočetní technice, jíž se zpracovávají osobní údaje, individuálními silnými hesly a ochrana těchto hesel před vyzrazením,

d) ochrana výpočetní techniky antivirovými programy; to platí také pro přenosná zařízení, pokud jsou pro ně takové programy běžně dostupné,

e) další vhodná opatření prováděná odpovědnou osobou pro ochranu přenosné výpočetní techniky nebo přenosných úložišť dat (například neustálý dohled, zamčený přepravní obal, folie na displeji, šifrování dat, osobní manipulace s úložištěm při kopírování dat do jiného přístroje),

f) šifrování souborů s větším množstvím osobních údajů nebo se snadno zneužitelnými nebo citlivými osobními údaji v případě odesílání souboru e-mailem nebo jeho uložení na sdílené úložiště.

(2) Obec vede evidenci výpočetní techniky, úložišť dat a programového vybavení používaných ke zpracování osobních údajů. U přenosné výpočetní techniky a úložišť dat se eviduje též osoba odpovědná za využívání přenosného zařízení a za jeho ochranu před neoprávněným přístupem. Obec zajišťuje, aby výpočetní technika a úložiště dat používaná ke zpracování osobních údajů nebyla využívána k soukromým účelům.

(3) Obec vede evidenci klíčů používaných k uzamykání listin s osobními údaji a uzamykání prostor, v nichž se zpracovávají osobní údaje.

(4) Obec dbá na řádné plnění povinností podle předpisů upravujících spisovou službu a archivnictví, zejména včas a řádně provádí skartační řízení.

Čl. 4

(1) Obec zřizuje funkci pověřence pro ochranu osobních údajů (dále jen „pověřenec“). Pověřenec plní povinnosti podle čl. 37 až 39 GDPR v souladu se smlouvou nebo jiným dokumentem upravujícím vzájemná práva a povinnosti obce a pověřence.

(2) Obec dále

a) vede záznamy o činnostech zpracování podle čl. 30 GDPR,

b) zajišťuje informování subjektů údajů podle čl. 13 a 14 GDPR,

c) naplňuje práva subjektů údajů, zejména práva na přístup k údajům podle čl. 15 GDPR a práva na opravu podle čl. 16 GDPR a

d) provádí ohlašování a oznámení porušení zabezpečení osobních údajů podle čl. 33 a 34 GDPR.

(3) Návrhy záznamů, informací, vyřízení žádostí a ohlášení a oznámení podle odstavce 2 zpracovává pověřenec.

(4) Obec poskytuje pověřenci potřebnou součinnost.

Čl. 5

(1) Obec vede evidenci opatření podle čl. 3, evidenci případných souhlasů se zpracováním osobních údajů a evidenci případů porušení zabezpečení osobních údajů.

(2) Obec pravidelně, nejméně jednou ročně vyhodnocuje plnění pravidel ochrany osobních údajů a přijímá opatření k nápravě. Vyhodnocení zpracovává pověřenec za součinnosti obce.

Příloha 3: Vzor hlášení incidentu subjektu údajů [5]

*[Hlavičkový papír společnosti]*

*[Jméno a příjmení subjektu]*

*[Adresa subjektu]*

*[Datum, místo]*

**Porušení zabezpečení osobních údajů**

Vážený/á *[Jméno a příjmení]*,

Vážíme si Vaší důvěry a respektujeme soukromí Vašich informací, proto Vás v rámci preventivního opatření informujeme o incidentu bezpečnosti dat, který *[může znamenat/znamená]* ohrožení Vašich osobních údajů.

*[V době od do/dne] [identifikace časového období porušení]*, došlo k *[celkový popis incidentu]*. Ohrožená data *[mohou obsahovat/zahrnují]* osobní údaje jako například *[identifikujte typy ohrožených údajů]*. Podle našich zjištění nebyly žádné následující údaje *[identifikujte typy neohrožených údajů]*.

Pro další podrobnosti případně kontaktujte našeho pověřence pro ochranu osobních údajů emailem *[email]* nebo na telefonu *[telefonní číslo]*.

Zůstáváme v úctě

*[Podpis]*

Příloha 4: Vzor hlášení incidentu dozorovému úřadu (Vlastní zpracování dle: [5])

| **Ohlášení porušení ochrany osobních údajů** | | | |
|---|---|---|---|
| Správce osobních údajů | | | |
| Kontaktní údaje | | | |
| Pověřenec | | | |
| Kontaktní údaje | | | |
| Popis incidentu/jeho povahy | | | |
| Datum a čas vzniku | | | |
| Popis pravděpodobných důsledků | | | |
| Popis příčin | | | |
| Kategorie osobních údajů | | | |
| Přibližný počet dotčených subjektů | | | |
| Přibližný počet dotčených záznamů | | | |
| Popis přijatých opatření | | | |
| Důvod odkladu zaslání oznámení (déle než 72 hod) | | | |
| Zpracoval: | | Dne: | |