Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Implementace evropské směrnice GDPR v obci Dolní Újezd

Bakalářská práce

Autor: Stanislav Hladík

Studijní obor: IM3-K

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové

duben 2019

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

…….

V Hradci Králové dne 28. 4. 2019

Stanislav Hladík

Poděkování:

Tímto bych rád poděkoval svému vedoucímu práce Mgr. Josefu Horálkovi, Ph.D. za jeho odbornou, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Dále bych rád poděkoval zaměstnancům Obecného úřadu obce Dolní Újezd za jejich vstřícný přístup a praktické rady pro tvorbu mé práce.

Anotace

Bakalářská práce „Implementace směrnice GDPR v obci Dolní Újezd“ se zabývá aktuálním tématem ochrany osobních údajů. Úvodní část práce se zabývá tím, co vlastně ochrana osobních údajů znamená a vysvětluje základními pojmy z oblasti ochrany osobních údajů. Analytická část se zaměřuje již na konkrétní otázky týkající veřejné instituce obce Dolní Újezd a odpovídá na ně. V praktické části se řeší konkrétní problémy ochrany osobních údajů a poskytuje se doporučení, jak vyřešit vše v souladu s GDPR. Jako poslední je zde praktická ukázka aplikace, která řeší některé konkrétní problémy s ochranou osobních údajů.

Annotation

The Bachelor Thesis „Implementation of the GDPR Directive in Dolní Újezd“ deals with the current topic of personal data protection. Introductory part of the thesis deals with what the protection of personal data means and explains basics concepts of personal data protection. Analytical part focus on specific issues concerning the public institution of Dolní Újezd and answers to them. The practical part deals with specific problems of personal data protection and provides recommendations, how to solve everything in accordance with GDPR. Lastly, there is a practical application, which solves some problems according to protection of personal data.

Obsah

Seznam tabulek

Seznam obrázků

Úvod

Každý člověk s nimi nakládá jinak, pro někoho se jedná o tak privátní komoditu, že si nepořídí klubovou kartičku do obchodu, aniž by si nepřečetl stohy, pro většinu lidí, právně nevzdělaných, naprosto nezajímavých a nesmyslných textů. Na druhé straně jsou však i lidé, kterým nedělá problém se bez váhání zaregistrovat všude, kde na ně vyskočí upozornění, i když za to dostanou leckdy i jenom miniaturní slevu nebo jinou drobnou výhodu.

V nynější době velký počet lidí nepřikládá ochraně svých osobních údajů nějakou velkou váhu. Může to být způsobeno tím, že si ani neuvědomují všechny náležitosti a rizika s tím spojená. Občasné rychlé „odkliknutí“ sdělení ze stránky, jestli souhlasíte s nastavením cookies, kvůli lepšímu chování webové stránky toho může být důkazem. Však po pořádném hloubání v paměti by snad kdokoli z nás mohl potvrdit, ne zrovna zodpovědné chování na Facebooku, Twitteru a podobných sociálních sítích.

Osobní údaje nás identifikují ve společném světě, dokáží nás rozlišovat od ostatních lidí. Vytváří totožnost jednotlivých osob, díky čemuž je každý člověk ve společnosti jedinečný. Výsadu uchovávat si své osobní informace v tajnosti má každý člověk. Zpracování osobních údajů o těchto lidech, musíme tolerovat, a to ať už chceme nebo nechceme. Při zákonem daných situacích, či při uzavírání nebo plnění smlouvy, dále toto narušení tolerujeme, když dobrovolně poskytujeme podpis za nějakým konkrétním účelem.

Toto všechno souvisí s ochranou osobních údajů. Oblast ochrany osobních údajů se stává v současné době velmi diskutovaným tématem. Děje se tak v důsledku prudkého rozmachu informačních a telekomunikačních technologií. Kvůli tomu vzniklo nařízení GDPR (General Data Protection Regulation). Toto nařízení bylo schváleno 27. dubna 2016 a v platnost vstoupilo 25. května 2018. Nařízení stanovuje rovné podmínky pro zpracování osobních údajů napříč zeměmi Evropské unie, protože v den platnosti nahrazuje vlastní legislativy jednotlivých států v oblasti ochrany osobních dat. Směrnice GDPR přináší razantní zpřísnění pravidel pro organizace zpracovávající osobní data (obce, firmy) v jakékoli podobě a téměř z jakéhokoli důvodu. Možné prohřešky proti tomuto nařízení je možné trestat velmi vysokými pokutami. [1]

Před novým obecním nařízením o ochraně údajů (GDPR) Evropského parlamentu, zajišťovala jakousi ochranu osobních údajů Směrnice 95/46 ES (obecné nařízení o ochraně osobních údajů), která se však svým (pro tuto dobu zastaralým) obsahem nemohla rovnat obecnému nařízení o ochraně osobních údajů (GDPR), jelikož při jejím vývoji nemohl nikdo předpokládat, že rozvoj informačních a telekomunikačních technologií povede k tak

masivnímu rozvoji zpracovávání osobních údajů. Tato směrnice se stala nedostačující pro rychle se rozvíjející lidskou civilizaci i z důvodu jen částečné harmonizace mezi jednotlivými státy v Evropě. Důkazem může být například Nizozemí, které stanovilo povinnost ohlašovat případy porušení zabezpečení ochrany osobních údajů, což ve Směrnici 95/46/ES nebylo zakotveno. [2]

GDPR se netýká jenom práva ani jenom oblasti informačních a telekomunikačních technologií. Soukromé společnosti i veřejná správa musejí vymyslet způsoby implementace této směrnice, aby s osobními údaji nakládaly v souladu s ní. V české republice je již zákon o ochraně osobních údajů platný. Ale vzhledem k poměrně nízkým sankcím dosud žádný subjekt neimplementoval všechny principy ochrany osobních údajů, jak předchozí zákon vyžadoval a jak bude vyžadovat směrnice GDPR. [2]

V teoretické části bude popsaná celková problematika směrnice GDPR, základní pojmy, na které každá společnost narazí při zpracovávání osobních údajů, těmi jsou mimo jiné informace, data nebo například soukromí, jenž úzce souvisí právě s osobními údaji každého jednotlivce. Dalším bodem bude zjištění, jak se obce Dolní Újezd celkově směrnice GDPR týká. Například jaká práva a povinnosti mají subjekty zpracovávající údaje, kdo může být pověřencem (DPO) pro ochranu osobních údajů, kdo může toho pověřence jmenovat a jaké má DPO povinnosti při zpracovávání osobních údajů. Poté bude následovat rozebrání problematiky, jak zabezpečit osobní údaje, aby nebyly zneužity cizími stranami. Následně zanalyzujeme potřeby zpracovatele osobních údajů a celkový dopad na chod obce Dolní Újezd.

Dále se zaměříme na problematiku softwarových a hardwarových řešení pro zavedení směrnice GDPR. Tím může být například navýšení serverového výkonu pro databáze, kde se uchovávají potřebná data. Dále například zavedené hardwarového firewallu pro ochranu uložených dat. V softwarové části by se jednalo o případné zdokonalení systému, aby se neporušovala směrnice GDPR. Dále pohled na softwarové nástroje, které dokáží zmapovat všechny údaje shromažďované obcí o občanech a v případě, že občan na základě směrnice GDPR nebude souhlasit se shromažďováním svých osobních údajů, tak tyto údaje ze všech informačních systémů obce vymazat v souladu i s ostatními zákony.

V praktické části se zaměříme na aplikování takových opatření, aby obec Dolní Újezd splňovala všechny povinnosti vyplívající ze směrnice GDPR. Prvním úkolem bude sepsání vzorové směrnice o zpracování osobních údajů, kterou se budou řídit všechny osoby zainteresované ve zpracovávání osobních údajů subjektů ochrany osobních údajů. Následně provedeme sepsání možných vzorových dodatků ke smlouvám, které se budou týkat

zpracovávání osobních údajů. Posledním výstupem bude praktická aplikace, která bude mít za úkol evidovat Žadatele do domu s pečovatelskou službou a měla by disponovat funkcemi jako například: Šifrování, pseudonymizace a anonymizace dat.

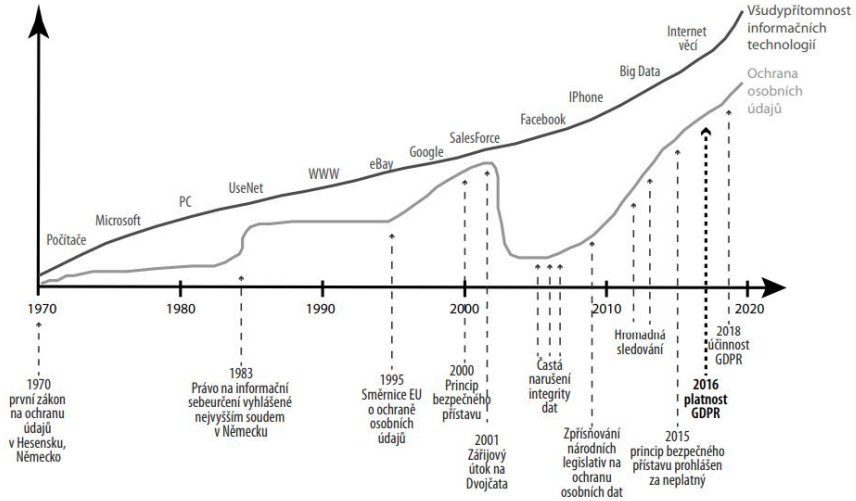
Celkovým cílem práce bude odhalit úskalí implementace směrnice GDPR a pomoci při jejím zavedení v platnost, aby se obec nepotýkala se stížnostmi ze strany svých občanů a aby bylo vše v souladu se směrnicí GDPR.

1. Obecné informace o GDPR

Zpracování údajů je činnost, kterou musí každý správce nebo zpracovatel provádět s osobními údaji, a to buď automatizovaně, nebo jinými prostředky. Může se jednat o se o shromažďování, zaznamenávání, uspořádání, strukturování, ukládání, úpravu, pozměnění, vyhledávání, používání, předávání výměnu informací apod.

GDPR (General protect data regulation) představuje nový rámec ochrany osobních údajů s cílem ochránit práva občanů Evropské unie proti neoprávněnému zacházení a zneužívání dat a osobních údajů. Co se týče dopadu GDPR, tak se dotýká firem, veřejných i soukromých institucí i jednotlivců, kteří přijdou do styku s osobními údaji třetích osob.

1.1. Historie ochrany osobních údajů a vznik GDPR



Obrázek č. 1: Časová osa vývoje GDPR, zdroj: [1]

Prvním dokumentem v historii, který se zabýval ochranou lidských práv a svobod dalo by se říci i omezeně ochranou osobních údajů se stala francouzská Deklarace práv člověka a občana z roku 1789.[3]

Z pohledu mezinárodního se však standardem a jedním ze základních dokumentů stala Všeobecná deklarace lidských práv z roku 1948, jenž vznikla pod taktovkou OSN. V tomto dokumentu je zajímavý čl. 12 v němž je uvedeno: „Nesmí být nikdo vystaven svévolnému zasahování do soukromého života ani útokům na svou čest a pověst a každý má proti takovýmto zásahům právo na zákonnou ochranu.“ [5]

Od začátku je jasné, že GDPR nevznikala na zelené louce, ale má mnoho předloh. Celkově vychází GDPR ze směrnice EU o ochraně osobních údajů (DPD). V nynější době je brána jako nejkomplexnější nařízení o ochraně osobních údajů na světě. Při srovnání například se americkou směrnicí HIPAA (Health Insurance Portability and Accountability Act of 1996 – Zákon o přenositelnosti a odpovědnosti v oblasti zdravotního pojištění).

1.1.1. Historie vzniku GDPR a vývoje ochrany osobních údajů

Prvotním milníkem, který vedl k uvědomění si problematiky ochrany osobních údajů a potřebu jejich řešení je podpis smlouvy o ochraně osobních údajů s ohledem na automatické zpracování osobních údajů. Tato smlouva byla podepsána **28. ledna 1981** Radou Evropy a v platnost vešla dne **1. října 1985**. Smlouvu tehdy schválilo 47 členů Rady Evropy vyjma Turecka.

Další významnou událostí, směřující k lepší globální ochraně osobních údajů byla Evropská směrnice 95/46 / ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Ta byla vytvořena jako první a základní dokument starající se o ochranu soukromí v Evropské Unii. Směrnice vešla v platnost dne **13. prosince 1995**.

Dne 1. prosince 2009 vznikly dvě pracovní skupiny WP29 a WPPJ (skupina pro politiku a spravedlnost), které vydaly dokument „Budoucnost soukromí“ v němž se tehdy Evropská komise zabývá novými výzvami v oblasti ochrany osobních dat v souvislosti s moderními informačními technologiemi.

Rok poté se Evropská komise zabývá ochranou údajů jednotlivců ve všech oblastech (např. vymáhání práva). Snaží se zaručit volný pohyb údajů v rámci EU. Dále se Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE) zaměřuje na budoucnost ochrany osobních údajů a změnu stávající směrnice 95/46 / ES.

V roce 2012 konkrétně **25. ledna** se v Evropské komisi rozhoduje o celkové komplexní reformě pravidel EU ochrany osobních údajů z roku 1995 a to za účelem posílení práv občanů, hlavně v online prostředí. Evropská komise deklarovala, že technologie se výrazně změnily a tím je také změněn způsob, jakým jsou zpracovávána osobní data. Ještě v témže roce je však zjištěna aktivita Spojených států amerických, které se výrazně snažily promluvit do průběhu projednávání kvůli ochraně zájmů amerických společností působících v Evropské unii. [6]

25. října 2012 se na poli evropského parlamentu diskutovalo jakým nástrojem bude nová ochrana osobních údajů aplikována na členské státy EU. Některé delegace navrhovaly směrnici namísto nařízení, díky čemuž by členské země Evropské unie měly větší flexibilitu si ochranu osobních údajů upravit, kde by to bylo potřebné. [6]

Nakonec však byla odsouhlasena forma nařízení, jak byla navržena Komisí.

Roky 2013 a 2014 se nesou ve znamení velké podpory GDPR z evropského parlamentu. V květnu roku 2013 London Economics zveřejňuje výsledky nezávislého průzkumu, který slouží k lepšímu porozumění výzev, které GDPR staví před podniky a organizace. V říjnu tohoto roku se na Výboru pro občanské svobody, spravedlnost a vnitřní věci (LIBE) Evropského parlamentu hlasovalo pro přijetí pozměňovacích návrhů, z nichž některé významně ovlivnily GDPR oproti návrhu vypracovaného evropskou komisí v lednu 2012 (např. výrazně zvýšené sankce, rozšířený územní rozsah, přenosy dat do třetích zemí, omezení profilování a pověřenec pro ochranu osobních údajů). [6]

12. března 2014 Se na plenárním zasedání Evropského parlamentu dává silná podpora GDPR s 621 hlasy pro, 10 proti a 22 zdržujícími se. Tím dochází k významnému pokroku v reformě ochrany osobních údajů. Tento krok je chápán jako nevratný a měl by zajistit efektivnější kontrolu osob nad jejich osobními údaji. [6]

Dále 10. října 2014 se Rada EU částečně shoduje na konkrétních aspektech návrhu nařízení, kterým se stanoví obecný rámec EU pro ochranu osobních údajů.

Rok 2015 již přináší reálné shody nad tím jaká bude obecná podoba GDPR tento obecný přístup byl nutný k tomu, aby mohla začít jednání Evropské rady s Evropským parlamentem s cílem vzniku celkové dohody o GDPR. [6]

17. prosince 2015 se Výbor pro občanské svobody, spravedlnost a vnitřní věci Evropského parlamentu dohodl a schválil výsledek jednání o ochraně osobních údajů. Tím byl schválen text GDPR včetně ustanovení o jednoznačném, konkrétním a srozumitelném souhlasu, dětech na sociálních sítích, právu na zapomenutí, právu vědět, že vaše údaje byly zneužity, srozumitelnosti jazyka a pokut ve výši 4 % celkového ročního obratu proviněné firmy.

Rok 2016 je z hlediska GDPR velmi důležitý. 27. dubna 2016 je oficiálně uveřejněno Nařízení Evropského parlamentu a Rady EU 2016/679.

1.2. Rozdíly mezi dosavadní ochranou osobních dat v ČR a evropskou GDPR

Jak jsem již zmínil předchůdcem směrnice GDPR byla v Evropě směrnice 95/46/ES a s ní související zákon v České republice 101/2000 Sb., o ochraně osobních údajů. Vypisovat zde všechny rozdíly mezi těmito dvěma směrnicemi by byl takřka nadlidský úkol, ale v kostce se dá říci, že v základních bodech se GDPR od původního zákona v České republice příliš neliší. Je to způsobeno i tím, že směrnice GDPR se snaží z původní evropské směrnice vycházet. Je nutné si uvědomit, že předchozí zákon již přestal odpovídat současné době, zejména prostředky používané ke zpracování údajů, které je v dnešní době daleko komplexnější (například při automatizaci zpracování osobních údajů). [7]

Jednou z mnoha změn, které bychom mohli zmínit je přímá použitelnost obecného nařízení, což vyplývá z jeho charakteru, jakožto nařízení. Dále pro některé subjekty však klade vyšší nároky při zpracovávání osobních údajů. To mohou být velcí správci osobních dat jako například banky, telekomunikační operátoři atd., tj. pro správce u kterých mohou být data uživatelů dále zpracovávány. [7]

1.3. Případné postihy subjektů, které se nebudou řídit směrnicí GDPR

Každý subjekt zpracovávání osobních údajů (tzn. Fyzická nebo také právnická osoba), má právo obdržet od správce nebo zpracovatele kompenzaci utrpěné újmy, pokud subjekt zpracování osobních údajů nabil dojmu, že s jeho osobními daty nebylo nakládáno podle platných právních norem, kterými jsou:

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 př 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. [2]

Pro všechny právní důvody zpracování osobních údajů platí, že si jsou rovny tzn. neplatí že osobní údaje se zpracovávají jenom se souhlasem subjektu údajů a pak už jen na základě nějakých výjimek. Je možné dokonce podotknout že většina zpracování osobních údajů je v životě prováděna na základě jiných právních důvodů, než je souhlas. Avšak souhlas se zpracováním osobních údajů je jedinečný v tom směru, že jako jediný vyžaduje aktivní zapojení subjektu údajů (udělení souhlasu). [2]

I přes tyto právní důvody se však musí s osobními údaji nakládat podle Zásad zpracování údajů, jimiž jsou:

a) Musejí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („Zásada zákonnosti, korektnosti a transparentnosti“).
b) Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené legitimní účely a nesmějí být zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely vědeckého či historického výzkumu nebo pro statistické účely se nepovažují za neslučitelné s původními účely. („Zásada omezení účelu“).
c) Přiměřené, relevantní a omezené na nezbytný rozsah k účelu, pro který jsou zpracovávány („Zásada minimalizace údajů“).
d) Přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („Zásada přesnosti“).
e) Uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány („Zásada omezení uložení“).
f) Zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („Zásada integrity a důvěry“). [8]

Obecné nařízení umožňuje při ukládání pokut poměrně velkou variabilitu, včetně neuložení peněžní pokuty. V tomto případě lze použít některá z nepeněžních nápravných opatření např.

a) Upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení.
b) Udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily to nařízení.
c) Nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení.
d) Nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem ve stanovené lhůtě.
e) Nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů.
f) Uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu.
g) Nařídit opravu, výmaz nebo omezení zpracování a ohlašování zákonných opatření příjemcům.
h) Odebrat osvědčení nebo nařídit, aby jej subjekt oprávněný k vydávání osvědčení odebral nebo nevydal.
i) Nařídit přerušení toků údajů příjemci ve třetí zemi nebo mezinárodní organizaci. [8]

V případě, že sice půjde o porušení Obecného nařízení, avšak s minimální společenskou škodlivostí, nemusí být pokuta udělena vůbec. Je možné, že bude postačovat některé nepeněžní nápravné opatření nebo pouze informování správce o jeho povinnostech vůči subjektu údajů a očekávání, že sám zpracování uvede do souladu na základě informací mu poskytnutých. Zákon o zpracování osobních údajů také navíc bude obsahovat ustanovení, podle kterého, dojde-li k nápravě protiprávního stavu bezprostředně poté co se tak stane, může Úřad pro ochranu osobních údajů od uložení pokuty upustit.

1.3.1. Peněžní pokuty a jejich výše

Obecné nařízení rozděluje druhy porušení do dvou kategorií, které jsou rozlišeny výší možných sankcí, a to podle možného dopadu porušení na zájem chráněný Obecným zařízením. Náhledy na tyto skutkové podstaty jsou poměrně široké, vždy ve vztahu porušení k povinnostem vyplývajících z určených článků. [2]

V případě, pokut ukládaných orgánům veřejné moci a veřejným subjektům, je maximální výše pokuty pro tyto subjekty maximálně 10 000 000Kč. Důvodem je snaha zohlednit, že pokuty udělené těmto subjektům plynou z veřejných rozpočtů a bylo by neúčelné ponechat pro ně nejvyšší možnou pokutu 20 000 000 EUR. Pro lepší porozumění nám může pomoci následující tabulka. [2]

Pokuty 10 000 000 EUR, nebo 2 % z celkového ročního obratu	
Správce a tam, kde připadá v úvahu i zpracovatel	povinností při zabezpečení ochrany osobních údajů
	podmínek pro najmutí a spolupráci se zpracovatelem
	povinnosti vyhotovit záznamy o činnostech zpracování
	povinnosti spolupráce s dozorovým úřadem
	povinností při ohlašování, resp. oznamování případu porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů
	povinnosti posoudit vliv na ochranu osobních údajů a absolvovat předchozí konzultaci
	povinnosti týkající se jmenování a podmínek pověřence
	povinnosti ustanovit zástupce pro správu nebo zpracovatele usídleného mimo Evropskou unii
	povinnosti týkající se činností při získávání osvědčení

Tabulka č. 1: Sazba nižších pokut podle GDPR, zdroj: [2]

Pokuty 20 000 000 EUR, nebo 4 % z celkového ročního obratu	
Správce a tam, kde připadá v úvahu i zpracovatel	zásad a zákonnosti zpracování
	podmínek vyjádření souhlasu
	podmínek pro zpracování zvláštních kategorií osobních údajů
	práv subjektu údajů
	podmínek pro předávání osobních údajů do třetí země
	povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které Obecné nařízení umožňuje upravit na vnitrostátní úrovni.
	povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 Obecného nařízení nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1 Obecného nařízení
	nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 Obecného nařízení (nápravné pravomoci) nebo neposkytnutí přístupu při uplatnění dozorové pravomoci

Tabulka č. 2: Sazba vyšších pokut podle GDPR, zdroj: [2]

2. Dopady GDPR na ochranu obsahující osobní údaje

O GDPR se občas mluví jako o přelomovém a revoluční předpisu. Avšak základní prvky současné právní úpravy se zásadně nemění a ve většině případů se jedná spíše o upřesnění původní právní normy. Při přípravě na Obecné nařízení si je důležité upřesnit jakou roli hraje daná instituce při zpracování osobních údajů, tzn. Jestli zpracovává osobní údaje pro své účely anebo zpracovává osobní data pro správce. Dále je velmi důležité si objasnit všechny pojmy, které se při implementaci GDPR do úřadu obce mohou naskytnout. [1]

2.1. Práva subjektů údajů

Práva subjektu údajů tvoří nedílnou součást ochrany osobních údajů při jejich zpracovávání. Práva dávají subjektu údajů možnost vyvážit mnohdy nerovný vztah mezi subjektem údajů a jejich správcem. [2]

V praxi se stává, že je výkon práv subjektů mnohdy podceňován a velmi často bývá přehlížen. Je však nutné poznamenat, že výkon práv subjektu údajů je jeden z vyšších zájmů a jeho možné porušení je zpravidla trestáno vyššími, z možných sazeb finančních pokut než při porušování méně závažných povinností. [2]

2.1.1. Právo být informován

Právo být informován určuje povinnosti správce osobních údajů informovat o zpracování, toto pravidlo se aplikuje obvykle prostřednictvím oznámení. [1]

Nařízení stanovuje, jaké informace by měl správce poskytovat a kdy by měli být dotyční informování a informace, které je správce povinen sdělit. Informace, které správce poskytuje by měly být:

a) Stručné, jasné, srozumitelné a snadno dostupné.
b) Psané jasným a jazykem srozumitelným pro všechny včetně dětí.
c) Zdarma, bez poplatků. [1]

Informace, které by správci měli poskytovat lze vyjádřit následovně:

Jaké informace musí být sděleny?	**Údaje získané přímo od subjektů**	**Údaje nejsou získány přímo od subjektu údajů**
Podrobnosti o přesunech dat do třetích zemí a poskytnutých zárukách	Ano	Ano
Doba uchovávání nebo kritéria používání k určení doby uchovávání	Ano	Ano
Existence jednotlivých práv subjektů údajů	Ano	Ano
Právo na odstoupení od smlouvy kdykoli, je-li to relevantní	Ano	Ano
Právo podat stížnost dozorovému orgánu	Ano	Ano
Zdroj, od kterého pocházejí osobní údaje a zda pochází z veřejně přístupných zdrojů	Ne	Ano
Zda je poskytování osobních údajů součástí zákonného nebo smluvního závazku nebo požadavku a možné důsledky neposkytnutí osobních údajů	Ano	Ano
Informace o existenci automatizovaného rozhodování, včetně profilování a informace p procesu rozhodování, jeho význam a možné důsledky	Ano	Ano
Kdy mají být informace poskytnuty?	V okamžiku získání	V přiměřené lhůtě po obdržení údajů

Tabulka č. 3: Povinné informace od správce, zdroj: [1]

Taktéž mezi informační povinnosti správce patří oznamovací povinnost ohledně polohy nebo výmazu osobních údajů. Správci musí oznámit jednotlivým příjemcům, kterým byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy jejich osobních údajů.

2.1.2. Právo na přístup k osobním údajům

Podobně jako je tomu u práva na informace, tak u práva na přístup k osobním údajům, jde především o transparentní přístup ke zpracování.

V GDPR je uvedeno, že důvod žádosti o přístup ke svým osobním údajům, je kvůli ověření zákonnosti zpracovávání a kvůli právu být si vědom, že se dané osoby zpracování údajů týká. Správci je uložena povinnost bezplatně poskytnout pouze první kopii zpracovávaných údajů, za další si může, ale i nemusí účtovat přiměřený poplatek.

Správce si však také musí hlídat časový rámec odpovědi, kdy GDPR říká, že informace musí být poskytnuty neprodleně a nejpozději do jednoho měsíce od obdržení žádosti. Správce má však právo prodloužit lhůtu na zpracování o další dva měsíce, ale jen v případě, že se jedná o složitý nebo četný požadavek. [9]

Podle nařízená má subjekt údajů právo žádat o tyto informace:

a) Potvrzení o zpracování jeho osobních údajů.
b) Přístup ke svým osobním údajům.
c) Další doplňující informace – to z velké části odpovídá informacím, které by měly být uvedeny v oznámení o ochraně osobních údajů.

V případě, že se správce rozhodne negativně odpovědět na žádost, Musí vysvětlit proč tomu tak učinil a poskytnout subjektu údajů informaci, že může podat stížnost dozorovému orgánu bez zbytečného odkladu, a to nejpozději do jednoho měsíce. [9]

2.1.3. Právo na opravu a doplnění údajů

V souladu se zásadou přesnosti, která říká, že osobní údaje musí být přesné a v případě potřeby také aktualizované. Musí správce bez zbytečného odkladu opravit nepřesné osobní údaje. Současně má subjekt osobních údajů právo na doplnění neúplných osobních údajů. Pokud správce takovou žádost obdrží, musí vyvinout neadekvátní činnost. Aby žádost prověřil a případně vykonal potřebné kroky k opravě či doplnění.

U těchto zásad však není správce povinen sám od sebe aktivně vyhledávat nepřesné osobní údaje např. formou žádostí o revizi osobních údajů. [9]

2.1.4. Právo na výmaz („právo být zapomenut“)

V rámci obecného nařízení má každý, koho se nějakým způsobem týká sběr a uchovávání osobních údajů, právo na to, aby správce bez zbytečného odkladu vymazal jeho osobní údaje. Správce má povinnost tyto osobní údaje bez zbytečného odkladu vymazat, avšak pokud je splněna alespoň jedna z následujících podmínek:

a) Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány.
b) Subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a současně neexistuje další právní důvod zpracování.
c) Subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování.
d) Osobní údaje byly zpracovány protiprávně.
e) Osobní údaje musí být vymazány ke splnění právní povinnosti stanovení v právu Unie nebo členského státu, které se na správce vztahuje.
f) Osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1. [9]

Na rozdíl od směrnice 95/46/ES není v obecném nařízení není uvedeny hranice, kdy je zpracovávání ještě v pořádku, a kdy už způsobuje dotyčnému škodu nebo újmu. Proto může správce podle následujících bodů požadavek výmazu odmítnout:

a) Při uplatnění práva na svobodu projevu a informace.
b) Splnění zákonné povinnosti nebo plnění úkolů veřejného zájmu nebo výkonu veřejné moci.
c) Za účelem veřejného zájmu, pro účely vědeckého výzkumu, historického výzkumu nebo pro statistické účely.
d) Pro výkon nebo obhajobu právních nároků. [9]

Speciálním případem, na který GDPR pamatuje, je žádost na vymazání osobních údajů u dětí. Zvláštní pozornost je zde z toho důvodu, že děti v době souhlasu se zpracováním osobních údajů si nemusí být plně vědomy rizik se upracováním v době udělení souhlasu. V tomto případě může o výmaz zažádat i plnoletý člověk, který byl v době souhlasu nezletilým.

Další z povinností správce je informovat subjekt zpracování údajů o vymazání osobních údajů, pokud došlo ke zpřístupnění osobních údajů třetím osobám.

2.1.5. Právo na omezení zpracování

Právo na omezení zpracování a Právo na výmaz mají jisté podobné rysy, ale zatímco v Právu na výmaz mohl subjekt osobních údajů požadovat zastavení zpracování údajů, což znamená, že pokud je zpracovávání osobních dat pozastaveno, má správce povoleno pouze ukládat osobní data, ale ne je dále zpracovávat. [8]

Existuje více způsobů, jak omezit zpracování osobních dat např: dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů nebo dočasné odstranění zveřejněných údajů z internetových stránek.

V automatizovaných systémech by se mělo docílit situace, kdy se na osobní údaje nevztahují žádné další operace nebo procedury, a tak nemohly být dále měněny.

K žádosti o omezení zpracování osobních údajů může dojít za těchto okolností:

a) Jednotlivec zpochybňuje přesnost osobních údajů, a to po dobu nutnou k tomu, aby mohl správce přesnost osobních údajů ověřit
b) Když je zpracování protiprávní a subjekt údajů odmítá výmaz osobních údajů a místo toho požaduje omezení jejich použití
c) Správce již osobníc údaje nepotřebuje pro účely zpracování, ale dotyčný je požaduje pro určení, výkon nebo obhajobu právních nároků
d) Subjekt vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů [8]

Jedním z podstatných znaků omezení zpracování je jeho dočasný charakter, čímž se liší výmazu osobních údajů. Velmi důležité je také, že pokud se správce rozhodne zrušit omezení zpracování, tak musí informovat subjekt údajů o této skutečnosti. [8]

2.1.6. Právo přenositelnosti

Právo přenositelnosti je v GDPR zjevná novinka oproti směrnici 95/46 ES. Nově si subjekt údajů může zažádat o kopii jeho dat v některém z běžných formátů např. CSV, XML, JSON.

Dobrým příkladem využívání práv na přenositelnost může být změna telefonního operátora, kdy si starý operátor, po Vašem souhlasu, vymění Vaše osobní údaje s novým operátorem. [8]

Existuje několik podmínek, které musí být souhrnně plněny, aby byla možnost využívat právo na přenositelnost, tj. Musí jít o zpracování osobních údajů založených na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) Obecného nařízení nebo na

smlouvě podle čl. 6 odst. 1 písm. b). Těmito omezeními se velmi zužuje možný výběr případů, na které se právo přenositelnosti vztahuje. Zároveň musí jít také o automatizované zpracování, na zpracování prováděné manuálně se přenositelnost nevztahuje. [8]

Jedním z hlavních předpokladů aplikace práva na přenositelnost je, že se jedná o osobní údaje týkající se daného subjektu údajů, a že se nejedná o anonymní údaje.

Recitál 68 Preambule Obecného nařízení říká, že zde vzniká možnost, že by mohly být v přenášeném souboru údaje, které se týkají více nežli jednoho subjektu údajů. Podle recitálu by se však tyto údaje neměly dotýkat práv a svobod dotyčných subjektů údajů.

Další z podmínek říká, že se přenášení musí týkat údajů přímo poskytnutých subjektem údajů. Jedná se především o údaje poskytnuté vědomě např. vyplňováním online formuláře na webu. Může se to zdát poněkud matoucí, ale za data vědomě poskytnutá subjektem jsou považovány i údaje získané sledováním činnosti subjektu údajů. Příkladem může být sledování činnosti a chování uživatelů v internetovém prostředí tzn. prostřednictvím cookies, a dalších záznamů na internetových stránkách. Jako další příklad mohou sloužit např. data z GPS aplikací (kde může být snímán pohyb uživatele, historie vyhledávání tras, naměřené fyzické hodnoty atd.) [8]

V případě přenositelnosti údajů jde o vcelku unikátní situaci, a to z toho důvodu, že tato činnost předpokládá součinnost dvou správců. Tento jev se předpokládá v odvětvích jako je například bankovnictví, telekomunikace aj. a aby bylo vůbec možné předání dat od jednoho správce ke druhému, je zde nutnost technické proveditelnosti. V Obecním nařízení však není blíže specifikováno, co je strukturovaný, běžně používaný a strojově čitelný formát. V tomto případě jde tedy o součinnost dotyčných správců, jak si s přenosem dat poradí. [8]

Ačkoli je přenositelnost dat právo, které zatím nebylo využíváno v žádné evropské zemi, lze ho brát jako nápad a směr, jakým by se měl ubírat vývoj v oblasti digitálních technologií při přenosech dat.

2.1.7. Právo vznést námitku

GDPR umožňuje subjektu údajů z konkrétních důvodů, kdykoliv vznést námitku proti zpracování osobních údajů tzn. že pokud konkrétní osoba nedostane možnost uplatnit některé ze svých práv např. Právo na výmaz, tak je jí Obecným nařízením umožněno vznést námitku. Tato možnost by měla vést k omezenému zpracování těch údajů, na které je daná námitka uplatněna. [8]

Každý jednotlivec má právo vznést námitku proti:

a) Zpracování založenému na oprávněných důvodech nebo plnění úkolů ve veřejném zájmu nebo vy výkonu veřejné moci.
b) Zpracování pro direct marketing.
c) Zpracování za účelem vědeckého/historického výzkumu a statistiky. [8]

Pokud subjekt údajů vznesl námitku proti zpracovávání některých osobních údajů, musí správce prokázat oprávněnost tohoto zpracování a důvody, které mají vyšší význam než zájmy, práva a svobody subjektu údajů. Do té doby, než bude poskytnuto toto odůvodnění, zpracování osobních údajů musí být pozastaveno.

Správce osobních údajů nemusí zpracovávání zastavit pokud:

a) Správce může prokázat přesvědčivé oprávněné důvody pro zpracování, které převažují nad zájmy, právy a svobodami jednotlivce.
b) Zpracování je určeno k vytvoření, výkonu nebo obraně právních nároků.

Subjekty údajů mohou vznést námitku proti daným typům zpracovávání údajů např. přímému marketingu, zpracovávání založením na oprávněných zájmech nebo v širším zájmu veřejnost, anebo pro výzkumné a vědecké účely. Zajímavostí že při podání námitky jsou zpracovávání údajů pouze omezena, kromě přímého marketingu, zde je podání námitky absolutní a zpracovatelé údajů musí disponovat metodami, jak jednoduše odstranit osobní údaje daného člověka ze souboru zpracovávaných dat. [8]

Na druhou stranu při zpracovávání osobních údajů z důvodu vědecké činnosti, kdy je zpracovávání nezbytné pro zdárné splnění úkolu, není nutné, aby zpracovatel vyhověl námitce na zpracování.

Dále, pokud zpracovatel provádí dané činnosti online, je jeho povinností nabídnout subjektům údajů možnost realizovat svá práva online a automatizovaně. [8]

2.1.8. Automatizovaného rozhodování včetně profilování

V nynější době je pro firmy velmi důležité schraňovat informace a vytvářet si profily svých zákazníků. Tyto profily jim poté pomáhají při rozhodování o prodeji služeb a výrobků tzn. profily jsou využity k provedení klíčových firemních rozhodnutí o nových službách, nových výrobcích atd.

Profilování je pro firmu výhodné z následujících důvodů:

a) Zvýší prodej a zisk.
b) Identifikuje nejziskovější zákazníky.
c) Identifikuje zákazníky rizikové a s nejmenším přínosem.

d) Umožní automatizaci některých marketingových procesů.
e) Zajišťuje efektivnější využití firemních zdrojů.

Firmy si údaje o svých zákaznících soustřeďují většinou do následujících skupin:

a) Demografické údaje: věk, pohlaví, výše příjmu.
b) Psychologické údaje: typ osobnosti, osobní preference.
c) Chování: Co má zákazník rád a co nerad, koníčky.
d) Minulost zákazníka: předchozí chování, schopnost splácet. [8]

Díky těmto skupinám a selekcím je firmám značně usnadněna komunikace. Pomáhají například lépe zacílit marketing nebo personalizaci nabídek. Na druhou stranu zde existuje riziko nesprávného zařazení zákazníka do některé ze skupin.

Profilování je možné rozdělit na typické příklady:

a) Rozhodování o solventnosti.
b) Monitorování chování návštěvníků webových stránek za účelem marketingu.
c) Hodnocení pracovního výkonu.
d) Nábor nových zaměstnanců.
e) Vhodnost klienta k nějaké službě.
f) Zhodnocení zdravotního stavu.
g) Stanovení osobních preferencí.
h) Identifikace zájmů a potřeb.
i) Zjištění místa pohybu.

Podle GDPR se dá za profilování označit činnost, která splňuje následující dvě podmínky: Jedná se o automatizované zpracování a osobní údaje se využívají k hodnocení některých osobních aspektů. [8]

Obecné nařízení říká, že automatizované zpracování jsou operace, které se uskutečňují zcela nebo zčásti pomocí automatizovaných postupů: ukládání na nosiče dat, provádění logických a aritmetických operací s těmito daty, změna, výmaz, vyhledávání nebo rozšiřování.

Typickým příkladem pro tuto pasáž může být zacílení reklamy na webových stránkách. Pokud budete na webu hledat například nový počítač, tak budete profilováni a po určitou dobu se Vám budou na webu zobrazovat reklamy s podobným okruhem zaměření. Tímto je jasné, že GDPR bere jako profilování mnoho marketingových aktivit. Pokud firmy naplní znaky profilování, tak musí plnit i povinnosti vyplývající z nařízení GDPR. [8]

2.1.9. Právo nebýt předmětem automatizovaného individuálního rozhodování

Právo nebýt předmětem automatizovaného individuálního rozhodování představuje cestu, jak bojovat proti výhradnímu automatizovanému rozhodování, které nabývá právních účinků vůči danému člověku. [8]

Výhradní automatizované rozhodnutí znamená např. V situaci, kdy by bylo zasíláno rozhodnutí o přestupku přímo ze systému zpracovávajícího překročení rychlosti, bez lidského posouzení.

Proti tomuto jednání se může subjekt údajů bránit a má právo nebýt předmětem takového rozhodování. [8]

Automatizované individuální rozhodování je však v některých případech umožněno např. je-li nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů, dále pokud je automatizované individuální rozhodování založeno na výslovném souhlasu subjektu údajů nebo je-li umožněno právem Evropské unie nebo členského státu.

Zvláštní kategorie osobních údajů mohou být pro automatizované rozhodování využity pouze v případě výslovného souhlasu, nebo pro nezbytné zpracování z důvodu veřejného zájmu na základě práva Evropské unie či členského státu. [8]

2.2. Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů, v Data Protection Officer (DPO) je funkce, kterou nově zavádí Obecné nařízení. Pověřenec pro ochranu osobních údajů by měl plnit funkci pomocníka, koordinátora a konzultanta při ochraně osobních údajů u daného správce nebo zpracovatele osobních údajů a zároveň by měl zprostředkovávat komunikaci mezi dozorovými úřady (Úřad pro ochranu osobních údajů). GDPR jednoznačně neurčuje povinnosti Pověřence pro ochranu osobních údajů, avšak v zásadě byl měl řešit následující problémy:

a) Poskytování informací a poradenství správci nebo zpracovateli.
b) Monitorování souladu zpracování s Obecným nařízením.
c) Spolupráce s Úřadem pro ochranu osobních údajů. [7]

Vhledem k tomu, že každá obec je považována za orgán veřejné moci (veřejný subjekt), dopadá na ni povinnost jmenovat svého pověřence. GDPR však nenakazuje povinnost každé obci mít svého jedinečného Pověřence pro ochranu osobních údajů. Zde je možné využít možnosti, aby pro určitý počet obcí vykonával tuto funkci např. pověřenec

vyššího územně samosprávného celku, nebo aby se několik obcí dohodlo a najaly si svého vlastního pověřence. Každé členské zemi je umožněno, aby si svojí vnitrostátní úpravou ustanovily povinnost jmenovat pověřence i pro jiné případy než pro:

a) Zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci soudních pravomocí.
b) Hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů.
c) Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10. [1]

České republika se rozhodla této možnosti však nevyužít a pro české správce a zpracovatele bude platit povinnost pouze určená Obecným nařízením. [1]

Z vyjmenovaných činností je patrné, že jsou úkoly pověřence založeny spíše na rizikovějších činnostech. Tudíž je povinnost jmenovat pověřence pro ochranu osobních údajů dána pouze vybraným správcům, u kterých představuje zpracování údajů riziko pro práva a svobody fyzických osob, nebo těm, kteří provádí zpracování, které je už ze své podstaty rizikové a u kterého je žádoucí dohled a zajišťování souladu zpracování kvalifikovanou osobou. [1]

Ačkoli je pověřenec jmenován pouze kvůli určitým zpracováním nebo subjektům zpracování, plní poté funkci pověřence pro všechny druhy operací zpracování prováděné správcem, který pověřence najal.

2.2.1. Vzdělání, mlčenlivost a postavení pověřence

Pověřenec pro ochranu osobních údajů je velmi důležitým prvkem ve správné implementaci a poté taky chodu GDPR v úřadu obce. Proto je velmi důležité se seznámit alespoň s nejčastějšími fakty o této pozici.

Co se týče vzdělání, tak z obecného nařízení vyplývá, že nejsou stanoveny konkrétní požadavky na vzdělání pověřence (tj. akademické tituly a certifikáty). Je to způsobeno velkým rozsahem forem zpracování u správců a zpracovatelů dat a každému z nich může vyhovovat pověřenec s jiným vzděláním, zkušenostmi i jazykovými dovednostmi. Z toho vyplývá že: „**Musí jít o osobu odborně zdatnou v daném odvětví, aby byla schopna plnit konkrétní úkoly pověřence u daného správce nebo zpracovatele“.** [1]

Dále existují domněnky, že by měl pověřenec pro ochranu osobních údajů disponovat certifikací nebo osvědčením. GDPR však nenařizuje pověřencům vlastnit takový certifikát, tudíž může daná osoba vykonávat práci pověřence pro ochranu osobních údajů i bez takového certifikátu. Jelikož ale Obecné zařízení vydávání certifikátů nevylučuje, můžou se v praxi objevit situace, kdy absolvent určitého kurzu obdrží certifikát o absolvování daného kurzu. Tento certifikát je ale pouze doplňkovým důkazem schopností pověřence pro ochranu osobních údajů, nikoli hlavním kritériem při výběru pověřence.

Otázce mlčenlivosti ze GDPR přímo nevěnuje. Je zde pouze konstatováno, že pověřenec je povinen držet mlčenlivost v souvislosti výkonem svých úkolů vázán tajemstvím nebo důvěrností v souladu s právem Evropské unie nebo členského státu. V České republice by měl mlčenlivost upravovat zákon o zpracování osobních údajů. Je možné však konstatovat, že každá osoba, která přijde do styku s osobními údaji musí dodržovat mlčenlivost u všech osobních údajů i bezpečnostních opatření, která se sběru osobních dat týkají. [1]

Povinnost mlčenlivosti však nelze uplatňovat vůči správci, zpracovateli, který pověřence jmenoval, orgánu činnému v trestném řízení, soudu nebo úřadu. Pokud jde o subjekt údajů, kterého se sběr dat týká, tak v tomto případě by se dat také neměla mlčenlivost týkat.

Vztah ke správci, nebo zpracovateli, kterým byl najat. Obecné nařízení vykládá, že je správci nebo zpracovateli pověřenec přímo podřízen. Není to však postavení, že by byl podřízen přímo statutárnímu orgánu, ale je vykládáno spíše z důvodu možnosti přímého kontaktu s vrcholovými pracovníky organizace Např. účastnění se porad vysokého managementu organizace. [1]

Pracovní role pověřence pro ochranu osobních údajů by měla být značné nezávislá. Podle Obecného nařízení nesmí pověřenec přijímat pokyny od správce nebo zpracovatele co se týče výkonu jeho povinností nebo jakých výsledků se má dosáhnout, jak prošetřovat stížnosti nebo jestli určité záležitosti konzultovat s dozorovým úřadem. Daná opatření však nejsou brána tak, že by správce nebo zpracovatel nemohl s pověřencem o daných tématech komunikovat. [1]

Pověřenec pro ochranu osobních údajů má i silné postavení v organizaci z toho důvodu, že nemůže být v souvislosti s plněním svých úkolů propuštěn nebo sankciován. Tento zákaz však nelze brát ve všech ohledech, tato pojistka vznikla proto, že někteří správci nebo zpracovatelé by mohli mít tendenci „oplácet“ pověřencovi za to, že plní své úkoly a v důsledku toho, to může mít pro vedení dopad na hospodářské výsledky. [1]

Samotné postavení pověřence v organizaci musí odpovídat úkolům, které je potřeba plnit. Je nezbytné, aby vedení organizace včas a náležitě zapojilo pověřence do chodu společnosti a do všech záležitostí souvisejících s jeho budoucími úkoly. Pověřenec by měl disponovat vcelku velkými oprávněními seznamovat se s vnitřním chováním organizace, to je jediná možnost docílit správného plnění úkolů ze strany pověřence. [1]

Pro práci v každé organizaci, kde je osoba pověřence pro ochranu osobních údajů vyžadována, jsou především nutné pověřencovi odborné schopnosti. Základem úspěchu je tedy především jmenování pověřence pro jeho odborné a profesní kvality, aby byl schopný plnit úkoly stanovené Obecným nařízením. GDPR nestanovuje konkrétní požadavky na vzdělání, nebo minimální úroveň dosaženého vzdělání, je to z toho důvodu, že každé prostředí a organizace mohou vyhovovat různým pověřencům s různými profesními kvalitami.

2.3. Správce a zpracovatel osobních údajů

Správce osobních údajů je jedním z nejdůležitějších pojmů v GDPR, bez kterého se neobejde žádné zpracování osobních údajů. Správce určuje účel a prostředky zpracování. Správce může pro zpracovávání osobních údajů využít i jiný subjekt než jeho samotného, a to zpracovatele osobních údajů. Zpracovatel na rozdíl od správce není povinný k činnosti zpracovávání údajů, záleží pouze na správci, jestli využije zpracovatele pro zpracovávání osobních dat. [8]

Pokud správce využívá, poté musejí být splněny požadavky z čl. 28 Obecného nařízení, kde zpracovatel:

a) Zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci.
b) Zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.
c) Přijme všechna opatření požadovaná podle článku 32.
d) Dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4.
e) Zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření.

f) Je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 a 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici.
g) V souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů.
h) Poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje. [8]

2.3.1. Správce

Podle nařízení je správce fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Můžou to být účely vyplývající z jeho činnosti (tj. zákonem stanovené činnosti), nebo může účely zpracovávat i pro vlastní oprávněné účely.

Pojem správce je již definován v zákoně 101/200 Sb., o ochraně osobních údajů a v souvislosti s tímto zákonem již nebyl změněn. [8]

V reálné situaci se může stát, že účely a prostředky si vyžádají dva nebo více správců, tím se stávají společnými správci. Základem pro kooperace správců je vymezení si podílů odpovědnosti za plnění povinností transparentním ujednáním. To je zejména v případech výkonu práv subjektu údajů a povinnosti poskytovat informace uvedené v článcích 13 a 14.

Pro subjekt údajů se však v ohledu na vykonávání svých práv nic nemění, dokonce je mu poskytnuta i zvýšená forma ochrana, protože může vykonávat svá práva u každého ze společných správců. [8]

V GDPR je také uvedeno, že pokud je ve zpracování zapojeno více správců, či zpracovatelů a nesou-li odpovědnost za jakoukoliv škodu způsobenou daným zpracováním, tak každý správce nebo zpracovatel nese odpovědnost za celou újmu, tak aby byla zajištěna účinná náhrada újmy subjektu údajů. [8]

2.3.2. Zpracovatel

Podle Obecného nařízení čl. 4 odst. 8 je zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. [2]

Primární úkol zpracovatele je zpracovávat osobní údaje „svěřené“ správcem způsobem určeným správcem a způsobem určeným správcem. J

Je důležité rozlišovat, jestli zpracovatel také neprovádí sběr dat pro své osobní účely, protože v tu chvíli se stává správcem daných údajů a musí být na něho tak pohlíženo.

Zpracovatel může být k přizván správcem ke zpracovávání prakticky kdykoliv. Většinou je to zapříčiněno tím, protože správce nemá dostatečné know-how nebo technické vybavení pro zpracovávání daných osobních údajů. [2]

2.4. Zabezpečení osobních údajů

Velmi důležitým předpokladem pro dosažení souladu zpracování osobních údajů s GDPR je dodržovat řádné zabezpečení osobních údajů. [8]

Kvůli velkému počtu zpracovatelů a správců osobních údajů a velkému počtu možností zpracování, není reálné klást na všechny správce a zpracovatele stejné požadavky co se bezpečnostních opatření. Podle čl. 32 odst. 1 Obecného nařízení, musí správce, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závazným rizikům pro práva a svobody fyzických osob, vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) Pseudonymizace a šifrování osobních údajů.
b) Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systému a služeb zpracování.
c) Schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů.
d) Procesu pravidelného testování posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti pracování. [8]

Šifrování a pseudonymizace dat jsou však pouze doporučujícími prostředky, tzn. že je pouze na správci, jestli tyto opatření použije nebo ne. Použitím šifrování a

pseudonymizace dat však správce nebo zpracovatel výrazně snižuje riziko zpracování a jeho případnou odpovědnost při nenadálém úniku dat. [8]

2.4.1. Pseudonymizovaná data

Pseudonymizace je v GDPR definována jako zpracování osobních údajů tak, „že nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, jsou-li tyto dodatečné informace uchovány odděleně a vztahují-li se na ně technická opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné osobě.“

Rozdíl mezi anonymními daty a pseudonymizovanými daty spočívá právě v možnosti zpětného přiřazení údajů zpět ke konkrétnímu subjektu údajů u pseudonymizovaných údajů. [8]

Jméno	Příjmení	Adresa	Vzdělání	Rodinný stav	Měsíční příjem
Josef	Novák	Gorkého 45, Pardubice	SŠ	Svobodný	20000 Kč/měsíc
			SŠ	Svobodný	20000 Kč/měsíc
Josef	Novák	Gorkého 45, Pardubice	SŠ	Svobodný	20000 Kč/měsíc

Osobní údaje Anonymní údaje Pseudonymizované údaje 0001

Tabulka č. 4: Druhy zabezpečení osobních údajů, zdroj: [8]

První řádek tabulky znázorňuje osobní údaje, které byly vypsány v celém rozsahu. Jelikož se zde vyskytuje v jednom řádku jednoznačně identifikovatelná osoba, je potřeba brát i všechny ostatní záznamy jako osobní údaje.

V případě druhého řádku se jedná o možnost, že by správce nenávratně smazal jméno, příjmení a adresu. Nevratným smazáním těchto údajů se ze zbylých dat stávají anonymní údaje, protože správce již nemá pomocné údaje, podle kterých by identifikoval, jakému subjektu údajů zbylé údaje patří. [8]

Třetí řádek znázorňuje pseudonymizaci, údaje v šedé zóně lze považovat za pseudonymizované, pokud jsou údaje z fialové zóny uchovávány odděleně a např. šifrovaně a pro potřeby správce jsou používány pouze údaje z šedé zóny s tím, že identifikační údaje jsou nahrazeny identifikačním číslem (ID).

0001	SŠ	Svobodný	20000 Kč/měsíc

Tabulka č. 5: Pseudonymizace dat, zdroj: [8]

Vazba mezi zbylými údaji a údaji potřebnými k identifikaci není zcela zničena, tudíž je možné údaje opět spojit dohromady. Správce tedy ví, že pod identifikačním číslem 0001 se ukrývá určitá osoba (Josef Novák).

Sběr dat metodou pseudonymizováním údajů přináší správci výhodu, že v případě úniku šedého rozsahu údajů nebude únik takovým problémem jako kdyby unikla data přímo spojená s identifikačními údaji osoby. Proto je i v Obecním nařízení doporučeno, aby správci, pokud to umožňuje situace, využívali pseudonymizaci dat. [8]

Velkou výhodou pseudonymizace dat je potřebná součinnost původního správce pro identifikování údajů, například při přenosu údajů dalšímu subjektu, který bude s daty dále pracovat (zpracování pro statistické údaje, zdravotnický výzkum aj.). Bez součinnosti původního správce by byl nový zpracovatel schopen zkoumat pouze anonymní data. [8]

2.4.2. Šifrovaná data

Vhodným doplňkem k pseudonymizaci údajů se jeví šifrování identifikačních údajů na databázi. Velkou výhodou pseudonymizace je, že pokud např. útočník zcizí pouze obecné údaje z jedné tabulky a nezcizí tabulku s identifikačními údaji, tak se mu do rukou dostanou pouze obecná data, se kterými nezpůsobí tolik škody jako kdyby disponoval i údaji tyto data identifikující. Pokud by se ovšem útočník dokázal dostat do celé databáze, kde by byly identifikační údaje nešifrované, byl by schopný si k obecným datům dohledat i jejich majitele. Jestliže však budou identifikační údaje šifrovány a klíčem bude disponovat pouze správce údajů nebo autorizovaná osoba, z identifikačních údajů bude o mnoho složitější vyčíst útočníkem požadovaná data. [9]

Ukázka tabulky bez šifrovaných údajů:

	Jmeno	Prijmeni	MistoNarozeni	DatumNarozeni	RodneCislo	ZadatelID
1	Stanislav	Hladík	Litomyšl	14. listopadu 1995	123456/1234	39
2	Radim	Hladík	Litomyšl	4. října 1999	987654/4321	40
3	Kateřina	Hladíková	Litomyšl	1. května 1993	654198/6547	41

Obrázek č. 2: Nešifrované údaje, zdroj: vlastní zpracování

Ukázka tabulky se zašifrovanými identifikačními údaji:

	Jmeno	Prijmeni	MistoNarozeniSifrovane	DatumNarozeniSifrovane	RodneCisloSifrovane	ZadatelIDSifrovany
1	Stanislav	Hladík	0x01000000CCC8D07C28...	0x01000000C6266C3DD0...	0x01000000EA5228...	0x010000007A2E...
2	Radim	Hladík	0x01000000E0E7980C7B...	0x010000000D8FF0C664D...	0x0100000069AE8A...	0x010000008BCA...
3	Kateřina	Hladíková	0x010000009957D10710...	0x01000000648ADE27CE...	0x0100000034AE1A...	0x01000000532F...

Obrázek č. 3: Šifrované údaje, zdroj: vlastní zpracování

Správci a zpracovatelé osobních údajů však také musí přijmout, s přihlédnutím k riziku zpracování, taková opatření, aby bylo zajištěno, že osoby mající k osobním datům přístup je budou zpracovávat pouze na pokyn správce. Výjimku tvoří situace, kdy je zpracování přímo nařízeno Evropskou unií nebo členským státem. [10]

Aby bylo docíleno takové povinnosti, musí správce nebo zpracovatel zavázat své zaměstnance, kteří mají k těmto údajům přístup (např. v pracovní smlouvě, dohodě o provedení práce nebo dohodě o pracovní činnosti). Také všechny třetí strany (které se například starají o IT systémy) je správce nebo zpracovatel nucen zavázat k důvěrnosti, a to vhodnými smluvními instrumenty. [10]

2.5. Dopad na chod obce

Jako je to u každé změny v pracovních postupech a pracovních zvycích, i u GDPR lze předpokládat, že její implementace bude mít na chod obce Dolní Újezd svůj vliv.

2.5.1. Nutnost provést vstupní analýzy

Základním předpokladem pro zavedení GDPR je detailní vstupní rozbor, s jakými osobními údaji se pracuje a jak se s těmito údaji pracuje. Tyto údaje jsme schopni zjistit pomocí různých analýz.

Analýzou osobních údajů zjistíme informace, které nám poté pomohou zjistit jaké změny bude nutné udělat v souladu s Obecným nařízením. Bude se jednat o všechny agendy obce spolu s informacemi, týkající se této agendy, jako například: Název, správce, zákonnost zpracování, účel zpracování, osoba pověřená zpracováním, rozsah zpracování, prostředky zpracování, příjemce zpracování, způsob vyřízení agendy (komunikace), doba uložení agendy.

Analýza procesů nám poté identifikuje konkrétní činnosti při zpracování (jaké původně byly) a jak tyto návyky a činnosti změnit, aby opět vyhovovaly GDPR. K analýze procesů je nutné podotknout, že v porovnání s většinou ostatních organizací, zpracovává Obecní úřad velké množství údajů podle zákona (legislativou je dáno, proč se mají konkrétní osobní údaje shromažďovat a není tudíž nutné žádat souhlas se zpracováním osobních údajů.) V případech osobních údajů, kde úřad získal souhlas již v minulosti, je nutné prověřit, zda souhlas splňuje podmínky vyplývající z GDPR.

Rizikové analýzy budou hrát velmi důležitou roli při zavádění GDPR do praxe úřadu. Protože dokáží identifikovat vliv nejrůznějších hrozeb, které plynou z případných chyb a

nedostatků. Povětšinou se jedná hrozby následující: Odcizení osobních údajů, ztráta osobních údajů, neoprávněné přístupy do systémů, poškození údajů (fyzické i softwarové), poskytnutí osobních údajů osobě, která nemá patřičná oprávnění a ztráta nebo odcizení osobních údajů.

Neméně důležitou je analýza bezpečnosti informačních systémů. V dnešní době je této analýze nutné klást potřebnou pozornost, protože většina informací v dnešním světě je ukládána elektronicky. Bezpečnost je potřebné řešit ať už pro ukládání údajů používá obec vlastní informační systémy, nebo cloudová řešení.

2.5.2. Další nutné náležitosti spojené s dopadem na obec

Po vstupních analýzách je také nutné prověřit a projednat nové smlouvy. Podle Obecného nařízení si každý správce může najmout libovolný počet zpracovatelů. Nařízení 2016/679 však jasně definuje pravidla, která musí splnit každý zpracovatel těchto osobních údajů.

Pokud například zpracování osobních údajů vyplývá ze smluv, musí obsahovat konkrétní ustanovení včetně kvalifikovaného souhlasu se zpracováním osobních údajů.

Pokud osobní údaje v některých případech zpracovává více subjektů. Je nutné mezi nimi smluvně upravit vztah zpracovávání. V dohodě musí být definován společný účel zpracování osobních údajů a také definována zodpovědnost za jejich bezpečnost. Musí se také ošetřit smluvní vztahy se subjekty, jimž poskytuje osobní údaje.

Velký vliv na chod obecního úřad a obce Dolní Újezd jako takové bude mít také sestavení rozpočtu vyčleněného na GDPR a to:

a) Příprava a implementace GDPR (Vstupní a rozdílové analýzy, změn v procesech a jejich doplnění, školení, konzultace, externí dodavatelé)
b) Udržení provozu v souladu s pravidly GDPR (Náklady na práci pověřence, správců či zpracovatelů)

3. Řešení v prostředí obce

Před řešením každé problematiky je potřeba provést důkladnou analýzu zpracovávaných a procesů, jak se s nimi nakládá. Po této operaci bude možné sestavit návrh na řešení jednotlivých úkonů. Velmi důležitý je také pohled zavedené informační systémy, kterými se dosavadní sběr dat a práce na agendách řešil. Pro agendy, které jsou v mnohých ohledech v obcích podobné jsou dostupné zavedené programy, které dané programy z větší části řeší. Jedná se například o programy: Triada, Munis, SW DataIT apod. Tyto nástroje dokáží pokrýt velké spektrum agend, které je potřeba řešit, avšak ne všechny. Pro agendy, kterým nejsou dané nástroje přizpůsobeny (povětšinou evidence malých spolků) je vhodné vyřešit, jak by mohl vypadat informační systém, jenž by dokázal s danými informacemi úkony například: ukládat data, dále data zpracovávat a další činnosti. Nejprve je však nutné, jak data vůbec vypadají, než se začne přemýšlet, jak vyřešit problematiku informačního systému.

3.1. Vstupní identifikace dat, která zpracovává obec Dolní Újezd

Data sbíraná obcí Dolní Újezd se dají rozlišit do tří skupin jsou to:

a) Data obsahující osobní údaje zpracovávaná pro vlastní agendy obce
b) Data obsahující osobní údaje zpracovávaná pro soukromé osoby
c) Data obsahující osobní údaje zpracovávaná pro veřejné agendy

Pro přehlednou práci s daty je důležité si zaznamenat všechny potřebné informace, týkající se každé jednotlivé agendy. Dobré je agendu správně nazvat, dále zaznamenat: Kdo bude správcem osobních údajů, zákonnost zpracování, účel zpracování agendy, osoba pověřená zpracováním (starosta, místostarosta, účetní), rozsah zpracování (osobní údaje, které se zaznamenají), prostředky zpracování (např. programy do kterých se zaznamenávají osobní údaje), příjemce zpracování, způsob komunikace, doba uložení agendy.

Data ze zpracování pro vlastní agendy obce si obec Dolní Újezd uchovává pro své vlastní potřeby. Pro osobní údaje, které jsou v této agendě sbírané je nutné dodržet sběr pouze osobních dat nutných k výkonu dané agendy (Evidence obyvatel, Podpisové certifikáty, Evidence psů atd.)

V této části se právě některé agendy pracující s osobními údaji řeší pomocí programů, k řešení těchto agend přímo určených například evidence obyvatel se provádí

pomocí specializovaného softwaru Munis, je to z toho důvodu, že program dobře komunikuje se státními servery pro evidenci obyvatel, což velmi usnadňuje práci. Některé agendy v této pasáži jsou však řešeny programy Microsoft Word, nebo Microsoft Excel. Ačkoli jsou tyto programy velmi vyspělé, tak jejich univerzálnost nedovoluje přímé modifikování pro jednotlivé agendy, a pro mnoho agend by bylo možné najít řešení, které by nabídlo lepší podmínky pro případnou automatizaci procesů.

Všechny agendy pro obec viz. Příloha 1 (Agendy obsahující osobní údaje zpracovávané pro potřeby obce)

Data ze zpracování pro soukromé osoby se týkají většinou těch osob, které zároveň žádají obec o provedení nějakého úkonu (Žádosti o výpis z rejstříku, Stížnosti a petice), zároveň příjemce zpracování těchto údajů je povětšinou sám žadatel zpracování.

I v této kategorii zpracovávaných dat se nacházejí agendy, u kterých by bylo vhodné naimplementovat řešení na míru, které by zjednodušilo a případně zautomatizovalo řešení daných problematik (jedná se například o agendy: evidence psů, evidence dětí do školky, evidence dětí do školy), na druhou stranu se zde nachází i agendy u kterých taková implementace zkrátka není možná, a to kvůli samotné charakteristice problému. Pokud bude například starosta obce vydávat nějaké povolení, je vhodnější dané povolení vytvořit v jakémkoliv kancelářském programu (např. Microsoft Word) a udělit jej přímo žadateli, nebo v případě hromadného povolení, pověsit na reálnou, nebo internetovou vývěsku.

Agendy zpracovávané pro soukromé osoby viz. Příloha 2 (Agendy obsahující osobní údaje zpracovávané pro soukromých osob)

Posledním druhem dat, které obec Dolní Újezd sbírá jsou **data, která obsahující osobní údaje zpracovávané pro veřejné agendy** (Finanční úřad, pojišťovna). Tyto agendy jsou vyžadovány takřka po všech obcích, tudíž se zde nachází mnoho softwaru, který dokáže potřebné služby pokrýt. Například pro agendu účetnictví je zde využíván program SW DataIT. Agendy zpracovávané pro veřejné agendy viz. Příloha 3 (Agendy obsahující osobní údaje zpracovávané pro veřejné agendy)

3.2. Analýza procesů a rizik obce

Analýza procesů a rizik v obci je jedním z nejdůležitějších prvků k zavedení kvalitní implementace GDPR v obci Dolní Újezd. Analýzou procesů se rozumí zachycení konkrétních činností a pracovních postupů, které vedou ke zpracování osobních údajů.

Analýza rizik nám pomáhá analyzovat případné chyby a nedostatky, jejichž pomíjení by mohlo vést až k peněžním pokutám.

3.2.1. Analýza procesu sběru osobních dat obce Dolní Újezd

V procesu sběru osobních dat figurují většinou čtyři role:

a. Občan obce
b. Administrativní pracovník obce
c. Kontrolor
d. Schvalovatel

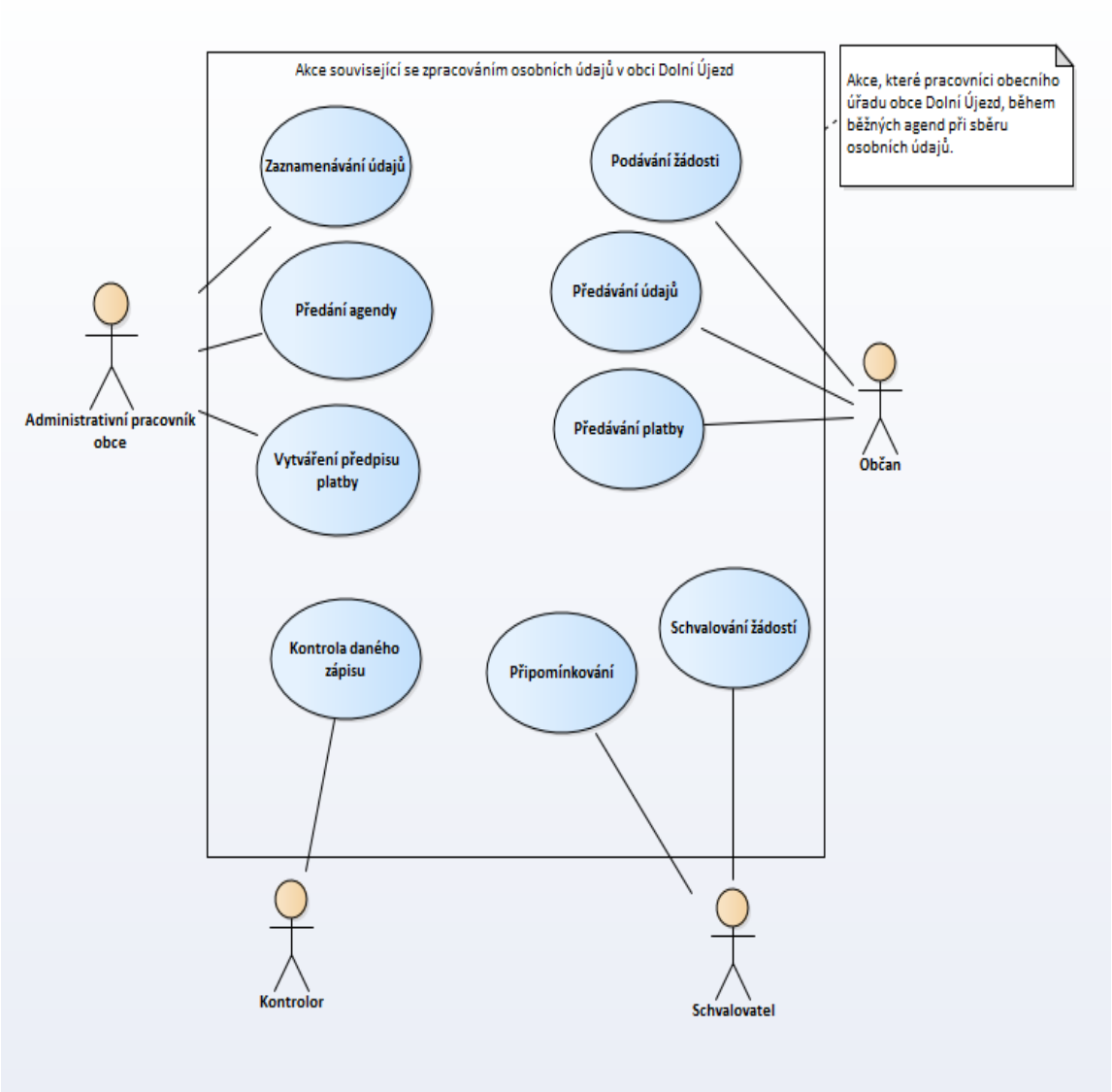
Občan obce může podávat podněty k různým agendám, předávat údaje administrativním pracovníkům obce, nebo předávat platby za určité agendy.

Administrativní pracovník obce zaznamenává údaje, které mu občan obce Dolní Újezd poskytne, dále předává zaznamenanou agendu k dalšímu zpracování a vytváří předpis případné platby.

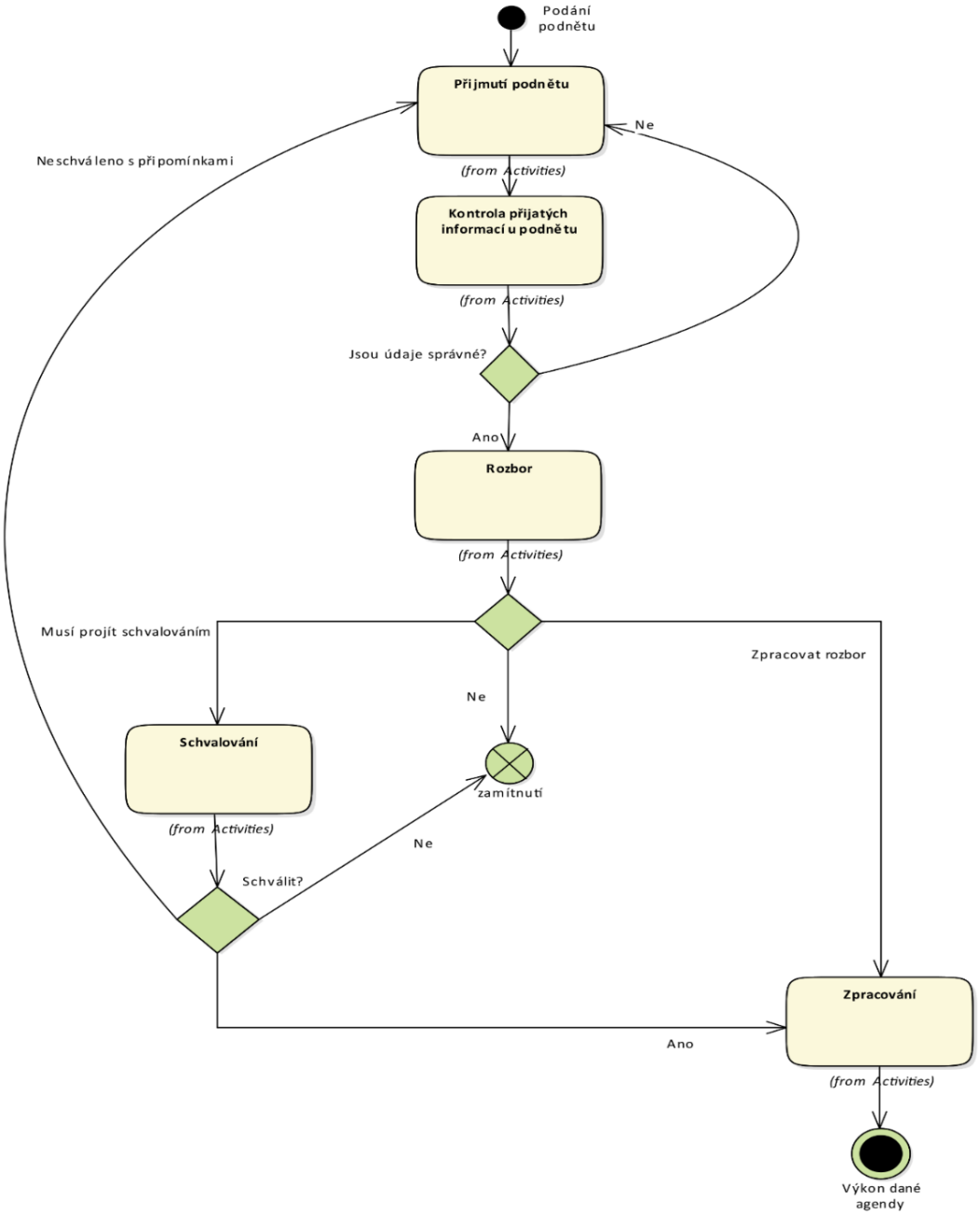
Kontrolní pracovník provádí kontrolu zadaných údajů a proveditelnost provedení agendy.

Schvalovatel schvaluje podněty a může je i libovolně připomínkovat. Pokud podnět neschválí, je podnět vrácen k doplnění potřebných údajů a k přehodnocení zpracování.

Při procesu sběru nejprve přijde občan obce s určitým podnětem. Tento podnět přijme příslušný administrativní pracovník obce a zkontroluje správnost dodaných údajů, pokud jsou údaje neúplné, nebo nesprávné jsou odeslány zpátky k doplnění údaji v prvním kroku diagramu. V případě, že jsou zadané údaje správné a pravdivé, přechází podnět k rozboru. V rozborové části se řeší jestli lze daný podnět přijmout co se týče obsahové části (např. přijmutí žadatele v domové s pečovatelskou službou). Pokud z nějakého důvodu je potřeba schválit, jde daný podnět do schvalovacího procesu, kde může být podnět schválen, vrácen k doplnění údajů s připomínkami anebo úplně zrušen. Pokud je podnět schválen, ta se zpracuje a může se přejít dále k výkonu dané agendy.



Obrázek č. 4: Use case sběru osobních dat v obci, zdroj: vlastní zpracování



Obrázek č. 5: Activity diagram sběru osobních dat, zdroj: vlastní zpracování

3.2.2. Analýza rizik v procesech

Jako každý správce nebo zpracovatel se musí mít obec Dolní Újezd na pozoru před možnými riziky, ať už je to únik dat, znehodnocení, či ztráta těchto dat.

V našem případě se z větší části jedná o tyto rizika:

a) Nedostatečně proškolení zaměstnanci
b) Narušení osobních údajů na straně zpracovatele
c) Únik dat
d) Chybné zadání údajů.
e) Ponechání osobních informací ve fyzické podobě bez dozoru.

Nedostatečně proškolení zaměstnanci

Řešením je proškolení zaměstnanců o GDPR a sním souvisejících nových povinnostech (povinnost doložit souhlas subjektu údajů se zpracováním osobních údajů, dodržování interní směrnice atd.) Předání těchto vědomostí lze řešit společnými školeními, nebo sepsáním interní směrnice, kterou budou všichni zaměstnanci povinni dodržovat.

Co se týče dnešní doby je také více než vhodné školit zaměstnance v oboru IT bezpečnosti (pokud pracovník pracuje s daty, velmi pravděpodobně pracuje i s počítačem).

Narušení osobních údajů na straně zpracovatele

Toto riziko nastává většinou v situacích: odcizení pracovního počítače, ztráta nosiče dat, ztráta přístupových hesel do informačních systémů.

V takovém to případě je velmi důležité problém řešit hned jakmile daný zaměstnanec zjistí potencionální výskyt problému. Velmi praktický je v tomto případě interní dokument Obecního úřadu, který řeší komu tento bezpečnostní incident nahlásit, jak zajistit dokumentaci k problému a jak minimalizovat způsobené škody.

Únik dat

Únik dat lze specifikovat dvěma způsoby:

a) Fyzický průnik k datům a jejich odcizení
b) Vzdálený přístup k datům a jejich odcizení

Při fyzickém přístupu k datům je pro potencionálního útočníka zapotřebí také trochu uživatelské nedbalosti. Například, pokud nechá zaměstnanec volně ležet svoje pracovní zařízení v místnosti, nebo v autě (Pro zkušeného útočníka je již minimální problém, pokud je zařízení vypnuté). Útočník se v tomto případě může k datům, které je uložené přímo

na zařízení. Pomocí různých nástrojů a bootovacích operačních systémů je možné se dostat k datům i bez zadání přístupového jména a hesla do původního operačního systému, který je na počítači nainstalován. [10]

K předejití těchto problémů se doporučuje využití šifrovacích nástrojů, které šifrují systémový disk počítače k předejití neautorizovaných operací v systému a v pevném disku např. malwarem na firmwarové úrovni. Mezi takové nástroje patří: Windows BitLocker, McAfee Encryption security tool aj. [10]

U vzdáleného odcizení dat se může jednat o víc technik, které se využívají k útokům na vzdálený počítač, nebo server. Mezi nejvíce používané techniky se řadí tzv. phishing. Pomocí phisingu se útočník snaží získat uživatelova citlivá data (přístupové údaje, hesla, údaje o platebních kartách, rodná čísla, čísla bankovních účtů), tento typ útoku se povětšinou šíří podvodnými emailovými zprávami nebo přesměrováním na falešné webové stránky. Proti phishingovým útokům se lze v zásadě bránit takto:

a) Být obezřetný a neklikat na žádné odkazy v emailové poště, která je jakkoli podezřelá (např. nesouvisející emailová adresa odesílatele s obsahem, nebo gramatické chyby v psaném textu)
b) Neotvírat přílohy podezřelých emailů
c) Nikomu nesdělovat citlivé informace (hesla, přístupové údaje)
d) Kontrolovat URL adresy navštěvovaných internetových stránek [12]

Dalším používaným způsobem průniku k datům je prolomení hesla k Wi-Fi síti v instituci a poté uskutečnění dalších kroků k získání citlivých dat. Avšak aby se tento problém podařilo jednoznačně eliminovat je důležité se zaměřit na více věcí než pouze zabezpečení Wi-Fi hesla:

a) Již na začátku každé firemní sítě by měl kvalitní síťový router se zabudovaným firewallem, aby se malwarové hrozby zachytávali již na začátku firemní sítě. Tento počáteční síťový prvek by měl disponovat technologiemi jako například: AMP (Advanced Malware Protection), NGIPS (Next-Generation Intrusion Prevention System), AVC (Application Visibility Control) a filtraci URL adres.
b) V dnešní době je již standardem k pracovním účelům využívat mobilní telefon. K dobrému zabezpečení komunikace a připojení u mobilních telefonů a zařízeních, které přistupují k firemní síti přes internet je doporučené využít VPN (Virtual private network). Tato technologie zabezpečí připojení přes internet do korporátní sítě a zajistí bezpečný

a šifrovaný přenos dat mezi těmito dvěma body, dále VPN pomáhá uchránit firemní síť od neautorizovaných přístupů.

c) Pokud obec nebo společnost při jednáních vyžadují, aby byl zákazník, nebo dodavatel připojen k internetu, je vhodné ve firemní síti zřídit Wi-Fi pro hosty, která bude oproti zaměstnanecké Wi-Fi řádně omezena na přístupech.
d) Dalším bodem je kvalitně zabezpečený server tzn. Antivirový program, interní komunikace přes https, a šifrované údaje na serveru (např. v SQL databázi).
e) Posledním bodem je ochrana samotných koncových zařízení: Na pracovních zařízeních by měl být nainstalovaný antivirový program, měl by se zakázat přístup na podezřelé weby a uživatelé by měli být řádně poučeni, jak se chovat v prostředí firemní sítě. [13]

Chybné zadání údajů

Ve skoro každém prostředí je nutnost se pomocí nějakých údajů, přihlásit do systému v počítači. Pokud však jsou však účty na počítačích a na serverech nastavené lokálně. Může být poté problém odblokovat účet po mnohačetném zadání chybných údajů.

Pro tyto a mnohé další případy se využívají LDAP adresářové služby, ve kterých se dají spravovat počítače a uživatelé, kteří fungují v doméně a pomocí těchto služeb může IT pracovník spravovat tyto účty v doméně, tudíž i odblokovat zamčený účet. [13]

Ponechání osobních informací ve fyzické podobě bez dozoru

Po zavedení Obecného nařízení je zakázáno ponechávat všechny písemnosti, které by mohli obsahovat osobní údaje, bez dozoru, na volně přístupných místech. K těmto problémům se také řadí ponechání odemčených svých počítačů v nepřítomnosti na pracovišti. [14]

Řešením této situace je opět proškolení zaměstnanců, že i při dočasném opuštění pracoviště musí uzamknout svůj profil na pracovním počítači a pečlivě uschovat a všechny dokumenty, ve kterých by se mohly nacházet osobní údaje.

3.3. Analýza dopadů GDPR na informační systémy

Informační systémy a úložiště, které se v obci Dolní Újezd využívají se dají rozlišit podle sbíraných dat, a k čemu jsou tato data využívána.

3.3.1. Informační systémy a úložiště pro agendy obce a uživatelů

Pro tyto data zatím neexistuje žádný specializovaný program, do kterého by byla zmíněná data vkládána. Data jsou ukládána do dokumentů v programech Microsoft Excel anebo Microsoft Word. Takto ukládaná data mohou mít mnoho problémů např.:

a) Data jsou uložena pouze na počítači. (Problém při nenadálém fyzickém poškození počítače)
b) Data nejsou šifrována ani anonymizována
c) Obtížný přístup k datům.

Pokud není úplně nezbytné ukládat data přímo jenom do počítače, bylo by vhodné zvolit jiné umístění, kam by se měla data ukládat.

Pro tyto účely jsou vhodné dvě řešení, jaké úložiště zvolit:

a) Uložit data do cloudového úložiště
b) Vybavit obecní pracoviště serverem dedikovaným pro úložné účely

Variantu cloudového úložiště lze charakterizovat jako úložný server, ke kterému mohou uživatelé přistupovat vzdáleně například pomocí internetového prohlížeče. Cloudové úložiště funguje na principu sdílení hardwarových a softwarových prostředků prostřednictvím internetové sítě.

Výhody a nevýhody cloudového úložiště:

Výhody	Nevýhody
Možnost dostat se k datům takřka odkudkoli	Pravidelné platby pronájmu úložiště
Klient se nemusí obávat fyzického zničení úložiště	Data jsou uložena na cizí infrastruktuře
Z velké části odpadá náročné nastavování úložiště	Data kolují po internetové síti
Není nutná velká prvotní investice do infrastruktury	Možná časová prodleva

Tabulka č. 6: Výhody a nevýhody cloudového úložiště, zdroj: vlastní zpracování

V dnešní době existuje nepřeberné množství, můžeme jmenovat například: Amazon AWS, Microsoft Azure, Google Cloud, Kahu nebo CloudVPS. Každá z těchto platform již nedisponuje už jenom úložným prostorem, ale jedná se o multiplatformní cloudovou službu zahrnující služby například: testování, nahrávání různých programovatelných projektů, Active Directory, databázové služby (MSSQL, MySQL) a mnoho dalších.

Vybavení obecního pracoviště serverem je variantou, pokud zpracovatel dat má raději když se mu data „nepotulují“ někde po internetu. V zásadě má ale fyzicky dostupné úložiště jednu obrovskou výhodu, a to v případě výpadku internetu nebo síťového přenosu je stále možné fyzicky k souborovému serveru dojít a data zachránit. V případě fyzického serveru se nabízí mnoho variant a možností jaký serverový hardware si pořídit a jak nakonfigurovat softwarovou část. Při výběru serverového počítače pro ukládání dat je třeba myslet na výkon, cenu, velikost úložiště, a především na to, jestli server podporuje hardwarový RAID, jedná se o sekundární ochranu dat (primární ochranou dat je zálohování), kde je, díky správně zvolenému typu RAID, možnost obnovit zpět ztracená data při výpadku počtu disků v závislosti na typu RAID. [18]

Nepoužívanějšími typy RAID jsou:

a) RAID 0 (prokládání)

   Ve skutečnosti se nejedná o RAID v pravém slova smyslu, protože jeho hlavním úkolem je zvýšit rychlost čtení a zápisu prokládaným ukládáním dat na různé disky, které jsou zapojené (pokud se rozbije jeden disk, všechna data budou ztracena)

b) RAID 1 (zrcadlení)

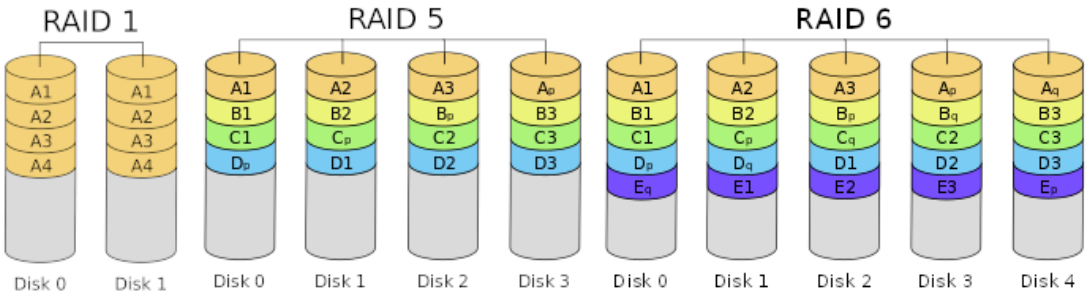
   Nejjednodušší, avšak velmi efektivní ochrana informací. Data jsou současně ukládána na dva disky. Pokud nastane ztráta jednoho disku, všechna data jsou uložena na disku druhém, zároveň je docíleno může být docíleno i zrychleného čtení dat (záleží na použitém řadiči). Nevýhodou je však potřeba dvounásobné hodnoty úložného prostoru.

c) RAID 5

   Tento typ vyžaduje alespoň 3 diskové jednotky, přičemž v každém z disků jsou uloženy samoopravné kódy, které dohromady zabírají kapacitu jednoho celého disku. Výhody jsou: vyšší rychlost čtení, díky paralelnímu přístupu k datům a odolnost vůči výpadku jednoho disku při větší efektivní kapacitě.

d) RAID 6

Posledním typem z těch používanějších, je RAID 6. Zde je zabírá samoopravný kód dva paritní bloky na každém disku a každý z těchto dvou kódů je vypočítán jiným způsobem. Výhodou je odolnost pole proti náhlému zkratu dvou disků, avšak je nutné sestavit diskové pole minimálně ze čtyř diskových jednotek. [18]



Obrázek č. 6: Příklady RAID polí, zdroj: [18]

Pro naše důvody bude vhodné zvolit RAID1, RAID5, nebo RAID6. V případě souborového nebo databázového serveru je však opravdu důležité, data aktivně zálohovat.

Co se týče softwarové části je zde možnost použití rozličného množství serverových operačních systémů (Microsoft Server, Ubuntu Server, Debian Server a jiné linuxové distribuce) v kombinaci s různými databázovými řešeními (Oracle Database, MySQL, Microsoft SQL Server, PostreSQL). Mezi jedny z nejpoužívanějších řešení se řadí kombinace linuxové distribuce Debian společně s MySQL databází, nebo operační systém Windows Server s databází MSSQL. Jaká distribuce bude použita je však z velké části na zkušenostech a pracovní orientaci administrátora. [15]

Databázové řešení MySQL má nespornou výhodu, že je bezplatným produktem i pro jiné než soukromé účely, což z něho dělá jedno z nejpopulárnějších řešení. Nevýhodou je však podpora a dokumentace, jež nejsou tak obsáhlé jako u proprietárních řešení.

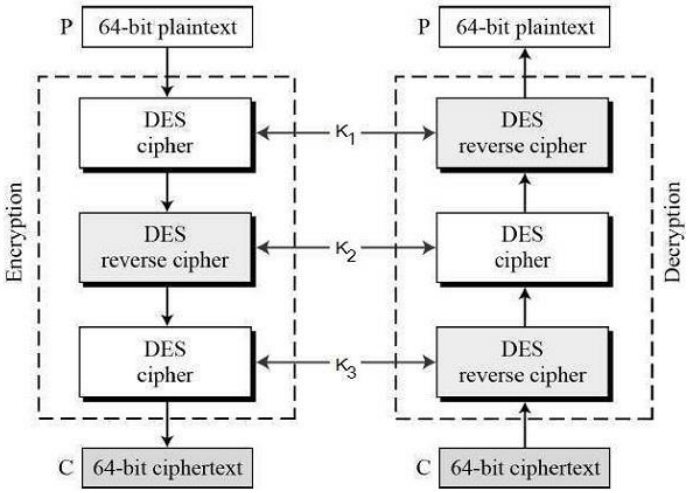
V našem případě jsem však zvolil řešení operačního systému Windows v kombinaci s MSSQL serverem (viz. Kapitola 3.5. Aplikace pro přijetí do domu s pečovatelskou službou) z důvodu lepší kompatibility s budoucí implementací Active Directory na obecním úřadě.

Databázový systém také dokáže zajistit šifrování dat, to jest způsob, jak zamezit neautorizovanému přístupu k datům.

Pro sběr dat pro vlastní agendy obce by bylo v každém případě vhodnější použít program, který by data ukládal do databáze (MSSQL, MySQL), jelikož databáze nabízí velmi široké možnosti práce s daty včetně jejich šifrování.

V MSSQL databázích je vícero druhů šifrování například metody: Encrypt By Key, Transparent Data Encryption, nebo Encrypt By Pass Phrase.

Pro naše účely však bude postačovat MSSQL šifrovací metoda Encrypt By Pass Phrase. Tato metoda používá algoritmus TRIPLE DES. Tento algoritmus generuje tři různé DES klíče 56 bitech, což dá dohromady délku klíče 168 bitů. [16]



Obrázek č. 7: Diagram metody Encrypt By Pass Phrase, zdroj: [16]

Výsledkem je zašifrování příchozích údajů z aplikace do nečitelné podoby. Toto uložení a zašifrování je provedeno v databázové proceduře a pouze po zadání hesla v aplikaci a zavolání inverzní procedury, která má na starosti výpis údajů a jejich rozšifrování je možnost vidět opět data v čitelné podobě. [16]

Všeobecným problémem lokálního serveru v privátní síti je přístup k datům odjinud než z té sítě, ve které je fyzicky nainstalován. V tomto případě je opět vhodné použití našeho databázového serveru v kombinaci s VPN řešením. VPN (Virtual private network) je druh připojení několika zařízení pomocí internetu, kde se dosáhne stavu, že spojené počítače spolu komunikují jako by byly propojeny v rámci jedné sítě. Takto by se velmi ulehčil přístup například k databázovému serveru, protože pomocí VPN by se pracovníci obce mohli k firemní síti připojit i z jiných míst než jen z obecního úřadu. [16]

3.3.2. Informační systémy a úložiště pro veřejné agendy

Pro tento druh agend již obec Dolní Újezd využívá specializovaný software zvaný Munis od společnosti Triada s.r.o, tento sofddsstware je navržen jako modulový systém a je možné jej skládat pro řešení agend, přesně určených pro obec Dolní Újezd.

Obecní úřad využívá tyto agendy:

a) Elektronická podatelna a elektronický podpis

   Elektronická podatelna je modul, který uživateli usnadňuje zajištění všech úkonů, které je organizace povinna provést při přijetí elektronického podání.

b) Elektronická spisová služba Munis ERMS

   Tento modul slouží pro příjem všech typů dokumentů a jejich následné zaevidování a předávání k dalšímu vyřízení vedoucímu pracovníkovi.

c) Evidence čísel popisných

   Modul Evidence čísel popisných slouží k evidenci budov, údajů o parcele, technické údaje, byty a nebytové prostory.

d) Evidence obyvatel

   Tento program umožňuje zpracování celkové kartotéky, ve které se dají sledovat mnohé údaje o občanovi s trvalým bydlištěm v obci.

e) Evidence oznámení (zákon o střetu zájmů)

   Modul Evidence oznámení umožňuje uživatelům provádět činnosti související s vedením registrů podle zákona 159/2006 Sb., o střetu zájmů.

f) Evidence smluv

   Evidence smluv umožňuje evidovat všechny typy smluv s možností vazby na projekty, granty a veřejné zakázky. Obsahuje také hlídání termínů vyplývajících ze smluv

g) Katastr nemovitostí

   Program Katastr nemovitostí slouží k prohlížení a poskytování dat katastrálním úřadem.

h) Legalizace a vidimace

   Program slouží k tisku „ověřovacího razítka“ na štítky, zahrnuje ověřování pravosti podpisů a ověřování shody opisů nebo kopie listin podle zák. č. 21/2006 Sb.

i) Matrika

   Modul řeší všechny náležitosti potřebné k vedení matričních agend na počítači podle zákona 308/200 Sb.

j) Správa adres

k) Program správy adres slouží k údržbě a vytváření struktury adres používaných v ostatních modulech informačního sytému Triada Munis.

l) Správa domů a bytů – WinDomy

   Agenda zajišťuje komplexní systém pro správu domů a různých typů prostor např. nájemní byty, vlastnické byty, nebytové prostory atd.

m) Úřední deska

   Modlu eviduje dokumenty na úřední desce ve spolupráce s modulem eDeska lze dokumenty publikovat i na web.

n) Volební seznamy

   V této agendě je umožněno zpracovávání kartotéky, ve které lze sledovat mnoho údajů o občanovi obce.

Modulový program Triada Munis disponuje ještě mnoha agendy, které si zde však popisovat nebudeme. Program Munis od společnosti Triada je však na GDPR připraven a má implementovaná veškerá potřebná opatření ke správnému výkonu všech agend obce, tudíž není třeba v rámci tohoto zpracovávání implementovat další náležitosti.

3.4. Doporučení ohledně pověřence

Jak již bylo zmíněno v předchozích kapitolách, pověřence si musí zřídit každá obec bez výjimky, dále každá instituce rozhodující o právech a povinnostech (např. školy), nebo jiná velká zdravotnická a sociální zařízení.

Pro obec Dolní Újezd se v tomto okamžiku jedná o zřízení úřadu pověřence pro obecní úřad a školu. V obci Dolní Újezd nefiguruje tolik institucí, aby plně pracovně vytížila jedno pověřence pro ochranu osobních údajů. Z těchto důvodů je dovoleno, mezi obcemi a malými institucemi, externího pověřence pro ochranu osobních údajů sdílet. V Obecném nařízení není záměrně definován hraniční počet institucí, které může pověřenec spravovat. Je to z toho důvodu, že pracovní náročnost u každé instituce může být variabilní. Co se však týká čísel z praxe, obecně se doporučuje maximálně 15–20 institucí pro pověřence. [8]

Pověřencem může být také interní zaměstnanec obce, avšak v tomto případě je vhodnější zvolit pověřence pro ochranu osobních údajů spíše externího, a to z důvodů, že pověřenec má být nezávislá a nestranná osoba, což by se v případě zaměstnance obce mohlo setkat se střetem zájmů. Druhý důvod je práce navíc pro již tak dost vytíženého zaměstnance obce. [8]

Dalším důležitým poznatkem je nestanovená klasifikace pověřence pro ochranu osobních údajů, a to z důvodu rozdílnosti prostředí. V prostředí technologických firem by bylo například rozumnější zvolit pověřence spíše z oborů příbuzných informačním technologiím, zatímco v oddělení justice odborníka spíše právnického vzdělání. Jelikož Obecní úřad v Dolním Újezdě netíhne úplně ani informačnímu, ani právnickému prostředí bylo by vhodné dosadit člověka s dostatečným povědomím z obou odvětví. [17]

Neméně důležitým bodem je také dosažitelnost pověřence, aby v případě nutnosti byl dosažitelný jak pro obec, tak pro Úřad pro ochranu osobních údajů i veřejnost. [17]

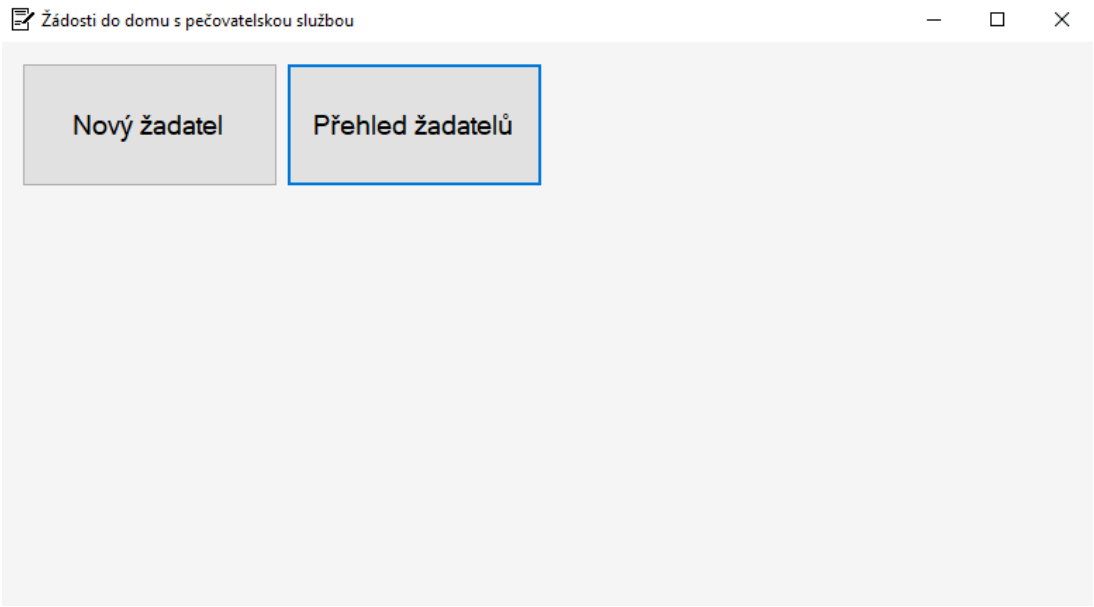
3.5. Aplikace pro přijetí do domu s pečovatelskou službou

Cílem práce bylo také přiblížit, jak je možné tvořit aplikace, které by dokázali nahradit stávající řešení a zároveň dokázali ukládat data na databázový server, šifrovali data a zároveň obsahovala další funkce, typické pro formulářové aplikace. Jako příklad vznikla formulářová aplikace Přijetí do DPS, tato umí zatím základní funkce:

a) Validace dat před nahráváním.
b) Nahrání a šifrování dat do databáze.
c) Dešifrování a výpis dat po ověření uživatele.
d) Vypsat všechna data, pseudonymizovaná data, nebo anonymizovaná data.
e) Exportovat data do .csv souboru.
f) Upravit vybraná data.
g) Smazat vybrané řádky.

Aplikace je naprogramovaná v jazyce c# ve frameworku .NET Framework. Na databázové straně aplikace je použit procedurální dotazovací jazyk T-SQL (Microsoft SQL).

Při spuštění aplikace uvítá uživatele jednoduchý rozcestník. Zde může vybrat možnost Nový žadatel pro uložení nového žadatele do databáze, nebo možnost Přehled uživatelů, pomocí které si může uložené žadatele vypsat a dále s nimi pracovat.



Obrázek č. 8: Rozcestník vytvořené aplikace, zdroj: vlastní zpracování

Programově je tento oddíl řešen pouze tak, že spouští další moduly programu.

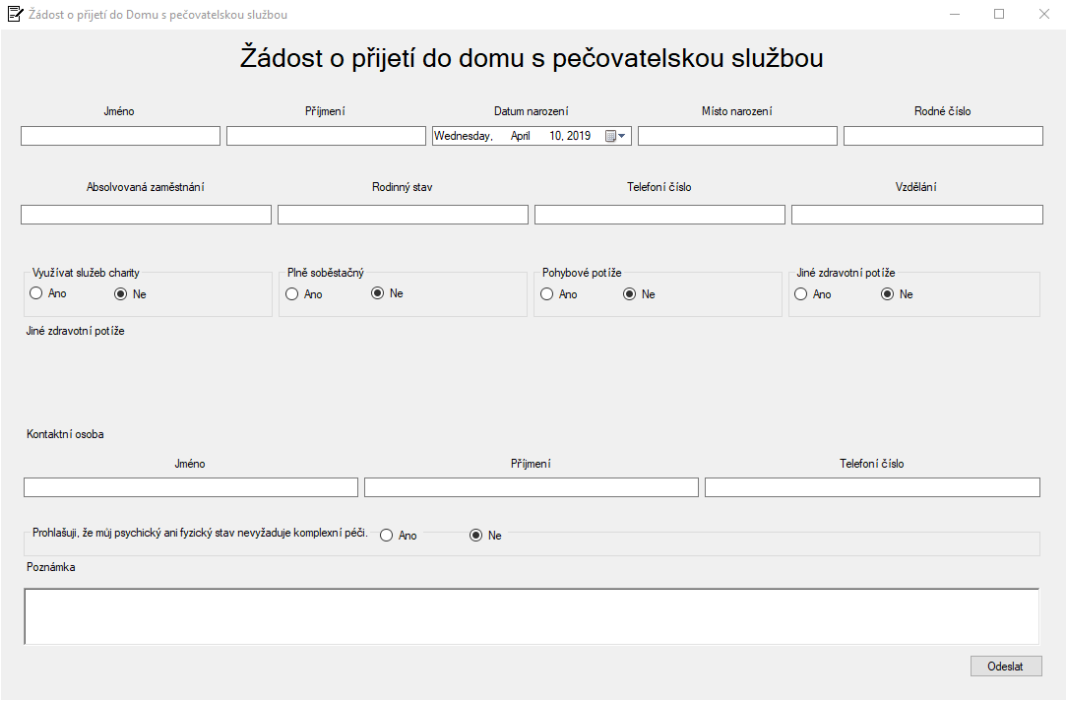
```
namespace PseudonymizaceDat
{
    public partial class Rozcestnik : Form
    {
        public Rozcestnik()
        {
            InitializeComponent();
        }

        // Po kliknutí na tlačítko Nový žadatel otevře formulář Datový formulář
        private void btnDatovyFormular_Click(object sender, EventArgs e)
        {
            Form datovyFormular = new DatovyFormular();
            datovyFormular.Show();
        }

        // Po kliknutí na tlačítko Přehled žadatelů otevře formulář Přehled žadatelů
        private void btnPrehledZadatelu_Click(object sender, EventArgs e)
        {
            Form prehledZadatelu = new PrehledZadatelu();
            prehledZadatelu.Show();
        }
    }
}
```

Obrázek č. 9: Kód rozcestníku ve vlastní aplikace, zdroj: vlastní zpracování

Po kliknutí na tlačítko Nový žadatel se pracovníkovi objeví formulářové okno vybízející k doplnění potřebných údajů o žadateli.



Obrázek č. 10: Formulář pro žadatele do DPS, zdroj: vlastní zpracování

Po zadání všech údajů program vyhodnotí, jestli jsou všechna pole vyplněna, jak by měla a zavolá metody, které předávají parametry procedurám v databázi, pro uložení a zašifrování údajů do tabulek.

```
// Po kliknutí na tlačítko Odeslat se provede kontrola údajů a zavolají se procedury
private void btnOdeslat_Click(object sender, EventArgs e)
{

    string updateZadatelID = "48";
    string updateKontaktniOsobaID = "19";

    // Pokud má tlačítko text "Upravit", vyvolá metodu upravit záznam
    if (btnOdeslat.Text == "Upravit")
    {
        Methods method;
        method = new Methods();

        bool pokracovat = VyplnenaPole();

        if (pokracovat == true)
        {
            Connect newConnection;
            newConnection = new Connect();
            newConnection.Connection();

            int prohlaseni = 0;
            if (rbtProhlaseniAno.Checked)
            {
                prohlaseni = 1;
            }
            else if (rbtProhlaseniNe.Checked)
            {
                prohlaseni = 0;
            }
            int vyuzivatSluzebCharity = 0;
```

Obrázek č. 11: Ukázka kódu pro kontrolu dat, zdroj: vlastní zpracování

```
// Metoda ukládající údaje žadatele do databáze
public int ZadatelINSERT(string datumNarozeni, string jmeno, string mistoNarozeni, string prijmeni, string rodneCislo)
{
    Connect newConnection;
    newConnection = new Connect();
    newConnection.Connection();

    SqlParameter returnParameterData = new SqlParameter();

    SqlCommand zadatelINSERT = new SqlCommand("INSERT_Zadatel", newConnection.Connection());
    zadatelINSERT.Parameters.Add("@datumNarozeni", SqlDbType.VarChar).Value = datumNarozeni;
    zadatelINSERT.Parameters.Add("@jmeno", SqlDbType.VarChar).Value = jmeno;
    zadatelINSERT.Parameters.Add("@mistoNarozeni", SqlDbType.VarChar).Value = mistoNarozeni;
    zadatelINSERT.Parameters.Add("@prijmeni", SqlDbType.VarChar).Value = prijmeni;
    zadatelINSERT.Parameters.Add("@rodneCislo", SqlDbType.VarChar).Value = rodneCislo;
    zadatelINSERT.CommandType = CommandType.StoredProcedure;
    var returnValue = (System.Int32)zadatelINSERT.ExecuteScalar();

    int ZadatelID = returnValue;

    return ZadatelID;

}
```

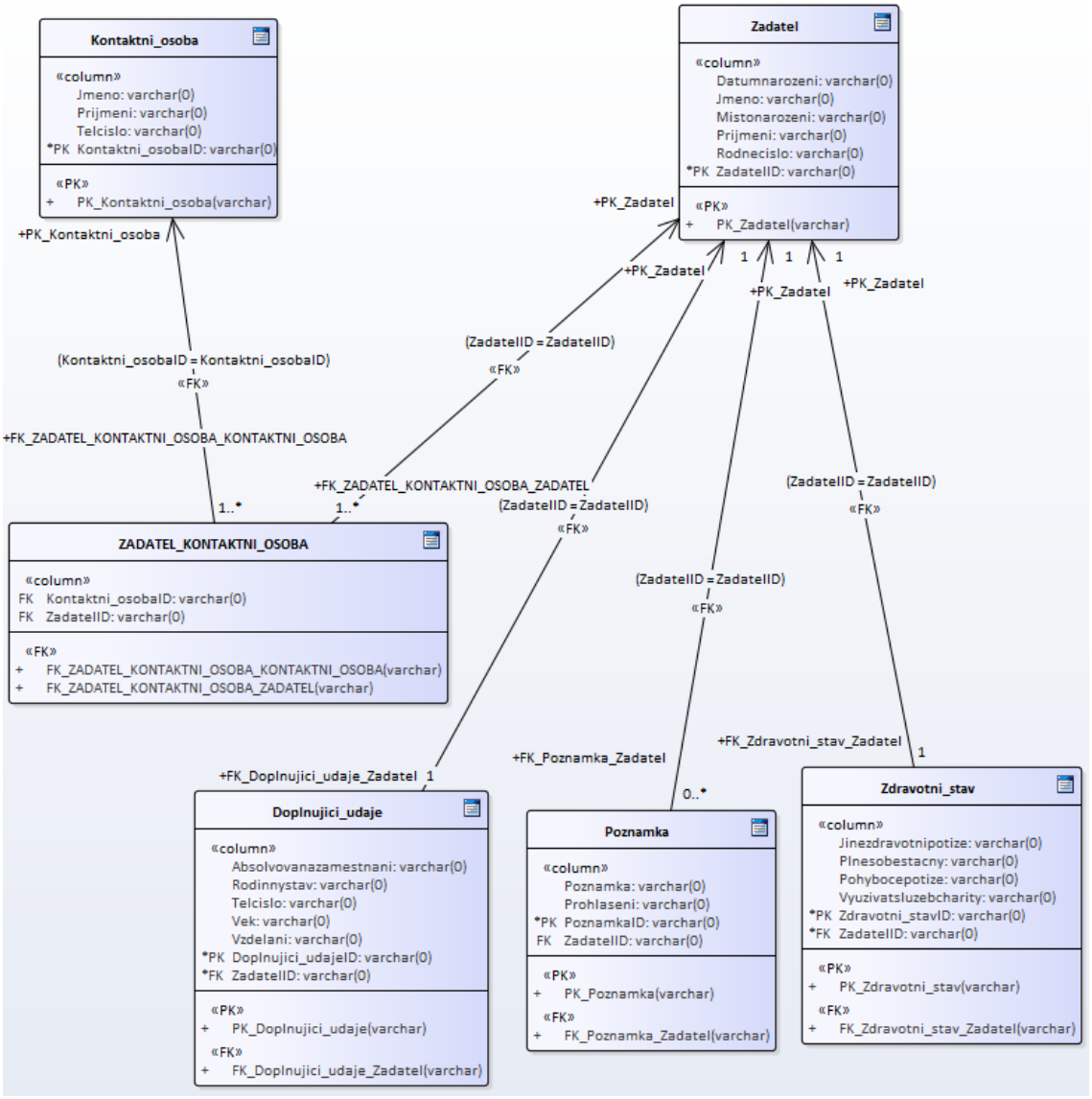
Obrázek č. 12: Předání parametrů SQL proceduře zdroj: vlastní zpracování

```
/****** Object:  StoredProcedure [dbo].[INSERT_Zadatel]    Script Date: 4/10/2019 10:48:17 AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
-- =============================================
-- Author:      <Stanislav Hladík>
-- Create date: <26.1.2019>
-- Description: <INSERT_Zadatel>
-- =============================================
ALTER PROCEDURE [dbo].[INSERT_Zadatel]
    -- Add the parameters for the stored procedure here
    @datumNarozeni VARCHAR(50),
    @jmeno VARCHAR(50),
    @mistoNarozeni VARCHAR(50),
    @prijmeni VARCHAR(50),
    @rodneCislo VARCHAR(50)
AS
BEGIN

    INSERT INTO dbo.Zadatel(DatumNarozeni, Jmeno, MistoNarozeni, Prijmeni, RodneCislo)
    VALUES(ENCRYPTBYPASSPHRASE('tdi202', @datumNarozeni),
           ENCRYPTBYPASSPHRASE('tdi202', @jmeno),
           ENCRYPTBYPASSPHRASE('tdi202', @mistoNarozeni),
           ENCRYPTBYPASSPHRASE('tdi202', @prijmeni),
           ENCRYPTBYPASSPHRASE('tdi202', @rodneCislo))
    SELECT ZadatelID
    FROM dbo.Zadatel
    WHERE ZadatelID=(SELECT max(ZadatelID) FROM dbo.Zadatel)
END
```

Obrázek č. 13: Procedura šifrující a ukládající data, zdroj: vlastní zpracování

Databáze je tvořena z pěti primárních tabulek a z jedné tabulky propojovací. Tabulky Zdravotni_stav, Poznamka, Doplnujici_udaje a ZADATEL_KONTAKTNI_OSOBA jsou propojené pomocí primárních a cizích klíčů s tabulkou Zadatel. Tabulka Kontaktni_osoba je propojena s tabulkou ZADATEL_KONTAKTNI_OSOBA.



Obrázek č. 14: Struktura databáze, zdroj: vlastní zpracování

Po zadání údajů do databáze vypadají identifikovatelné osobní údaje takto:

	DatumNarozeni	Jmeno	MistoNarozeni	Prijmeni	RodneCislo	ZadatelID
1	0x02000000EF9A82...	0x020000000...	0x02000000B93F65...	0x0200000037...	0x020000006EC4...	1050
2	0x0200000002137A...	0x020000000...	0x02000000ACC674...	0x0200000015...	0x020000009228...	1051

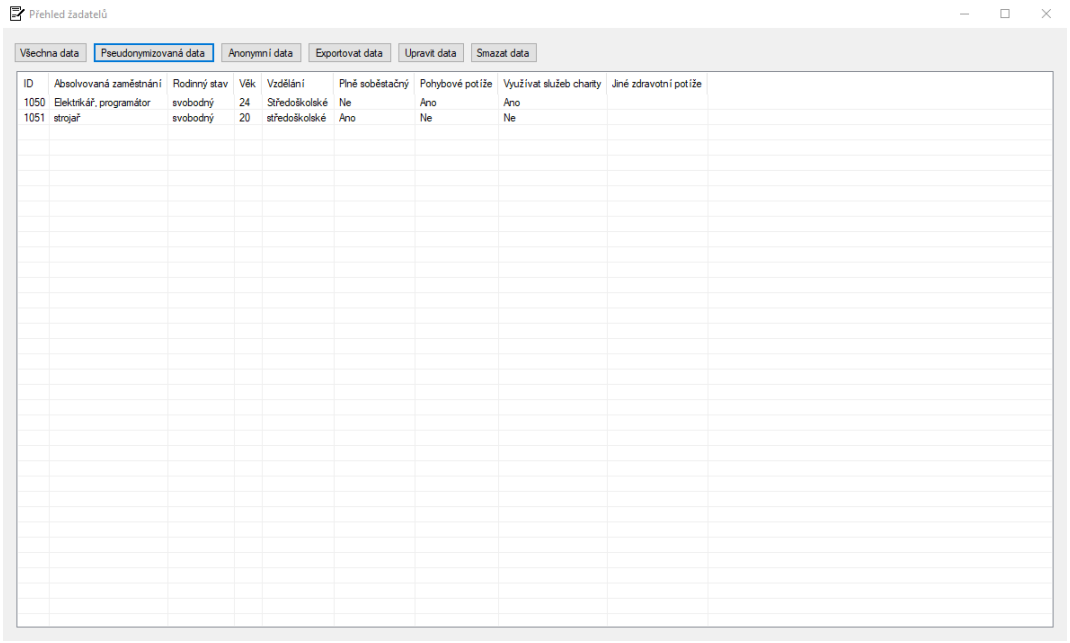
Obrázek č. 15: Uložená šifrovaná data, zdroj: vlastní zpracování

Údaje, které nepřispívají k identifikaci subjektu takto:

	Poznamka	Prohlaseni	PoznamkaID	ZadatelID
1	Žďatel požaduje dvoulůžkový pokoj	1	1025	1050
2		1	1026	1051

Obrázek č. 16: Uložená nešifrovaná data, zdroj: vlastní zpracování

Po stisknutí druhého tlačítka v rozcestníkovém formuláři se pracovník dostane k formuláři, který, po zadání hesla, vypisuje údaje uložené v databázi.



Obrázek č. 17: Formulář výpisu dat, zdroj: vlastní zpracování

Na pozadí opět probíhá kód napsaný v c#, který ze SQL procedury převezme parametry a podle zvoleného výpisu načte data do řádků.

```
// Volání metod pro výpis údajů do listView
string[,] returnValueZadatel = method.ZadatelSELECT(datumNarozeni, jmeno, mistoNarozeni, prijmeni, rodneCislo, zadatelID);
string[,] returnValueDoplnujiciUdaje = method.DoplnujiciUdajeSELECT(zadatelID, doplnujiciUdajeID, vzdelani, vek, telCislo, rodinnyStav, absolvovanaZamestnani);
string[,] returnValueZravotniStav = method.ZdravotniStavSELECT(jineZdravotniPotize, plneSobestacny, pohybovePotize, vyuzivatSluzebCharity, zadatelID, zdravotniStavID);

int radky = returnValueZadatel.GetLength(0);
int sloupce = returnValueZadatel.GetLength(1);
int pomRadky = 0;
int pomSloupce = 0;
int pom = 0;

while (pomRadky < radky)
{
    while (pom != 1)
    {
        ListViewItem lvi = new ListViewItem(returnValueZadatel[pomRadky, pomSloupce]);
        pomSloupce++;
        lvi.SubItems.Add(returnValueZadatel[pomRadky, pomSloupce]);
        pomSloupce++;
        lvi.SubItems.Add(returnValueZadatel[pomRadky, pomSloupce]);
        pomSloupce++;
        lvi.SubItems.Add(returnValueZadatel[pomRadky, pomSloupce]);
        pomSloupce++;
        lvi.SubItems.Add(returnValueZadatel[pomRadky, pomSloupce]);
        pomSloupce++;
        lvi.SubItems.Add(returnValueZadatel[pomRadky, pomSloupce]);

        pomSloupce = 0;
```

Obrázek č. 18: Převzetí dat ze SQL databáze, zdroj: vlastní zpracování

```
/****** Object:  StoredProcedure [dbo].[INSERT_Zadatel]    Script Date: 4/10/2019 12:26:31 PM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
-- =============================================
-- Author:      <Stanislav Hladík>
-- Create date: <26.1.2019>
-- Description: <INSERT_Zadatel>
-- =============================================
ALTER PROCEDURE [dbo].[INSERT_Zadatel]
    -- Add the parameters for the stored procedure here
    @datumNarozeni VARCHAR(50),
    @jmeno VARCHAR(50),
    @mistoNarozeni VARCHAR(50),
    @prijmeni VARCHAR(50),
    @rodneCislo VARCHAR(50)
AS
BEGIN

    INSERT INTO dbo.Zadatel(DatumNarozeni, Jmeno, MistoNarozeni, Prijmeni, RodneCislo)
    VALUES(ENCRYPTBYPASSPHRASE('tdi202', @datumNarozeni),
           ENCRYPTBYPASSPHRASE('tdi202', @jmeno),
           ENCRYPTBYPASSPHRASE('tdi202', @mistoNarozeni),
           ENCRYPTBYPASSPHRASE('tdi202', @prijmeni),
           ENCRYPTBYPASSPHRASE('tdi202', @rodneCislo))
    SELECT ZadatelID
    FROM dbo.Zadatel
    WHERE ZadatelID=(SELECT max(ZadatelID) FROM dbo.Zadatel)
END
```

Obrázek č. 19: Procedura předávající data, zdroj: vlastní zpracování

Data v řádcích lze také smazat a upravit, k čemuž slouží opětovné volání SQL procedur, jenž mají tyto úkony na starost. Poslední funkcionalitou je export dat do .csv souboru, díky čemuž, v případě potřeby, bude možné přehrát data na jinou platformu.

3.6. Interní směrnice ochrany osobních údajů pro obec Dolní Újezd

Interní směrnice znamená vnitřní neveřejný předpis, kterým obec Dolní Újezd upravuje práva a povinnosti svým zaměstnancům a činným osobám v souvislosti s GDPR.

Samotná interní směrnice by měla projít přes kontrolora a schvalovatele po vydavatele této směrnice. Interní směrnice se věnuje obecným povinnostem zaměstnanců, pravidlům pro zpracování a zabezpečení agend, pravidlům pro nakládání s osobními údaji, řešení incidentů, informační povinnosti, přenesení odpovědností a oprávnění, kontrolní a auditní činnost a tomu, jak se chovat v případě rizik.

3.7. Doložky k interní směrnici osobních údajů

Dalším praktickým výstupem práce jsou Doložky k interní směrnici osobních údajů. Doložka o mlčenlivost se použije jako dodatek při vytváření nově zaměstnanecké smlouvy u nových pracovníků, u kterých se předpokládá, že přijdou do kontaktu s osobními údaji.

Doložky Odpověď na žádost subjektu osobních údajů a Odpověď na žádost subjektu osobních údajů jsou formuláře pro vícenásobné použití u daných agend. Poslední doložkou je Doložka o mlčenlivosti třetích stran, ta se použije v každé smlouvě se subjektem třetí strany, aby se předešlo zcizení informací od subjektu třetí strany.

Závěr

Cílem práce Implementace směrnice GDPR v obci Dolní Újezd bylo aplikování této evropské směrnice do prostředí obce s pověřeným obecním úřadem.

V teoretické části práce jsme si nejprve řekli potřebné informace o směrnici pro ochranu osobních údajů, jelikož bez teoretických znalostí nelze aplikovat praktická řešení. V Historii vzniku GDPR jsme se dozvěděli, že ochrana osobních údajů se řeší mnohem déle než poslední tři roky, kdy se o problematice ochrany osobních údajů začalo mluvit i mezi lidmi zajímajícími se o toto téma pouze okrajově. Následovaly rozdíly mezi dosavadní legislativní úpravou ochrany osobních údajů a GDPR a Případné postihy pro ty subjekty, které se nebudou evropskou směrnicí řídit, zde jsme si vypsaly ty nejvíce propírané body případných postihů. Přesto, že výše pokut při nedodržení pravidel může být velmi vysoká, orgány zodpovědné za udělování pokut si mohou vystačit i s pouhou upomínkou.

Druhá část bakalářské práce byla také teoretického rázu. Objevily se zde informace o dopadech GDPR na osobní údaje a o pojmech úzce souvisejících se samotným GDPR. Padly zde zmínky od Práva subjektu údajů až po Právo na vznešení námitky. V dalších bodech této kapitoly se řešilo, co vůbec znamená automatizované zpracování, jelikož o tomto tématu je v GDPR s oblibou často zmiňováno. Součástí druhé části bakalářské práce byly také informace o všech funkcích, které musí, nebo mohou být součástí zpracovávání osobních údajů. Velmi důležitým pojmem je zde Pověřenec pro ochranu osobních údajů, což je jedna z nejdůležitějších funkcí nynější směrnice pro ochranu osobních údajů, dále se zde objevuje, kdo je správcem osobních údajů a kdo zpracovatelem a jak tyto dva pojmy od sebe odlišit a rozeznat. Od správce a zpracovatele jsme se přesunuli k teorii o zabezpečení dat. Dále jsme se dozvěděli, že pojmy anonymizovaná a pseudonymizovaná data jsou pojmy, které nelze jeden za druhý zaměňovat, a že ke kvalitnímu zabezpečení osobních údajů nám velmi pomůže šifrování dat. Dopady na chod obce nám osvětlí, co všechno bude muset obec podniknout pro správnou implementaci GDPR do prostředí obce Dolní Újezd.

V třetí části jsme se dostali k samotnému řešení v obecním prostředí, vstupní analýza dat, kde jsme si rozdělili data do tří skupin podle zpracovávání, byla vstupní analýzou, následovala analýza procesů sběru dat, kde jsme použili use case diagram pro znázornění osob zainteresovaných ve sběru dat a activity diagram pro znázornění obecného pracovního procesu při sběru osobních informací. Třetí analýzou v pořadí byla analýza rizik v procesech, kde byly odhaleny nejožehavější problémy spojené se zpracováním osobních

údajů a zabezpečením při tomto úkonu, zde byla sepsána i doporučení, která pomohla předejít případným rizikovým chováním uvnitř organizace.

Analýza dopadů GDPR na informační systémy byla jednou z obsáhlejších agend a věnovala se informačním systémům pro agendy, které byly zmíněny v datové analýze, zaznělo zde doporučení, jaký databázový systém a řadič disků by měl vyhovovat nárokům na ukládání dat z různých agend.

Praktické výstupy z práce byly vytvořeny tři. Interní směrnice ochrany osobních údajů je nezbytným dokumentem s doporučeními, co mají jednotliví zaměstnanci obecního úřadu za povinnosti a jak by se mělo chovat vůči zacházení s osobními údaji, ke kterým mají ze své pozice přístup. Dále byly vypracovány doložky k interní směrnici, které pomohou doplnit smlouvy o nezbytné náležitosti například Doložka o mlčenlivosti.

Posledním z praktických výstupů je aplikace Žádosti o přijetí do domu s pečovatelskou službou. Tato aplikace slouží k zadání údajů pro pracovníka obce do formulářové aplikace, ze které se data odešlou na databázový server, kde se zašifrují a uloží. Data může vypsat opět pouze pracovník, který zadá potřebné přístupové údaje a může je vypsat v úplné, pseudonymizované, nebo anonymizované formě. Dále aplikace disponuje funkcemi smazat, upravit, nebo exportovat data.

Je zřejmé, že možnosti do budoucna jsou u implementace GDPR do prostředí obce Dolní Újezd (a nejen tam) velmi široké. Například v implementaci protokolu LDAP a adresářových služeb Active Directory, které by velmi usnadnili přístupy všem zaměstnancům obce a zároveň by byly schopné tyto přístupy učinit více transparentní v rámci bezpečnosti. Samotnou aplikaci pro žádosti je samozřejmé do budoucna rozšířit o další moduly například Evidence psů, Evidence poplatků za popelnice aj. I zde se dá uvažovat o propojení aplikace s adresářovými službami Active Directory, což by opět umožnilo jednodušší přístup k funkcím aplikace.

Z výše vypsaných možností je zřejmé, že v závěru této práce se určitě nedá konstatovat, že je práce na implementace směrnice GDPR hotová, spíše se hodí podotknout, že práce teprve začíná.

Použité zdroje

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

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

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

[4] KROUPA, Jiří. *Deklarace práv člověka a občana*. Věda a život, Praha, 1989

[5] *Úplné znění Ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky: Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky; Úplné znění zákona č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny; Některé další související právní předpisy.* Vyd. 5. Praha: Armex, 2009. Edice kapesních zákonů. ISBN 978-80-86795-78-2.

[6] *Evropský parlament Výroby: Občanské svobody, spravedlnost a vnitří věci* [online]. [cit. 2018-11-26]. Dostupné z: http://www.europarl.europa.eu/committees/cs/libe/home.html#

[7] Základní příručka k GDPR: GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 17.04.2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=3938

[8] EVROPSKÁ UNIE. *Nařízení Evropského parlamentu a Rady (EU) 2016/679: o ochraně fyzikých osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES*. In: . Brusel: Úřední věstník Evropské unie, 2016, ročník 2016, 2016/679.

[9] GDPR. *GDPR* [online]. Copyright © 2017 ALL RIGHTS RESERVED [cit. 17.04.2019]. Dostupné z: https://fly-eye.cz/blog-detail-1.html

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

[11] Technical documentation, API, and code examples | Microsoft Docs. [online]. Dostupné z: https://docs.microsoft.com/en-us/

[12] Co je phishing? | Vyhněte se e-mailovým podvodům a útokům | Avast. [online]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

[13] Business Network Security Checklist – Cisco. *Cisco – Global Home Page* [online]. Dostupné z: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/network-security-checklist.html

[14] ŠPATNÉ PŘÍKLADY IMPLEMENTACE GDPR – PDF. *Představujeme Vám pohodlné a bezplatné nástroje pro publikování a sdílení informací.* [online]. Copyright © DocPlayer.cz [cit. 11.04.2019]. Dostupné z: https://docplayer.cz/68343023-Spatne-priklady-implementace-gdpr.html

[15] ENCRYPTBYPASSPHRASE (Transact-SQL) - SQL Server | Microsoft Docs. [online]. Dostupné z: https://docs.microsoft.com/en-us/sql/t-sql/functions/encryptbypassphrase-transact-sql?view=sql-server-2017

[16] Triple DES. *Java NIO, PyTorch, SLF4J, Parallax Scrolling, Java Cryptography, YAML, Python Data Science, Java i18n, GitLab, TestRail, VersionOne, DBUtils, Common CLI, Seaborn, Ansible, LOLCODE, Current Affairs 2018, Apache Commons Collections* [online]. Copyright © Copyright 2019. All Rights Reserved. [cit. 11.04.2019]. Dostupné z: https://www.tutorialspoint.com/cryptography/triple_des.htm

[17] Vnitro v tichosti vydalo manuál pro obce k GDPR: Pověřence musí mít všechny obce! - Česká justice. *Domovská stránka – Česká justice* [online]. Copyright © 2018 Všechna práva vyhrazena [cit. 11.04.2019]. Dostupné z: https://www.ceska-justice.cz/2017/09/vnitro-v-tichosti-vydalo-manual-pro-obce-k-gdpr-poverence-musi-mit-vsechny-obce/

[18] Jaké jsou typy polí RAID a jaké jsou jejich výhody a nevýhody? - Linux E X P R E S. *Linux E X P R E S* [online]. Copyright © 2019 CCB, spol. s r. o., všechna práva vyhrazena. [cit. 17.04.2019]. Dostupné z: https://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky

Seznam příloh

Příloha č. 1: Agendy obsahující osobní údaje zpracovávané pro soukromé osoby

Název agendy	Správce osobních údajů	Zákonnost zpracování *	Účel zpracování **	Osoby pověřené zpracováním ***	Rozsah zpracování ****	Prostředky zpracování *****	Příjemce zpracování ******	Způsob komunikace	Doba uložení agendy *******
Žádosti, obecné žádosti, žádost o výpis z rejstříku	Obec	c) e)	Zákon č. 114/1992 Sb., o ochraně přírody a krajiny (dřeviny); zákon Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník	Starosta	jméno, příjmení, adresa, dat. nar.	MS Word, Excel Czech Point	Žadatel	Osobní	Než pomine účel zpracovávání
Stížnosti a petice	Obec	c) e)	Zákon č. 500/2004 Sb., správní řád a zákon č. 85/1990 Sb., o právu petičním	Starosta	jméno, příjmení, adresa, datum narození	MS Word, Excel	Stěžovatel	Osobní	Než pomine účel zpracovávání
Povolení	Obec	c) e)	Zákon č. 114/1992 Sb., o ochraně přírody a krajiny (dřeviny) a zákon č. 13/1997 Sb., o pozemních komunikacích, zákon č. 183/2006 Sb., stavební zákon, zákon č. 500/2004 Sb. správní řád	Starosta	jméno, příjmení, adresa, datum narození	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovávání
Dary a dotace	Obec	c) e)	Zákon č. 89/2012 Sb., občanský zákoník (dary), zákon č. 250/2000 Sb., o územních rozpočtech podmínky poskytnutí dotací	Starosta	jméno, příjmení, adresa, datum narození	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovávání
Včelaři	Obec	c) e)	Zákon č. 326/2004 Sb., o rostlinolékařské péči a související Vyhláška č. 327/2012 Sb. o ochraně včel, zvěře, vodních organismů a dalších necílových organismů při použití přípravků na ochranu rostlin	Starosta	jméno, příjmení, adresa, datum narození	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovávání
Evidence psů	Obec	c) e)	Zákon č. 565/1990 Sb., o místních poplatcích	účetní	jméno, příjmení, adresa, datum narození	SW DataIT MS Word, Excel	Obec, majitel psa	Osobní	Než pomine účel zpracovávání
Žáci do 1. třídy	Obec	c)	Zákon č. 561/2004 Sb., školský zákon	Ředitelka ZŠ, účetní	jméno, příjmení, adresa, rodné číslo	MS Word, Excel	ZŠ	Osobní	Než pomine účel zpracovává

									ní nezbytně nutnou
Děti do školky	Obec	c)	Zákon č. 561/2004 Sb., školský zákon	Ředitelka ZŠ, účetní	jméno, příjmení, adresa, rodné číslo	MS Word, Excel	ZŠ	Osobní	Než pomine účel zpracovává ní
Vítání občánků	Obec	e)	oprávnění získat OsÚ dle § 36a ve spojení s § 149a zákona č. 128/2000 Sb., o obcích	Zastupitelé	jméno, příjmení, adresa, datum narození	MS Word, Excel, obrázky	zastupitel	Osobní	Než pomine účel zpracovává ní
Vedení kroniky	Obec	c) e) a)	Zákon č. 132/2006 Sb., o kronikách obcí	Kronikář	jméno, příjmení, adresa, datum narození	MS Word, Excel, obrázky	Veřejnost (nahlédnout ve vymezené době na OÚ)	Osobní	Než pomine účel zpracovává ní
Kódy k EZS	Obec	e)	Organizačně technické opatření	Zaměstnanec obce	kód, jméno, příjmení	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovává ní
Evidence klíčů	Obec	c)	Organizačně technické opatření	Zaměstnanec obce	kód klíče, jméno, příjmení	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovává ní
Evidence razítek	Obec	c)	Zákon č. 499/2004 Sb., o archivnictví a spisové službě	starosta	číslo razítko, jméno, příjmení	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovává ní
Zápůjčky	Obec	f)	Zákon č. 89/2012 Sb., občanský zákoník, zákon č. 128/2000 Sb., o obcích	starosta	jméno, příjmení, adresa	MS Word, Excel	Vypůjčitel	Osobní	Než pomine účel zpracovává ní
Zápisy (nahrávky) z jednání zastupitelstv a	Obec	c) e)	Zákon č. 128/2000 Sb., o obcích	Zaměstnanec obce	jméno, příjmení, adresa	Zápisník, nebo Word, Excel	Žadatel	Osobní	Než pomine účel zpracovává ní
Zápisy z jednání výborů/komi sí	Obec	c) e)	Zákon č. 128/2000 Sb., o obcích	Zaměstnanec obce	jméno, příjmení, adresa	Zápisník, nebo Word, Excel	Žadatel	Osobní	Než pomine účel zpracovává

									ní nezbytně nutnou
Kamerový systém MP	Obec	c)	Oprávnění dle § 24b zákon č. 553/1991 o obecní policii	Zaměstnanec obce	obrazový záznam	Nezveřejňují se	Žadatel	Osobní	Než pomine účel zpracovávání
Czech Point	obec	c) e)	Zákon č. 356/2000 Sb., o informačních systémech veřejné správy	starosta	jméno, příjmení, adresa, dat. nar..	Czech Point	Žadatel	Osobní	Než pomine účel zpracovávání
Vodné stočné	obec	c) e)	Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník	účetní	jméno, příjmení, adresa, IČO, DIČ, dat. nar., e-mail, tel.	SW DataIT MS Word, Excel	Poplatník	Osobní	Než pomine účel zpracovávání
Pohřebnictví	obec	c) e)	Zákon č. 256/2001 Sb., o pohřebnictví	účetní	jméno, příjmení, adresa, datum nar..	SW DataIT MS Word, Excel	Poplatník	Osobní	Než pomine účel zpracovávání
Evidence osob navštěvujících knihovnu	obec	c) f)	zákon č. 257/2001 Sb., Knihovní zákon	knihovník	jméno, příjmení, adresa, datum narození	MS Word, Excel	Vypůjčitel	Osobní	Než pomine účel zpracovávání
Evidence čísel popisných	obec	c) e)	Zákon č. 128/2000 Sb., o obcích (obecní zřízení)	Starosta, účetní	jméno, příjmení, adresa, dat. nar.	SW DataIT MS Word, Excel	Obyvatel	Osobní	Než pomine účel zpracovávání
Poskytnutí plné moci	obec	c) e)	zákon č. 89/2012 občanský zákoník,	Starosta, účetní	jméno, příjmení, adresa, dat. nar.	SW DataIT MS Word, Excel	Zmocněnec, zmocnitel	Osobní	Než pomine účel zpracovávání
Úřední deska	obec	c) e)	Zákon č. 128/2000 Sb., o obcích (obecní zřízení)	Starosta, účetní	jméno, příjmení, adresa, datum narození	MS Word, Excel	Občané, zmocnitel	Osobní	Než pomine účel zpracovávání
Odpadové hospodářství	obec	b) c)	Zákon č. 565/1990 Sb., o místních poplatcích, resp. zákon č. 185/2001 Sb., o odpadech	Účetní, Zaměstnanec obce	jméno, příjmení, adresa, datum narození tel. email	SW DataIT MS Word, Excel	Smluvní strana	Osobní	Než pomine účel zpracovávání

Majetkové přiznání veřejných funkcionářů	obec	e)	zákon č. 159/2006 Sb. o střetu zájmů,	Starosta	jméno, příjmení, adresa, datum narození.	MS Word	Funkcionář	Osobní	Než pomine účel zpracovávání
Ztráty a nálezy	obec	c) e)	zákon č. 89/2012 Sb., občanský zákoník,	Starosta	jméno, příjmení, adresa, datum	MS Word, Excel	Nálezce	Osobní	Po dobu zákonem vedenou jako nezbytně nutnou
Pečovatelská služba (rozvoz obědů)	obec	e)		Účetní, Zaměstnanec obce	jméno, příjmení, adresa, datum	SW DataIT MS Word, Excel	Odběratel	Osobní	Než pomine účel zpracovávání
Legalizace a vidimace	obec	c)	zákon č. 21/2006 Sb., o ověřování (…)	zaměstnanec obce	jméno, příjmení, dat. nar., adresa, průkaz totožnosti	MS Word, Excel	Žadatel	Osobní	Než pomine účel zpracovávání
Zvláštní příjemci důchodu	Obec	b)		Zaměstnanec obce	jméno, příjmení, adresa, datum	MS Word, Excel	Příjemce	Osobní	Než pomine účel zpracovávání
Matriky	obec	c)	zákon č. 301/2000 Sb., o matrikách	Zaměstnanec obce	jméno, příjmení, adresa, datum	Papírové záznamy, specializovaný software	Žadatel	Osobní	Než pomine účel zpracovávání
Seznamy voličů	obec	c)	Zákony o volbách (všechny)	Zaměstnanec obce	jméno, příjmení dat. nar., adresa	MS Word, Excel	občan obce	Osobní	Než pomine účel zpracovávání

Příloha č. 2: Agendy obsahující osobní údaje zpracovávané pro potřeby obce

Název agendy	**Správce osobních údajů**	**Zákonnost zpracování ***	**Účel zpracování ****	**Osoby pověřené zpracováním *****	**Rozsah zpracování ********	**Prostředky zpracování *********	**Příjemce zpracování **********	**Způsob předání**	**Doba uložení agendy ***********
Evidence obyvatel	Obec	c) e)	Zákon č. 133/2000 o evidence obyvatel	Starosta, účetní	Jméno, příjmení, adresa, r. č., místo narození	Triada	Obec	Datová schránka, email	Než pomine účel zpracovávání
Evidence hasičů	Obec	c) e)	Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník,	Starosta	Jméno, příjmení, adresa, dat. nar.	MS Word, Excel	Obec	Datová schránka, email	Než pomine účel zpracovávání
Podpisové certifikáty	Obec	f)	Evidence držitelů elektronického podpisu	Starosta, účetní	jméno, příjmení, adresa, r. č	Certifikační automaty	Obec	Datová schránka, email	Než pomine účel zpracovávání
Evidence psů	Obec	c) e)	Zákon č. 565/1990 Sb., o místních poplatcích	Účetní	jméno, příjmení, adresa, datum narození	MS Word, Excel	Obec, majitel psa	Datová schránka, email	Než pomine účel zpracovávání
Stížnosti a petice	Obec	c) e)	Zákon č. 500/2004 Sb., správní řád a zákon č. 85/1990 Sb., o právu petičním	Starosta	jméno, příjmení, adresa, datum narození	MS Word, Excel	Obec, stěžovatel	Datová schránka, email	Než pomine účel zpracovávání

Příloha č. 3: Agendy obsahující osobní údaje zpracovávané pro veřejné agendy

Název agendy	**Správce osobních údajů**	**Zákonnost zpracování ***	**Účel zpracování ****	**Osoby pověřené zpracováním *****	**Rozsah zpracování ********	**Prostředky zpracování *********	**Příjemce zpracování **********	**Způsob předání**	**Doba uložení agendy ***********
Daňové doklady, Faktury, účetnictví	obec	c)	Všechny podle zákona č 563/1991 Sb., o účetnictví	Účetní	Jméno, příjmení, adresa, dat. nar., e-mail, tel.	SW DataIT MS Word, Excel	FU	mail	Než pomine účel zpracovávání
Personální a mzdová agenda	obec	c)	Všechny podle zákona č 563/1991 Sb., o účetnictví, zákona č. 312/2002 Sb., o úřednících ÚSC, nařízení vlády č. 318/2017 Sb., o odměnách ZO	Účetní, starosta	Jméno, příjmení, adresa, dat. nar., r. č., e-mail, tel. včetně dětí.	SW DataIT MS Word, Excel	OSSZ, FU, pojišťovna	Datová schránka	Než pomine účel zpracovávání
Smlouvy	obec	b) c)	Zákon č. 128/2000 o obcích (obecní zřízení); zákon č. 89/2012 občanský zákoník	Účetní, starosta	Jméno, příjmení, adresa, dat. nar. tel. email	SW DataIT MS Word, Excel	Registr smluv, smluvní strana	Osobní	Než pomine účel zpracovávání
Vedení kroniky	Obec	c) e) a)	Zákon č. 132/2006 Sb., o kronikách obcí	Kronikář	Jméno, příjmení, adresa, datum narození	MS Word, Excel, obrázky	Veřejnost (nahlédnout ve vymezené době na OÚ)	Osobní	Než pomine účel zpracovávání
Veřejné opatrovnictví	Obec	c)	Zákon č. 89/2012 Sb., občanský zákoník, zákon č. 128/2000 Sb.,	Starosta	Jméno, příjmení, adresa, dat. nar.	MS Word, Excel, Spisová služba Triada	CSSZ, soudy, opatrovaný	Osobní	Než pomine účel zpracovávání
Audiovizuální záznamy z akcí	obec	e) f)		Pracovník obce	Záznamy osob	Specializovaný software	veřejnost	Osobní	Než pomine účel zpracovávání

Příloha č. 4: Vysvětlivky k agendám

Vysvětlivky k agendám:

*Možnosti zákonnosti zpracování GDPR

a) Se zpracováním svých osobních údajů udělil subjekt údajů souhlas pro jeden či více konkrétních účelů (platný souhlas uděluje osoba starší 16 let).
b) Zpracování je nezbytné pro splnění smlouvy, 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.

Zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu OSÚ.

**Popis, o jakou agendu se jedná a za jakým účelem je zpracovávána.

***Pověřené osoby (zaměstnanci, třetí strany), které jsou pověřené osobní údaje zpracovat.

****Údaje, které jsou nutné zpracovávat pro dosažení účelu, např. jméno, rodné číslo, datum narození aj.

*****Prostředky (SW), které jsou potřebné pro zpracování agend.

******Organizace, kterým jsou osobní údaje z agend předávány

*******Minimální doba uložen

Interní směrnice pro ochranu osobních údajů

Obec Dolní Újezd

Činnost	Jméno a příjmení	Funkce	Datum	Podpis
Vypracoval:				
Kontroloval:				
Schválil:				
Vydal:				

Historie změn

Verze	Datum	Schválil	Popis změny

Obsah

1. Úvodní ustanovení

1.1. Účel dokumentu

a) Směrnice o ochraně osobních údajů upravuje postup zaměstnanců při nakládání s osobními údaji a při stanovení účelu, prostředků a způsobu zpracování těchto údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů a Nařízení EU 2016/679 General Data Protection Regulation (GDPR) ze dne 27. dubna 2016.

b) Obec je správcem a zpracovatelem osobních údajů a určuje účel, prostředky a odpovědnost za zpracování osobních údajů, provádí jejich zpracování a odpovídá za ně. Další Správci, pro které Obec zpracovává osobní údaje, jsou uvedeni v Registru agend.

c) K zajištění ochrany osobních údajů je přijat soubor technicko – organizačních opatření, která jsou obsažena v této směrnici a dalších organizačně řídících dokumentech, na něž se tento dokument odkazuje.

1.2. Základní pojmy

Pojmy v této směrnici jsou vykládány v souladu s jejich významem uvedeným v tomto článku a v souladu se zákonem

a) **Obec** – pro tyto účely tohoto dokumentu se obcí rozumí obec Dolní Újezd

b) **Osobním údajem** – veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, např. na jméno, identifikační číslo.

c) **Účel zpracování –** důvody kvůli nimž jsou osobní údaje zpracovávány.

d) **Zvláštní kategorie osobních údajů („citlivé údaje“)**, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, je povoleno v čl. 9 Nařízení EU 2016/679, který uvádí výjimky kdy je možné tyto údaje zpracovávat.

e) **Subjektem údajů** je fyzická osoba, k níž se osobní údaje vztahují

f) **Správce osobních údajů** určuje účely a prostředky zpracování

g) **Zpracovatel** je právnická nebo fyzická osoba pověřená Správcem. Zpracovatel zpracovává osobní údaje podle pokynů správce a je správci odpovědný.

h) **Zpracování osobních údajů** je jakákoliv operace nebo soubor operací s osobními údaji, který je prováděn automatizovanými postupy, nebo bez nich například: shromažďování, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, přenos, šíření nebo jakékoliv jiné operace týkající se přístupu k datům.

i) **Profilování** je jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k dané osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situaci, zdravotnímu stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu.

j) **Porušení zabezpečení** je činnost, která vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

k) **Agenda** je souhrn informací sdružených podle společného účelu do jednoho administrativního celku

l) **Pověřenec pro ochranu osobních údajů** je pozice v rámci organizace, v níž působí zaměstnanec nebo externí pracovník jako ochránce osobních údajů zaměstnanců, občanů, klientů, zákazníků, dodavatelů, a dalších fyzických osob, jejichž údaje Správce osobních údajů zpracovává.

m) **Úřad pro ochranu osobních údajů (ÚOOÚ)** – dozorový úřad

n) **General Data Protection Regulation (GDPR)** je nařízení Evropské Unie č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů

o) **Systematičnost zpracování OÚ** je takové zpracování, které naplňuje jednu či více z následujících podmínek

    1) Dochází k němu na základě určitého systému
    2) Je dopředu připravené, organizované nebo metodické
    3) Dochází k němu na základě obecného plánu pro shromažďování osobních údajů nebo je prováděno na základě určité strategie.

2. Agendy, které obsahují osobní údaje a jejich atributy

a) Starosta je pověřený vést v aktuální podobě Registr agend obsahující údaje a určuje, v souladu s touto směrnicí, které údaje/atributy (odpovědnosti, oprávnění, účel, zákonnost, rozsah a způsob zpracování) jsou pro každou agendu v registru vedeny. Registr je k nahlédnutí pro zaměstnance na úřadu obce.
b) Rozsah zpracování agenda nesmí přesáhnout rámec stanovený registrem agend

3. Obecné povinnosti zaměstnanců

Tato kapitola se týká všech zaměstnanců včetně starosty obce a také pověřence pro ochranu osobních údajů. Každý zaměstnanec má povinnost:

a) Zachovat mlčenlivost o všech osobních údajích a opatřeních přijatých obcí k ochraně osobních údajů, s nimiž se v průběhu práce setkal, pokud není smluvní nebo zákonná povinnost tyto osobní údaje poskytnout třetím stranám. Podmínky interního přesunu informací jsou dány touto směrnicí.
b) Zpracovávat osobní údaje se smí pouze ke stanovenému účelu, v rozsahu předepsaném v registru agend.
c) Nakládat s osobními údaji, k nimž má přístup, takovým způsobem, aby nedošlo k neoprávněnému nebo náhodnému přístupu jiných osob. Dále aby nedošlo k jejich zneužití, ztrátě, neoprávněnému zpracování, nebo k jinému nezákonnému účelu, než k jakému je určen výkonem své pracovní činnosti.
d) Být maximálně součinný zaměstnavateli, správci a pověřenci.
e) Nepořizovat žádné audiovizuální záznamy fyzických osob. Pokud si situace žádá takovou činnost, kontaktovat Pověřence, aby určil soulad s pravidly GDPR.
f) Zaměstnanec, který provádí nové zpracování osobních údajů oznámí tuto skutečnost Pověřenci pro ochranu osobních údajů před začátkem zpracovávání. Pověřenec následně posoudí, zda se jedná o oprávněné zpracování, dobu uchování a informování subjektu údajů.

g) Dát pozor na korektnost zpracovávání. Jestliže je zjištěna nesprávnost při zpracovávání např. překlep, údaj může opravit. Jestliže je zjištěna nesrovnalost (změna údajů) kontaktuje pověřence a ten zajistí nápravu.
h) Znemožnit nepovolaným osobám přístup k jakýmkoliv informacím (nahlédnutí, pořízení fotografie)
i) V době nepřítomnosti na pracovišti musí být všechny citlivé údaje uloženy v uzamykatelných skříních. Každý zaměstnanec by měl dále dbát na co nejmenší počet věcí na jeho stole, což přispěje prevenci před náhodným zapomenutím citlivých dokumentů na pracovním stole.
j) Veškeré ruční poznámky a vytisknuté dokumenty po jejich použití bezpečně skartovat.

3.1. Povinnosti a odpovědnosti starosty obce

a) Schvaluje interní předpisy GDPR a registry agend v aktuální podobě
b) Zajišťuje provádění externích a interních auditů
c) Dodržuje kontrolu nad zpracováváním údajů k jasně definovanému účelu
d) Zajišťuje korektnost a aktuálnost zpracovávaných osobních údajů
e) Dodržuje skartační dobu, tj. doba nezbytně nutná ke zpracování osobních údajů
f) Zajišťuje seznámení a dodržování interních norem zaměstnanci obce
g) Zajišťuje, aby byly dodrženy smluvní požadavky při uzavírání smluvních vztahů s osobami třetích stran.
h) Kontroluje dodržování technických opatření.
i) Navrhuje Pověřence pro ochranu osobních údajů.

3.2. Povinnosti a odpovědnosti pověřence pro ochranu osobních údajů

a) Má odpovědnost za oblast ochrany osobních údajů v obci.
b) Zodpovídá za správné vedení a aktualizování dokumentace v souladu s GDPR, aktualizaci této dokumentace nejméně jednou za rok. Aktualizované dokumenty je povinen předkládat starostovi obce.
c) Nese odpovědnost za styk s úřadem pro ochranu osobních údajů
d) Musí být informován o každém bezpečnostním incidentu a podílí se na jeho řešení.
e) Upozorňuje na skutečnost, které by mohly vést k potenciálním hrozbám pro řádné zabezpečení osobních údajů.

f) Vede evidenci udělených souhlasů se zpracováním osobních údajů a vyřizuje žádosti subjektu údajů v řešení jejich nároků a práv.

g) Vede záznamy o činnostech zpracování v obci.

3.3. Povinnosti zaměstnance při práci s výpočetní technikou

a) Při opuštění pracoviště je zaměstnanec povinen uzamknout počítač a při opětovném návratu k počítači se přihlašovat pomocí hesla.

b) Nesdělovat svá hesla a heslo změnit, pokud zaměstnanec nabyde podezření o prozrazení.

c) Heslo by mělo obsahovat min. 8 znaků v kombinaci písmen, velkých písmen číslic a speciálních znaků.

d) Zaměstnanec nesmí pracovat pod cizím účtem.

e) Instalovat software bez souhlasu správce počítačů.

f) Spouštět podezřelé odkazy a přílohy z cizích e-mailových adres.

4. Pravidla pro zpracování a zabezpečení agend s osobními údaji

a) Starosta obce stanovuje v Registru agend minimální a maximální dobu ukládání agend v souladu se skartačním řádem, závaznými předpisy a účelem zpracování agendy.

b) Likvidace osobních údajů je fyzické zničení nosiče, na kterém jsou údaje uloženy, popřípadě jejich nenávratné smazání z úložiště.

c) Zálohování dat probíhá podle termínů schválených starostou obce.

d) Přístupová práva uděluje administrátor IT infrastruktury podle Plánu přístupových práv a po konzultaci se starostou.

e) Starosta je oprávněn jednorázově rozhodovat o přidělení výjimečných práv, ty však musejí být pouze na omezenou dobu.

f) Součástí smluv se zaměstnanci musí být doložka o mlčenlivosti.

4.1. Zabezpečení prostor

a) Při opuštění pracovník prostor je zaměstnanec povinen uzamknout dveře a zavřít okna

b) Neoprávněná osoba nesmí být zanechána v prostoru OÚ bez dozoru.

c) Při ztrátě klíčů k zaměstnání tuto událost okamžitě nahlásit.

d) Je zakázáno pořizovat si duplikáty klíčů.

4.2. Pravidla pro ukládání osobních údajů v elektronické podobě

a) Soubory s osobními údaji se ukládají výlučně na síťových úložištích pro ukládání dokumentů určených.
b) Na pracovních počítačích smí být data uložena pouze po dobu práce na dokumentu.

5. Zvláštní pravidla pro práci s osobními údaji

a) Všichni zaměstnanci s přístupem do spisové služby mají přístup ke všem kontaktním údajům, z důvodu registrace.

5.1. Souhlas se zpracováním osobních údajů

a) Souhlas se zpracováním osobních údajů musí být zřetelně odlišitelný od jiných záznamů a musí obsahovat informace o tom, kdo souhlas uděluje, účel zpracování, ke zpracování, jakých údajů je souhlas dáván, na jaké období a jakému správci.
b) Poskytnutí souhlasu musí být obec schopná doložit po celou dobu působení souhlasu.
c) Obec musí přiměřeným způsobem ověřit, kdo souhlas se zpracováním údajů uděluje.
d) Pokud subjekt souhlas odvolá, zpracovávání musí být okamžitě ukončeno.
e) Odvolání souhlasu musí být pro subjekt stejně snadné jako jeho udělení.

5.2. Pořizování audiovizuálních záznamů

a) Zveřejňování materiálů z obecních akcí je možné bez souhlasu subjektů údajů jestliže:
    1) Je primárním cílem akce poskytování informací veřejnosti o chodu obce a jejích aktivitách, prezentace dosažených úspěchů, informace o proběhlých či plánovaných akcích.
    2) Zaznamenávaným osobám nejsou přiřazovány další osobní údaje a na základě toho nejsou vytvářeny další evidence.
    3) Nejedná se o znevažující záznamy, které mají za cíl zesměšňovat, dehonestovat osoby
    4) Nemá jiný účel nežli informační

5) Osoby shromážděné v místě akce o pořizování záznamů předem vědí, nebo mohou vědět, aby se mohli rozhodnout nebýt jeho součástí.
6) Není využíváno pro marketingové účely a slouží výhradně k dokumentaci a informování o akci.
7) Zveřejňuje se pouze na vlastní informační média (vlastní web, Facebook)

b) Souhlasu podléhá pořizování audiovizuálních záznamů za těchto předpokladů:
1) Jsou pořizovány za účelem marketingové propagace.
2) Pořizují se za účelem zpeněžení.
3) Fotografie jsou doplněny dalšími údaji.

c) Na žádost dotčené osoby musí být fotografie neprodleně odstraněna

5.3. Záznamy a zápisy z jednání obecních orgánů

a) Průběh jednání zastupitelstva obce je zaznamenáván, z jednání je pořizován zápis a záznam, které jsou uloženy u starosty obce.

b) Pouze občan obce, která dosáhl 18 let věku a fyzická osoba, která dosáhla věku 18 let a vlastní na území obce nemovitost má právo nahlížet do úplného znění usnesení a zápisů z jednání zastupitelstva a do úplného znění usnesení rady, výborů zastupitelstva a komisí rady.

c) Ostatní osoby mají právo na informace dle zákona o svobodném přístupu k informacím.

d) Při zveřejňování informací z jednání a usnesení orgánů obce v médiích, na internetu a v tisku, jsou osobní údaje fyzických osob anonymizovány s výjimkou souhlasu se zveřejněním.

5.4. Ochrana osobních údajů členů volených orgánů a zaměstnanců obce

a) Osobní údaje o veřejné činné osobě, funkcionáři či zaměstnanci obce vypovídající o jeho veřejné nebo úřední činnosti a o jeho funkčním nebo pracovním zařazení mohou být poskytnuty i bez jeho souhlasu.

b) Ostatní údaje veřejně činných osob, funkcionářů a zaměstnanců mohou být poskytnuty nebo zveřejněny pouze s jejich předchozím písemným souhlasem.

c) Veřejně činná osoba je zde člen zastupitelstva, člen výboru zastupitelstva a člen komise rady.

5.5. Nakládání s osobními údaji v souvislosti vítání občánků a setkání jubilantů

a) Obec v rámci své působnosti realizuje „Vítání občánků“.
b) Při této akci jsou v souladu se zákonem použity osobní údaje: jméno, příjmení, datum narození dítěte a jméno, příjmení a adresa rodičů.
c) Osobní údaje uvedené v předchozím odstavci jsou poté použity při předání darů rodičům při obřadu.
d) Obec v rámci své působnosti realizuje společenskou událost „setkání jubilantů“.
e) Pro účel realizace akce „setkání jubilantů“ jsou, v souladu se zákonem, použity osobní údaje v rozsahu jméno, příjmení, datum narození a trvalý pobyt jubilantů.
f) Osobní údaje uvedené v předchozím odstavci jsou poté použity při předání darů jubilantům při obřadu.

5.6. Nakládání s osobními údaji pro udílení čestného občanství a pamětních listů obce

a) Obec v rámci své samostatné působnosti má právo udělit fyzickým osobám, které se významnou měrou podíleli na rozvoji obce, čestné občanství.
b) Obec v rámci své samostatné působnosti má právo udělovat pamětní listy
c) Pro účely udílení čestných občanství a pamětních listů jsou využívány tyto osobní údaje: jméno, příjmení, datum narození, trvalý pobyt kandidátů.
d) Osobní údaje vypsané v odstavci c) jsou použity pro evidenci čestných občanů obce a pro evidenci osob, kterým byl udělen pamětní list obce.

5.7. Vedení kroniky obce

a) Do obecní kroniky se zaznamenávají informace a zprávy o důležitých událostech v obci. V kronice jsou obsaženy písemné, obrazové i zvukové záznamy (elektronická kronika). Tyto záznamy obsahují, v nutném rozsahu, údaje o osobách, které se zúčastňovali těchto událostí, nebo se jich týkaly. Do kroniky má možnost nahlédnout každý občan obce ve vymezené době na obecním úřadě.
b) Do kroniky může být, po posouzení obcí, zahrnuta i událost týkající se soukromého života určitě osoby, například sňatek osoby, narození dítěte nebo významné životní jubileum. Pokud je to relevantní, lze v některých případech uvést i bydliště nebo datum

narození těchto osob. Zápis v kronice však nesmí představovat nepřiměřený zásah do životů dotčených osob.

c) Pro zařazení soupisu místních občanů a jejich jména, příjmení, adresy bydliště, datum narození nebo rok úmrtí, popřípadě dalších osobních údajů (jubilea, soupis osob, které se přistěhovali nebo odstěhovaly, soupis nově narozených dětí v daném roce) je třeba získat souhlas těchto subjektů údajů.
d) Při zpracování oprávněně zveřejněných osobních údajů v souladu se zvláštním právním předpisem, prováděných bez souhlasu subjektu údajů, tím není dotčeno právo na ochranu soukromí a osobního života takového subjektu údajů. Nelze proto bez souhlasu zařazovat do kroniky např. soupisy majitelů nemovitostí s popisnými čísly těchto nemovitostí i přesto, že jsou tyto údaje veřejně dostupné v katastru nemovitostí.
e) Pokud kronika obsahuje výše popisované soupisy místních občanů, k jejichž zpracování v kronice bylo nutné získat souhlas subjektů údajů, je nutný jejich souhlas i ke zpřístupňování osobních údajů pořizováním výpisů, opisů, kopií nebo k jeho zveřejňování součásti kroniky na webových stránkách.

5.8. Nakládání s osobními údaji v souvislosti se svobodným přístupem k informacím

a) Osobní údaje smí obec poskytnout žadateli jen s výhradním souhlasem osoby, které se to týká.
b) Není-li poskytnu takový souhlas, musejí být údaje vhodnou formou anonymizovány.
c) Bez souhlasu se smí poskytovat informace o veřejně činné osobě, funkcionáři či zaměstnanci obce, které jsou v souvislosti s jeho veřejnou nebo úřední činností a jeho funkčním nebo pracovním umístěním.

5.9. Nahlížení do obecních spisů podle právního řádu

a) Bez omezení přístupu mají právo nahlížet do spisů účastníci řízení, jejich zástupci a dále osoby, které prokážou právní zájem nebo jiný vážný důvod, nebude-li tím porušeno právo některého z účastníků, nebo dotčených osob.
b) Ostatním osobám lze poskytnout informace ze správního spisu pouze na základě žádosti podle zákona o svobodném přístupu k informacím.

6. Incidenty a jejich řešení

a) Každý obecní zaměstnanec včetně správce informačních systémů je povinen ohlásit starostovi každou událost, která by mohla mít nebo má vliv na bezpečnost osobních údajů.
b) Starosta dokumentuje bezpečnostní incidenty včetně skutečností týkajících se porušení bezpečnosti osobních údajů, příčin, jejich odstranění a přijetí nápravných opatření.
c) Starosta obce je součinný s Pověřencem pro ochranu osobních údajů při kategorizaci incidentů:
    1) Incident – jedna nebo více nechtěných, neočekávaných událostí, kterých existuje riziko kompromitace a ohrožení bezpečnosti osobních údajů.
    2) Závažný incident – incident s velkou pravděpodobností špatného následku, nebo následkem zasahujícím do práv subjektů údajů.
d) Pověřenec pro ochranu osobních údajů je povinen má povinnost ohlásit každý závažný incident v oblasti zabezpečení osobních údajů Úřadu pro ochranu osobních údajů nejpozději do 72 hodin od zjištění incidentu
e) Starosta obce je povinen okamžitě a bezodkladně ohlásit závažný incident v oblasti zabezpečení osobních údajů postiženým subjektům. Oznámení musí splňovat podmínky podle čl. 3, odst. 3 GDPR.

7. Informační povinnost vůči subjektu údajů

7.1. Informační povinnost správce

a) Starosta obce odpovídá za informace o rozsahu a způsobu zpracování:
    1) Uchazeči o zaměstnání, občanovi, vztahům odběratelsko-dodavatelským.
    2) Zaměstnancům (např. formou pracovní smlouvy)
b) Informace musí obsahovat:
    1) Kontaktní údaje správce a kontaktní údaje Pověřence pro ochranu osobních údajů.
    2) Účel zpracování, pro které jsou osobní údaje určeny a právní základ pro zpracování.
    3) Příjemce a kategorie příjemců osobních údajů.

4) Právo subjektů údajů odvolat kdykoli souhlas se zpracováním osobních údajů, podání stížnosti u dozorového úřadu a právo požadovat od správce přístup ke svým osobním údajům. Dále může požadovat opravu, výmaz nebo omezení zpracování osobních údajů a právo vznést námitku proti zpracování a právo na přenositelnost údajů.
5) Případný úmysl správce předat údaje do zemí třetích stran.

c) Další informace, které nejsou nezbytné ke spravedlivému a transparentnímu zpracování ve vztahu k subjektu údajů nemusí správce poskytovat.

7.2. Žádosti subjektu osobních údajů

a) Subjekt údajů má právo získat od správce potvrzení, zda jeho osobní údaje jsou, či nejsou zpracovávány, a pokud ano, nabývá práva přístupu k těmto informacím:
    1) Účely zpracování
    2) Kategorie dotčených údajů
    3) Příjemci a kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích.
    4) Plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li to možné určit, kritéria stanovující tuto dobu.
    5) Existence práva požadovat od správce opravu nebo výmaz osobních údajů, které se týkají subjektu údajů nebo omezení jejich zpracování nebo vznést námitku proti tomuto zpracování.
    6) Právo podat stížnost u dozorového úřadu.
    7) Veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány přímo od subjektu údajů
    8) Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a informace týkající se tohoto postupu.
b) Správce poskytne na žádost subjektu osobních údajů kopii zpracovávaných osobních údajů. Za další poskytnuté kopie smí účtovat přiměřený poplatek na základě administrativních nákladů. Právo získat kopii se nesmí nepříznivě dotknout práv a svobod jiných osob.
c) Starosta je povinen přiměřeným způsobem ověřit totožnost žadatele.

8. Přenesení odpovědností a oprávnění na subjekty třetích stran

a) Pokud musí Správce určit Zpracovatele nebo jinou Oprávněnou osobu třetí strany, musí zvážit související rizika a zabezpečit přenesení povinností, kompetencí a odpovědností vyplývající ze směrnice do smluvního ujednání, které bude obsahovat.
    1) Organizační a technické podmínky zpracovávání osobních údajů:
        a. Způsob a rozsah zpracování osobních údajů.
        b. Rozsahy a formy přístupu k informacím a způsobu validace přístupů.
        c. Stanovení minimálních bezpečnostních požadavků pro zabezpečení informací.
        d. Způsob, jakým se zajistí integrita informací poskytovaných dodavatelem.
        e. Způsob, jak řešit incidenty.
        f. Způsob a rozsah vedení záznamů souvisejících se zpracováním osobních údajů.
        g. Nouzové plány pro zajištění dostupnosti informací nebo služeb poskytovaných dodavatelem.
        h. Způsob a přenesení sjednaných odpovědností na zaměstnance dodavatele, další subdodavatele atp.
    2) Doložku o mlčenlivosti třetích stran.
    3) Odkazy na kodexy a pravidla chování, které musí být dodavatel povinen dodržovat.
b) Ve smlouvách se musí jednoznačně stanovit, jestli má dodavatel právo využít, při plnění zakázky, další subdodavatele, v jakém rozsahu a za jakých podmínek. V případě opačném musí smlouva využívání subdodavatelů zakázat.
c) Smlouvy s „jednorázovými“ dodavateli (např. revizní technici, opraváři, poradci, úklid atp.), kteří by na základě jejich obsahu mohli získat přístup k osobním údajům, nebo k informačním majetkům Obce, musí obsahovat Doložku (ustanovení) o mlčenlivosti třetích stran viz příloha č. 4.

9. Kontrolní, auditní činnost a řízení rizik

9.1. Kontrolní činnost

a) Starosta je povinen průběžně kontrolovat způsob zpracovávání osobních údajů a dodržování pravidel s tím spojených.

9.2. Řízení rizik

a) Starosta provádí posuzování shody účelu zpracování s rozsahem a způsobem zpracování každé agendy. Výsledek posouzení zaznamenává v Registru agend. Posouzení umožňuje zejména přijímání dostatečných opatření ke zmírňování rizik zpracování.
    1) V prvotním posouzení se musí přihlédnout k povaze, rozsahu, kontextu a účelům zpracování a vyhodnotit, zda zpracování disponuje faktory pro vysokou pravděpodobnost rizika pro práva a svobody fyzický osob. Zde je posuzováno:
        a. Systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, založeného na automatickém zpracování, včetně profilování a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby závažný dopad.
        b. Rozsáhlost zpracování zvláštních kategorií údajů.
        c. Rozsáhlost systematického monitorování veřejně přístupných prostor.
        d. Zpracování, které Úřad pro ochranu osobních údajů vyhodnotil jako rizikové.
        e. Zpracování, u kterého je pravděpodobné, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob.
    2) Rizika se posuzují jako:
        a. Nízká rizikovost – tzn. Pokud není splněna žádná z podmínek a.-e. v předchozím bodě.
        b. Vysoká rizikovost – tzn. Pokud je splněna alespoň jedna z podmínek a.-e. v předchozím bodě.
    3) Pokud se vyskytují vysoká rizika, musejí být přijímána opatření pro snížení rizikovosti zpracování osobních údajů.

4) Následné posouzení se provádí pokaždé při významných změnách ve způsobu a rozsahu zpracování osobních údajů, minimálně ale jednou za tři roky.

9.3. Analýza bezpečnostních rizik informačních technologií

a) v Analýza rizik zohledňuje bezpečnost při zpracování osobních údajů ve všech oblastech, které mají souvislost se strategií informačních technologií. Za tuto analýzu odpovídá starosta obce as provádí se minimálně jednou za rok, nebo při výskytu vysokého rizika zpracování.
    1) V analýze rizik se musí zohlednit všechny hrozby působící na bezpečnost informací a posoudit úrovně zranitelnosti v technickém a organizačním zabezpečení.
    2) Pro agendy, kde se rizikovost vyhodnotila jako vysoká se musejí přijmou taková opatření, která rizika snižují. Přijímaná opatření musejí být přiměřená možnostem obce a přiměřená ceně dopadů.

9.4. Konzultace s Úřadem pro ochranu osobních údajů

a) Pokud je i po přijetí důsledných opatření riziko hodnoceno jako vysoké, je povinné toto zpracování konzultovat s dozorovým úřadem. Konzultace s dozorovým úřadem by měla předcházet zpracování osobních údajů, pokud je to možné.

9.5. Interní audit

a) Interní audit je prováděn Pověřencem pro ochranu osobních údajů nebo starostou obce. Interní audit má za úkol prověření interních procesů a plnění úkolů pro zpracování osobních údajů a ověření dodržování přijatých technických a organizačních opatření. O provedeném auditu musí být pořízen zápis.

Doložky k Interní směrnici pro ochranu osobních údajů

Obec Dolní Újezd

Obsah

1. Doložka o mlčenlivosti zaměstnanců

Zaměstnanec/brigádník/stážista „má povinnost zachovávat mlčenlivost o osobních údajích, se kterými se seznámil/a při výkonu své pracovní činnosti a rovněž o všech bezpečnostních opatřeních jejichž zveřejnění by mohlo ohrozit zabezpečení osobních údajů. Povinnost zachovávat mlčenlivost platí i po skončení pracovního poměru“.

2. Odpověď na žádost subjektu osobních údajů

Odpověď na žádost subjektu osobních údajů			
Adresát – subjekt osobních údajů			
Datum podání žádosti			
Popis žádost / požadavku subjektu osobních údajů			
Odpověď – sdělení správce osobních údajů			
Zdůvodnění sdělení			
Seznam příloh			
Zpracoval		Dne	

3. Ohlášení porušení ochrany osobních údajů

Odpověď porušení ochrany osobních údajů			
Správce osobních údajů			
Jméno a kontaktní údaje pověřence			
Popis incidentu / jeho povahy			
Popis pravděpodobných důsledků			
Popis příčin			
Důvod odkladu zaslání oznámení (déle než 72 hodin)			
Popis přijatých opatření			
Kategorie osobních údajů		Přibližný počet dotčených subjektů	
Datum a čas vzniku		Přibližný počet dotčených záznamů	
Zpracoval		Dne	

4. Doložka o mlčenlivost třetích stran

Pro účely této doložky se rozumí Objednatelem Správce osobních údajů a Poskytovatelem Zpracovatel osobních údajů.

„Zpracovatel osobních údajů se zavazuje, že jeho zaměstnanci, a pokud to tato smlouva výslovně umožňuje, další subdodavatelé a jejich zaměstnanci, nebudou neoprávněně a mimo smluvní ujednání nakládat s osobními údaji, se kterými přijdou v rámci plnění předmětu smlouvy do styku. Nebudou zcizovat a zpřístupňovat informace o činnosti, systému řízení a kontroly, které se vztahují ke Správci osobních údajů. Stejně tak zachovají mlčenlivost o všech skutečnostech a bezpečnostních opatřeních na ochranu informací, se kterými se seznámí při své činnosti v rámci plnění předmětu této smlouvy a nebudou vyvíjet žádnou činnost, která nesouvisí s předmětem této smlouvy.

Zpracovatel osobních údajů je odpovědný i za zcizení nebo zpřístupnění informací třetí straně nebo osobám, které nejsou zainteresovány na výkonu předmětu činnosti této smlouvy z nedbalosti.

Zpracovatel osobních údajů, ani její zaměstnanci nesmí bez vědomí a prokazatelného souhlasu Správce osobních údajů, pořizovat žádné kopie dat včetně testovacích dat a informací, k nimž získají přístup na základě plnění předmětu smlouvy.

Zpracovatel osobních údajů je povinen dodržovat ustanovení smlouvy, zákon č. 101/2000 Sb. a Nařízení EU 2016/679 a v případě jejich porušení nese plnou odpovědnost s tím, že je povinna uhradit Správci osobních údajů smluvní pokutu ve výši xxx,- Kč za každé takové porušení.

Zpracovatel osobních údajů seznámí s podmínkami smlouvy všechny své zaměstnance, kteří získají nebo mohou získat přístup k informacím Správce osobních údajů.

Správce osobních údajů má právo provést kontrolu u Zpracovatele osobních údajů a rovněž má právo odmítnout přístup k informacím a informačním zařízením zaměstnancům Zpracovatele osobních údajů, kteří neprokáží potřebné znalosti nebo jejichž chování bude v rozporu s předmětem této smlouvy nebo obecně závazných právních předpisů, aniž by to Zpracovatelem osobních údajů bylo považováno za porušení potřebné součinnosti ze strany Správce osobních údajů.

Tímto ustanovením není dotčeno právo Správce osobních údajů požadovat náhradu vzniklé škody, která může zaviněním Zpracovatelem osobních údajů nebo jeho zaměstnance vzniknout Správci osobních údajů“.

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Hladík Stanislav	Dolní Újezd 477, Dolní Újezd	I1600403

TÉMA ČESKY:

Implementace evropské směrnice GDPR v obci Dolní Újezd

TÉMA ANGLICKY:

Implementation of the European GDPR Directive in Dolní Újezd

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je zmapovat požadavky evropské směrnice 95/46/ES (GDPR) a navrhnout jejich implementaci v obci Dolní újezd. V teoretické části práce autor zpracuje základní požadavky a dopady GDPR na státní správu. V praktické části pak autor zpracuje návrh řešení požadavků směrnice GDPR v konkrétní obci a zpracuje návrh požadované řídicí dokumentace a její implementace do ISMS obce.

Návrh osnovy:
Úvod
Úvod do problematiky GDPR
Dopady GDPR na organizace
Řešení požadavků GDPR
Řídicí dokumentace
Implementace a dopad na ISMS
Závěr

SEZNAM DOPORUČENÉ LITERATURY:

Obecné nařízení o ochraně osobních údajů prakticky: GDPR parkticky [online]. 2017 [cit. 2018-01-19]. Dostupné z: https://www.gdpr.cz/

ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 9788075540973.

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

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....