

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Aspekty zavedení GDPR ve veřejné správě ČR

Bc. Jitka Bolechová

Diplomová práce
2020

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Bc. Jitka Bolechová**
Osobní číslo: **E17530**
Studijní program: **N6209 Systémové inženýrství a informatika**
Studijní obor: **Informatika ve veřejné správě**
Téma práce: **Aspekty zavedení GDPR ve veřejné správě ČR**
Zadávající katedra: **Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je kritickým pohledem shrnout oblast GDPR, zhodnotit její dosavadní vývoj a stav a zaměřit se na její dopady na veřejnou správu. Problematika GDPR se stala velmi aktuální v roce 2018, kdy vchází v platnost nová právní úprava týkající se i všech subjektů veřejné správy. Práce by měla objasnit, jaký vliv měla implementace GDPR na informační systémy ve veřejné správě, na chod orgánů veřejné správy i na rozpočty dotčených subjektů.

Osnova:
-Definice a popis GDPR
-Zavádění GDPR v ČR
-Vliv na veřejnou správu
-Vliv na rozpočty obcí

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

NEZMAR, Luděk. GDPR: Praktický průvodce implementací. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.
NAVRÁTIL, Jiří. GDPR pro praxi. Praha: Aleš Čenek, 2018. ISBN 978-80-7380-689-7.
ŽÚREK, Jiří. GDPR pro praxi. Olomouc: ANAG, 2018. ISBN 978-80-7554-097-3.
Bird&Bird, ed. Ochrana osobních údajů, GDPR. Olomouc: ANAG, 2017. ISBN 978-80-7488-241-8.
MVČR – Ochrana osobních údajů [online]. Praha: MVČR. 2018. Poslední změna 27.04.2018. [cit. 27.07.2018].
Dostupné z: <http://www.mvcr.cz/gdpr/>

Vedoucí diplomové práce: **Ing. Pavel Jirava, Ph.D.**
Ústav systémového inženýrství a informatiky
Datum zadání diplomové práce: **2. září 2019**
Termín odevzdání diplomové práce: **30. dubna 2020**

L.S.

doc. Ing. Romana Provázníková, Ph.D.
děkanka

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 2. září 2019

PROHLÁŠENÍ

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 29.5. 2020

Jitka Bolechová

PODĚKOVÁNÍ:

Tímto bych rád poděkovala svému vedoucímu práce panu Ing. Pavlovi Jiravovi, Ph.D. za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování diplomové práce, paní Kateřině Korejtkové za užitečné rady a odborné konzultace a paní starostce obce Běstvína, Ing. Marii Brožkové, taktéž za její čas a poskytnuté informace.

ANOTACE

Práce kritickým pohledem shrnuje problematiku GDPR, zhodnotí její dosavadní vývoj a stav a zaměří se na její dopady na veřejnou správu. Práce by měla objasnit, jaký vliv měla implementace GDPR na informační systémy ve veřejné správě, na chod orgánů veřejné správy i na rozpočty dotčených subjektů.

KLÍČOVÁ SLOVA

GDPR, implementace, obce, rozpočty.

TITLE

Aspects of GDPR implementation in the Czech Republic public administration

ANNOTATION

This thesis critically summarizes the issue of GDPR, evaluates its current development and status and focuses on its impact on public administration. The thesis should clarify the impact of the implementation of GDPR on information systems in public administration, on the operation of public administration bodies and on the budgets of the entities concerned.

KEYWORDS

GDPR, implementation, municipality, budget.

OBSAH

ÚVOD.....	11
1 ÚVOD DO GDPR.....	12
1.1 POZADÍ VZNIKU GDPR.....	12
1.1.1 Historie GDPR	13
1.2 CHARAKTERISTIKA GDPR, CÍLE A PŘÍSTUPY.....	15
1.2.1 Cíle GDPR.....	15
1.2.2 Přístupy k GDPR	16
1.2.3 Povinnosti dle GDPR	17
2 GDPR.....	18
2.1.1 Osobní údaj.....	18
2.1.2 Hodnota osobního údaje	20
2.1.3 Právo na soukromí.....	20
2.1.4 Souhlas	21
2.1.5 Zpracovatel osobních údajů.....	21
2.1.6 Zpracování osobních údajů.....	22
2.1.7 Jmenování pověřence	22
2.1.8 Porušení zabezpečení osobních údajů	23
2.1.9 Zákon o ochraně osobních údajů.....	24
2.1.10 Nový zákon o ochraně osobních údajů	24
2.1.11 Pracovní skupina WP29	25
2.1.12 Správce osobních údajů.....	25
2.1.13 Pověřenec pro ochranu osobních údajů.....	27
2.1.14 Záznamy o činnostech.....	28
2.1.15 Právními důvody zpracování osobních údajů	29
2.1.16 Souhlas se zpracováním osobních údajů.....	29
2.1.17 Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti	31
2.1.18 Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů 31	31
2.1.19 Zpracování osobních údajů zveřejněných na internetu	31
2.1.20 Předávání osobních údajů do jiných zemí.....	32
2.1.21 Sankce a pokuty	33
2.2 OBECNÉ DOPADY NA VEŘEJNOU SPRÁVU	34
2.2.1 Změny v základních registrech.....	34
2.2.2 Změny v Katastru nemovitostí	35
3 PŘÍPADOVÁ STUDIE – IMPLEMENTACE GDPR V OBCI BĚSTVINA.....	37
3.1 OBEC BĚSTVINA	37
3.1.1 Situace v obci	37
3.1.2 Implementace GDPR do obce Běstvína	37
3.1.3 Analýza rizik	40
3.1.4 Rizika GDPR v souvislosti s ostatními zákony	52
3.1.5 Zavedení bezpečnostních opatření	54
3.1.6 Rozpočet spojený s GDPR v obci	56
3.1.7 Rozpočet spojený s GDPR v ČR	58
3.1.8 Metoda Best practice	58
3.1.9 Archivace – dobrá praxe v obci Běstvína.....	59
3.2 CZECH POINT – INFORMAČNÍ SYSTÉM	60
3.3 INFORMAČNÍ SYSTÉM ORG	62
3.1 GDPR KRITICKÝM POHLEDEM.....	63
4 DOTAZNÍKOVÉ ŠETŘENÍ	65
4.1.1 Vyhodnocení dotazníkového šetření	65

4.1.2 Závěr dotazníkového šetření.....	74
ZÁVĚR.....	75
POUŽITÁ LITERATURA.....	77
PŘÍLOHA A.....	81

SEZNAM OBRÁZKŮ

Obrázek 1: Průběh přijímání GDPR.....	15
Obrázek 2: Podrobné rozdělení osobních údajů	19
Obrázek 3: Implementace GDPR na OÚ.....	38
Obrázek 4: Znak zabezpečení SSL certifikátem.....	55
Obrázek 5: CZECH POINT.....	61
Obrázek 6: Komunikace mezi ISZR a ORG	63

SEZNAM TABULEK

Tabulka 1: Analýza rizik	46
Tabulka 2: Analýza rizik-zákony	49
Tabulka 3: Rozpočet obce Běstvína	56
Tabulka 4: Výdaje na GDPR.....	57
Tabulka 5: Počet odpovědí na otázku č. 1 na otázku č. 1	66
Tabulka 6: Počet zaměstnaných respondentů na otázku č. 2.....	67
Tabulka 7: Počet odpovídajících respondentů na otázku č. 3.....	68
Tabulka 8: Počet odpovídajících respondentů za otázku č. 4.....	69
Tabulka 9: Počet odpovídajících respondentů za otázku č. 5.....	71

SEZNAM GRAFŮ

graf 1: V jaké věkové kategorii se pohybujete?	66
graf 2: Jste zaměstnán/a?	67
graf 3: Absolvoval/a jste školení/kurz/získání základních informací o GDPR?	68
graf 4: Víte, o čem pojednává nové nařízení o GDPR?	69
graf 5: Zaznamenali jste, že v místě Vašeho bydliště, na OÚ, byly provedeny změny v rámci GDPR?.....	70
graf 6: Byl/a jste kontaktován/a nějakou firmou o udělení souhlasu? Pokud ano, uveďte, jakou společností	72
graf 7: Jaké společnosti/firmy Vás kontaktovali o udělení souhlasu o zpracování dat?	72

SEZNAM ZKRATEK A ZNAČEK

AIFO	Agendový identifikátor fyzické osoby
EU	Evropská unie
ES	Evropské společenství
GDPR	General Data Protection Regulation
ISKN	Informační systém katastru nemovitostí
OÚ	Obecní úřad
Sb.	Sbírka zákonů
ÚOOÚ	Úřad pro ochranu osobních údajů
ZIFO	Zdrojový identifikátor fyzické osoby

ÚVOD

GDPR bylo před květnem 2018 velmi probírané téma a aktuálně stále je. Nejen pro celou Českou republiku představovala nová legislativa velkou změnu v ochraně osobních údajů. Obří mediální nátlak vyvolal strach a paniku jak u firem, tak u pracovníků veřejné správy a tohoto strachu využily firmy, které začaly nabízet své služby, jako například zpracování analýzy rizik, či svého vlastního pověřence, za vysokou cenu. Na GDPR jako takové je nahlíženo jako na bezúčelovou věc, která má občany a úředníky spíše obtěžovat, než aby jim ulehčila práci. Setkáváme se spousty názorů na věc.

Cílem Diplomové práce je kritickým pohledem shrnout problematiku GDPR, zhodnotit její dosavadní vývoj a stav a zaměřit se na dopady ve veřejné správě. Dále objasnit, jaký vliv měla implementace GDPR na informační systémy ve veřejné správě, na chod orgánů, a i na rozpočty daných subjektů.

V práci je představena historie GDPR od počátků a také jsou zde vymezené základní pojmy, samotné znění legislativy, a další pojmy spojené s GDPR. Následně je představena obec Běstvina, která je analyzována. Je zde nastíněná aktuální situace v obci, jak probíhala implementace GDPR na úřad a kam všude to mělo dopad. V následné analýze rizik budou vyobrazeny veškeré součásti obce, na které má legislativa dopad a které je potřeba pravidelně kontrolovat. Budou zde detailně popsány jednotlivé úkony obce, které by mohly podléhat riziku. Součástí práce také bude dotazníkové šetření, které se zaměřuje na názor občanů obce Běstvina, kdy nejpodstatnější součástí výzkumu je názor občana na GDPR. Zda je pro ně spíše přínosem nebo obtěžováním a zda zaznamenali změny na úřadu s příchodem zmiňované legislativy. V práci bude také pojednáváno o implementaci GDPR do IS veřejné správy, a dopady na ně. V neposlední řadě budou zmíněny i rozpočty jak obce, tak České republiky.

GDPR je velmi zajímavé a rozmanité téma, a co občan to názor. Závěrem práce tedy bude zhodnocení GDPR z kritického pohledu. Porovnání významu zavádění GDPR na úřady a ve firmách, v kterých úkonech je toto nařízení zbytečné, kde všude je riziko, či co mohla vláda udělat z mého pohledu lépe.

1 ÚVOD DO GDPR

Pod obecným nařízením GDPR se skrývá aktualizovaný právní rámec ochrany osobních údajů v evropském prostoru. Od roku 2018 vstoupily v platnost pravidla pro zpracování osobních údajů. V České republice zákon vešel v platnost 25. května 2018. [18]

1.1 Pozadí vzniku GDPR

GDPR vstupuje v platnost v květnu roku 2018. Od měsíce května je každá organizace, společnost, instituce, obec, škola či zdravotnické zařízení, které zpracovává, či ukládá osobní údaje z kteréhokoliv členského státu EU, povinna splnit požadavky, které jsou součástí tohoto nařízení. [18]

Toto nařízení dává občanům větší práva než doposud. Všem zpracovatelům ukládá povinnost, zodpovědněji nakládat s osobními údaji. Při porušení ochrany osobních údajů hrozí všem, kdo informace uchovávají, nebo zpracovávají, mnohem větší sankce než doposud. [18]

Pro společnosti to znamená, že musí zavést celou řadu nových postupů, aby všechny podmínky a požadavky splňovaly. Pokud vezmeme v potaz stále méně stabilní ekonomické a politické prostředí, všechny podniky proto musí reagovat vyšší rychlostí adaptace a větší mírou respektu k duševnímu vlastnictví. [18]

Organizace jsou proto nuceny, aby rychle inovovaly. Tlak na firmy může být vyvíjen i konkurenčními firmami. Nové předpisy představují velkou zodpovědnost. Je potřeba znát přesné znění předpisů, to pak může zajistit, že dodržování nových předpisů nebude tak nákladné a ve skutečnosti to může být použito jako nová podmínka konkurenceschopnosti. Kdyby například telefonní společnosti A unikly osobní údaje zákazníků, telefonní firma B by mohla tohoto oslabení firmy A využít, a zákazníky převést k sobě.

K tomu, aby bylo možné uplatnit k březnu 2018 nařízení o obecné ochraně údajů v EU, bylo nutné, aby všichni, kdo spravují a zpracovávají údaje, zavedli příslušná organizační a technické opatření. [18]

Reálná hodnota osobních údajů vyšla na povrch teprve nedávno. Krádež osobních údajů vystavuje občany EU vysokému riziku. Osvojené techniky dnešní doby umožňují vlastníkům údajů analyzovat data o zákaznících, předvídat jejich individuální chování a do jisté míry je i ovlivňovat. GDPR je tak reakcí na rychlou digitalizaci a kybernetizaci našeho prostoru. Nicméně zda to bude úspěšné nám poví až čas. [18]

Toto nařízení se nicméně netýká pouze jen entit v rámci EU, ale sahá i za hranice. Firma v Tokiu nebo nevládní organizace USA, působící na území EU, musí vyhovět požadavkům GDPR stejně, jako firmy, které jsou v EU. [18]

1.1.1 Historie GDPR

GDPR je v současné době souhrnná zákonná norma, která ochraňuje soukromí občanů.

Směrnice o ochraně osobních údajů je v platnosti již dvacet let. Stanovuje minimální standard zákona o ochraně osobních údajů. Kdy převážná část států patřící do EU přijala nějakou legislativu, která se zabývá řešením problémů ohledně ochrany osobně identifikovatelných informací. [18]

Do května 2018 je platná směrnice 95/46/ES o ochraně údajů. Tato směrnice vešla v platnost roku 1995. Byla zaměřena zejména se na dva cíle: chránit základní právo na ochranu údajů a zaručit volný pohyb osobních údajů mezi členskými státy. [13]

Směrnice byla doplněna rámcovým rozhodnutím Rady, která jako obecný nástroj na úrovni Unie upravuje ochranu osobních údajů v oblasti policejní a justiční spolupráce v trestních věcech. Následný technologický pokrok v posledních letech přinesl nové výzvy, které se týkaly ochrany osobních údajů, a z toho důvodu bylo nezbytné vypracovat legislativní úpravu. [13]

Největším problémem této legislativy bylo to, že některé státy, které nebyly součástí EU shromažďovaly údaje o občanech EU. Dalším problémem byla také zastaralost legislativy. [13]

Potřebné úpravy legislativy jsou také zakotvené v Lisabonské smlouvě. Je zde uvedeno, že *„každý má právo na ochranu osobních údajů, které se jej týkají“*. Ve smlouvě se také dále píše, že *„Evropský parlament a Rada přijmou řádným legislativním postupem pravidla o ochraně fyzických osob při zpracování osobních údajů...“*. Navíc v čl. 8 Listiny základních práv EU je ochrana osobních údajů zakotvena jako základní právo. [13]

Evropská rada vyzvala Komisi o zhodnocení funkčnosti nástrojů EU pro ochranu osobních údajů. První návrhy řešení se vyskytly ve Stockholmském programu. Poté, v listopadu roku 2010 se Komise ve svém sdělení o Komplexním přístupu k ochraně osobních údajů v EU uvedla, že základní právo na ochranu osobních údajů potřebuje být komplexnější a jednodušší politiku. Další důvody, které byly také zmíněny jsou technologický rozvoj a zejména nutnost zohlednit rozvoj digitální ekonomiky na celém vnitřním trhu EU. [13]

Proto, že se jednalo o důležitou revizi, proběhla i veřejná konzultace. O přezkoumání se jednalo více než dva roky. Veřejná porada proběhla ve dvou fázích, a to:

- Debata o právním rámci pro základní právo na ochranu osobních údajů se konala od 9. července 2010 do 15. ledna 2011. Komise obdržela 168 odpovědí, z toho 127 od jednotlivých osob, obchodních organizací a sdružení a 12 od orgánů veřejné moci.
- Debata o komplexním přístupu Komise v ochraně údajů v rámci EU, probíhala od 4. listopadu 2010 do 15. ledna 2011. Zde komise získala okolo 305 odpovědí, z nichž 54 odpovědí bylo od občanů, 31 od orgánů veřejné moci a zbylých 220 od soukromých organizací, zde se jednalo zejména o obchodní sdružení a nevládní organizace. [13]

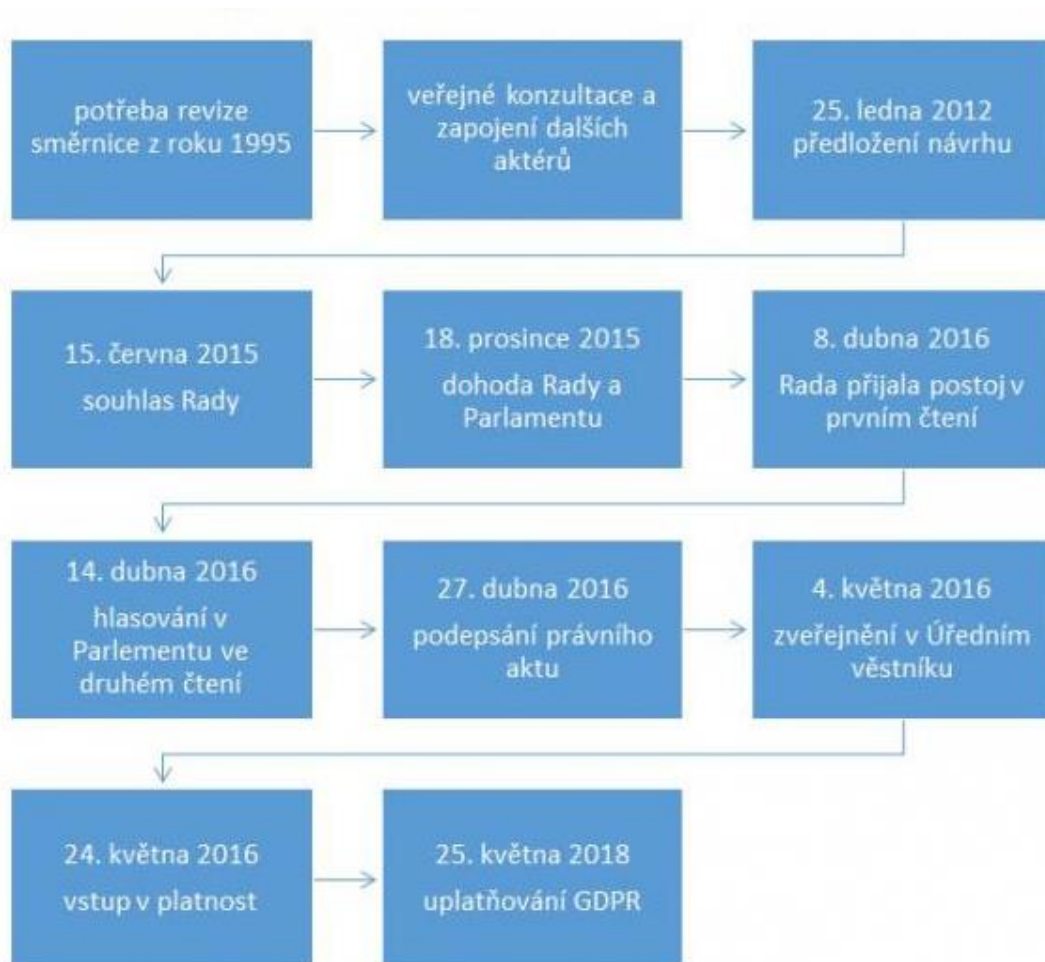
V červenci 2011 bylo Evropským parlamentem schválen v rámci usnesení zpráva, která podpořila činnost Komise k reformě rámce pro ochranu osobních údajů. V následujících měsících roku 2011 potom Rada EU přijala závěry, kde podpořila touhu Komise o tuto reformu. Po řadě jednání byl představen návrh o ochraně fyzických osob, která se týká zpracovávání osobních údajů a o volném proudění těchto údajů, a to konkrétně 25. ledna roku 2012. Před konečným přijetím návrhu byl dokument v průběhu čtyř let několikrát projednáván v institucích EU. Nejvíce se nový legislativní čin řešil mezi členskými státy v Radě EU (viz obrázek níže). [13]

V průběhu června 2015 dosáhla Rada po mnoha kolech jednání obecného přístupu. Obecný přístup znamená, že Rada dosáhla politické dohody, na jejímž základě mohla zahájit jednání s Parlamentem. [13]

Dohoda mezi Parlamentem, Komisí a Radou byla přijatá 15. prosince 2015. Následně je potvrzeno dohodnuté znění po jednání s Parlamentem. V průběhu června 2015 dosáhla Rada po mnoha kolech jednání obecného přístupu. Obecný přístup znamená, že Rada dosáhla politické dohody, na jejímž základě mohla zahájit jednání s Parlamentem. [13]

Po doporučení Výboru pro občanské svobody, spravedlnosti a vnitřní věci pro druhé čtení pak na začátku dubna 2016, byl parlamentem schválen postoj Rady v prvním čtení. Ke konečnému podpisu došlo 27. dubna 2016. [13]

Na níže uvedeném obrázku může vidět schéma průběhu přijímání GDPR v ČR.



Obrázek 1: Průběh přijímání GDPR

Zdroj: [13]

1.2 Charakteristika GDPR, cíle a přístupy

GDPR představuje nový právní základ ochrany osobních údajů v EU, a má velký vliv na ochranu údajů zemích EU, ale i těch zemí, které nejsou členy EU. Jedná se o nařízení, nikoliv o směrnici. Proto, že bylo GRPD vydáno jako nařízení, a ne směrnice, jde všestranně použít ve všech členských státech Evropské unie, ale také na Islandu, v Norsku a také v Lichtenštejnsku. Proto se jedná o právní normu sjednocující, což je velice důležité z pohledu mezinárodního pohybu informací. [17]

1.2.1 Cíle GDPR

Mezi hlavní cíle GRPR patří:

- Regulace ochrany osobních údajů ku poměrům dnešní doby
- Ve všech zemích EU a ostatních zemí, kterých se toto týká sjednocení práva ochrany osobních údajů

- Podpoření práv v oblasti ochrany osobních údajů osob, které jsou předmětem údajů a docílení sjednocené literatury GDPR odpovídajícími úřady konkrétních zemí EU, kterých se toto nařízení týká
- Posílit věrohodnost EU a zemí, které jsou součástí EU (a i těch zemí, kterých se nařízení GDPR týká), pro země, které se chtějí podílet na rozvoji obchodu s Evropskou unií, a s tím související předávání osobních údajů. [17]

1.2.2 Přístupy k GDPR

- Princip odpovědnosti správce
- Přístup založený na riziku

Princip odpovědnosti správce znamená, že je správce odpovědný, za dodržení zásad ohledně zpracování osobních údajů a také je v povinnosti správce tento soulad odložit. Také má právo tento doklad doložit prostřednictvím kodexu, osvědčení a certifikace, či případné záznamy o zpracování činností. [17]

Kodexy mají správcům sloužit jako pomůcka pro správné praxe při zpracování osobních údajů, a to s ohledem na specifičnost daného sektoru. Budou je moci vydávat subjekty, které zastupují různé třídy zpracovatelů, nebo správců. Návrh musí být předložen Úřadu pro ochranu osobních údajů, a ten vydá pokyn, zda je kodex, či návrh v souladu s Obecným nařízením, pokud ano, schválí jej. Pak se tímto kodexem mohou řídit správci v daném sektoru, např. ve zdravotnictvím. [19]

Osvědčení slouží k prokázání toho, zda je zpracování v souladu s obecným nařízením. Toto není povinnost. Správce nebo zpracovatel může předat soulad zpracování osobních údajů s obecným nařízením. Osvědčení mohou vydávat jenom subjekty, které jsou k tomu akreditovány. [19]

Přístup založený na riziku vypovídá o tom, že správce od počátku zpracování osobních údajů je povinen brát na vědomí povahu, rozsah, účel a kontext zpracování a také musí přihlídnout k možným rizikům pro práva a svobody fyzických osob a tomu je potřeba, aby zabezpečil osobní údaje. V užším slova smyslu mluvíme o přístupu, které je založena na riziku jako o praktikování některých povinností pouze v takovém případě, když zpracování údajů může znamenat riziko pro práva a svobody fyzické osoby. [17]

Pokud se jedná o tento rozsah založený na riziku, uplatňují se zejména tyto nové povinnosti, ohlašování a posuzování vlivu zpracování na ochranu osobních údajů a povinné konzultace

s Úřadem pro ochranu osobních údajů. Jejich praktikování jde ruku v ruce s přítomností rizika nebo také s vysokým rizikem pro právo svobody fyzických osob. [17]

1.2.3 Povinnosti dle GDPR

S GDPR přicházejí nové povinnosti. Jsou to především tyto:

- povinnost vypracování posouzení dopadu činnosti na ochranu osobních údajů,
- vykonávat předběžné konzultace s Úřadem pro ochranu osobních údajů,
- hlásit porušení bezpečnosti osobních údajů do 72 hodin od doby, kdy se o tom správce dozví
- povinnost umožnit přenositelnost osobních údaj od jednoho k druhému správci, a také povinnost jmenovat osobu, která bude pověřena ochrany údajů.

Jednotlivým bodům se budu dále věnovat v kapitolách. [21]

2 GDPR

GDPR vymezuje pojmy jako osobní údaj a subjekt údajů, kdy osobním údajem rozumíme jakoukoli informaci, která se nějakým způsobem vztahuje k danému objektu. Kdežto Subjektem údajů je člověk, a tedy fyzická osoba, k níž se vztahují jakékoliv osobní, citlivé informace. [21]

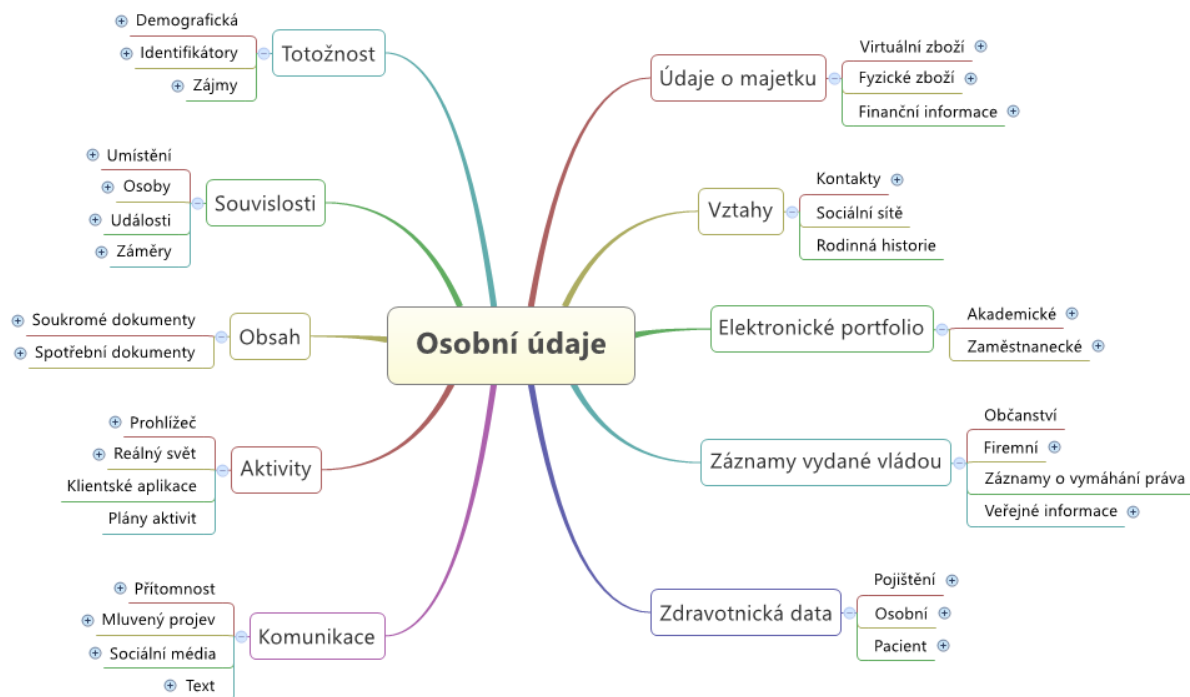
2.1.1 Osobní údaj

Osobní údaje jsou různé informace o identifikovaném či identifikovatelném subjektu údajů či identifikovatelné fyzické osoby. Identifikovatelnou fyzickou osobou je takový fyzická osoba, kterou je možné přímo nebo nepřímo identifikovat, a to tak že se odkazujeme na určitý identifikátor, jako je například jméno, číslo, či síťový identifikátor, nebo se může jednat o jeden či více zvláštních prvků fyzické, fyziologické, genetické, ekonomické, kulturní nebo společenské identity určité fyzické osoby. [21]

Obecné osobní údaje je například jméno, pohlaví, věk, datum narození, osobní stav, IP adresa či fotografický záznam. GDPR se vztahuje i na fyzické osoby, které podnikají, proto mezi tyto osobní údaje řadíme i organizační údaje, jako například e-mailová adresa, telefonní číslo, nebo různé identifikační údaje vydané státem. Mezi osobní údaje patří i zvláštní kategorie, která je nazývána citlivé údaje. [21]

Citlivé osobní údaje představují speciální kategorií podle GDPR, a ta obsahuje údaje o rasovém nebo etnickém původu, politických názorech, náboženském vyznání, filozofickém vyznání, členství v odborech, informace o zdravotním stavu, o sexuální orientaci a trestních deliktech nebo pravomocném odsouzení osob. Do této kategorie patří genetické a biometrické údaje a osobní údaje dětí. Biometrickým údajem jsou například osobní údaje, které vyplývají z konkrétního technického zpracování týkající se fyzických anebo fyziologických znaků osoby, které umožňují právě tuto osobu jednoznačně identifikovat. Mezi typické znaky biometrických citlivých údajů řadíme snímek obličeje, otisk prstu, nicméně mezi tyto údaje patří také judikatury a podpisy. [22]

Podrobnější rozdělení osobních údajů z jiného hlediska je znázorněno i na obrázku dva níže.



Obrázek 2: Podrobné rozdělení osobních údajů

Zdroj:[9]

Z obrázku 2 je patrné, že se nutně nemusí jednat pouze i osobní údaje člověka, ale jde i o údaje, které vypovídají o charakteru osoby. Sděluje informace o tom, jaké jsou jeho preference, zvyklosti, co rád nakupuje, jaké má zájmy, jakou formou komunikuje apod. [9]

Jedná se o údaje, které mohou subjekt údajů poškodit ve společnosti, v zaměstnání, ve škole anebo mohou být příčinou diskriminace. Nově tato kategorie zahrnuje i genetické a biometrické údaje. [22]

Z GDPR jsou nicméně vyjmuty anonymizované údaje a pseudonymizované údaje. U anonymizovaných údajů se jedná o údaje zemřelých osob, a údaje vyplývající z nějaké činnosti v osobní rovině povahy, které nemají obchodní nebo institucionální charakter. Jsou to tedy takové údaje, které jsou pro fyzické osoby osobní a nehodlají je s nikým sdílet. [22]

U pseudonymizovaných údajů je možné určit, koho se týkají, ale potřebujeme k tomu dodatečné informace. Například Správce údajů shromažďuje údaje se jménem, příjmením, věkem a nejvyšším dosaženým vzděláním. Jméno a příjmení nahradí číselným kódem a zvláště uchovává soubor se jménem, příjmením a tímto číselným kódem. Kdo má přístup k oběma souborům zároveň, je schopen určit, ke komu se informace o věku a vzdělání vztahují, a proto je tyto údaje potřeba chránit výše uvedenými předpisy. Existence dvou oddělených souborů informací jsou pro pseudonymizaci klíčové. [5]

Zpracování citlivých údajů patří mezi ty údaje, které jsou přísně kontrolovány. [22]

V rámci dvoustranného tržního mechanismu fungují online platformy jako sprostředkovatelé, co shromažďují data od spotřebitelů a informace, které získají pak dále prodávají zejména reklamním firmám. Data dále tyto firmy zpracují, a mohou podle nich vytvářet reklamní kampaně pro konkrétní zákazníky. Firmy pak umisťují výrobky co nejefektivněji a rozesílají zákazníkům reklamní letáčky přesně podle jejich zájmů. Je odstraněna asymetrie informací a firmám se pak zvyšuje zisk. Spotřebitelé si nicméně často neuvědomují, jak nebezpečné pro ně je, pokud své osobní údaje dostatečně nechrání. [22]

2.1.2 Hodnota osobního údaje

Osobní údaje vytvářejí ekonomickou hodnotu pro digitální trh. Konkrétně má ekonomickou hodnotu zejména pro online platformy jako jsou sociální sítě, online videa (Youtube) nebo vyhledávače. Nařízení definuje osobní údaje jako všechny informace o identifikované fyzické osobě, ať už jde o jakoukoliv informaci, která se týká dané fyzické osoby. Osobní údaje pak můžeme brát jako ekonomické aktivum. Toto aktivum je tvořené například identitami a také chováním daného jedince. Osobní údaje jsou tak obchodovány výměnnou za vyšší kvalitu produktů a služeb. Množství údajů, které je ukládáno roste velice rychle a poukazuje na to, že v dnešním světě bylo vytvořeno 90 procent dat během dvou let [18].

Online platformy fungují v rámci dvoustranného tržního mechanismu jako zprostředkovatel. Ty shromažďují data od spotřebitelů a tyto nasbíraná data potom prodávají, a to zejména reklamním firmám. Firmy nad těmito daty provádějí analýzu dat a spotřebitelé pak dostávají oznámení, doporučení či reklamu cílenou podle jejich zájmů či chování. To pak vede k asymetrii informací, kdy jedna strana je ve výhodě, protože mají více informací než strana druhá [18].

Dostáváme se pak k problému, kterého si spotřebitelé nejsou plně vědomi. Neuvědomují si, jak mohou být jejich online údaje použity v byznysu a dostatečně si své osobní údaje nechrání. Může pak dojít i k neochotě osobní údaje sdílet [18].

2.1.3 Právo na soukromí

Soukromí je vysvětlováno v jednotlivých pramenech odlišně. Je možné ho představit jako oblast intimního, potažmo osobního života jedince, kde platí, že pokud to jedinec neodsouhlasí, nemůže za něj nikdo vystupovat. Literatury se shodují, že mezi tuto oblast patří jak myšlenkový směr, tak i ten fyzický. Pro představu jde o oblasti jako např. obydlí nebo rodinný život. Co se

týče českého právního řádu, je tento pojem vymezen neurčitě a je zvažován u každého případu dle okolností [32].

Pokud mluvíme o soukromí, musíme vzpomenout nejvíce skloňovaný soud s tímto pojmem. Tím je Evropský soud pro lidská práva. Ten jako první rozhodoval o případu týkajícího se práva na soukromí. Konečný verdikt zněl, že „není možné uvést definici soukromí ani taxativní výčet jeho složek“. V dalších případech se zabíral vymezením obsahu soukromí a verdikt byl, že podstatnou součástí soukromí jsou údaje spojené s osobností jedince jako je pohlaví, sexuální orientace, jméno a příjmení. V dalším případě se zabíral záležitostí narušení soukromí, kde obžalovaný zveřejnil fotografii bez souhlasu, kterou publikoval v tisku. Této stížnosti bylo vyhověno a bylo to poprvé, co soud uznal podobnou stížnost [32].

První případ, který se řešil u soudu ohledně zveřejnění osobních údajů na internetu byla kauza Lindqvist, kde Švédka zveřejnila bez souhlasu na webové stránce údaje o osobách, kteří vykonávali dobrovolnickou činnost v její farnosti. Švédský soud uznal její vinu a uložil ji peněžitou pokutu [32].

2.1.4 Souhlas

Souhlas je jedním z nejdůležitějších pojmů pro komplexní oblast zpracování osobních údajů. Souhlasem subjektu se chápe jakýkoli svobodný, informovaný, konkrétní a jednoznačný projev vůle. Subjekt tím dává potvrzení, či svolení k dobrovolnému zpracování jeho osobních údajů. Tudíž obecné nařízení neklade důraz na písemný souhlas. Jde zejména o to, aby byl souhlas konkrétní a jednoznačný. Dále obecné nařízení také upozorňuje na to, že mlčení neznamená souhlas, když uvádí, že mlčení, předem zaškrtnutá políčka nebo nečinnost by pak neměla být shledávána jako souhlas [11].

Poskytnutí souhlasu je obecně právním úkonem, který je svým charakterem jednoznačný. Pokud jde o dohodu, kdy na jedné straně je správce či zpracovatel a na druhé straně fyzickou osobu, nejde o dohodu. Pro posouzení platnosti je nutné brát v potaz úpravu právních úkonů v obecném právním předpisu [11].

2.1.5 Zpracovatel osobních údajů

Zpracovatelem osobních údajů je fyzická nebo právnická osoba, agentura, orgán veřejné moci anebo jiný subjekt, který jménem správce zpracovává osobní údaje. Mezi zpracovatelem a správcem je jistý rozdíl, a to takový, že v rámci operací a činností pro správce může dělat jen takové operace, které mu svěřil správce, kterými byl sám správce pověřen. Je nutné uvést,

že zpracovatel je zpracovatelem pouze ve vztahu k osobním údajům, které mu byly poskytnuty správcem. Nejde tedy o osobní údaje, které zpracovává pro účely, které se jej přímo dotýkají.[23]

Zpracovatelé jsou osoby, které mají přístup k osobním údajům. Jde o takové osobní údaje, které shromáždil správce nebo které jsou zpracovávány. Zpracovatelem může být i společnost, která osobní údaje nijak nezpracovává, ale data ukládá na jejich serverech. Mezi správcem a zpracovatelem musí být smluvní vztah, který musí splňovat specifické požadavky Obecného nařízení. Zpracovatel nese odpovědnost za bezpečné a spolehlivé zpracování osobních údajů. Zpracovatel nesmí bez vědomí správce přizvat dalšího zpracovatele do procesu. To znamená, že by nikdy neměla nastat situace, že by správce nevěděl, kdo nebo jak údaje zpracovává. [18]

2.1.6 Zpracování osobních údajů

Pokud pojednáváme o zpracování, jde o jakékoli činnosti s osobními údaji nebo soubory, které obsahují osobní údaje, které jsou zpracovány pomocí nebo bez pomoci automatizovaných postupů, mezi které patří shromažďování, zaznamenání, použití, zpřístupnění přenosem, šíření nebo seřazení či kombinace, omezení výmaz a v neposlední řadě zničení.[18]

Pokud budeme hovořit o zpracování ve smyslu Obecného nařízení, nemůžeme ho považovat jako jakékoli používání s osobním údajem. Jde o sofistikovanou činnost, a tu správce s osobními údaji vytváří za konkrétním účelem a činí ji systematicky. Pokud budeme pracovat s osobním údajem tak, že nebude zpracován, ochranu poskytuje zákon č 89/2012 Sb., občanský zákoník. Obecným nařízením se tak jako správci řídí pouze ty subjekty, které zpracovávají osobní údaje ve smyslu definice zpracování. [18]

Zpracovatelem může být i společnost, která osobní údaje nijak nezpracovává, ale jsou uloženy na jejích serverech. Zpracovatel nese odpovědnost za bezpečné a spolehlivé zpracování osobních údajů. Zpracovatel nesmí bez vědomí správce přizvat dalšího zpracovatele do procesu. To znamená, že by nikdy neměla nastat situace, že by správce nevěděl, kdo nebo jak údaje zpracovává. [18]

2.1.7 Jmenování pověřence

Povinnost jmenovat pověřence se netýká nutně všech subjektů, co zpracovávají osobní údaje. Povinnost vychází z nařízení v případě, že:

- Zpracování vykonává orgán veřejné moci nebo veřejný subjekt,
- pokud se jedná o operace zpracování takové, že je potřeba je rozsáhle pravidelně a systematicky monitorovat,

- jestliže je hlavní činností správce nebo zpracovatele rozsáhlé práce se zvláštní kategorií údajů nebo osobních údajů týkající se rozsudků trestních věcí a činů[12] .

Nařízení neurčí přesně, jakou kvalifikaci má pověřenec, ale pouze říká, že pověřenec pro ochranu osobních údajů musí být zvolen na základě profesních kvalit, a to hlavně na základě svých odborných kvalit práva a praxe v oblasti ochrany osobních údajů. Tito jedinci by měli být schopni své úkoly a povinnosti nezávislým způsobem. Důležité jsou znalosti z oblasti národní a evropské legislativy a samozřejmě praxe v oboru ochrany osobních údajů a velká znalost nařízení[12] .

Plnit úkoly by měl být pověřenec schopen jednak vzhledem k jeho osobním kvalitám a znalostem a také s ohledem na postavení v organizaci. Pověřenec přináší do firmy zejména základní prvky nařízení. Jde o zásady zpracování dat práva subjektů údajů, záměrná a standardní ochrana osobních údajů, záznamy o činnostech zpracování, zabezpečení zpracování a ohlašování, a oznamování případů porušení zabezpečení ochrany osobních údajů[12] .

Hlavním úkolem pověřence tedy je podávání informací a poradenství zpracovateli či správci, i zaměstnancům, kteří mají podíl na zpracování. Pověřenec má taky za úkol monitorovat soulad zpracování s Nařízením a dalšími předpisy, podává na vyžádání poradenství, pokud se jedná o radu, spojenou s ochranou osobních údajů[12] .

2.1.8 Porušení zabezpečení osobních údajů

Obecné nařízení definuje porušení zabezpečení jako: *„Porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních dat.“ [11]*

Pod pojmem zničení osobních údajů se schovává situace, kdy údaje už neexistují nebo neexistují v takové formě, která by byla pro správce nějakou použitelné. Poškozené data jsou takové osobní údaje, které byly změněny, narušeny anebo jsou už úplně jiné. Ztrátu, pokud se jedná o osobní údaje je nutno vykládat tak, že údaje možná ještě existují, nicméně správně je již nemá ve své moci, ztratil nad nimi kontrolu, nemá je v držení anebo nad nimi ztratil kontrolu. Neoprávněné či protiprávní zpracování zahrnuje poskytnutí osobních údajů příjemcům, kteří nemají právo tyto data přijímat, nebo k nim mít přístup, nebo tyto data jakkoli zpracovávat. [11]

2.1.9 Zákon o ochraně osobních údajů

Často se můžeme setkat v mediích se články, které v občanech, kteří mají implementaci GDPR na starost, vyvolávají pocit strachu, jen z toho důvodu, aby využívali advokátní kanceláře a IT firem. Práva, o kterých se často pojednává, jako je ku příkladu právo na výmaz byla ustanovena i dosavadním zákoně. [29]

Dosavadní platný zákon je založen na směrnici 95/46/ES. Citovaná legislativa zní následovně: *„Každé osobě musí být umožněno docílit, podle povahy případu, opravu těchto údajů nebo jejich vymazání, jestliže byly zpracovány v rozporu s vnitrostátním právním řádem uplatňujícím základní zásady stanovené v této Úmluvě.“* Díky této směrnici je taktéž možné získat osobní údaje o osobě od subjektu, u kterého je veden v databázi. Toto je vztaženo k evropské směrnici. Nicméně v české úpravě zákona se pojednává o tom, že jestliže subjekt zjistí, že správce osobních údajů pojednává v rozporu se zákonem, má možnost urgovat správce, aby jeho osobní údaje daného subjektu byly smazány. Nicméně aktuálně je to tak, že sám správce rozhoduje, jestli jsou údaje zpracovány dle zákona, nebo ne [33],[29].

2.1.10 Nový zákon o ochraně osobních údajů

Tento zákon pojednává o reformě již zmíněné směrnice 95/46/ES. Reforma se dotýká všech členů Evropské unie. Současný zákon o ochraně osobních údajů nebyl dostatečně připravený pro takový enormní rozvoj technologií jak už informačních, tak stále nově se vyvíjejících. A přesně proto potom zákon ztrácel na významu. V důsledku nedostatečného zákonu pak docházelo k tomu, že data byla nedostatečně ochráněna, nebo stále častější zneužívání databází, které obsahují osobní data. Dalším problémem, který se objevil je to, že některé země Evropské unie si zákon o ochraně osobních údajů upravovala rozdílně a zákon pak nebyl sjednocen ve všech zemích EU. Způsobilo to rozdílný výklad a osobní údaje pak byly chráněny v každé zemi rozdílně a došlo i na firmy, které působí napříč celoevropským trhem [20].

Nový zákon o ochraně osobních údajů je v platnosti v celém svém znění ve všech státech EU. Účelem tohoto zákonu je sjednotit ochranu osobních údajů. Odborníci se zde nicméně rozcházejí v názorech: Rozporují s tím, zda má být zákon pouze přizpůsobený směrnici, či nahrazen zcela novým. Důležitým úkolem pro správce a zpracovatele je, aby pracovali s osobními údaji jen tak, aby nedocházelo k narušení bezpečnosti nebo aby se vyhnuli zásahu do soukromí občana. Toto vychází ze základního práva EU a také z činnosti mezinárodního práva, který se dotýká ochrany osobních údajů [20]

Hlavní posun oproti staré směrnici je ten, že správce nebo zpracovatel, je povinen dodržovat nařízení i když nemá sídlo v EU. Jedná se o situaci, kdy subjekt nabízí jakékoliv služby nebo

jiné věci na unijním trhu, ale spravuje je z jiné části světa. Zde panuje shoda odborníků, že tento článek je napsán nešťastně a bude působit velké problémy. Hlavní kritizovanou chybou je špatně zformulované a velmi široké vymezení působnosti. Proto výklad není jasný a dosti se liší. Zde je velmi diskutovanou otázkou, zda tento článek bude akceptován mimo unijními zeměmi bez jakékoliv zahraniční úmluvy [20].

Můžeme obecně říci, že nařízení jako takové dává větší kontrolu a ochranu na stranu občana. Ten je díky tomu více informován, jak je z jeho osobními údaji nakládáno. [20]

Správce nebo zpracovatel jsou povinni umístit podmínky pro zpracování na viditelné místo, kde musí být napsány srozumitelně, a také musí být čitelné, což znamená naformátovaný text a dostatečně velké písmo. Takže se již nemůže stát, že správce umístí tento souhlas mezi obecné ustanovení nebo obchodní podmínky, kde je navíc text psán v jednom odstavci, a ještě zmenšeným písmem. Stejně jednoduché jako odsouhlasení zpracování osobních údajů musí být i jejich vymazání z webu. Často kladená otázka je, jestli data budou vymazána ze všech úložišť, které správce vlastní. Dnes již v každé instituci existuje zálohování dat - tzn. když občan požádá o výmaz z vyhledávání, dojde tak pouze v části jejich domén. Z toho vyplývá, že pokud budeme vyhledávat tento obsah v ČR, bude blokován, ale v případě přístupu k těmto datům mimo EU, data budou dohledatelná [20],[30].

2.1.11 Pracovní skupina WP29

Do začátku účinnosti Obecného nařízení byla dle ustanovení zřízena Pracovní skupina WP29, ta se skládá z jednoho zástupce dozorového úřadu každé členské země a jednoho zástupce Evropského inspektora ochrany údajů a Evropské komise. Ke dni účinnosti Obecného nařízení – 25. května 2018 – se Pracovní skupina změnila na Evropský sbor pro ochranu osobních údajů (zkráceně Sbor) [35].

Úkolem Sboru je především zajišťování jednotného uplatňování Obecného nařízení a za tím účelem monitorovat jeho funkci a vydávat pokyny, doporučení a osvědčené postupy, a to i pro některé stanovené oblasti a instituty Obecného nařízení [25].

2.1.12 Správce osobních údajů

„Správce se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;“ [18]

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

- jaké osobní údaje budou shromažďovány,
- zda je zapotřebí souhlas subjektu,
- po jakou dobu budou údaje uchovávány,
- kdo bude data shromažďovat,
- jaký bude účel zpracování,
- jak budou data zabezpečena,
- jaká je míra rizika pro subjekt údajů,
- o informovanosti subjektu. [18]

Pokud nastane situace, že v jedné situaci má více správců odpovědnost, je potřeba přesně stanovit a říct, kdo za co odpovídá. Správce je také povinný přesvědčit se o seriozitě dodavatele a zjistit, zda má zajištěné opatření tak aby bylo vyhověno GDPR a byla zajištěna ochrana práv subjektů. Tuto situaci je možné vysvětlit v případě e-shopu, kdy si majitel najme někoho, kdo mu bude stránky zpracovávat. V tu chvíli se stává z osoby, která stránky spravuje a udržuje správce. Ten musí zajistit ochranu údajů a minimalizovat rizika. Je povinen zajistit potřebná opatření

a tyto opatření mít pod dohledem, pro případ, že by nebyla účinná. Nelze tedy implementovat požadavky GDPR a tím považovat práci za hotovou. Jedná se o stálý proces, který je nutné pravidelně dokazovat a určité činnosti opakovat. [18]

Jestliže zpracování osobních údajů nese vysoké riziko v případě, že by správce nepřijal opatření pro zmírnění rizika, je správce povinen zpracování osobních údajů, konzultovat s Úřadem pro ochranu osobních údajů, tedy v případě, když správce přijme opatření ke zmírnění vysokého rizika, a riziko i přesto přetrvává. Účelem konzultace je tedy mít pod kontrolou hrozící vysoké riziko s dozorovým úřadem. [19]

Správce je také povinen, v některých případech, provést posouzení vlivu na ochranu osobních údajů. Posouzení se musí provést ještě před začátkem zpracování. Pokud byl zvolen nějaký pověřenec pro ochranu osobních údajů, správce si od něj vyžádá jeho posudek. [19]

Posouzení vlivu na ochranu osobních údajů se vyžaduje:

- pokud se jedná o systematické a rozsáhlé vyhodnocování osobních případů, které se týkají fyzických osob, a které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí
- pro rozsáhlé zpracování speciálních kategorií údajů nebo rozsudků v trestních věcech
- pro rozsáhlé uspořádané sledování veřejně přístupných prostorů

Nad těmito možnostmi je nutné udělat posouzení vlivu u zpracování, které splní kritéria podle seznamu druhů operací zpracování, které podléhají povinností posouzení vlivu, které vydal daný úřad. Je tedy zřejmé, že se to netýká každého zpracování, ale jen v případě, když se jedná o opravdu vysoké riziko zpracování osobních údajů. [19]

2.1.13 Pověřenec pro ochranu osobních údajů

Důležitou součástí prokazování souladu s GDPR je jmenování pověřence pro ochranu osobních údajů anebo také DPO (Data Protection Officer). [7]

Hlavním úkolem pověřence je monitorování souladu zpracování osobních údajů s povinnostmi, které plynou z nařízení, konání interních auditů, řízení agendy interní ochrany dat a školení pracovníků. [7]

Mezi povinnosti pověřence jmenovat nastává ve třech případech, a to:

- zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů),
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů,
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. [7]

Nápomocná osoba s odbornými znalostmi by měla poskytnout pomoc ve všech třech případech, v oblasti právních předpisů a postupů, které se týkají ochrany údajů. Pověřenci by měli být schopni dodržovat a plnit své povinnosti a úkoly nezávislým způsobem, bez ohledu na to, zda se jedná o zaměstnance, nebo externě zprostředkovat službu. Některé organizace mohou dospět k závěru, že dobrovolně pověřit pověřence může být užitečné, a to pak budou dozorové orgány podporovat. [7]

Úkol ve veřejném zájmu a výkon veřejné moci může být plněn nejenom státním orgánem, ale také jinými fyzickými nebo právnickými osobami, kterým je tato pravomoc svěřena

na základě národních předpisů. Může jít například o oblast veřejné dopravy, zásobování vodou a energiemi, silniční infrastrukturu nebo veřejnoprávní vysílání. [7]

2.1.14 Záznamy o činnostech

Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:

- jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
- účely zpracování;
- popis kategorií subjektů údajů a kategorií osobních údajů;
- kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace
- je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření

Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;
- účely zpracování;
- kategorie zpracování prováděného pro každého ze správců;
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace
- je-li to možné, obecný popis technických a organizačních bezpečnostních opatření
- Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu. [16]

2.1.15 Právními důvody zpracování osobních údajů

Tyto důvody o zpracování osobních údajů rozumíme oprávnění správce osobní údaje zpracovat a pracovat s těmito informacemi. Důležitým předpokladem jsou pak právní důvody proto, aby se vůbec mohlo správně mluvit o legálním zpracování, protože pokud by správce neměl právní důvod ke zpracování osobních údajů, nebylo by už jasné, zda plní povinnosti vzhledem k zpracování a právním důvodům, a zda údaje nezpracovává nezákonně či nelegálně. V takovém případě by byl pak povinen tyto osobní údaje smazat. [18]

Je spousta různých účelů, proč správce uchovává, nebo zpracovává osobní údaje. Je zde i možnost, kdy správně může jedny osobní údaje zpracovávat i pro více účelů. Tyto účely mohou vznikat a zanikat různě v čase, aniž by bylo zapotřebí údaje likvidovat. Likvidovat údaje má správce povinnost až v momentě, kdy už nemá důvod k dalšímu zpracování údajů. [18]

2.1.16 Souhlas se zpracováním osobních údajů

Osobní údaje je možné zpracovávat pouze tehdy, pokud je na místě alespoň jeden, z těchto uvedených právních důvodů:

- subjekt údajů udělil souhlas pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů. [34]

Souhlasem ke zpracování osobních údajů pak rozumíme svobodný, dostatečně informovaný a jednoznačný projev vůle, a ten subjekt či fyzická osoba prohlašuje a dává svolení ke zpracování osobních údajů. Jde o aktivní projev vůle ke zveřejnění, zpracování, kdy subjekt

nesmí mít nucen. Souhlas objekt vždy poskytuje za nějakým účelem, přičemž je nutné, aby subjekt byl obeznámen s účelem zpracování. [34]

Souhlas je také odvolatelný. Pokud se subjekt odvolá, neznamená to, že by byl správce povinen osobní údaje zlikvidovat, protože odvolání se děje za nějakým účelem, pro který jsou osobní údaje zpracovány, a správce může údaje zpracovávat za jiným účelem, a pro ten využije jiný právní důvod zpracování než souhlas subjektu údajů. Jinými slovy, v případě odvolání souhlasu je správce povinen přestat zpracovávat osobní údaje pro účely definované v souhlasu. Pokud souhlas byl jediným právním důvodem zpracování, bude zpravidla následovat i likvidace osobních údajů. Souhlas se pak uděluje správci tak, aby nemohl zpracování podřadit pod jiný právní důvod (např. správce si nezajišťuje souhlas se zpracováním osobních údajů, pokud osobní údaje zpracovává pro plnění smlouvy se subjektem údajů, nebo pro zpracování v pro účely nezbytné personální agendy apod.). [34]

Pokud subjekt neposkytne souhlas, i přesto v některých situacích můžeme zpracovávat osobní údaje, a to tehdy, pokud je to nezbytné pro splnění smlouvy. Například pokud jsme provozovateli e-shopu, které posílá zbožím zákazníkům na poštu, je takovým údajem nejspíše jméno zákazníka, adresa doručení a někdy i telefonní číslo. Součástí by ale nikdy neměly být žádné informace navíc, například datum narození, ale je pochybné informace zpracovávat v případě, že si zákazník zboží vyzvedne osobně, v tom případě pak není nutné údaje zpracovávat. [1]

Osobní údaje také máme právo zpracovávat bez souhlasu tehdy, jeli to nutné pro vyřízení právních povinností. Jedná se zejména o případy, kdy zákon ukládá povinnost, uchovávat paragony a faktury obsahující jména zákazníků. [1]

Dalším důvodem, pro zpracování osobních údajů bez souhlasu, jsou tzv. oprávněné zájmy správce. Jedná se o případ, kdy jste poskytnul nějakému zákazníkovi službu, a on vás nezplatí. Zákazníka hodláte dát k soudu, a čili je jasné, že údaje nebudete mazat, protože je budete ještě potřebovat. Při odvolávání se na oprávněné zájmy správce musíte vždy postupovat opatrně a vždy posuzovat, zda v konkrétním případě nad vašimi zájmy správce nepřevažují zájmy nebo základní práva a svobody subjektu údajů. [1]

Jestliže jsou osobní údaje zpracovávány na základě jiného důvodu než souhlasu, je nutné subjekt dopředu informovat o povinných náležitostech, za jakým účelem budou údaje zpracovávány, a na jaké právní zásadě tak bude učiněno. V praxi to můžete implementovat obdobně jako výše popsany souhlas, jen namísto „Souhlasím se zpracováním osobních údajů (s odkazem na celý text souhlasu)“ budete zákazník potvrzovat „Beru na vědomí informace o zpracování osobních údajů (s odkazem na celou informaci)“. Pokud se zpracovávají údaje,

v rámci objednávky, máme od zákazníka jeho osobní údaje, které nám poskytne dobrovolně. Je potom na místě, aby zákazník zpracování informací vzal na vědomí. A se zpracováním souhlasil. Nicméně tyto dvě fáze nemůžeme spojit do jedné. Pokud neudělí souhlas k druhé fázi, údaje nemohou být zpracovány, pouze bude vyřízena objednávka. [1]

2.1.17 Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti

V souvislosti s nabídkou informačních služeb přímo dítěti, je zpracování údajů o dítěti zákonné pouze v případě, pokud je dítě starší 16 let. Pokud je dítě mladší 16 let, je zpracování zákonné pouze do takové míry, pokud byl souhlas se zpracováním osobních údajů schválen nebo vydán osobou, která za dítě zodpovídá. Členské státy mohou pro tyto právní účely stanovit nižší věk, ne však nižší 13 let. Správce by měl v takovýchto případech vyvinout přiměřenou technologii pro ověření případů, při nichž byl souhlas vydán či schválen osobou, která za dítě zodpovídá. [16]

2.1.18 Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci. [16]

2.1.19 Zpracování osobních údajů zveřejněných na internetu

V některých případech musí subjekt snést i zveřejňování osobních údajů na internetu, a to například ve veřejném rejstříku, tím je dán i účel, za kterým jsou tyto údaje zveřejňovány, jedná se například o publicitu, podnikání, veřejný katastr nemovitostí apod. Tyto případy jsou dány ze zákona. To, že je zveřejnění dané ze zákona ale neznamená, že údaje můžeme dál předávat a zpracovávat. [34]

Dalším situací zveřejňování osobních údajů na internetu je taková situace, kdy subjekty dobrovolně sdílejí a zveřejňují informace. Tyto údaje nelze dál zpracovávat a zveřejňovat i přesto, že byly zveřejněny dobrovolně. Veřejnost údajů nikdy a priori neznamená možnost jejich dalšího bezmezného zpracovávání. [34]

Fyzická osoba má práva vznést námitku proti zpracování osobních údajů a požádat firmu, společnost či organizaci o ukončení zveřejňování a zpracovávání údajů, pokud jsou zpracovány pro:

- účely vědeckého přímého marketingu,
- účely vědeckého nebo historického výzkumu a statistických údajů,
- vlastní oprávněné zájmy nebo při provádění úkolu ve veřejném výkonu nebo zájmu veřejné moci. [15]

Pokud vznesete námitku proti přímému marketingu, společnost musí přestat používat vaše osobní údaje a vyhovět vaší žádosti, aniž by žádala poplatek. [15]

Společnost/organizace však může nadále zpracovávat vaše osobní údaje i přes vaše námitky, pokud:

- v případě zpracovávání pro účely vědeckého/historického výzkumu a statistiky je zpracovávání nezbytné pro splnění úkolu provedeného ve veřejném zájmu,
- v případě zpracovávání na základě oprávněných zájmů nebo při splnění úkolu provedeného ve veřejném zájmu / při výkonu veřejné moci může společnost/organizace prokázat, že má závažné oprávněné důvody, které převažují nad vašimi zájmy, právy a svobodami. Proto je nutné najít rovnováhu. [15]

Společnost by vás měla informovat o vašem právu vznést námitku, když vás poprvé kontaktuje. Například při koupi lístků na koncert. Poté, co jsou lístky koupeny, je osoba obtěžována každou reklamou, či upoutávkou na další koncerty. V takovém případě osoba může kontaktovat online prodejce o tom, že žádné reklamy dostávat nechce. Společnost by po takovéto žádosti měla přestat zpracovávat osobní údaje, neměla by posílat emaily, a také by si za tuto službu neměla nic účtovat. [15]

2.1.20 Předávání osobních údajů do jiných zemí

V rámci Evropské údaje platí zásada, že volný pohyb osobních údajů není v souvislosti se zpracováním osobních údajů omezen ani zakázán. Ovšem neznamená to za právní důvod k sdílení osobních údajů jakémukoli správci. Možnost předávat osobní údaje bez omezení v Evropské unii se týká institucionálního zabezpečení, tedy je vyjádřeno to, že v zemích Evropské unie platí stejný vysoký standard právního rámce ochrany osobních údajů při jejich zpracování a není tak nutné dodatečně zajišťovat jejich institucionální bezpečnost. Pokud chce správce osobní údaje předat jinému správci, musí mít právní důvod, protože i předání je činnost o zpracování. Právní důvod má správce tehdy, pokud předává osobní údaje mimo země EU.

Nicméně musí být splněny podmínky pro předání osobních údajů z pohledu institucionálního zabezpečení. Nařízení o ochraně osobních údajů platí v zemích jako je Island, Norsko, Lichtenštejnsko, a proto je potřeba i na tyto země pohlížet jako na země EU [26].

Pokud správce chce předat jinému správci osobní údaje do země mimo Evropskou unii, musí být zajištěna jejich institucionální ochrana, tj. nelze (až na výjimky) předávat osobní údaje do zemí, kde není zajištěna dostatečná právní ochrana osobních údajů, resp. správce nepřijal instrumenty, které tuto ochranu při předávání zajistí. [26]

Možnosti předávání:

- založené na rozhodnutí o odpovídající ochraně,
- založené na vhodných zárukách,
- o závazná podniková pravidla,
- o standardní smluvní doložky,
- výjimky pro specifické situace, kdy nelze aplikovat jeden ze dvou shora uvedených bodů.

Komise může rozhodnout, že jedna země zaštituje odpovídající ochranu osobních údajů, potom se nevyžaduje zvláštní povolení a pro předávání osobních údajů nejsou kladeny žádné administrativní překážky [26].

Pokud komise nevydá rozhodnutí o úrovni ochrany osobních údajů v dané zemi, údaje mohou být poskytnuty třetí zemi, pokud správce, který data přijímá, poskytne vhodné záruky a v případě, že jsou k dispozici vymahatelná práva subjektu údajů. Vhodným prostředkem pro vymáhání je například závazná podniková pravidla a standardní smluvní doložky [26].

2.1.21 Sankce a pokuty

Pokuty se ukládají na základě okolností každého jednotlivého případu. Ukládání sankcí a pokut musí být účinné, přiměřené a zejména odrazující. Podstatné je, že ne za každé porušení musí být udělena sankce či pokuta, ale správce, který nařízení poruší, může dostat napomenutí, anebo může dostat nařízeno, aby vyhověl žádosti od subjektu údajů. Výše pokut je rozdělena do dvou skupin, dle porušení, jakého se správce dopustí. [26]

Výše pokuty může být:

- Do výše 10 000 000 eur (nebo až do 2 % celkového celosvětového obratu, jde-li o podnik)
- Do výše 20 000 000 eur (nebo až do 4 % celkového celosvětového obratu, jde-li o podnik)

Tyto dvě skupiny se liší zejména dle závažnosti prohrěšení správce. Do nižší sazby spadá například porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, zatímco do vyšší sazby jsou zahrnuta například porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů, podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů [26].

2.2 Obecné dopady na Veřejnou správu

Ve veřejné správě, na základně stanoviska pracovní skupiny WP 29, je souhlas pro zpracování osobních údajů, jako důvod daný zákonem, skoro vyloučen, a to proto, že postavení veřejné správy a občanů je v nerovnosti. Pokud by se jednalo o případ, kdy orgán veřejné moci nevystupuje ve svém nejvyšším postavením, je zpracování na základě souhlasu možné. Například pokud obec nabídne služby internetového připojení, nicméně i zde lze zpracování založit na důvodu plnění smlouvy. Nejpodstatnější změnou pro veřejnou právu tedy bylo to, že musí mít svého pověřence. Institut pověřence pro ochranu osobních údajů je v České republice něčím novým. [14]

GDPR má také dopady do informačních systémů veřejné správy. Velikost dopadu je závislá na rozsahu zpracovávané agendy. Největší dopad to proto má na centrální rejstříky. Například katastr nemovitostí, které prováděl Český úřad zeměměřický a katastrální a to tam, že odstranil osobní údaje z dat poskytovaných ve výměnném formátu ISKN. [14]

2.2.1 Změny v základních registrech

V největším množství se osobní údaje zpracovávají v systémech základních registrů. V jiných informačních systémech se zpracovává jen určitý výběr fyzických osob, nicméně základní registr obyvatel obsahuje všechny údaje o všech občanech České republiky. O cizincích, kteří mají trvalý pobyt v České republice, a i o dalších občanech, kteří mají přidělen agendový identifikátor, anebo kterým to stanoví zákon. Protože jde jednoznačně o největší databázi s osobními údaji ve veřejné správě, muselo být toto zpracování patřičně zabezpečeno.

Po technické stránce je ochrana osobních údajů v základních registrech zajištěna zejména systémem agendových identifikátorů fyzické osoby, což je přímo ukázkové využití pseudonymizace popsané v GDPR. Aby toto rozdělení ale skutečně fungovalo a vedlo k adekvátní ochraně osobních údajů, musí být správně vydefinovány jednotlivé agendy, tedy účely, pro které jsou referenční údaje ze základních registrů využívány. [14]

V souvislosti se zavedením GDPR provedl nejspíše každý orgán veřejné správy analýzu rizik. Nicméně v oblasti definic agend v základních registrech to bylo nejspíše podceněno. ÚOOÚ provedlo šetření. Výsledkem šetření je, že nastavení přístupů pro oprávněné subjekty a jejich rozsah neodpovídá požadavkům ochrany osobních údajů. Zkvalitnění vyžaduje rozsáhlou koordinaci napříč ministerstvy a dalšími centrálními orgány státní správy. Proto přišly následující opatření. Každý orgán veřejné moci musí při každém dotazu do základních registrů tento rozsah znovu specifikovat, a to vždy podle úkonu, pro který chce data čerpat, a také zákonného zmocnění tyto data použít. Uvedený postup jednoznačně zajistí větší míru ochrany osobních údajů v základních registrech, ale poměrně významným způsobem degraduje smysluplnost aktuálních definic agend v základním registru práv a povinnosti. [14]

2.2.2 Změny v Katastru nemovitostí

Katastr nemovitostí je soubor údajů o nemovitostech v České republice zahrnující jejich soupis a popis a jejich geometrické a polohové určení. Jeho součástí je evidence vlastnických a jiných věcných práv a dalších, zákonem stanovených, práv k těmto nemovitostem. Katastr nemovitostí obsahuje řadu důležitých údajů o pozemcích a vybraných stavbách a o jejich vlastnících. Jde o zdroj informací, které mají za úkol ochránit práva k nemovitostem zejména pro daňové a poplatkové účely, taktéž slouží pro ochranu životního prostředí, zemědělského a lesního půdního fondu, nerostného bohatství a v neposlední řadě pro tvorbu dalších informačních systémů. [31]

Pro informace o tom, jaké změny byly potřeba provést v informačních systémech v Katastru jsem vznesla dotaz na samotný Katastr nemovitostí. Informace o změnách jsou zpracovány zde: Nejvýznamnější úpravy informačního systému katastru nemovitostí (ISKN) v návaznosti na GDPR souvisely s přijetím novely vyhlášky č. 358/2013 Sb., o poskytování údajů, která s účinností od 1. 1. 2019

- upravila oddělení osobních údajů od ostatních údajů obsažených ve výměnném formátu katastru prostřednictvím pseudonymizace,
- nastavila jednoznačná, snadno kontrolovatelná pravidla pro šíření údajů katastru
- stanovila konkrétní povinnosti při prokázání totožnosti uživatelů dálkového přístupu.

Úpravy ISKN byly instalovány v závěru roku 2018 a organizačně byl zaveden systém pravidelných kontrol, umožňující detekovat případné porušení nově nastavených pravidel.

Dále byly provedeny úpravy ISKN umožňující:

- přehlednou evidenci a vyhledání příjemců údajů ve smyslu § 52 odst. 5 katastrálního zákona,
- zajištění přístupu subjektu údajů k osobním údajům ve smyslu čl. 15 GDPR a
- rozšířené logování u výstupů, u kterých je na základě § 52 katastrálního zákona stanovena povinnost zjišťovat totožnost příjemce (údaje z přehledu vlastnictví z území České republiky a ze sbírky listin), resp. výstupů se srovnatelným obsahem. Logování bylo rovněž zavedeno pro případy, kdy se při nejednoznačném zadání zobrazuje více osob.

V oblasti spisové služby byly provedeny úpravy související s vedením jmenného rejstříku a dále byla v rámci elektronického systému spisové služby vytvořena zvláštní funkcionality umožňující evidenci a aktualizaci záznamů o činnostech zpracování.

Ve vztahu k vedení základního registru územní identifikace, adres a nemovitostí žádné úpravy prováděny nebyly, neboť tento informační systém veřejné správy s osobními údaji nepracuje.

3 PŘÍPADOVÁ STUDIE – IMPLEMENTACE GDPR V OBCI BĚSTVINA

Případová studie je zaměřena na porovnání teorie a praxe zavedení GDPR v České republice. Kritickým pohledem pojednává o zavedení směrnice. Součástí případové studie je také dotazník, který se zkoumá, jak občané znají GDPR. Dále se zabývá implementací GDPR v obci Běstvina. Zkoumá, jak byl úřad zasažen, finance, které na to byly vynaloženy. Pro obec byla vypracována analýza rizik. Taktéž je zpracována metoda Best practice, neboli dobrá praxe, a metoda case practise.

3.1 Obec Běstvina

Pro analýzu GDPR v rámci veřejné správy byla vybrána obec Běstvina. Běstvina leží na jižním úpatí Železných hor. Vznik vesnice je spojen s Liběckou stezkou a byzantskou kulturou. Existence této zemské stezky navazující na Zlatou stezku je doložena nálezy římských mincí. [10]

Území obce se rozkládá na ploše 1407 ha. Součástí obce jsou místní části: Spačice, Rostejn, Pařížov a Vestec. V obci žije celkem 524 obyvatel. Je zde obecní úřad, pošta, potraviny, školka, zdravotní středisko, kominiectví, malířství a natěračé, slévárnu barevných kovů, stavební podnik a dále. Jednu čtvrtinu obce pokrývají lesy. [10]

3.1.1 Situace v obci

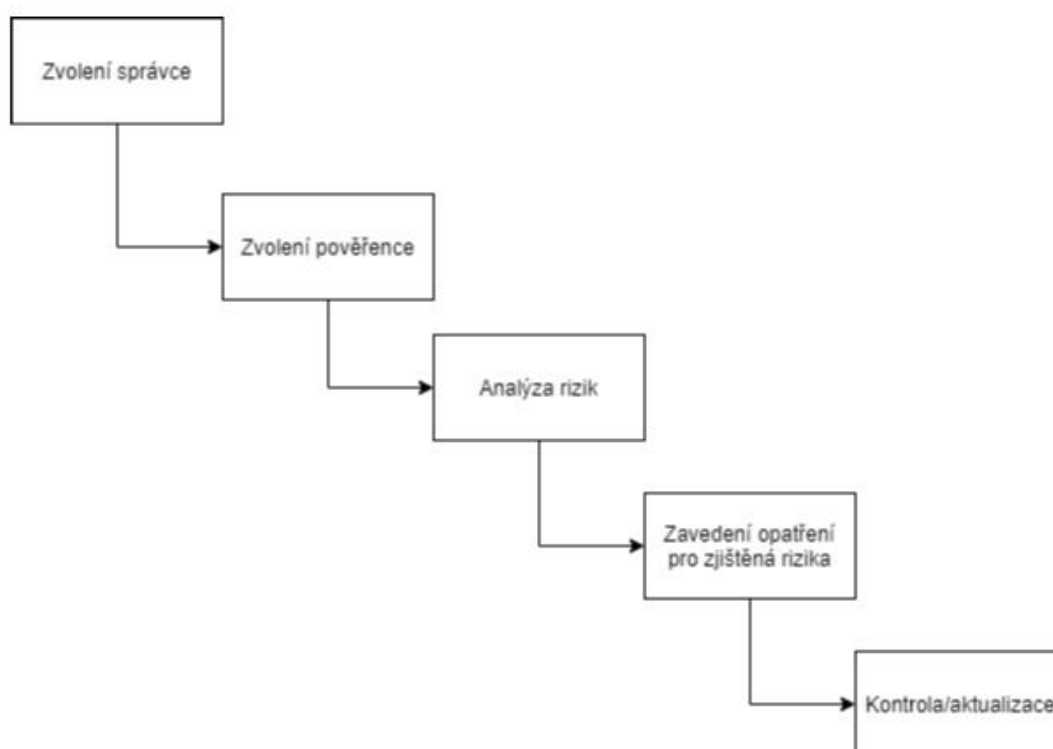
Každá obec musí mít svého správce a pověřence GDPR. V Obci Běstvina je správcem sama paní starostka, Ing. Marie Brožková, a pověřencem pro obec byla zvolena členka zastupitelstva, paní Ing. Zdena Brožková, ale to až po roce. Nejprve byla pověřencem obce paní Kateřina Korejtková. Paní Korejtková se ochranou osobních údajů zabývá již několik let a má proto dlouholetou praxi a velké znalosti.

3.1.2 Implementace GDPR do obce Běstvina

Situace ohledně zavedení nové legislativy byla dosti medializována. Obci se ozvalo velké množství firem, které jim za sta tisíce nabízeli své pověřence a služby, které nebyly potřeba. Nicméně pro obec jako takovou se příchodem legislativy v důsledku nic nezměnilo, protože ani před novou legislativou nebylo možné zveřejňovat osobní údaje občanů, nechávat nezabezpečený úřad apod.

Kroky implementace:

- zvolení správce,
- zvolení pověřence,
- analýza rizik,
- zavedení opatření pro zjištěná rizika,
- pravidelné revize analýzy rizik.



Obrázek 3: Implementace GDPR na OÚ

Zdroj: Vlastní zpracování

Zvolení správce:

Správce je zvolena osoba, která určuje zpracování osobních údajů a primárně zpracovává osobní údaje. Správce a pověřenec nemůže být tatáž osoba, protože není možné, aby kontroloval sám sebe. Správce je v podstatě obec Běstvína a starostka zastupuje tento subjekt. Nikdo neurčuje, že správcem musí být starostka, ale vychází to z titulu funkce. Denně pracuje s údaji a taktéž je zpracovává, komunikuje s občany, a má dohled nad chodem obce.

Má povinnost zveřejňovat na úřední desku informace o koupi, či prodeji nemovitosti, pozemků, důležité akce (např. sběr nebezpečného odpadu) a jiné. Správce má tedy primárně za úkol chránit osobní údaje všech občanů, zodpovídá za správné zpracování, a také za to, aby osobní údaje nebyly odcizeny a zneužity třetí stranou.

Paní starostka se z vlastní iniciativy zúčastnila v roce 2018 školení pro obce. Školení bylo zorganizováno zdarma, v rámci MAS – místní akční skupina Železných hor. Ze zákona, po správci, nejsou požadovány žádné speciální školení či kurzy o GDPR. Hlavním cílem tohoto kurzu bylo podat úřadům informace o zavedení GDPR na obecní úřady a ujistit je, že nemusejí dělat drastické opatření a najímat si pověřence za desítky tisíc korun.

Zvolení pověřence:

Pověřencem obce se stala nejprve paní Kateřina Korejtková, jako externista. Paní Korejtková se obci sama nabídla, protože v rámci MAS Železné hory poskytovala poradenství a pověření v jednom nejen pro obce, ale i pro školy v okolí města Třemošnice. Úkolem pověřence na obci Běstvina je tedy zanalyzovat situaci, doporučit opatření, která by měla obec provést. V případě, že dojde k porušení ochrany osobních údajů, zastupuje obec pověřenec a řeší porušení s ÚOOÚ. Paní Korejtkové úřad zaplatil jednorázovou částku 3000 Kč a pokud by vyvstal nějaký problém nad rámec (např. zveřejnění fotky na obecním webu bez souhlasu občana), za každou hodinu je vyúčtováno 350 Kč/h. Po zavedení základních opatření, byla zastupitelstvem zvolena členka zastupitelstva paní Ing. Zdena Brožková, která má s úřadem uzavřenou dohodu o provedení práce na 3000 Kč/měsíc.

Analýza rizik:

Obecní úřad musí vést záznam o činnosti. Nicméně není k dispozici žádný platný vzor, kterého by se měla obec řídit. Proto jsem v rámci případové studie zpracovala analýzu rizik pro obec Běstvina. Podrobněji se můžete o analýze rizik dočíst v kapitole 2.1.3. Analýza rizik. Analýzu rizik vytváří pro obecní úřad pověřenec. Analýza je zpracována proto, aby obec věděla, kam všude GDPR zasáhne, kde jsou potřeba provést opatření a na co nezapomenout. Hlavní součástí analýzy je odhalit budoucí hrozby. Tuto analýzu správce a pověřencem aktualizují a revidují každý rok.

Zavedení opatření pro zjištěná rizika:

Po vypracování analýzy rizik přicházejí na řadu již samotná opatření vyplývající z povinnosti legislativy. Každý úřad podniká jiné opatření v závislosti na účelu zpracování. Záleží na velikosti obce, jaké evidence úřad používá, a jak měla obec doposud zabezpečené archivy. V reálné situaci obec Běstvina nemusela zavádět drastická opatření, protože i před zavedením

legislativy, byla povinna dodržovat zásady zpracování dle platného zákona č. 101/2000 Sb., o ochraně osobních údajů.

Provedená opatření:

- zabezpečení webových stránek,
- zajištění přístupů do PC,
- lepší zabezpečení OÚ.

Pravidelné revize analýzy rizik:

Každý rok správce a pověřenec revidují analýzu rizik. Kontrolují, zda nebyla provedena nějaká změna a není tak potřeba aktualizovat analýzu rizik.

3.1.3 Analýza rizik

V rámci případové studie jsem vytvořila pro obecní úřad analýzu rizik. Definovala jsem povinnosti správce, oblast analýzy rizik a formu analýzy rizik.

Povinnosti správce v obci Běstvina:

- Vedení záznamů o činnosti: jméno a kontakt správce a pověřence, účel zpracování, popis kategorie osobních údajů, případně lhůty na výmaz, popis technických a organizačních opatření, kategorie příjemců, komu budou osobní údaje zpřístupněny.
- Posouzení vlivu na ochranu osobních údajů (při zvyšovaném riziku), shromažďování citlivých údajů či monitorování veřejných prostor kamerovým systémem. Správce si vyžádá posudek pověřence.
- Při zvýšeném riziku nakládání s údaji si správce požádá o konzultaci dozorový orgán (ÚOOÚ).
- Ohlašování porušení zabezpečení osobních údajů (správce nahlašuje ÚOOÚ do 72 hodin).
- Ohlašování porušení zabezpečení osobních údajů subjektu údajů (osobě).

Ohlášení obsahuje:

- jméno a kontakt pověřence,
- popis povahy daného případu, kategorii a počet dotčených subjektů,
- popis pravděpodobných důsledků porušení zabezpečení,
- popis opatření, které správce přijal s cílem vyřešit dané porušení.

Oblast analýzy rizik:

- nastavení kompetencí
- zabezpečení osobních údajů
- evidence dokumentů

Formy analýzy rizik:

- zpracování po oblastech agent, na základě samostatné působnosti dle zákona č. 128/2000 Sb. o obcích
- zpracována po oblastech činností obce mimo působení zákonů v platném znění

Každou z agend lze dále rozpracovat do karty jednotlivých procesů dle specifických potřeb, pravidla k ochraně osobních údajů mohou být stanovena vnitřními předpisy (organizační řád, pracovní řád, spisový a skartační řád)

Zpracovaná analýzu rizik pro obec Běstvína je vyobrazena v tabulce č. jedna.

Účel zpracování	Forma zpracování	Druh osobních údajů	Citlivé údaje ANO/NE	Subjekt, kterého se zpracování týká	Technické zabezpečení	Zpracování dat externí/interní	Osoba nakládající s údaji	Riziko ANO/NE
Zákon o obcích	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, r.č., trvalé bydliště, datová schránka	NE	Občan, zaměstnanec, volený zástupce	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Starostí, účetní	NE
Účetnictví	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, trvalé bydliště, sídlo podnikání, datová schránka, IČO/DIČ, bankovní spojení, podpis	NE	Občan, zaměstnanec, volený zástupce, smluvní strana	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní/Externí	Starosta, místostarosta, účetní	NE
Zaměstnanecká agenda	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, e-mail, telefon, místo narození, stát narození, státní příslušnost, místo pobytu, zdravotní pojišťovna, bankovní spojení, rodné příjmení, předchozí zaměstnavatel, stav, rodinný příslušník, děti, doklady o vzdělání, doklady o důchodu, osobní spis, platový výměr, výpis z rejstříku trestů, zdravotní prohlídka, invalidita, zdravotní znevýhodnění, žádost o příspěvky,	ANO	Zaměstnanec	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Starosta, místostarosta, účetní	NE

		potvrzení o pracovní neschopnosti, prohlášení poplatníka k dani z příjmu ze závislé činnosti, podpis, údaje o zdravotním stavu, osobní spis.						
Střed zájmů	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, r.č., trvalé bydliště, datová schránka	NE	Občan, zaměstnanec, volný zástup	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Starosta, zaměstnanec úřadu	NE
Správní řízení	Elektronicky, fyzicky	Jméno, příjmení, adresa, bydliště, datum narození, IČO, číslo bankovního účtu	NE	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu	NE
Czech Point	Elektronicky, fyzicky	Jméno, příjmení, datum narození, rodné číslo, místo narození, rodné příjmení, trvalé bydliště, číslo dokladu totožnosti, podpis	NE	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu	NE

Evidence obyvatel	Elektronicky, fyzicky	Jméno, příjmení, datum narození, místo narození, rodné číslo, trvalé bydliště, doručovací adresa, předchozí pobyt, číslo OP, omezení způsobilosti, údaje o opatrovníkovi, oprávněná osoba, podpis	NE	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu	NE
Místní poplatky	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, datová schránka, místo pobytu, průkaz totožnosti, bankovní spojení, výměry důchodů, kopie průkazu ZTP, TP	ANO	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu, starosta	NE
Poskytování informací	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, trvalé bydliště, e-mail, datová schránka, podpis, rasový či etnický původ, politické názory, náboženské vyznání, filozofické přesvědčení, členství v odborech, genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu, údaje o sexuálním životě, údaje o sexuální orientaci	ANO	Žadatel	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu, starosta	ANO
Spisová služba	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, místo narození, rodné číslo, trvalé bydliště	NE	Občan	Heslo do PC Klíč od archivu	Interní	zaměstnanec úřadu	NE

					Klíč od objektu OÚ			
Evidence ověřování vidimace	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, místo narození, rodné číslo, trvalé bydliště, IČO, DIČ	NE	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	zaměstnanec úřadu, starosta	NE
Vedení obecní kroniky	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, místo narození, trvalé bydliště	NE	Občan	Heslo do PC	Externí	Kronikář	NE
Volební systém	Elektronicky, fyzicky	Jméno, příjmení, datum narození, věk, trvalé bydliště, omezená svéprávnost, podpis, údaje o zdravotním stavu	ANO	Občan, volený zástupce	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu, starosta	ANO
Povolení ke kácení	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, rodné číslo, trvalé bydliště, datová schránka	NE	Občan	Heslo do PC Klíč od archivu Klíč od objektu OÚ	Interní	Starosta	NE
Pronájmy obecních prostor	Elektronicky, fyzicky	Jméno, příjmení, titul, datum narození, místo narození, rodné číslo, trvalé bydliště, místo pobytu, typ místa pobytu, státní příslušnost, e-mail, telefon, datová schránka, zaměstnavatel, výše příjmu, osoby sdílející společnou domácnost, nesvéprávnost, insolvence, tav, příbuzenský vztah, průkaz totožnosti, žádost o	ANO	Občan	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu, zastupitelé obce	NE

		nájem, podpis, údaje o zdravotním stavu						
Hřbitovní poplatky	Elektronicky, fyzicky	Jméno, příjmení, rodné číslo, trvalé bydliště, číslo hrobu, podpis	NE	Občan	Heslo do PC (každý vlastní) Klíč od archivu Klíč od objektu OÚ	Interní	Zaměstnanec úřadu, starosta	NE
Společenské a propagační akce	Elektronicky, fyzicky	Jméno, příjmení, datum narození, trvalé bydliště, fotografie	NE	Občan	Heslo do PC	Externí	Starosta, zaměstnanec	ANO

Tabulka 1: Analýza rizik

Zdroj: Vlastní zpracování

V následující tabulce je vyobrazené, které zákony ovlivňují účel zpracování. Pro lepší přehled jsou zákony a záznamy o činnostech v samostatné tabulce.

Účel zpracování	Podléhající zákonu
Zákon o obcích	128/2000 Sb. - Zákon o obcích
Účetnictví	128/2000 Sb. - Zákon o obcích, 563/1991 Sb. - Zákon o účetnictví, 235/2004 Sb. - Zákon o dani z přidané hodnoty, 250/2000 Sb. - Zákon o rozpočtových pravidlech územních rozpočtů, 219/2000 Sb. - Zákon o majetku ČR a jejím vystupování v právních vztazích, 220/2013 Sb. Vyhláška o požadavcích na schvalování účetních závěrek některých vybraných účetních jednotek
Zaměstnanecká agenda	262/2006 Sb. - Zákoník práce, 435/2004 Sb. - Zákon o zaměstnanosti, 251/2005 Sb. - Zákon o inspekci prací, 312/2002 Sb. - Zákon o úředních uzemní samosprávných celků, 341/2017 Sb. - Nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě 222/2010 Sb. - Nařízení vlády o katalogu prací ve veřejných službách a správě, 586/1992 Sb. - Zákon o daních z příjmu, 187/2006 Sb. - Zákon o nemocenském pojištění, 120/2001 Sb. - Exekuční řád, 182/2006 Sb. - Insolvenční zákon, 582/1991 Sb. - Zákon o organizaci a provádění sociálního zabezpečení, 589/1992 Sb. - Zákon o pojistném na sociální zabezpečení a příspěvků na státní politiku zaměstnanosti, 155/1995 Sb. - Zákon o důchodovém pojištění, 37/2003 Sb. - Nařízení vlády o odměnách za výkon funkce členům zastupitelstev, 592/1992 Sb. - Zákon o pojistném na všeobecné zdravotní pojištění, 128/2000 Sb. - Zákon o obcích
Střed zájmů	159/2006 Sb. - Zákon o střetu zájmů

Správní řízení	563/1991 Sb. - Zákon o účetnictví
Czech Point	128/2000 Sb. - Zákon o obcích, 361/200 Sb. - Zákon o provozu pozemních komunikací a o změnách některých zákonů, 247/2000 Sb. - Zákon o získávání odborné způsobilosti k řízení motorových vozidel a o změnách některých zákonů, 500/2004 Sb. - správní řád, 269/1994 Sb. - Zákon o Rejstříku trestů, 256/2013 Sb. - Zákon o katastru nemovitostí (katastrální zákon), 133/2000 Sb. - Zákon o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), 300/2008 Sb. - Zákon o elektronických úkonech a autorizované konverzi dokumentů, 365/2000 Sb. - Zákon o informačních systémech veřejné správy, 364/2009 Sb. - Vyhláška o kontaktních místech veřejné správy, 192/2009 Sb. - Vyhláška o stanovení podrobností provádění autorizované konverze dokumentů, 634/2004 Sb. - Zákon o správních poplatcích, 561/2004 Sb. - Školský zákon
Evidence obyvatel	111/2009 Sb. - Zákon o základních registrech, 133/2000 Sb. - Zákon o evidenci obyvatel, 296/2004 Sb. - Vyhláška, kterou se provádí zákon o evidenci obyvatel, 500/2004 Sb. Správní řád, 634/2004 Sb. - Zákon o správních poplatcích, 561/2004 Sb. - Školský zákon
Místní poplatky	565/1990Sb. - Zákon o místních poplatcích, 280/2009 Sb. - Daňový řád, 634/2004 Sb. - Zákon o správních poplatcích, 128/2000 Sb. - Zákon o obcích, 182/2006 Sb. - Insolvenční zákon
Poskytování informací	106/1999 Sb. - Zákon o svobodném přístupu k informacím
Spisová služba	499/2004 Sb. - Zákon o archivnictví a spisové službě a o změně některých zákonů

Evidence ověřování vidimace	21/2006 Sb. - Zákon o ověřování
Vedení obecní kroniky	132/2006 Sb. - Zákon o kronikách obcí
Volební systém	130/2000 Sb. - Zákon o volbách do zastupitelstev krajů, 491/2001 Sb. - Zákon o volbách do zastupitelstev obcí, 247/1995 Sb. - Zákon o volbách do Parlamentu České republiky, 62/2003 Sb. - Zákon o volbách do Evropského parlamentu, 275/2012 Sb. - Zákon o volbě prezidenta republiky, 22/2004 Sb. - Zákon o místním referendu, 1/1993 Sb. - Ústava České republiky 2/1993 Sb. - Listina základních práv a svobod, 128/2000 Sb. - Zákon o obcích
Povolání ke kácení	114/1992 Sb. - Zákon o ochraně přírody a krajiny, 175/2006 Sb. - Vyhláška, kterou provádějí některá ustanovení zákona o ochraně přírody a krajiny
Pronájmy obecních prostor	128/2000 Sb. - Zákon o obcích, 89/2012 Sb. - Občanský zákoník, 563/1991 Sb. - Zákon o účetnictví
Hřbitovní poplatky	128/2000 Sb. - Zákon o obcích, 256/2001 Sb. - Zákon o pohřebnictví
Společenské a propagační akce	Souhlas, ke konkrétnímu účelu

Tabulka 2: Analýza rizik-zákony

Zdroj: Vlastní šetření

Při tvorbě analýzy rizik jsem zvažovala i to, kde hrozí riziko, viz tabulka jedna, poslední sloupec. Jak víme z projektového managementu, při každé činnosti hrozí riziko. Je již na osobě, která analýzu vytváří, jak velké riziko musí hrozit, aby se zpracovatel analýzy rozhodl, že tato část je opravdu riziková.

Ve své analýze rizik jsem stanovila možné riziko u tří položek analýzy.

Poskytování informací

V případě poskytování informací se jedná o riziko. Občan se dostaví na obecní úřad, a bude chtít sdělit na základě Zákonu 106/1999 Sb. O svobodném přístupu k informacím, informaci o tom, kdo vykonával stavbu osvětlení v obci. Obec je povinna mu tuto informaci sdělit, nicméně tím předává povinnost o dodržení ochrany osobních údajů osobě, které informace poskytuje. Pokud by bylo pak informací zneužito, problém již nejde za obecním úřadem, ale za právě zmiňovanou třetí osobou. Jisté riziko úniku informací zde tedy je.

Volební systém

I přesto, že je volební komise proškolená, a ví, že by nikde neměli vynášet informace o občanech, které zjistí například z občanského průkazu, nebo z výpisu z evidence obyvatel, jisté riziko zde je. V obci Běstvína jsou v komisi občané obce, kteří se dobře znají. Riziko spočívá v tom, že by mohl člen komise zjistit, že má pan Novák za týden narozeniny, a bude mu padesát let. Tuto informaci by sdělil v místním obchodu prodavači, a ten by tuto informaci poskytl dál, až by se dostala k panu Novákovi. Pan Novák by tuto událost následně mohl nahlásit jako porušení ochrany jeho osobních údajů a musel by tuto aktivitu projednávat ÚOOÚ.

Společenské a propagační akce

Je patrné, že společenské akce jsou taktéž rizikovou částí. V obci se bude konat oslava výročí založení sboru dobrovolných hasičů. Akce se koná pod záštitou obce, je veřejná, ale budou se na ní pořizovat fotografie a kamerový záznam. Od všech občanů, kteří budou vyfoceni nebo natočeni na kameru, by měla obec získat souhlas o fotografování a zveřejňování záznamů. I kdyby byl jeden občan zachycen pouze z části a obec by fotku zveřejnila, může tuto událost občan napadnout s tím, že je to jeho porušování osobních údajů a taktéž by mohl tuto činnost nahlásit úřadu pro ochranu osobních údajů.

Následně jsem uvedla další aktivity, kde by mohlo dojít k porušení GDPR.

Vítání občánek

Pokud se v obci narodí nový občan, rodiče jsou povinni tuto událost nahlásit na OÚ. V Běstvíně probíhá vítání občánek jednou za rok. Paní starostka se tedy podívá do evidence obyvatel

a zjistí, kterých nově narozených dětí se vítání občánků týká. Z pozice paní starostky má právo na to, tyto osobní údaje zjistit a tyto údaje nesmí nikde nezveřejňovat. Paní starosta poté rozešle pozvánky všem, kteří jsou zváni, kdy součástí pozvánky je i oznámení, že tato akce bude focena do Běstvinské kroniky, a pokud nechtějí, ať udělí nesouhlas o fotografování.

Podobným případem je i gratulování jubilantům obce. Občan může udělit nesouhlas o gratulování. V některých obcích vyvěšují gratulace na webové stránky. V Běstvině se tyto údaje nezveřejňují.

Hromadné zasílání SMS občanům

Dalším případem je hromadné rozesílání SMS s obecním hlášením. Tuto službu si občané mohli bezplatně objednat u paní starostky, kdy každý občan dobrovolně dal své telefonní číslo paní starostce s tím, že číslo nebude zneužito a bude sloužit pouze pro účely rozesílání informačních SMS. Tato služba je zřízena pomocí internetové stránky www.rozhlaspobce.cz, kde je i uložená zmiňovaná databáze telefonních čísel. Paní starostka obce je na těchto stránkách zaregistrována, a pokud se chce přihlásit musí zadat odolné heslo, které obsahuje malá a velká písmena, číslo a také speciální znak. Tato služba fungovala i před zavedením nové legislativy. Po zavedení GDPR byla obec ujistěna zřizovatelem stránek o dostatečné bezpečnosti stránek.

Kamerový systém v obci

V obci jsou nainstalovány dvě kamery. Jedna je umístěna na návsi, na vzácnou šesticípou kapličku. Druhá kamera je umístěna u kontejnerů. Kamery jsou zde umístěny pouze za účelem bezpečnostního opatření. Pokud by byla kaplička poničena, nebo by někdo vyvážel ke kontejnerům odpad, který tam nepatří, starostka může záznam předat Policii ČR. Záznam nicméně nikde veřejně vystavovat nemůže.

Zveřejňování informací na úřední desce

Spousty informací je paní starostka povinna zveřejňovat na úřední desce (např. usnesení ze zastupitelstva, prodej nemovitosti). Obec například prodává obecní pozemek fyzické osobě. Aby se tento prodej mohl uskutečnit, musí být v usnesení uvedeno jméno, příjmení a datum narození (rodné číslo starostka obce nezveřejňuje). Usnesení je součástí informací, které obec předává katastru nemovitostí, bez usnesení by to katastr nemohl zanést. Zároveň toto usnesení musí být vyvěšeno na úřední desce, dle 128/2000 Sb. Zákon o obcích, a na internetu. To znamená, že paní starostka usnesení musí upravit tak, že začerní jméno, datum narození a bydliště na usnesení tak, aby nebyly tyto údaje identifikovatelné a mohla usnesení zveřejnit. Pokud by paní Starostka opomněla nějakou informaci začernit, šlo by o porušení GDPR.

Další případ se týká exekucí či veřejných dražeb. Přes datovou schránku přijde na obecní úřad například informace o exekuci občana již s konkrétní informací o občanovi. Tato informace přichází od soudu, a požadují po obci, aby to bylo vyvěšené na úřední desce. Obecně bych čekala, že postup při zveřejňování bude stejný, jako v předchozím případě, ale opak je pravdou. Pokud se jedná o exekuci, tak to musí být zveřejněno s veškerými informacemi o občanovi, kterého se exekuce týká.

Volby

Další případnou hrozbou jsou volby. U voleb je GDPR vlastně porušováno. Komise je sice proškolená o průběhu voleb a je také seznámena o tím, že nesmí nikde vynášet žádné citlivé údaje. Nicméně stejně, každý, kdo k volbám dorazí, předá do ruky komisi občanský průkaz, kde jsou uvedeny citlivé údaje. Pokud by komisi občanský průkaz neukázal, nemůže odvolit. Jde zde o situaci, že buď musí udělit souhlas, v tomto případě se jedná tedy o ukázání občanského průkazu, anebo nemůže odvolit. Nic jiného mu tedy nezbyvá.

Komise musí taktéž zaznamenávat volební účast. U voleb jsou tedy k dispozici výpis z evidence obyvatel, kde si komise odškrtnává počet občanů, kteří odvolili. V těchto seznamech je nejen jméno a příjmení, ale také datum narození a místo bydliště. Například, Josef Novák má trvalé bydliště na obecním úřadě z důvodu, že má svou nemovitost v exekuci. Komise by tuto informaci pak mohla zneužít.

3.1.4 Rizika GDPR v souvislosti s ostatními zákony

Dodržování nové legislativy sebou nese i spoustu rizik, kterým je nutné se vyvarovat.

Návaznost zákona o zpracování osobních údajů a zákona o svobodném přístupu k informacím

Jako první bych se ráda zmínila o propojení zákona o GDPR se zákonem 106/1999 Sb. Zákon o svobodném přístupu k informacím. Na základě tohoto zákona by někdo mohl chtít účelově nacytat obecní úřad – díky tomuto zákonu je obec povinna komukoliv poskytnout informace. Občan bude chtít například poskytnout veškeré smlouvy o koupi, které byly provedeny nad hodnotu 50000 Kč. Obec, jako veřejný správce, je povinna mu tyto informace předat. Tím, že mu obec tyto informace předá, je na občana přenesená povinnost, o dodržování GDPR. Nesmí informace, nabyté ze smluv, které si vyžádal, předat třetí osobě. A na základě zákona 106/1999 Sb. by mohl občan vynést citlivé údaje.

Aby se obec ochránila, s předáváním těchto informací, musí být občanovi udělena písemná informace o tom, že se tímto stává držitelem citlivých informací a je na něj převedena

povinnosti GDPR. Pokud by údaje vynesl ven, další následné kroky by už nebyly vinou obecního úřadu ale občana.

Návaznost zákona o zpracování osobních údajů a zákona o Archivnictví

Se zákonem o ochraně osobních údajů také úzce souvisí zákon 499/2004 Sb. Zákon o archivnictví a spisové službě. Obecní úřad musí mít schválený plán archivace dokumentů. K tomuto úkonu je pověřený památkový ústav Chrudim. Tento zákon upravuje státní politiku a formu archivnictví. Obec vytvoří plán archivace a ten následně předloží ke schválení památkovému ústavu. Jedná se například o evidenci obyvatel-zrušení trvalého bydliště nebo platba popelnic. OÚ je povinen držet záznamy o platbě popelnic z důvodu dohledání, kdo popelnice nezaplatil. Protože by tyto informace nějaký subjekt mohl na základě zákona o svobodném přístupu k informacím po obecním úřadu vymáhat. Evidence jsou vedeny dvě. Jedna elektronická a jedna papírová.

Tyto informace je obec povinna archivovat deset let. Zákon 499/2004 Sb. o archivnictví říká, že tyto záznamy musí být uloženy v zamčené skříni a skříň musí být v uzamykatelné místnosti. Zaměstnanci obecního úřadu jsou povinni chovat seznam archivovaných listin, a i seznam informací, které byly po uplynutí deseti let zničeny skartací. Tyto náležitosti chodí kontrolovat z památkového ústavu.

Riziko spojené v GDPR nastává v případě, že by obec provedla skartaci smlouvy o koupi obecní nemovitosti, která obsahuje osobní údaje pana Nováka. Obec tuto smlouvu po uplynutí archivační povinnosti skartuje, nicméně neudělá záznam o zničení. :o obecním úřadu by někdo chtěl informace na základě zákona č. 106/1999 Sb. Zákon o svobodném přístupu k informacím vydat. V takovémto případě by nastal pro obec velký problém, protože neudělala záznam o zničení, a pan Novák by mohl obecní úřad obvinít, že prodala jeho osobní údaje třetí straně. Proto je potřeba správně a poctivě vést archivační listy.

OÚ Běstvina vlastní počítačový program e-spis LITE, které vyhovuje všem standardům GDPR pro archivační účely.

3.1.5 Zavedení bezpečnostních opatření

Obecné opatření

Obecní úřad Běstvína je umístěn v budově spolu s kadeřnictvím a poštou. Samotné místnosti obecního úřadu, jako je kancelář OÚ a archivační místnost, jsou zabezpečeny zámekem, od kterého vlastní klíče pouze starostka a zaměstnankyně úřadu. Dalším zabezpečením je zámek na celé budově a bezpečnostní alarm. Všechny skříně uvnitř kanceláře jsou zabezpečeny taktéž zámekem. Tyto opatření samozřejmě fungují již řadu let.

Zabezpečení počítačů

Starostka i zaměstnankyně obce mají každá svůj vlastní počítač, který by měl být zabezpečený heslem. Obě musí mít ke svému počítači unikátní heslo, a to by nemělo být nikde viditelné, napsané například na papírku na stole apod. V počítači je vedeno účetnictví, přístup do evidence obyvatel, ale také veškerá korespondence, přístupy na webové stránky obce, úřední desku, a v neposlední řadě program CZECH POINT. Jak paní starostka, tak i zaměstnankyně obce mají přístup úplně všude. Z pohledu malých obcí jsou tyto veškeré zabezpečení zbytečné právě z důvodu, že obě mají přístup všude. Další věcí, kterou je potřeba zabezpečit jsou prohlížeče používané paní starostkou a zaměstnankyní obce. Jsou zabezpečeny metodou SSL certifikátem.

SSL spojení funguje na základě asymetrické šifry. Obě strany mají dva klíče – veřejný a soukromý. Veřejné heslo je zveřejněné a musí být zajištěno předání všem, který ho hodlají používat. Díky klíči kdokoliv zašifruje zprávu a může si být jistý, že jí rozšifruje pouze ten, kdo vlastní veřejný klíč a použije ho k rozšifrování. [4]

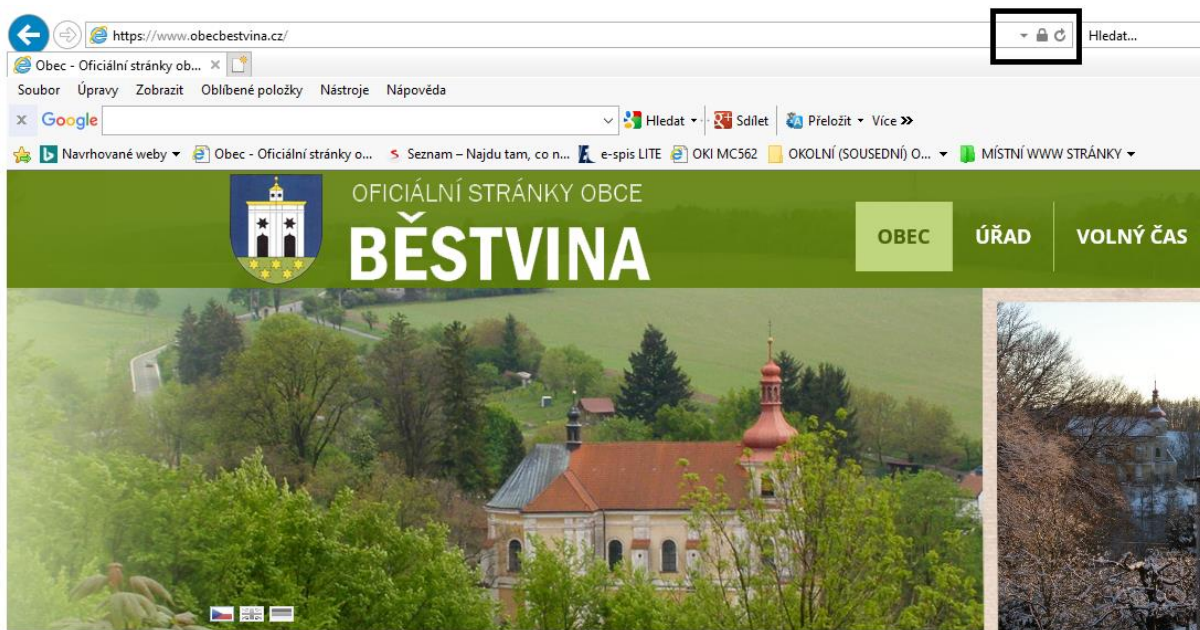
Ustanovení SSL:

- Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
- Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací, a hlavně certifikát serveru.
- Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
- Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
- Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.

- Klient a server si navzájem potvrdí, že od té chvíle bude jejich komunikace šifrovaná tímto klíčem.
- Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
- Aplikace od té chvíle dál komunikují přes šifrované spojení. Například POST požadavek na server se do této doby neodešle. [4]

Jakmile se připojíme na internet, stačí pouze otevřít prohlížeč, nebo se přihlásit do emailu, ihned se po síti posílá velké množství informací. Skrz internetový prohlížeč posílá informace uživatel (v tomto případě paní starostka) a server (obecní stránky obce). Celý obsah webových stránek a i to, co paní starostka právě na webu dělá, je součástí zmiňovaných informací, které proudí sítí. Mezi uživatelem a serverem stojí řada síťových prvků, a proto je potřeba spojení zabezpečit. Pokud by prohlížeče obce nebyly zabezpečené, mohl by se někdo přes tyto toky dostat i k paní starostce do počítače (ukrást hesla, přístupy apod). Pokud by se tak stalo, je jasné, že by mohl hacker ukrást například evidenci obyvatel, a došlo by k hrubému porušení GDPR.

Důvodem zřízení SSL certifikátu je tedy zřejmé. Kvůli ochraně osobních údajů. To, že jsou prohlížeče chráněné je poznat tak, že je na konci okénka pro zadávání URL, obrázek zámečku. Pokud tedy paní starostka komunikuje s občany, například přes emailovou adresu, je tímto certifikátem chráněn obsah a citlivé údaje by se neměly dostat mimo komunikaci paní starostky a občana. Na obrázku čtyři, je černým obdélníkem vyznačený zmiňovaný zámeček. To znamená, že počítač je web a že měl být přenos dat bezpečný.



Obrázek 4: Znak zabezpečení SSL certifikátem

Zdroj: Vlastní zpracování

3.1.6 Rozpočet spojený s GDPR v obci

Obecní úřad v rozpočtu nemá žádnou speciální položku, která by zastupovala výdaje na GDPR. Položky pro GDPR jsou proto zahrnuty v položce činnost místní obce.

Schválený rozpočet obce Běstvina pro rok 2018	VÝDAJE v tis. Kč
obsah	Schválený rozpočet 2017
ostatní neinv. Transfery nezisk, apod. org. - včelaři	3,00
správa v lesním hospodářství	100,00
vnitřní obchod	25,00
pozemní komunikace	175,00
chodníky	3065,00
pitná voda	2,00
předškolní zařízení	400,00
opravy kulturních památek	330,00
rozhlas a televize	11,00
ostatní činnosti kultury, církv., sděl. Prostř.	30,00
využití volnočasových aktivit dětí a mládeže	30,00
všeobecná ambulantní péče	87,00
bytové hospodaření	50,00
nebytové prostory	8,00
veřejné osvětlení	340,00
pohřebnictví	10,00
komunální služby a úz. Rozvoj obce	1527,00
sběr a svoz komunálního odpadu	460,00
péče o vzhled obcí a veř. Zeleň	594,70
osobní asistence, pečovatelská Služba	40,00
ostatní správa v krizovém řízení - varovné zprávy	0,20
pod. krizové řízení a nouzový plán	10,00
PO - dobrovolná část /hasiči/	234,00
zastupitelstvo obce	671,00
činnost místní správy	946,90
obec. Výdaje z finančních operací	20,00
VÝDAJE CELKEM	9169,80

Tabulka 3: Rozpočet obce Běstvina

Zdroj: [28]

V tabulce 3 jsou zobrazeny plánované výdaje obce pro rok 2018. Výdaje na GDPR jsou zahrnuty v položce činnost místní správy. Všechny položky výdajů na GDPR byly jednorázového typu.

Položky	Výdaje/Kč
Pověřenec 1	3000
Pověřenec 2	3000
Zabezpečení PC	4000
Cestovní výdaje (školení - starostka, účetní)	500
Školení - pověřenec 2	2000
Celkem	12500

Tabulka 4: Výdaje na GDPR

Zdroj: Vlastní zpracování

Celkové plánované výdaje činnosti místní správy pro rok 2018 činí 946 900 Kč, a z toho 12500 Kč plánovaných výdajů na GDPR. Celkovou částku plánovanou na výdaje spojené s GDPR jsou zobrazené v tabulce 4.

Všechny tyto výdaje jsou jednorázové. Mohlo by se ale stát, že by pověřenec musel řešit nějakou mimořádnou situaci (např. pokud by obec neoprávněně zveřejnila citlivé údaje o občanovi). Současný pověřenec GDPR v obci si pak účtuje za každou odpracovanou hodinu 200 Kč/h. Tyto mimořádné výdaje by pak opět šly z položky činnosti místní správy a bylo by to řešeno formou rozpočtového opatření.

Rozpočtové opatření je změna v rozpočtu. V listopadu 2017 zastupitelstvo obce připravuje a schvaluje rozpočet pro rok 2018. V průběhu roku 2018 se může stát, že v některé položce peníze chybí nebo naopak přebývají. Peníze je pak potřeba přesunout, kdy každou tuto změnu musí dopředu schválit zastupitelstvo obce. Jedná se například o opravu osvětlení v obci. Výdaje na osvětlení jsou plánované na 100 000 Kč. V průběhu prací se zjistí, že oprava bude nákladnější, a to o 50 000 Kč. Je tedy potřeba dofinancovat položku ve výdajích, a to o 50 000 Kč. Tuto změnu ale nejdříve musí schválit zastupitelstvo a až poté se může výdajová položka zvýšit o potřebnou částku. V obci Běstvína se zastupitelstvo schází jednou za dva měsíce. I kdyby šlo o navýšení rozpočtu pouze o jednu korunu, zastupitelstvo tuto změnu musí schválit. V praxi to ale funguje tak, že pokud jde o změnu do 30 000 Kč, může tuto změnu schválit paní starostka, a zastupitelstvu změnu dodatečně předložit. Pokud by tedy nastaly mimořádné výdaje na pověřence, kdy by bylo potřeba řešit situace porušení GDPR, a částka by nepřesáhla 30 000 Kč, paní starostka si změnu schválí sama.

3.1.7 Rozpočet spojený s GDPR v ČR

Velká většina činností spojených se sjednáváním, legislativní adaptací i prováděním GDPR byla hrazena v rámci standardních aktivit podle běžného rozpočtu Ministerstva vnitra (analýza legislativy, příprava nových předpisů, metodická podpora obcí a krajů, informace pro státní správu, nastavení vnitřního systému ochrany osobních údajů, vyřizování žádostí subjektů údajů atd.). Na těchto činnostech se podíleli a podílejí stávající zaměstnanci a státní zaměstnanci Ministerstva vnitra (tj. nebylo například zřízeno nové místo pověřence a jeho činností byl pověřen stávající státní zaměstnanec). Rozpočet na GDPR jako takový tedy nelze specifikovat.

Ministerstvu vnitra jsem položila dotaz, jak GDPR ovlivnilo rozpočet státu.

„Ve snaze pomoci obcím a krajům při reakci na GDPR zadalo Ministerstvo vnitra v na přelomu let 2017 a 2018 externě zpracování systémových analýz pro obce a kraje, jejichž cena byla 1 627 450 korun, resp. 1 766 600 korun.“

Zdroj: Ministerstvo vnitra ČR

Na základě odpovědi z Ministerstva Vnitra je patrné, že drobná pomoc ze strany státu zde byla. Byla vypracována systémová analýza pro obce a kraje. Pro obce byla finanční částka nižší než pro kraje.

3.1.8 Metoda Best practice

Best practice

Best practice, neboli dobrá praxe, představují, že existují techniky procesy a aktivity, díky nim se dá zlepšit efektivita práce. Jedná se tedy o ověřené postupy a žádoucí výstupy, díky kterým dosáhnete právě použitím metody Dobré praxe, kterou již někdo vytvořil a zveřejnil. Cílem je snížit riziko, narazit na méně problémů a méně závažných problémů, také tím zabránit nepředvídatelným komplikacím. Metoda rovněž napomáhá dojít k vytyčenému cíli cesty efektivněji a rychleji. [6]

Case practice

Case practice neboli případová studie jedna z kvalitativního výzkumu. Charakteristikou této metody je detailní studium jednoho nebo málo případů kvůli aplikace získaných poznatků nebo porozumění případům. [24]

3.1.9 Archivace – dobrá praxe v obci Běstvina

Příkladem dobré praxi v obci Běstvina je archivace.

Jakýkoliv dokument, který obecní úřad přijme, jak poštou, e-mailem nebo datovou poštou, musí úřad archivovat. Může jít taktéž o osobní podání. V případě, že obec zahajuje jednání, např. starostka obce někomu píše – i to se musí evidovat.

Veškeré tyto dokumenty a informace jsou vkládané do programu E-spis Lite. Pokud přijde oznámení datovou poštou, vždy je to zadané do E-spis lite, protože datová pošta a tento program je propojený. Písemnosti, které jsou dodány poštou, nebo je někdo osobně přinese, jsou taktéž potřeba zaevidovat. Pokud jde například o oznámení o prodeji slepic, neeviduje se to.

Program tomuto dokumentu vytvoří košilku, která se přidává ke každé písemnosti. Dopisy a sdělení můžou nabývat různého stavu rozpracovanosti – nevyřízené, rozpracované, vyřízené. Ke každému stavu se tiskne nová košilka, která musí být přiložená u dopisu. S všemi těmito informacemi o dopise, které jsou v E-spis Lite, pracovník obce vyhodnotí, čeho se dopis týká a na základě toho přiřadí dokumentu spisový a skartační znak. Pokud je tedy ve stavu vyřízené, protože bylo na zprávu poslanou datovou poštou odpovězeno, vytiskne se nová košilka se stavem vyřízeno a na základě skartačního a spisového znaku se dokument archivuje.

Po přiřazení skartačního a spisového znaku jsou dokumenty uloženy do příručního archivu, který je zabezpečený. Dle čísel, některé mají označení A a některé S, se dané dokumenty archivují. Některé dokumenty musí obec archivovat pět let, některé deset let a některé dokumenty se nesmějí vyhodit nikdy.

Jednou za rok obec udělá výpis z archivu, co by mělo být již skartováno a tento výpis pošle do Chrudimi archivačnímu úřadu. Úřad rozhodně o tom, které dokumenty můžou být skartovány, které jsou potřeba ještě archivovat, například proto, že se k dokumentu pojí ještě jiný skartační znak, anebo které dokumenty obec musí archivačnímu úřadu odevzdat (např kronika obce). Poté obec provede skartaci. O skartovaných dokumentech se musí udělat opět záznam, který je na základně spisového znaku opět uložen do příručního archivu.

Dobrá praxe spočívá zejména v tom, že pokud by došlo například k nějaké živelné pohromě, příruční archiv by například vyhořel, všechny dokumenty z příručního archivu jsou taktéž uloženy v programu E-spis Lite, to znamená že všechny dokumenty jsou dohledatelné.

3.2 CZECH POINT – informační systém

Informační systém CZECH POINT je Český Podací Ověřovací informační Národní Terminál. Cílem je, aby občan nemusel navštívit několik úřadů, aby problém vyřešil. Občan díky CZECH POINTu může komunikovat se státem z jednoho místa tak, aby obíhala data a ne občan. Jedná se o maximální využití údajů, která vlastní stát, ku minimalizaci požadavků na občany. Občan tak může komunikovat se státem z jednoho univerzálního místa. Je možné získat a ověřit data z veřejných i neveřejných informačních systémů. Dále lze úředně ověřit listiny a dokumenty, zjistit informace o probíhajícím správním řízení, a podat žádost o zahájení správního řízení, například pokud chce vlastním nemovitosti zrušit trvalé bydliště třetí osobě. [2]

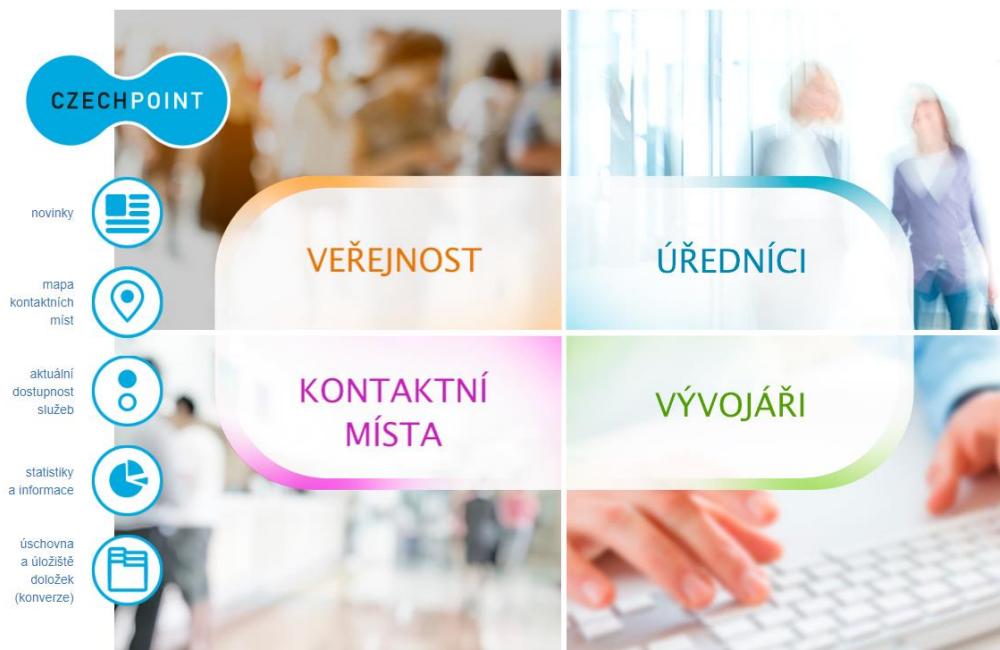
Pokud chce občan zjistit z CZECH POINTu informace, na které má ze zákona právo, například výpis z trestního rejstříku, dostaví se na obecní úřad. Obecní úřad po něj nejprve bude vyžadovat identifikační údaje kvůli jednoznačnému ověření totožnosti žadatele. Jednoznačným identifikátorem může být například občanský průkaz. Další údaje, jako jméno, příjmení, datum narození jsou automaticky získávány ze základních registrů. Získané údaje jsou používány výhradně pro poskytnutí služby, na základě požadavku občana, a slouží pouze při komunikaci s cílovým informačním systémem. Údaje nejsou dále v rámci Czech POINTU uchovávány a ani se dále nezpracovávají. Pokud se informace posílají datovou poštou, zůstávají zde maximálně po dobu devadesáti dnů do doručení. Vzhledem k tomu, že zpracování osobních údajů je dáno zákonem, nemusí žadatel podepisovat žádný souhlas o zpracování osobních údajů. Na Obrázku pět je zobrazena úvodní stránka portálu.

Ohledně implementace zvláštních opatření do IS CZECH POINT jsem se znovu vznesla dotaz na Ministerstvo vnitra.

„Žádné funkcionality ani jiné úpravy do IS ohledně GDPR proto nebylo třeba implementovat.“

Před zavedením GDPR nebylo možné volně vyhledávat informace o jiných občanech a byly zde dostatečná bezpečnostní opatření, proto nebylo nutné žádné implementace provádět.

Kontrolní funkci nad IS Czech POINT vykonává ÚOOÚ.



Czech POINT reg.č. CZ.1.06/1.1.00/03.05921
 Tento projekt je spolufinancován z prostředků Evropské Unie Evropského fondu pro regionální rozvoj prostřednictvím Integrovaného operačního programu.
 © 2020 Ministerstvo vnitra České republiky, všechna práva vyhrazena
 Mapa serveru | Kontakty | Prohlášení přístupnosti | RSS

Obrázek 5: CZECH POINT

Zdroj: [3]

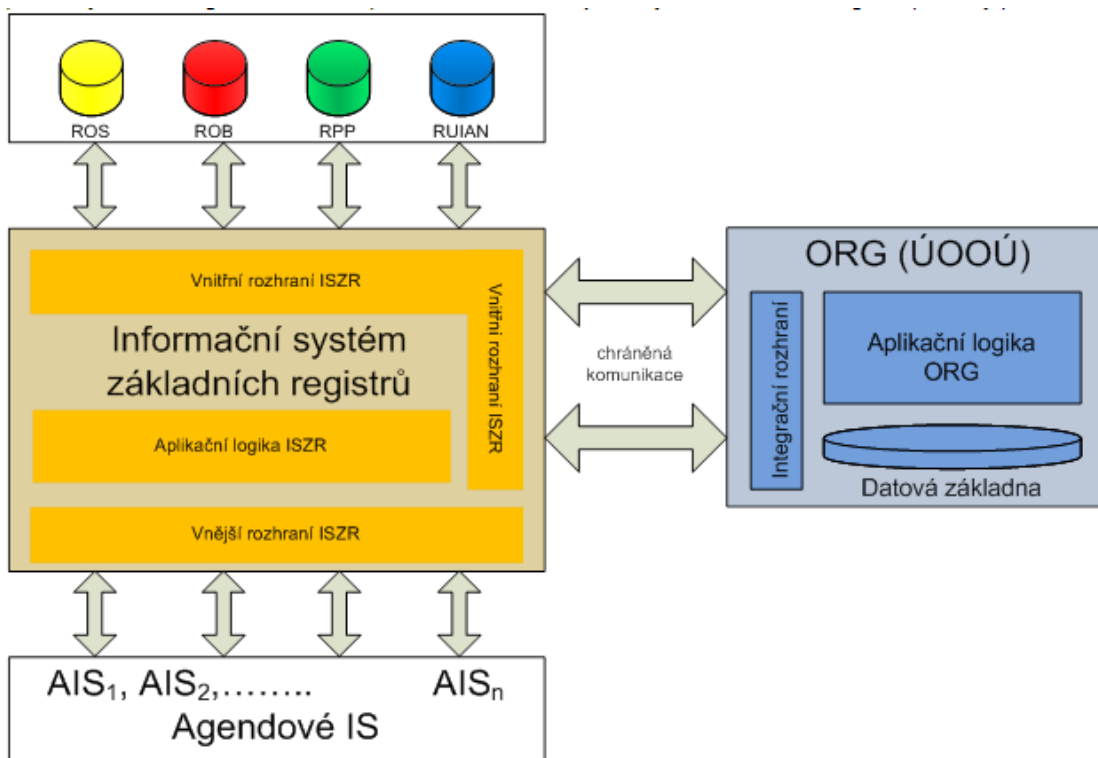
3.3 Informační systém ORG

Informační systém byl vyvinut v roce 2012 za účelem ochrany osobních údajů.

Tento informační systém byl vytvořen úřadem pro ochranu osobních údajů. IS ORG je součástí systému základních registrů. Má za úkol zajišťovat procesy, které úzce souvisí s rozpoznáním fyzických osob a ochranou jejich osobních údajů. [27]

Základní myšlenkou systému je podpora ochrany osobních údajů v celém systému. Je nahrazeno dosavadní používání rodného čísla, jako univerzální identifikátor fyzické osoby, systémem bezvýznamových identifikátorů. Identifikátory se pro každé agendy či skupiny agend musí lišit a není tak možné při znalosti jednoho identifikátoru vyhledávat osobní údaje o konkrétní osobě. Jediné místo, kde jsou všechny identifikátory uloženy je právě ORG. V systému nejsou uloženy žádné další osobní údaje fyzických osob, takže ani to, že úřad zná všechny identifikátory neznámá, že má možnost identifikátor přiřadit konkrétní osobě. Rodné číslo, ze kterého se dá odvodit jak datum narození, tak i pohlaví, je nahrazeno novými identifikátory ZIFO – zdrojový identifikátor fyzické osoby. Číslo je unikátní pro každou fyzickou osobu. Pro každou agendu se ze zdrojového identifikátoru (ZIFO) odvodí tzv. agendový identifikátor fyzických osob (AIFO). Z agendového identifikátoru nebude možné odvodit základní ani jiný agendový identifikátor. Převodník údajů je jediné místo, které uchovává a zpracovává seznam identifikátorů AIFO. Přitom se neví nic o osobě, která se pod AIFO skrývá. [27]

Pro zajištění bezpečnosti osobních údajů v systému základních registrů bude možné převádět identifikátory z jedné agendy na identifikátory v jiné agendě pouze v ORG, a to na základě autorizovaného požadavku oprávněného subjektu. Pro větší ochranu osobních údajů každého z občanů. Bydliště či místo a datum narození jsou uloženy jen v jednom z registrů a uživatelé, kteří mají oprávnění, si mohou pro svou potřebu údaje stahovat. Komunikaci mezi Základním registrem a ORG je vyobrazena na obrázku níže. [27]



Obrázek 6: Komunikace mezi ISZR a ORG

Zdroj: [27]

Financování investiční části požadovaného systému bylo zajištěno usnesením vlády č. 1019/2009 a je spolufinancováno z projektu Evropské unie ve výši 85 % uznatelných nákladů na základě vydání právního aktu o poskytnutí dotace ze dne 30. 11. 2010.

3.1 GDPR kritickým pohledem

Základní myšlenkou této směrnice je, aby s osobními údaji bylo nakládáno jako doposud, ale nesmějí být vědomě předávány třetí straně. Toto nařízení vydané Evropským parlamentem a Radou EU nahrazuje Směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Pokud by tato situace nastala, je osoba, která to způsobila, povinna toto provinění nahlásit na úřad pro kontrolu osobních údajů do 72 dní. Legislativa se ale nejvíce dotkla veřejné správy, jako jsou školy, obce, úřady, nemocnice a podobné zařízení, namísto aby bylo dohlíženo zejména na firmy, které s osobními daty obchodují. Všechny obce, jakkoliv velké, musí mít svého pověřence, kdežto firmy, kde je větší pravděpodobnost úniku osobních údajů, musí mít svého pověřence až od 300 zaměstnanců. Ráda bych porovнала zavedení GDPR v Německu a v České republice. V Německu neměly obce povinnost začít se řídit novým zákonem o

GDPR. Dotklo zejména firem, a to z důvodu, aby zabránili firmám prodávat nashromážděné informace o zákaznících.

S legislativou o GDPR také souvisí dorovnávací zákony. Projednávání o nové legislativě bylo ponecháno až na dobu nezbytně nutnou a vláda poté nedokázala pořádně vyhodnotit rizika a nedostatky nového zákona o ochraně osobních údajů. Zákon totiž říká, že postih hrozí v případě přeprořádání informací třetím stranám. Což se netýká obcí, ale právě již zmiňovaných firem.

Další nedostatek vidím v tom, že se Ministerstvo vnitra ČR pustilo do vydávání manuálů pro obce a do vydávání metodik velice pozdě. Dle mého názoru, byl v České republice před zavedením GDPR na obce obrovský mediální nátlak právě z toho důvodu, že nebyly zavčas vydány metodiky a manuály. Díky tomuto mediálnímu tlaku se obce bály, co všechno to pro ně bude znamenat, jaké ochranné prvky budou muset podniknout, a pokud je neskuteční zavčasu, jak velké sankce to pro ně bude znamenat. Obce si tedy začaly najímat pověření pro GDPR, ještě před tím, než vzešlo naplnění směrnice a bez toho, aniž by měly jasně danou povinnost. Obce uzavíraly smlouvy za nemalé peníze, ale nikdo nevěděl, co vlastně po pověřenci budou chtít. Byly vytvořené a podepsané smlouvy bez jasně vymezených činností pro pověření. Nemluvě o tom, že tyto smlouvy byly uzavírány na několik let dopředu.

Z vyhlášky vyplývají pouze dvě povinnosti. První je, že obec je povinna mít pověření. Druhá povinnost zní, že pokud nastane nějaké ÚOOÚ, je úřad povinen tuto aktivitu ohlásit na úřad pro kontrolu osobních údajů do 72 hodin, nicméně už neříká, co je součástí činnosti pověření. Z mého pohledu je vyhláška neúplná a obcím skutečnost a povinnost, zavést GDPR vůbec neusnadnila.

Dalším velkým problémem vyhlášky je, že jsou obce povinné vést záznam o činnostech, ale není řečeno jak. Neexistuje žádný oficiálně platný vzor o záznamu o činnostech. Každá obec si to proto musela vypracovat po svém.

I přesto, že byla zavedena různá opatření, nakonec to jsou sami lidé, kteří o sobě vědomě zveřejňují nejvíc informací. Konkrétně sociální sítě, jsou největším příkladem toho, že lidé o sobě bezmyšlenkovitě sdílí vše a neuvědomují si, že k těmto informacím se může dostat skoro každý a získaných údajů zneužít.

Pokud se člověk hlásí do nové práce, je dnes skoro zvykem, najít si ho na sociální síti, a zjistit, co sdílí, jaké má přátelé a další citlivé informace. Proto by se měly zejména lidé chránit, ne před tím, že obecní úřad zveřejní fotku z dětského karnevalu, kde jsou vidět, ale před tím, co sami o sobě sdílejí na internetu.

4 DOTAZNÍKOVÉ ŠETŘENÍ

V rámci případové studie jsem provedla kvantitativní výzkum a sbírala jsem data od občanů obce Běstvína. Dotazník byl vytvořen za účelem získání informací o tom, jak jsou občané informováni o GDPR. Pro studii je neméně důležitý názor občanů, kteří jsou nedílnou součástí obce. Zajímala jsem se pohled na GDPR a zda občané tuší, jaké dopady mělo GDPR na chod obce.

Pro získání informací od občanů byla vybrána kvantitativní metoda sběru dat formou dotazníkového šetření. Dotazník, který jsem respondentům předkládala, obsahoval otevřené, i uzavřené otázky (zpracované otázky v kapitole 3.4.1). Zpracování výsledků probíhalo samozřejmě anonymně.

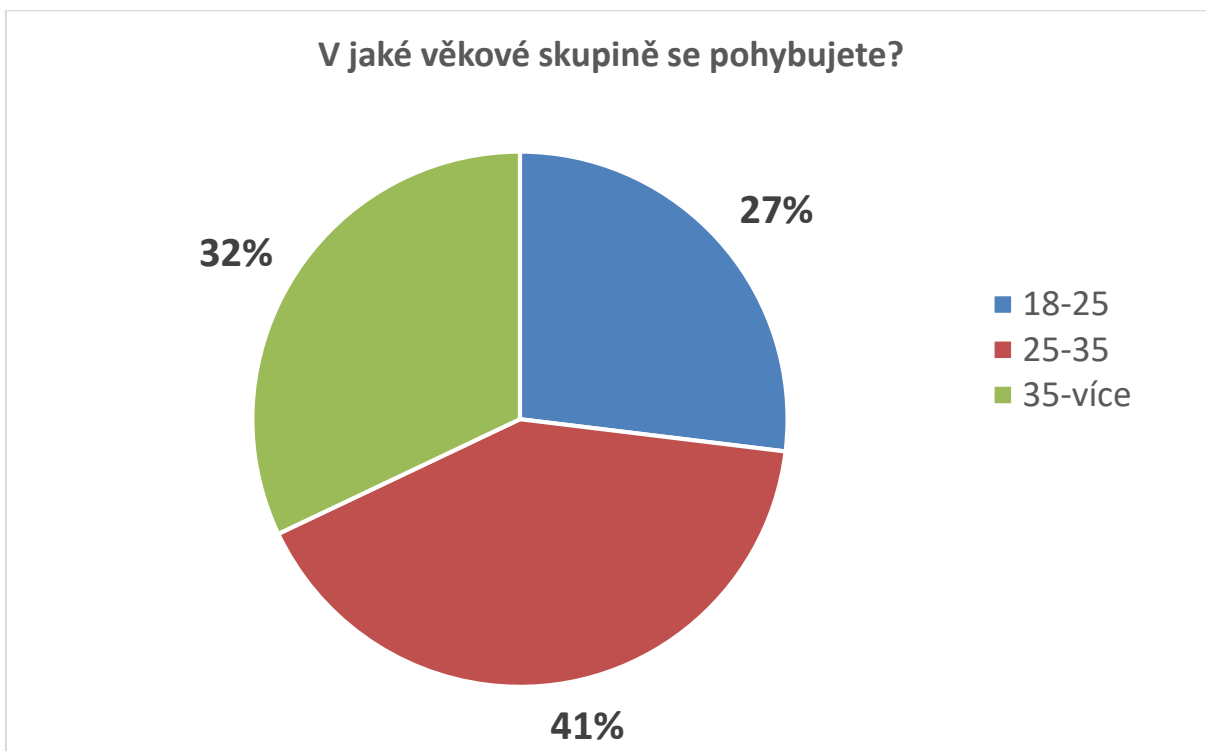
Osloveni byli pouze občani starší 18 let. Dotazník zveřejněn na sociálních sítí a osobním kontaktem s občany.

4.1.1 Vyhodnocení dotazníkového šetření

Vzhledem k tomu, že byl dotazník šířený pomocí sociálních sítí, neznám přesné číslo oslovených respondentů. Osobně jsem oslovila 20 lidí, a to zejména pracovníky obecního úřadu a starší občany, kteří nemají sociální sítě. Dotazník byl také umístěn na oficiální stránky obce Běstvína. Odpovědi jsem následně zapracovala do výsledků ze zmiňované stránky, kde byl dotazník vytvořen a uložen. V Běstvěnině žije dohromady 545 obyvatel. Celkem na dotazník odpovídalo 78 občanů obce Běstvína.

Otázka č. 1: V jakém věkovém skupině se pohybujete?

V rámci dotazníku byli dotazovaní rozdělení do tří skupin. Zaměřovala jsem se pouze občany starší 18 let. První skupina obsahuje občany v rozmezí 18-25 let, druhá 25-35 let a třetí skupina 35 let a více. Jak můžeme vidět na grafu číslo 1, nejvíce odpovídajících bylo ve druhé skupině, a tedy ve věku 25 až 35 let. Věkové rozdělení pro mě bylo důležité, abych měla představu, jak hodně budou ovlivněny následující otázky věkem dotazovaných.



graf 1: V jaké věkové kategorii se pohybujete?

Zdroj: vlastní šetření

V tabulce 5 jsou vyobrazeny přesné počty dotazovaných.

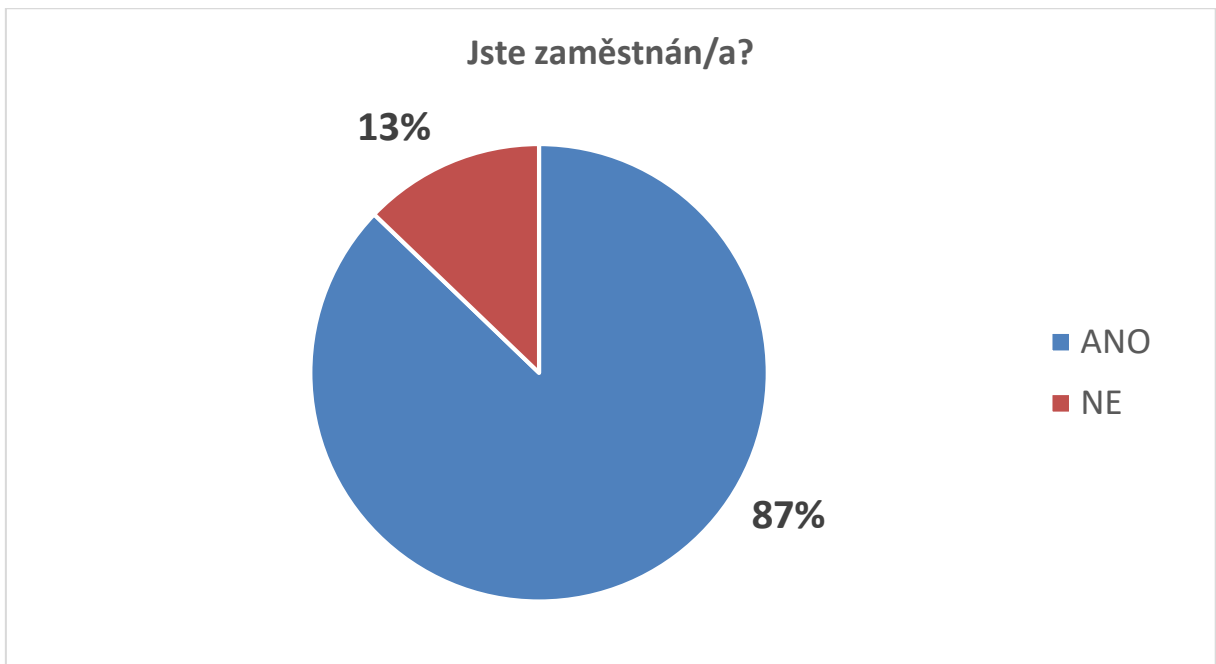
Věk	Responzí	Podíl
18-25	21	26,90 %
25-35	32	41,00 %
35 a více	25	32,10 %

Tabulka 5: Počet odpovědí na otázku č. 1 na otázku č. 1

Zdroj: Vlastní šetření

Otázka č. 2: Jste zaměstnán/a?

Respondenti, kteří na dotazník v rámci šetření odpovídali, byli z 87 % zaměstnaní a z necelých 13% nezaměstnaní. Tato otázka je také důležitá pro následné vyhodnocení šetření. Ovlivňuje znalost směrnice GDPR. Tato otázka má návaznost v otázku č. 3. Pokud je občan zaměstnán jak v soukromém nebo veřejném sektoru, je pravděpodobné, že se musel seznámit s novými opatřeními týkajícími se zavádění GDPR.



graf 2: Jste zaměstnán/a?

Zdroj: Vlastní šetření

V tabulce 6 jsou vyobrazeny přesné počty dotazovaných.

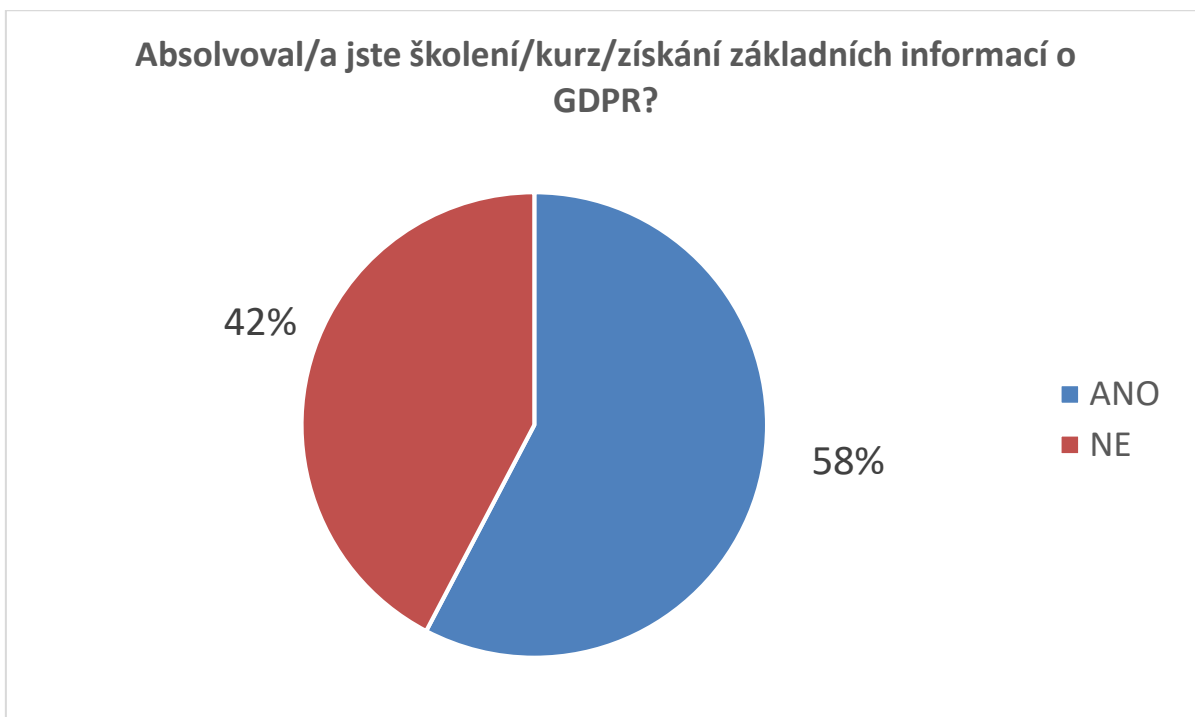
Zaměstnán/a	Počet	Podíl
ANO	68	87,20 %
NE	10	12,80 %

Tabulka 6: Počet zaměstnaných respondentů na otázku č. 2

Zdroj: Vlastní šetření

Otázka č. 3: Absolvoval/a jste školení/kurz/získání základních informací o GDPR?

V třetí otázce odpovědělo celkem 68 dotazujících, že jsou zaměstnání. Očekávala jsem, že v každé firmě muselo dojít k nějakému školení či rychlému kurzu o seznámení s příchodem GDPR. A i přesto, v otázce číslo 3, přes 40 % respondentů odpovědělo, že školení neabsolvovali a základní informace o GDPR nemají.



graf 3: Absolvoval/a jste školení/kurz/získání základních informací o GDPR?

Zdroj: vlastní šetření

V tabulce 7 jsou vyobrazeny přesné počty dotazovaných.

Absolvování kurzu/školení	Počet	Podíl
ANO	45	57,70 %
NE	33	42,30 %

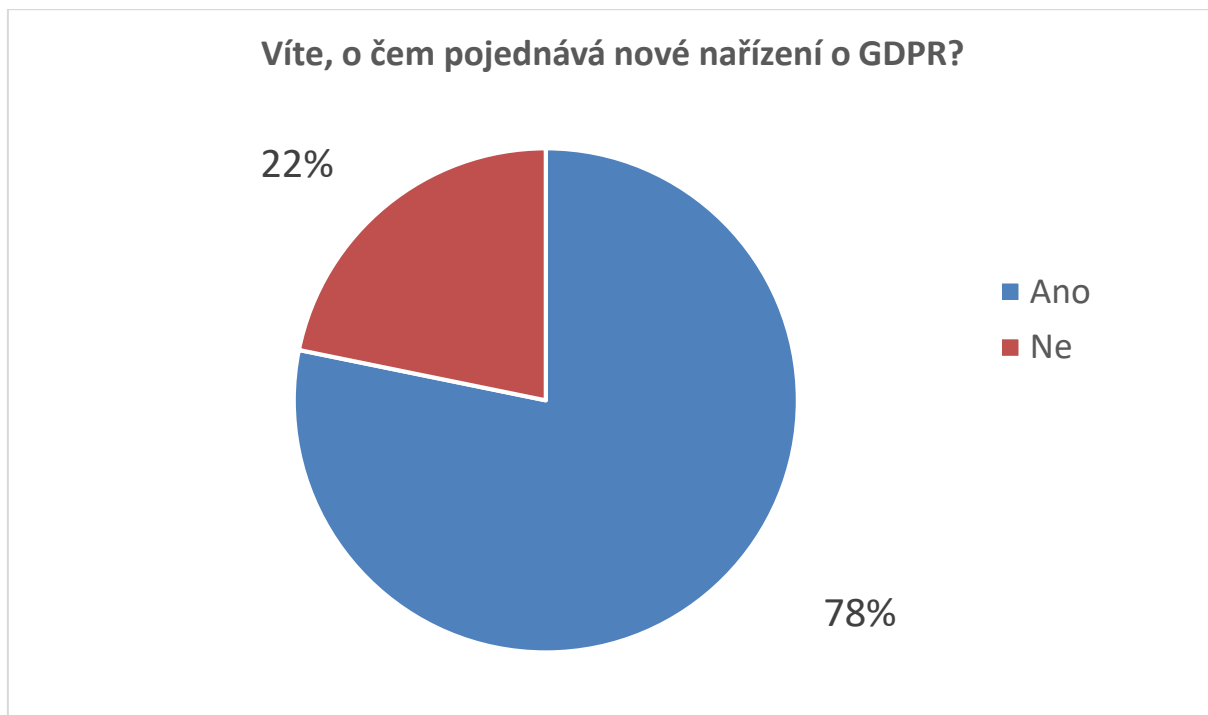
Tabulka 7: Počet odpovídajících respondentů na otázku č. 3

Zdroj: Vlastní šetření

V tabulce 7, z celkových dotazovaných 77 občanů, 45 lidí absolvovalo nějaký kurz/školení o GDPR a 33 občanů ne. Pokud vezmeme v potaz to, že v předchozí otázce o zaměstnání odpovědělo 10 občanů, že nepracuje, tak 22 zaměstnaných respondentů neabsolvovalo žádné školení.

Otázka č. 4: Víte, o čem pojednává obecné nařízení o GDPR?

U této otázky jsem byla velice zvědavá na výsledek. Z celkových 77 respondentů, celých 61 neví, o čem směrnice pojednává. Zde se dostáváme k jádru problému, kdy je lidem všeobecně vcelku jedno, co se děje. Pro většinou z nich je GDPR jen další obtěžování navíc. Neuvědomují si, že GDPR se týká opravdu každého a že nejde o pouhé udělení souhlasu při focení do obecní kroniky.



graf 4: Víte, o čem pojednává nové nařízení o GDPR?

Zdroj: Vlastní šetření

V tabulce 8 jsou vyobrazeny přesné počty dotazovaných.

Znalost směrnice o GDPR	Počet	Podíl
ANO	61	78,20 %
NE	17	21,80 %

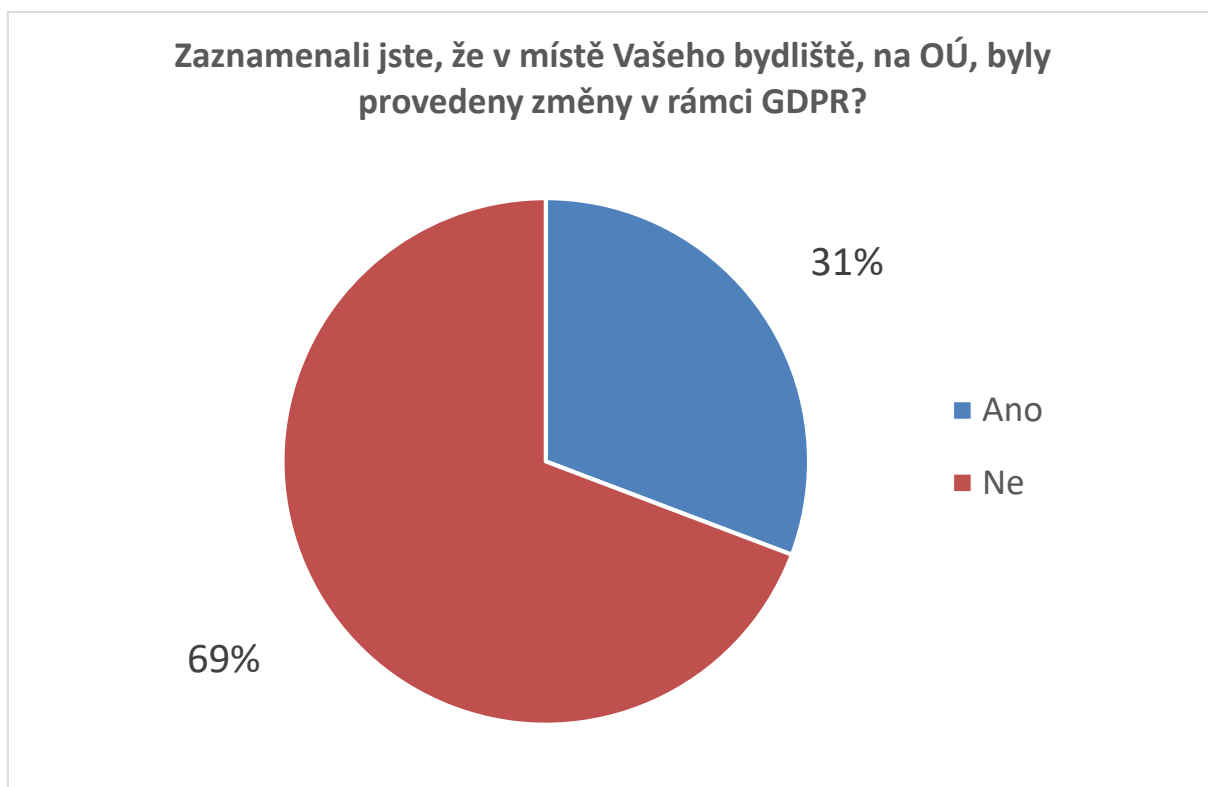
Tabulka 8: Počet odpovídajících respondentů za otázku č. 4

Zdroj: Vlastní šetření

Respondenti, se kterými jsem vyplňovala dotazník osobně, byli dotázáni, proč si směrnici nepřečetli. Drtivá většina mi odpověděla, že je to zbytečně složité, a že je to ani nezajímá. Občané si s ochranou osobních údajů nepřipouští riziko, které může nastat, pokud si dostatečně osobní údaje nebudou chránit.

Otázka č. 5: Zaznamenali jste, že v místě Vašeho bydliště, na OÚ, byly provedeny změny v rámci GDPR?

Na tuto otázku odpovědělo necelých 70 % respondentů záporně, 30 % kladně, viz graf 5. Výsledek této otázky není v celku překvapivý, vzhledem k předchozím výsledkům. Občané se o GDPR nezajímají a směrnici neznají. Z výzkumu vyplynulo, že jediné, co někteří občané zaznamenaly, je ukládání souhlasu při veřejných akcích, jako například dětský karneval nebo vítání občánků.



graf 5: Zaznamenali jste, že v místě Vašeho bydliště, na OÚ, byly provedeny změny v rámci GDPR?

Zdroj: Vlastní šetření

Jako příklad bych zde ráda uvedla zmiňované vítání občánků. V obci fungují noviny, které jsou vydávány pravidelně, každý měsíc. V měsíci listopadu proběhlo vítání občánků, kde fotil do místních novin fotograf. Obec musela předložit všem zúčastněným formulář, o souhlasu zveřejnění fotek v měsíčníku obce. Pokud by tak obec neučinila a fotky zveřejnila, mohl by je některý z občanů nařknout, a to na základně zveřejnění jeho osoby bez udání souhlasu. Občan obec nahlásí na Úřadu pro ochranu osobních údajů, ÚOOÚ se musí ohlásit OÚ, a domluvit se s paní starostkou, kdy může přijet na kontrolu. Na OÚ jsou pak přítomni z ÚOOÚ a občan, který událost nahlásil, pověřitel a správce. ÚOOÚ situaci vyhodnotí, a může udělit pokutu. Nicméně, díky GDPR jsme se vrátili zpět, na úroveň lidských vztahů, pokory a úcty k druhým, kdy se vše dá vyřešit domluvou.

V tabulce 9 jsou vyobrazeny přesné počty dotazovaných.

Zaznamenali jste změny na OÚ?	Počet	Podíl
ANO	24	30,80 %
NE	54	69,20 %

Tabulka 9: Počet odpovídajících respondentů za otázku č. 5

Zdroj: Vlastní šetření

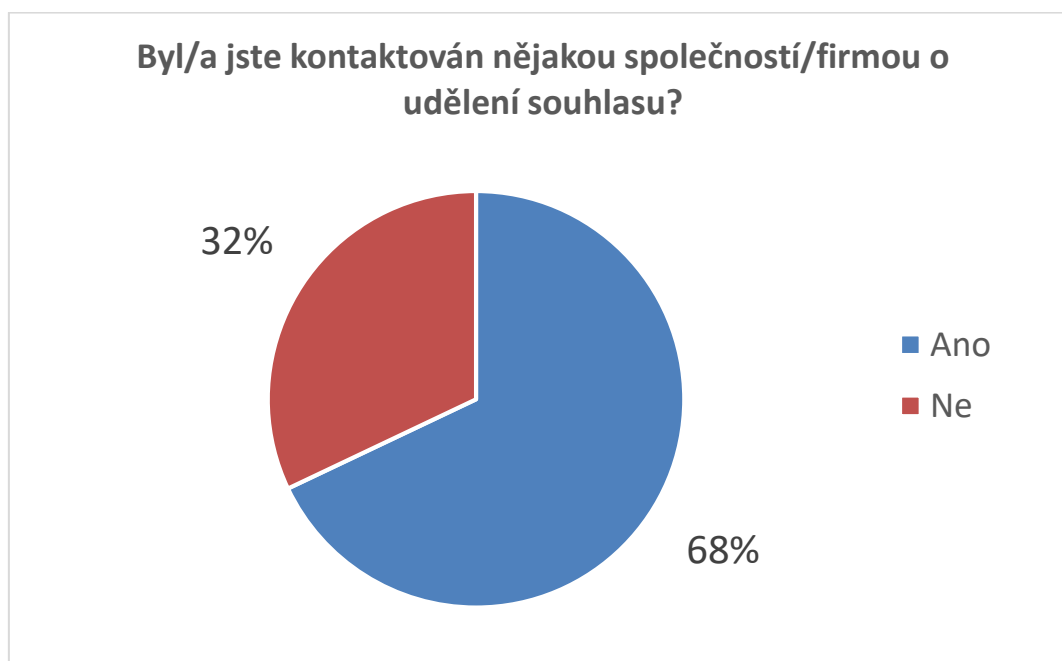
Otázka č. 6 Víte, o jaké opatření se jedná? (odpovídejte i v případě, že jste na předchozí otázku odpověděl/a NE)

Tato otázka byla zadaná jako otevřená. Zajímalo mě, jaké změny občané zaznamenaly. K otázce byla přidána i poznámka, aby respondenti odpovídali i v případě záporné odpovědi na otázku č. 5, a to proto, že o opatření podvědomí mají, ale nezaznamenali je na příslušném OÚ.

Přes 70 % respondentů odpovědělo buď ne, anebo že neví. Ostatní odpovědi jsou vcelku jednostranné. Mnoho občanů zaznamenalo již výše zmiňované povolení při zveřejnění fotografií. Někteří občané odpověděli neurčitě. Vědí, že jde o ochranu osobních údajů, ale jejich odpověď není konkrétní. Dle výsledků z předchozích otázek je patrné, že o GDPR nemají mnoho informací.

Otázka č. 7 Byl/a jste kontaktován/a nějakou firmou o udělení souhlasu? Pokud ano, uveďte, jakou společností.

Z grafu 7 je patrné, že většina respondentů byla oslovena nějakou firmou, ať už korporátní nebo soukromou, o udělení souhlasu pro zpracování osobních údajů.



graf 6: Byl/a jste kontaktován/a nějakou firmou o udělení souhlasu? Pokud ano, uveďte, jakou společností

Zdroj: Vlastní šetření

Nejvíce respondentů bylo kontaktováno telefonní společností, pojišťovnou či e-shopem. Na grafu 8 jsou uvedené nejčastější odpovědi respondentů.



graf 7: Jaké společnosti/firmy Vás kontaktovali o udělení souhlasu o zpracování dat?

Zdroj: Vlastní šetření

Zde bych se ráda zmínila o neumožnění neudělení souhlasu. Osoba si bude chtít na e-shopu objednat nějaké zboží, a při objednávání zboží musí zakliknout, že souhlasí se zpracováním dat. Pokud by ale toto nepovolil, nemohl by si ze stránek nic objednat. Nevychází z toho možnost nesouhlasu. Buď občan souhlasí, nebo si nemůže nic objednat.

Otázka č. 8: Myslíte, že je GDPR přínosem pro občana? Proč se tak domníváte?

U této otázky se mi dostalo spousty rozsáhlých odpovědí. Více respondentů se přikládá spíše k záporné odpovědi. Vychází to z nezájmu občanů o ochranu osobních údajů. Ti, co odpovídali kladně, měli již nějakou znalost o zákonu, o ochraně osobních údajů, na který nová legislativa navazuje. V rámci veřejné správy, před zavedením GDPR, nebylo možné zveřejňovat osobní údaje, či je sdělovat třetím stranám. Nejčastější odpovědí bylo, že díky GDPR nastalo zbytečné papírování, a všeobecně byla vyslovena nedůvěra k legislativě. Respondenti v GDPR často vidí mediální tlak. Vybrané odpovědi jsou uvedeny níže.

„Myslím, že ano. Je potřeba, v dnešní době sociálních sítí, chránit si své soukromí.“

„Ano, dozví se tak, k jakým účelům se zpracovávají jeho osobní údaje, než dá souhlas a má právo být i vymazán, pokud si myslí, že se zpracovávají neoprávněně“

„Nechá se to stejně obejít. Na internetu je hromada věcí zadarmo, tak je potřeba něčím platit. Takže toto není ta správná cesta.“

„Spíše ano, ale v určitých směrech nás to může brzdit.“

„Ne, zbytečné papírování.“

„Myslím si, že ne. Podle mě to nefunguje, tak jak by mělo a k údajům se nežádoucí firmy stejně dostanou.“

„V ČR byly kvalitní zákony na ochranu osobních údajů zavedeny už dříve. Ted' s GDPR se spíš jedná o zbytečnou paniku a přehnaná opatření. Jak pro občana, tak pro společnosti pracující s údaji, se jedná o přehnané komplikace.“

„Ne, je to akorát další papírování na víc. Pokud někdo chce o nás vědět, beztak si to někde najde“

„Ne, jedná se o další administrativní zátěž“.

Otázka č. 9: Je legislativa o GDPR přínosná pro společnost, případně proč?

Tato otázka byla opět položena jako otevřená otázka. Z předchozích výsledků odpovědí jsem usuzovala, že na tuto otázku bude opět více respondentů odpovídat záporně. Protože již fungoval zákon o ochraně osobních údajů, respondenti novou legislativu vnímají jako zbytečnou anebo se domnívají, že se stejně nic nezměnilo. Vybrané odpovědi jsou vyobrazeny níže.

„Měla by být, ale jedná se spíše o byrokracii, jelikož se toho stejně moc nezměnilo.“

„Není možné soudně řešit držení informací o druhé straně.“

„Pokud se bude dodržovat správně, tak ano. Osobní údaje můžou být zneužité, díky GDPR by se to stávat nemělo, protože se k nim nedostanou neoprávněné osoby.“

„Přináší to více starostí, ale má to své odůvodnění.“

„V tuto chvíli zásadní přínos nevidím.“

„Pro fyzickou osobu spíš ne.“

„ Z důvodu možného zneužití osobních údajů. V praxi, ale osobní údaje uvádíme skoro všude. Plusem je, že společnost, které osobní údaje poskytnete, nesmí informace předat dál. “

„Nemyslím si, že jen více papírování a na vše je výjimka. “

„ Ano, je spousta společností, které si mezi sebou prodávaly údaje o zákaznících. Tomu by to mělo zamezit, aby se naše údaje nedostaly tam, kam nechceme. Případně, že se tak stane, máme možnost se ozvat a žádat vymazání. “

4.1.2 Závěr dotazníkového šetření

Výsledek mého dotazníku nepřinesl žádné neočekávané výsledky. Ohlasy jsou spíše negativní a GDPR se neshledalo s úspěchem, dle respondentů z obce Běstvína. Respondenti o legislativě velké povědomí nemají, a nezaznamenali na obecním úřadu žádné velké změny. Vychází to z toho, že před zavedením legislativy o GDPR zde fungoval zákon č. 101/2000 Sb., který byl v roce 2019 zrušen a úřadům uděloval taktéž povinnost chránit osobní údaje.

Občané vidí v legislativě spíše zbytečné papírování navíc, obtěžování ze stran pojišťoven, telefonních společností apod. Podrobnější znalost legislativy také občané nemají a v důsledku o to nemají ani valný zájem. Vidí to spíše jen jako zbytečně zveličenou věc, která stojí akorát peníze navíc, a ty by mohly být investovány lépe. Nejhorším závěrem dotazníku je, že si občané samy své osobní údaje tolik nehlídají a největšími šířiteli informací jsou právě respondenti sami. Například v rámci sociálních sítí typu Facebook nebo Instagram. Spousty uživatelů zde bezmyšlenkovitě zveřejní citlivé informace, aniž by si uvědomovali, že kdokoliv tyto informace může zneužít proti nim.

ZÁVĚR

Cílem práce bylo zanalyzování implementace GDPR ve veřejné správě. Dále objasnit, jaké dopady to mělo na složky veřejné správy, které změny byla nucena provést, jaký dopad měla implementace na rozpočet, a kritickým pohledem vše zhodnotit.

Pro případovou studii byla vybrána obec Běstvína. Obecní úřad však nebyl nucen implementovat nové bezpečnostní prvky. Velký zásah do rozpočtu obce nebyl taktéž potřeba, a to z toho důvodu, že i před zavedením nebylo možné nezabezpečit veškeré dokumentace, které obsahují citlivé a osobní údaje občanů. Vše provádějí jako doposud.

Obec byla nucena, na základě legislativy, najmout svého vlastního pověřence, který bude pravidelně kontrolovat, zda nehrozí činnost, která by legislativu porušovala. Také najala firmu, která jim lépe zabezpečila počítače. To byly veškeré změny, které obec provedla. Pro obec jsem vypracovala analýzu rizik, kde jsou shrnuté veškeré složky, které je potřeba kontrolovat. Pokud by nastala aktivita, která by rozporovala legislativu, pověřenec s ÚOOÚ tuto aktivitu budou řešit. Pověřenec je placen jednorázově, jednou za rok.

V práci jsou taktéž popsány činnosti, kde dochází k porušování GDPR. Nicméně tyto činnosti nelze lépe opatřit (např. volby). Legislativa o GDPR ovlivňuje některé činnosti obce, nicméně jsou zákony, které jsou této legislativě nadřizené.

Také bylo zpracováno dotazníkové šetření, které vyplňovali občané obce Běstvína. Cílem bylo zjistit, jak legislativu vnímají, zda zaznamenali nějaké změny a zda mají pocit, že je GDPR přínosem pro společnost. Výsledek nicméně není překvapivý. Valná většina respondentů odpovídala negativně. GDPR vnímám jako nesmyslné podepisování dokumentů, jako například ve školách.

Pro menší obce, jako je například právě Běstvína, je GDPR nepřínosné. Na malé obci nedochází k zneužívání citlivých údajů. Lidé si nestěžují a žádné problémy se nevyskytují. Ochotně sdělují veškeré osobní údaje, jako je například telefonní číslo, nebo email, aby jim úřad mohl zasílat potřebné informace. Je to oboustranně výhodné. Údaje o občanech slouží na úřadě zejména proto, aby zajistily chod obce, a občani měli informace včas. Na úřadě pracují pouze dvě osoby, a to paní starostka a účetní, a ty mají přístupy ke všem databázím, evidenci obyvatel a ke všem písemnostem.

Právě lidé jsou sami pro sebe největší riziko úniku citlivých údajů. Bezmyšlenkovitě sdílí spoustu citlivých údajů na internetu, na sociálních sítích jako je Facebook a Instagram. Pokud si bude chtít někdo něco zjistit o konkrétním člověku, nedá mu to příliš mnoho práce.

Vzhledem k tomu, že i předchozí český zákon č. 101/2000 Sb., o ochraně osobních údajů, byl poměrně přísný, naplnila se jednoznačně slova dozorového úřadu, že nová pravidla ochrany osobních údajů jsou evoluční reakcí na rozvoj informační společnosti, a nikoliv zásadní revolucí přinášející převratné změny.

Tato práce může sloužit k získání přehledu o GDPR. Kam všude GDPR zasahuje, jaký vliv mělo na chod Veřejné správy a na chod IS Veřejné správy.

POUŽITÁ LITERATURA

- [1] Co byste měli vědět o GDPR, pokud podnikáte na Internetu. *IPC-IPC Corporation s.r.o* [online]. Praha: IPC Corporation, 2018 [cit. 2019-07-24]. Dostupné z: <https://ipcc.cz/co-byste-meli-vedet-o-gdpr-pokud-podnikate-na-internetu/>
- [2] Co je Czech POINT? *Czech POINT a GDPR-Czech POINT* [online]. Ministerstvo vnitra České republiky, c2020 [cit. 2020-04-19]. Dostupné z: <https://www.czechpoint.cz/public/statistiky-a-informace/co-je-czech-point/>
- [3] Co je Czech POINT? *Czech POINT a GDPR-Czech POINT* [online]. Ministerstvo vnitra České republiky, c2020 [cit. 2020-04-19]. Dostupné z: <https://www.czechpoint.cz/>
- [4] Co je SSL certifikát? *Domain Master* [online]. Plzeň: INTERNET CZ, 2017 [cit. 2020-03-11]. Dostupné z: <https://www.domainmaster.cz/napoveda/caste-dotazy/ssl-certifikaty/co-je-ssl-certifikat-108/>
- [5] Co je, co není a co bude osobní údaj podle GDPR. *Frank Bold Advokáti* [online]. Praha, 2018 [cit. 2019-07-24]. Dostupné z: <https://www.fbadvokati.cz/cs/clanky/541-co-je-co-neni-a-co-bude-osobni-udaj-podle-gdpr>
- [6] Co jsou příklady dobré praxe. *Kurikulum S* [online]. Praha: NÚOV, 2012 [cit. 2020-03-17]. Dostupné z: <http://www.nuov.cz/kurikulum/co-jsou-priklady-dobre-praxe>
- [7] *DPO čili Pověřenec pro ochranu osobních údajů* [online]. Praha: Mgr. Eva Škorníčková, 2017 [cit. 2019-09-05]. Dostupné z: <https://www.gdpr.cz/gdpr/osobni-udaje/>
- [8] GDPR – nařízení o ochraně dat, které ovlivní i vaši firmu. *Bezpečnost dat s produktem Safetica* [online]. Brno: Safetica Technologies, 2017 [cit. 2020-02-24]. Dostupné z: <https://www.safetica.cz/blog/co-prinasi-nova-norma-na-ochranu-dat-gdpr/>
- [9] GDPR easily and understandably. *THE DIGITAL ENABLERS* [online]. California: KPCS Consulting, 2018 [cit. 2020-02-24]. Dostupné z: <https://www.atom.ms/en/>
- [10] Informace o obci-Oficiální stránky obce Běstvína. *Oficiální stránky obce Běstvína* [online]. Běstvína: Galileo Corporation, 2016 [cit. 2017-03-14]. Dostupné z: <http://www.obecbestvina.cz/obec-1/informace-o-obci/>
- [11] JANEČKOVÁ, Eva. *GDPR-Řešení problémů v praxi obcí*. Praha: Grada Publishing, 2019. ISBN 978-80-271-2719-4.
- [12] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.

- [13] KOMÍNKOVÁ, Magda. Jak vznikalo nařízení o ochraně osobních údajů (GDPR)? *Euroskop.cz - Zpravodajství* [online]. Plzeň: Euroskop, 2018, 27. 3. 2018 [cit. 2018-12-26]. Dostupné z: <https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/>
- [14] LECHNER Ph.D., Tomáš. GDPR ovlivnilo i základní registry. *Časopis IT Systems* [online]. 2019, (3), 1 [cit. 2020-04-23]. Dostupné z: <https://www.systemonline.cz/it-pravo/gdpr-ovlivnilo-i-zakladni-registry.htm>
- [15] Mohu požádat společnost/organizaci, aby přestala zpracovávat mé osobní údaje? *Evropská komise* [online]. Praha, 2017 [cit. 2019-09-03]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_cs?pk_source=google_ads&pk_medium=paid&pk_campaign=gdpr2019
- [16] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. In: . Brusel: EU, 2016, ročník 2016, 2016/679. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS>
- [17] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
- [18] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
- [19] Nové přístupy a povinnosti. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2017, 27.10.2017 [cit. 2018-12-26]. Dostupné z: <https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=3938>
- [20] NULÍČEK, Michal. GDPR-obecné nařízení o ochraně osobních údajů [online]. Praha: Wolters Kluwer, 2017 [cit. 2020-01-08]. Praktický komentář. ISBN 978-807-5527-653.
- [21] *Obecné nařízení o ochraně osobních údajů prakticky* [online]. Praha: Mgr. Eva Škorníčková, 2017 [cit. 2018-11-15]. Dostupné z: <https://www.gdpr.cz/gdpr/osobni-udaje/>
- [22] *Obecné nařízení o ochraně osobních údajů prakticky* [online]. Praha: Mgr. Eva Škorníčková, 2017 [cit. 2018-11-15]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/>

- [23] *Obecné nařízení o ochraně osobních údajů prakticky* [online]. Praha: Mgr. Eva Škorníčková, 2017 [cit. 2019-07-31]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/zpracovatel-osobnich-udaju/>
- [24] PETRUSEK, Miloslav, Hana MAŘÍKOVÁ a Alena VODÁKOVÁ. *Velký sociologický slovník*. Praha: Karolinum, 1996. ISBN 80-718-4310-5.
- [25] *Praktická skupina 29* [online]. Praha: Mgr. Eva Škorníčková, 2017 [cit. 2018-11-15]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/>
- [26] Předávání osobních údajů do jiných zemí. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2017, 27.10.2017 [cit. 2019-01-10]. Dostupné z: <https://www.uoou.cz/10-p-edavani-osobnich-udaj-do-jinych-zemi/d-27284>
- [27] Role Úřadu. *Role Úřadu: Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2013 [cit. 2020-03-11]. Dostupné z: <https://www.uoou.cz/role-uradu/ds-1937/p1=1937>
- [28] Schválený rozpočet obce Běstvína pro rok 2018. *Oficiální stránky obce Běstvína* [online]. Běstvína: Obec Běstvína, 2017 [cit. 2020-04-19]. Dostupné z: <https://www.obecbestvina.cz/>
- [29] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Eurlex [online]. Brusel: EU, 1994 [cit. 2020-01-08]. Dostupné z: <http://www.eurlex.cz/dokument.aspx?celex=31995L0046>
- [30] Transparency report. Transparency report [online]. San Francisco: Google, 2017 [cit. 2020-01-08]. Dostupné z: <https://transparencyreport.google.com>
- [31] Účel katastru. Katastr-nemovitost [online]. Praha 8: ČÚZK [cit. 2020-05-05]. Dostupné z: <https://www.cuzk.cz/Katastr-nemovitosti/O-katastru-nemovitosti/Ucel-katastru.aspx>
- [32] VOJTĚCH ŠIMÍČEK (ED.). *Právo na soukromí* [online]. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011 [cit. 2020-01-08]. ISBN 80-210-5449-2.
- [33] Zákon č. 101/2000 Sb., o ochraně osobních údajů [online]. Praha: ÚOOÚ, 2000 [cit. 2020-01-08]. Dostupné z: https://www.uoou.cz/files/101_cz.pdf
- [34] Zásady a právní důvody zpracování. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2017 [cit. 2019-07-24]. Dostupné z: <https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271>

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

Průzkum informovanosti občanů o GDPR

Dobrý den,

jsem studentka Univerzity Pardubice a v rámci své Diplomové práce na téma

Aspekty zavedení GDPR ve veřejné správě ČR, si Vás dovoluji požádat o vyplnění tohoto dotazníku.

Cílem dotazníku je zjistit, jak velké povědomí mají občané o GDPR.

Dotazník je anonymní a získané informace budou zpracovány v rámci diplomové práce. Není-li u příslušné otázky přímo uveden návod k doplnění odpovědi, vyberte pouze jednu možnost. Děkuji Vám za spolupráci.

1. V jakém věkovém skupině se pohybujete?

Nápověda k otázce: *Vyberte jednu odpověď*

- 18-25
- 25-35
- 35 a více

2. Jste zaměstnán/a?

Nápověda k otázce: *Vyberte jednu odpověď*

- ANO
- NE

3. Absolvoval/a jste školení/kurz/získání základních informací o GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

- ANO
- NE

4. Víte, o čem pojednává obecné nařízení o GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

ANO

NE

5. Zaznamenali jste, že v místě Vašeho bydliště, na OÚ, byly provedeny změny v rámci GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

ANO

NE

6. Víte, o jaké opatření se jedná? (odpovídejte i v případě, že jste na předchozí otázku odpověděl/a NE)

7. Byl/a jste kontaktován nějakou firmou o udělení souhlasu? Pokud Ano, uveďte, jakou společností.

8. Myslíte, že je GDPR přínosem pro občana? Proč se tak domníváte?

9. Je směrnice o GDPR přínosná pro společnost, případně proč?