Analýza dopadů nakládání s osobními údaji v rámci implementace GDPR na činnost a hospodaření ve vybraném MěÚ

Lenka Němečková

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav regionálního rozvoje, veřejné správy a práva
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lenka Němečková**
Osobní číslo:	**M16069**
Studijní program:	**B6202 Hospodářská politika a správa**
Studijní obor:	**Veřejná správa a regionální rozvoj**
Forma studia:	**prezenční**
Téma práce:	**Analýza dopadů nakládání s osobními údaji v rámci implementace GDPR na činnost a hospodaření ve vybraném MěÚ**

Zásady pro vypracování:

Úvod

Definujte cíle práce a použité metody zpracování práce.

I. Teoretická část

- **Představte teoretické poznatky týkající se dané problematiky.**

II. Praktická část

- **Uveďte příklad zneužívání osobních údajů.**
- **Analyzujte dopady implementace GDPR na činnost a hospodaření ve vybraném MěÚ.**
- **Na základě provedené analýzy zhodnoťte dopady na chod vybraného MěÚ a navrhněte zdokonalení současného stavu práce s GDPR.**

Závěr

Rozsah bakalářské práce:	**cca 40 stran**
Rozsah příloh:	
Forma zpracování bakalářské práce:	**tištěná/elektronická**

Seznam odborné literatury:

CALDER, Alan. EU GDPR a Pocket Guide. 1st ed. United Kingdom: IT Governance Publishing, 2016, 96 s. ISBN 978-1-84928-832-3.
NAVRÁTIL, Jiří et al. GDPR pro praxi. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 339 s. ISBN 978-80-7380-689-7.
NEZMAR, Luděk. GDPR: praktický průvodce implementací. 1. vyd. Praha: Grada, 2017, 301 s. ISBN 978-80-271-0668-4.
ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018, 343 s. ISBN 978-80-7554-152-9.

Vedoucí bakalářské práce:	**JUDr. Olga Kapplová, Ph.D.** Ústav regionálního rozvoje, veřejné správy a práva
Datum zadání bakalářské práce:	**14. prosince 2018**
Termín odevzdání bakalářské práce:	**14. května 2019**

Ve Zlíně dne 14. prosince 2018

L.S.

doc. Ing. David Tuček, Ph.D.
děkan

RNDr. Pavel Bednář, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen na elektronickém nosiči v příruční knihovně Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně 9. 5. 2019

Jméno a příjmení: LENKA NĚMEČKOVÁ

.....
podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřena na problematiku Obecného nařízení o ochraně osobních údajů. Cílem této práce bylo zjištění dopadů nakládání s osobními údaji v rámci implementace Obecného nařízení na činnost a hospodaření vybraného městského úřadu. Data byla zpracována pomocí nástrojů dopadové analýzy. Provedenou analýzou bylo zjištěno, že Obecné nařízení mělo určité dopady na činnost a hospodaření vybraného městského úřadu. V práci byla navržena řešení, která umožňují další zlepšení práce s Obecným nařízením. Na základě zjištěných dopadů byly navrženy kroky k docílení vyššího souladu s požadavky Obecného nařízení. Výsledky této práce umožňují vybranému městskému úřadu se zamyslet nad dalšími kroky v implementaci Obecného nařízení.

Klíčová slova: městský úřad, GDPR, ochrana osobních údajů, zpracování osobních údajů, pověřenec pro ochranu osobních údajů

ABSTRACT

The bachelor thesis is focused on the problematic of the General Data Protection Regulation. The aim of this thesis was to find out impacts of treating with personal data within the implementation of the General Regulation on activities and economy in the selected city office. The data were processed with the aid of impact analysis tools. The performed analysis found out that the General Regulation had certain impacts on activities and economy of the selected city office. In this thesis were proposed solutions which allow further improvement of work with the General Regulation. On the basis of the detected impacts steps have been proposed to achieve higher unity with requirements of the General Regulation. The results of this thesis allow the selected city office to think about next steps in the implementation of the General Regulation.

Keywords: city office, GDPR, personal data protection, personal data processing, data protection officer

Ráda bych poděkovala JUDr. Olze Kapplové, Ph.D. za odborné vedení při zpracování mé bakalářské práce. Vážím si předaných osobních zkušeností, poskytnutých cenných rad a připomínek, které mne nasměrovaly správnou cestou. Děkuji taktéž osobám, které vstřícně a ochotně poskytovaly veškeré potřebné informace k dokončení bakalářské práce.

OBSAH

ÚVOD

Problematice ochrany osobních údajů se nikdy nijak zvlášť nevěnovala pozornost mezi lidmi, zejména tak, jako v poslední době. Mnoho lidí nemělo velké povědomí ani o zákonu č. 101/2000 Sb. o ochraně osobních údajů a o změně kterých zákonů, i když působil na území České republiky již řadu let. Povědomost o ochraně lidské osobnosti a osobních informací jako takových se začalo šířit až na přelomu let 2015 a 2016, kdy se projednávalo nové nařízení Evropské unie o ochraně osobních údajů. Široká veřejnost označovala nařízení jako velký převrat a úplnou novinku v dané oblasti, což znepokojilo většinu populace a začala se šířit panika po celé Evropě, zejména však v České republice. Tato situace nebyla úplně na místě, protože se o žádný převrat nejedná. Zbytečná panika a strach z nové právní úpravy vyplynuli z nevědomosti veřejnosti, která si nezjistila potřebné podrobnosti.

Vzhledem k neúprosnému vývoji lidské společnosti v oblasti internetu, sociálních sítí a k celkovému vývoji informačních technologií, které jsou v současné době jeden z nejvíce rozvíjejících se odvětví, bylo zapotřebí řešit problematiku ochrany osobních údajů a samotných lidí, protože stávající legislativa již zdaleka nepokrývala vymoženosti dnešní doby, stávala se zastaralou a docházelo k nejrůznějším hackerským útokům za účelem odcizení a následného zneužití osobních dat. Z těchto důvodů je zapotřebí se této problematice věnovat a upravovat legislativu tak, aby byla odrazem současnosti a zmírňovala případné přestupky a nezákonná jednání, které se ve světě dějí.

Bakalářská práce tedy reaguje na aktuální situaci jak v České republice, tak i v Evropské unii a na související problémy v okruhu ochrany osobních údajů ve veřejné správě, přičemž se to reálně dotýká i dalších odvětví, tj. podnikání, neziskového a soukromého sektoru apod. Práce se přesněji zaměřuje na oblast územní samosprávy, neboli na vybraný městský úřad, a to jakým způsobem byli ovlivněni novou právní úpravou, co to pro ně znamenalo z hlediska jejich výkonu práce či organizace úřadu. Městský úřad proto, jelikož mnoho úřadů, ať už městských nebo obecních, které se nacházejí v mé blízkosti, si neví rady s tímto novým nařízením. Neví jak začít, co vše mají zavést, změnit, analyzovat, vypracovat či aktualizovat a pokud něco udělají, tak neví, jestli to mají správně a odpovídá to Obecnému nařízení a dalším souvisejícím předpisům, aby je nepostihli případné sankce či jiné postihy.

Nedílnou součástí mé bakalářské práce je podání návrhu na zlepšení výkonu práce s Obecným nařízením ve vybraném městském úřadě, což je zároveň jeden z cílů bakalářské

práce. Návrh byl sepsán na základě zjištění dopadů na činnost a hospodaření vybraného městského úřadu, což jsem provedla v rámci analýzy dopadů v praktické části. Analýzu dopadů jsem zpracovala na základě absolvovaných rozhovorů s příslušnými pracovníky ve vybraném městském úřadu, tj. s osobou vykonávající pozici pověřence pro ochranu osobních údajů, vedoucí personálního oddělení a další. V praktické části jsem taktéž zhodnotila nákladové zatížení na implementaci Obecného nařízení do stávající činnosti úřadu.

Výsledkem práce je navržení činností, které by bylo vhodné provést ve vybraném městském úřadě, díky nimž docílí zdokonalení současného stavu práce s Obecným nařízením. Provedenou analýzou dopadů a současného stavu včetně následného návrhu na zlepšení souladu vykonávané práce s tímto nařízením mohou využít i jiné úřady jako inspiraci k dalším krokům implementace Obecného nařízení do činností úřadu a k porovnání se svým současným stavem. To znamená, že tato bakalářská práce bude mít přínos i pro další subjekty, ne jen pro vybraný městský úřad.

CÍLE A METODY ZPRACOVÁNÍ PRÁCE

Hlavním cílem mé bakalářské práce je zjištění dopadů na základě účinnosti nové legislativy Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Obecné nařízení“) zaměřené na činnost a hospodaření vybraného městského úřadu. Dalším cílem je vyhodnocení současného stavu práce s Obecným nařízením na chod úřadu a následné zpracování návrhu pro zdokonalení práce s touto legislativou, díky kterému se mohou posunout zase o krok kupředu.

V teoretické části jsem provedla stručný rozbor vývoje legislativy v oblasti ochrany osobních údajů na území České republiky a zabývala jsem se také otázkou, proč bylo nutné stávající zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů změnit případně zrušit. Hlavní část teorie jsem věnovala samotnému Obecnému nařízení, studovala jsem, na jakých principech a zásadách funguje, jaké nové povinnosti přineslo a zda došlo k dalším změnám například v oblasti práv subjektu údajů. Zaměřila jsem se i na osobu vykonávající funkci pověřence pro ochranu osobních údajů, která je nově klíčovou postavou v dané problematice. V neposlední řadě jsem zpracovala přehled základních pojmů, které se týkají dané problematiky, bez jejichž porozumění by bylo těžké se v oblasti ochrany osobních údajů orientovat.

V praktické části jsem zpracovala analýzu dopadů, zaměřenou na oblast činnosti a hospodaření mnou vybraného městského úřadu. Analýzu jsem uskutečnila na základě získaných informací z teoretické části bakalářské práce a ze spolupráce s pracovníky vybraného úřadu, tj. s pověřencem pro ochranu osobních údajů či s vedoucí personálního oddělení a dalšími. Zpracovala jsem ji pomocí rozhovorů, dotazování, diskuzí a konzultací zainteresovaných pracovníků, ve kterém jsem se zaměřovala na jednotlivé změny práce s ohledem na Obecné nařízení, nové povinnosti z něj vyplývající a na zajištění vhodné úpravy vnitřních předpisů. V návaznosti na výsledek rozhovorů a dotazování jsem popsala jednotlivé dopady na činnost a hospodaření, kde jsem se věnovala i nákladovému zatížení a podala návrh na zdokonalení současného stavu práce na městském úřadě s Obecným nařízením.

I. TEORETICKÁ ČÁST

1 LEGISLATIVA O OCHRANĚ OSOBNÍCH ÚDAJŮ V ČR

1.1 Vývoj právní úpravy o ochraně osobních údajů na území ČR

Jak zmiňuje Navrátil et al. (2018, s. 28), v r. 1918, kdy vznikla Československá republika, byl přijat Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního, což bylo spojení předešlých dvou zákonů, které byly v platnosti na našem území, tj. zákon č. 87/1862 Sb.z.s., o ochraně svobody osobní a zákon č. 88/1862 Sb.z.s., na ochranu svobody domovní. Až do 90. let 20. století se ochraně osobních údajů nevěnovala velká pozornost, jen v oblasti cestovních a jiných dokladů fyzických osob.

Dle Žůrka (2018, s. 18) v období vzniku samostatné České republiky začala být ochrana osobních údajů posuzována samostatně, ale pouze v oblasti informačních systémů, a to přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Tato legislativa nepohlížela na tuto problematiku jako na celek a neřešila oblasti, které bylo potřeba řešit.

První zákon, který se již dotýkal témata ochrany osobních údajů, byla Listina základních práv a svobod č. 2/1993 Sb., která upravovala jak soukromí fyzické osoby, tj. čl. 7 odst. 1 *„Nedotknutelnost osoby a jejího soukromí je zaručena.“*, tak i zneužití osobních údajů a to v čl. 10 odst. 3 *„Každý má právo na ochranu před shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“*. (ČESKO, 1993)

Nejen Žůrek (2018, s. 19) označuje za důležitý moment přijetí prvního komplexního zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon č. 101/2000 Sb.“), který se věnoval ochraně osobních údajů při jejich zpracování jako celku. Na základě tohoto zákona byl zřízen Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) jakožto dozorový úřad, který dohlíží nad dodržováním zásad a povinností při zpracování osobních údajů. V roce 2004, kdy vstoupila Česká republika do Evropské unie, byl zákon č. 101/2000 Sb. několikrát změněn a to v důsledku Směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice 95/46/ES“), které byly nutné jako splnění podmínek pro vstup do EU v oblasti ochrany osobních údajů a kvůli sjednocení právní úpravy.

Nejnovějším plnohodnotným právním rámcem pro ochranu osobních údajů je Obecné nařízení, často používané ve zkratce GDPR, vycházející z anglického názvu General Data Protection Regulation.

1.2 Zákon č. 101/2000 Sb.

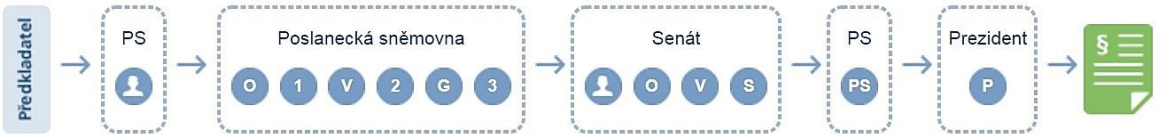
Nezmar (2017, s. 28) zmiňuje mimo jiné i to, že na území České republiky je již delší dobu účinný zákon č. 101/2000 Sb., který nahrazuje nové Obecné nařízení, a to v oblasti práv a povinností při zpracování osobních údajů, tzn. původní práva a povinnosti byly nahrazeny právy a povinnostmi z Obecného nařízení, protože se jedná o nařízení EU, které je použitelné bez dalších úprav pro všechny členské státy. Na zákonu č. 101/2000 Sb. tedy zůstane úprava otázek ohledně ÚOOÚ (např. jeho organizace, atd.) a některé věci, které utvoří z ochrany osobních údajů uzavřený celek a zároveň nejsou upraveny Obecným nařízením, nebo v určitých věcech předpokládá úpravu na úrovni jednotlivých států.

V souvislosti s touto úpravou není zákon č. 101/2000 Sb. v současné době použitelný, protože je v některých případech v rozporu s Obecným nařízením, a proto muselo dojít k řádné adaptaci právního řádu České republiky dle požadavků Obecného nařízení EU. Původně se mluvilo o novelizaci stávajícího zákona, avšak vláda se dohodla na zpracování úplně nového zákona, tj. zákon o zpracování osobních údajů. To znamená, že dnem, kdy vejde v platnost znění nového zákona, se ruší účinnost zákona č. 101/2000 Sb. (Ministerstvo vnitra, 2017)

1.2.1 Adaptační zákon

Jak je uvedeno ve sněmovním tisku (č. 138, 2017), zákon o zpracování osobních údajů, často zmiňovaný jako tzv. adaptační zákon, vláda předložila Poslanecké sněmovně návrh zákona 28. 3. 2018. Text návrhu zákona byl schválen Poslaneckou sněmovnou dne 5. 12. 2018, kdy prošel třetím čtením. Dne 8. 1. 2019 byl návrh zákona postoupen Senátu, který jej projednal 30. 1. 2019 s tím, že návrh vrátil Poslanecké sněmovně s pozměňovacími návrhy. O návrhu vráceném Senátem se hlasovalo 12. 3. 2019, a zároveň bylo vydáno usnesení Poslanecké sněmovny, ve kterém byl vysloven souhlas s návrhem zákona o zpracování osobních údajů ve znění schváleném Senátem. Zákon byl doručen prezidentovi k podepsání 2. 4. 2019. Dne 10. 4. 2019 byl zákon podepsán prezidentem a rozhodnutí bylo doručeno tentýž den do Poslanecké sněmovny. Nový zákon byl publikován ve Sbírce zákonů pod č. 110/2019 Sb., a nabyl účinnosti dne 24. 4. 2019. Jednotlivé

kroky legislativního procesu při projednávání nových návrhů zákonů zobrazuje také následující obrázek.



Obrázek 1 Legislativní proces projednávání návrhů zákonů (Poslanecká sněmovna, 2019)

Zákon o zpracování osobních údajů, upravuje takové záležitosti, ve kterých Evropská unie předpokládá úpravu Obecného nařízení na úrovni jednotlivých států. Mezi upravované oblasti, jak popisují Krančúnová s Kuĺhovou (2017), patří například problematika:

- sociálních síti vzhledem k dětem a mladistvým, kdy bude zapotřebí souhlas zákonného zástupce v souvislosti se zpracováním jejich osobních údajů, kterou prozatím stanovili na 15 let;
- povinnosti mlčenlivosti pověřence, která se bude vztahovat i k jeho podřízeným pomáhajícím s výkonem a plnění úkolů pověřence. Tato povinnost by měla být platná nejen během, ale také po skončení výkonu práce pověřence. Odříci tuto povinnost bude moci jen správce, případně zpracovatel;
- definování pojmu „veřejný subjekt“, ve kterém Česká republika shledává určité odlišnosti, kdo konkrétně bude do této oblasti spadat a kdo ne;
- vydávání osvědčení či certifikátů, při splnění určitých podmínek, se kterým mohou prokázat soulad zpracování s Obecným nařízením. Evropská unie dává členským státům na výběr, zda tato osvědčení bude vydávat dozorový úřad či akreditační úřad. Na úrovni České republiky bude akreditovat osvědčení Český institut pro akreditaci, o.p.s.;
- zaniknutí pozice inspektorů, kteří tvoří strukturu ÚOOÚ včetně předsedy a dvou místopředsedů. Tato pozice bude nahrazena výkonem kvalifikovaných státních zaměstnanců ÚOOÚ;
- sankcí za přestupky, jež by měly být dle nynějšího znění návrhu zákona mírnější pro fyzické a právnické osoby, oproti stanoveným sankcí v Obecném nařízení, tj. vymezení horní hranice 10 milionů Kč pro orgány veřejné moci, zejména pro to, že tyto subjekty nabývají financí ve většině případů ze státního rozpočtu a docházelo by v případě přestupku k pouhému přelévání finančních prostředků, pro podnikatelské subjekty je prozatím vymezena horní hranice na 20 milionů Kč.

2 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Je zapotřebí nejprve popsat, co to vlastně Obecné nařízení je. Dle Nezmara (2017, s. 27) se jedná o Obecné nařízení, které má na starosti ochranu osobních údajů fyzických osob, v oblasti zpracování a volného pohybu těchto údajů, a to po celém území Evropské unie, která tak chrání své občany proti zneužití jejich dat.

Jako stěžejní cíl si Evropská unie (2016) stanovila *„dotvoření prostoru svobody, bezpečnosti a práva a hospodářské unie, k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobým životním podmínkám fyzických osob“*. Což podle Navrátila et al. (2018, s. 30) znamená, že tímto Obecným nařízením má být uzpůsobena legislativa ochrany osobních údajů tak, aby odpovídala současnosti a byla jednotná ve všech členských zemích Evropské unie a v ostatních zemích, na které to dopadá a musí se jím řídit. Dále chtějí podpořit práva na ochranu údajů všech subjektů údajů a tím docílit totožného výkladu Obecného nařízení dozorovými úřady v členských zemích EU. V neposlední řadě by tato úprava měla přispět k posílení důvěry EU s členskými státy, i se státy, které chtějí spolupracovat v oblasti obchodu a dalších záležitostí s Evropskou unií.

2.1 Důvody vzniku nového nařízení

Vývoj vzniku Obecného nařízení popisuje Komínková (2018) na Euroskopu, přičemž začátkem bylo schválení Směrnice 95/46/ES před 24 lety. Plnila svou funkci několik let, ale začala být dosti zastaralá, což se dá označit za největší současný problém. Protože od té doby došlo k neúprosnému posunu lidské společnosti kupředu, a to zejména v oblasti informačních technologií. Bleskovým tempem se začal vyvíjet internet, služby poskytované internetovými stránkami, elektronické obchodování, bankovnictví, rozvoj cloudových úložišť a v neposlední řadě proběhl „boom“ ve světě sociálních sítí. Všechny tyto vymoženosti dnešní doby o nás sbírají informace a zpracovávají naše údaje, kolikrát aniž by, jsme o tom věděli.

Dalším důvodem pro revizi právní úpravy v dané oblasti je fakt, že byla zjištěna v minulosti činnost tajných služeb některých nečlenských států EU. Tajné služby sbíraly osobní údaje o občanech Evropské unie, a ne zrovna v malém rozsahu a objemu. Dále můžeme do důvodů zahrnout prevenci, před protizákonnou manipulací s osobními údaji a jejich zneužívání. Potřeba sjednocení legislativy v rámci Evropské unie a tím mimo jiné

zvýšit důvěru občanů EU. V neposlední řadě můžeme označit jako jeden z důvodů rozvoj digitální ekonomiky, jenž míří kupředu.

Na uvedený vývoj technologií včetně snahy o dosažení nových směrů EU bylo potřeba dle Navrátila et al. (2018, s. 28 – 29) reagovat a to zdokonalením legislativy o ochraně osobních údajů, aby byla přísnější, komplexnější a odpovídala současné situaci. Proto vstoupilo v platnost a později v účinnost Obecné nařízení, které zohledňuje vývoj technologií a posouvá ochranu osobních údajů na daleko vyšší úroveň.

2.2 Nové přístupy práce

Nařízení je postaveno na dvou nových přístupech, tj. princip odpovědnosti správce a přístup založený na riziku.

Princip odpovědnosti správce definuje Navrátil et al. (2018, s. 32) tak, že správce nese odpovědnost za své provedené úkony, za zpracování osobních údajů, za dodržení pokynů a zásad zpracování údajů stanovených Obecným nařízením v čl. 5 odst. 1. Rovněž nese povinnost za doložení souladu s nařízením, např. pomocí kodexu, osvědčením, certifikací či předložením záznamů o činnosti zpracování osobních údajů.

Přístup založený na riziku popisuje Navrátil et al. (2018, s. 32) jako týkající se hlavně nových povinností, které popisuji v podkapitole 2.4 Nové povinnosti dle Obecného nařízení. ÚOOÚ (© 2013) definuje tento přístup jednak z širšího pohledu, kdy správce musí zohledňovat povahu, rozsah, kontext a účel zpracování osobních údajů již od samého začátku zpracování údajů a současně musí být schopný odhadnout případná rizika pro práva a svobody fyzických osob, a podle těchto hrozeb uzpůsobit samotné zabezpečení osobních údajů. V koncepci s Obecným nařízením se jedná kromě toho i o další povinnosti pro správce (pozor, ne pro všechny správce). Přičemž se tyto povinnosti aplikují proto, aby se zamezilo vznikajícím rizikům, ať už menších či větších, pro práva a svobody fyzických osob při zpracování osobních údajů či porušení zabezpečení.

2.3 Principy a zásady

V bodě 26 Obecného nařízení Evropská unie (2016) uvádí, že *„zásady ochrany údajů by se měly uplatňovat na všechny informace týkající se identifikované nebo identifikovatelné fyzické osoby“*. Což znamená, že tyto zásady se nevztahují na zpracování anonymních či anonymizovaných osobních údajů Jak popisuje Žůrek (2018, s. 60) ve své publikaci, zása-

dy jsou jako základna pro zpracování osobních údajů a jako základ pro celou jejich ochranu při zpracovávání. Jedná se o obecnější pojetí dílčích povinností, které Obecné nařízení dále rozepisuje, a které musíme dodržovat.

Obecné nařízení čl. 83 odst. 5 dle Evropské unie (2016) stanovuje, že za porušení těchto zásad je možné uložit tu nejvyšší sankci, neboli správní pokutu, a to až do výše 20.000.000 EUR nebo 4 % celosvětového ročního obratu. Zda sankce bude ve formě eur nebo procent, záleží na výši vypočítané částky, kdy se uloží jako správní pokuta částka vyšší.

Jelikož Obecné nařízení navazuje na již existující právní úpravu ochrany osobních údajů, ne všechny zásady jsou nové, jak píše Navrátil et al. (2018, s. 66 – 67), protože plní svůj úkol tak jak mají a je netřeba je měnit. Mezi nezměněné zásady zpracování údajů patří např. zásada legitimity zpracování, zásada účelovosti, zásada časového omezení, zásada potřebnosti a přiměřenosti, zásada průhlednosti a bezpečnosti, atd.

Na druhou stranu, nových zásad, které definuje Evropská unie (2016) v Obecném nařízení ve čl. 5 je jen několik. Zásady lze shrnout do těchto bodů:

- zákonnost, korektnost, transparentnost;
- omezení účelu;
- minimalizace údajů;
- přesnost;
- omezení uložení;
- integrita a důvěrnost.

2.3.1 Zákonnost, korektnost, transparentnost

Zákonné zpracování osobních údajů považuje Evropská unie (2016) v takovém případě, kdy je splněna minimálně jedna z podmínek uvedených ve čl. 6 odst. 1 Obecného nařízení. To znamená, že správce může zpracovávat osobní údaje pouze v takovém případě, jestliže má k tomu alespoň jeden právní důvod. Právním důvodem se rozumí oprávnění správce údaje zpracovávat za jistým legitimním účelem.

Zásada korektnosti znamená, že správce nesmí tajit záměr, kvůli kterému osobní údaje zpracovává a zároveň by měl dát subjektu údajů informace o tom, kdo bude údaje zpracovávat, v jakém rozsahu a jakým způsobem bude probíhat zpracování včetně toho, komu budou tyto informace dále svěřovány.

Zásadu transparentnosti definuje Žůrek (2018, s. 60 – 62), jako ukládající poslání subjektu údajů zpřístupnění informací a srozumitelnost těchto informací, které dostává od správce nebo na ně má právo. Informace by měly být tedy snadno dosažitelné, např. na internetu – ovšem pouze ve vhodném případě. Srozumitelné, aby jim bylo snadné porozumět.

2.3.2 Omezení účelu

Zásada účelového omezení je podle Nulíčka et al. (2017, s. 107-109) řazena k těm nejdůležitějším vzhledem ke zpracování údajů, a to z toho důvodu, že nám popisuje, jakým způsobem může správce s osobními údaji manipulovat a využívat je. Tím, že správce stanoví účel, si vymezí důvod, proč získané informace zpracovává a nadále je oprávněn osobní údaje zpracovávat podle daného účelu, až na nějaké výjimky (tzv. další zpracování). Omezení účelu je důležité také proto, že na něm záleží další zásady zpracování osobních údajů, tj. minimalizace údajů a omezené uložení. Účelové omezení může stanovovat přímo zákon, ale pokud tak není, je klíčovým okamžikem vymezení účelu správcem potřebné pro zpracování údajů. Toto stanovení omezení účelu se musí uskutečnit nejpozději při momentu sběru informací.

Účel zpracování osobních údajů musí naplňovat několik vlastností, jako je určitost, slovní vyjádření a legitimita. Určitost účelového omezení znamená, že musí být konkrétně stanovený, z jeho vyjádření musí být jasné, jaké manipulace se získanými údaji dovoluje a nedovoluje, a zároveň aby byl v souladu s Obecným nařízením. Pokud správce vymezí účel příliš do detailu, sám si svazuje ruce a omezuje se v případném dalším zpracování, nehledě na to, že v takovém případě se zvyšuje riziko, kdy se zpracování může odchýlit od daného účelu a nebude to tím pádem v souladu se zásadou účelového omezení. Na druhou stranu, by se měl správce vyhnout obecným formulacím, protože zahrnují širokou škálu možnosti zpracování údajů, což není žádoucí. Vlastnost slovního vyjádření, je myšleno v tom smyslu, že správce si vymezí účel zpracování a řídí se podle něj, ale přitom musí účelové omezení říci i subjektům údajů, kterých se to dotýká. Musí ovšem použít takových jazykových prostředků při definování účelu, aby jak správce, tak i subjekty údajů a zpracovatelé tomu rozuměli a vyložili si účel všichni stejně.

Jako poslední vlastnost, která by měla účel naplňovat je legitimita. Jedná se o soulad s právní legislativou. Nejen, že musí být v souladu s Obecným nařízením, ale mimo jiné i s dalšími zákony.

2.3.3 Minimalizace údajů

Jak píše Evropská unie (2016) ve čl. 5 odst. 1 písm. c), tak osobní údaje musí být *„přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány“*, tj. definice zásady minimalizace údajů podle Obecného nařízení.

Co to nicméně znamená? Znamená to další povinnost pro správce, který sbírá informace za účelem pozdějšího zpracování, kdy opatřované osobní údaje musejí být v harmonii s přesně vymezeným účelem zpracování včetně rozsahu nepostradatelném pro splnění konkrétního účelu. Aby správce tuto povinnost naplnil, musí si přesně stanovit tzv. minimální rozsah faktických osobních údajů, které bude opravdu potřebovat pro následné zpracování údajů konkrétního účelu. Jakmile si správce stanoví rozsah osobních údajů, které má k dispozici, pro budoucí zpracování, je nezbytné, aby byl schopen u každého dílčího údaje říci, proč právě on je nezbytný pro naplnění stanoveného účelu.

Rozsah by neměl být podle Janečkové (2018, s. 7) zbytečně široký, nadbytečné osobní údaje by měl správce odstranit, v nejlepším případě by je neměl vůbec začít sbírat. Záměrem této zásady je docílení takového zpracování dat, při kterém nám bude stačit ke splnění účelu ta nejužší část osobních údajů.

2.3.4 Přesnost

V takové podobě jak osobní údaje získáme při jejich shromažďování, tak je musíme i zpracovávat bez jakékoli změny. V případě nutnosti je můžeme pouze podrobit aktualizaci, ale v žádném případě je nesmí správce měnit. Jen takové zpracovávání informací můžeme označit za správné a vedoucí k naplnění účelu, pro který bylo zpracování údajů stanoveno.

Správce nemusí „pátrat“ po zastaralosti získaných informací, po jejich možné aktualizaci, aby se neustále dožadoval u subjektů údajů nových, aktualizovaných dat. Jiná situace je ta, kdy sám subjekt údajů chce na základě žádosti pozměnit své osobní údaje. V případě, že u správce dojde ke zjevné odlišnosti dat, musí zavést opatření, které zjevně odlišné údaje buď odstraní, nebo opraví tak, aby byl zaručen soulad s účelem zpracování osobních údajů. Opravovat může správce údaje ve výjimečných situacích, kdy je jasné, že se jedná o viditelný překlep např. v křestním jménu subjektu nebo doména u e-mailových adres. (Žůrek, 2018, s. 63 – 64)

2.3.5 Omezení uložení

O omezení uložení píše Nulíček (2017, s. 113 – 115) ve své knize, kde definuje tuto zásadu, jako ukládající povinnost uchovávat osobní údaje jen po takovou dobu, která je nezbytná pro naplnění účelu zpracování. Pokud má správce jeden druh osobního údaje, může jej využít pro více účelů na základě svých oprávnění (např. jméno subjektu údajů). Na druhou stranu, jestliže správce uchovává takové informace o subjektech údajů, které již nepotřebuje pro stanovený účel zpracování, musí tyto údaje odstranit z evidence nebo je anonymizovat.

V některých případech je nutné informovat subjekty údajů o době, po kterou budou využívány. Týká se to většinou takových situací, ve kterých je to nutné pro zajištění zásady transparentnosti a korektnosti. Ať už tato doba bude definována počtem dní, měsíců, let, nebo např. ukončením poskytování určité služby. Vždy se bude kontrolovat, zda data nebyla evidována po dobu delší, než bylo stanoveno.

2.3.6 Integrita a důvěrnost

Tuto zásadu popisuje Valentová (2018, s. 106) coby povinnost manipulovat s osobními údaji takovým způsobem, abychom zajistili jejich bezpečnost, což je v problematice Obecného nařízení klíčové. Musí se přijmout opatření jak technické, tak i organizační zajišťující již zmíněnou bezpečnost zpracovávaných informací včetně ochrany před zneužitím, protiprávním zpracováním nebo před zpracováním bez potřebného oprávnění. Ochrana údajů by se měla vztahovat i na nahodilou ztrátu, zničení či poškození osobních údajů.

2.4 Nové povinnosti dle Obecného nařízení

Obecné nařízení stanovuje také pro správce několik nových povinností, tj.:

- vytvoření záznamů o činnostech;
- posouzení vlivu na ochranu osobních údajů;
- povinnost zabezpečení a hlášení bezpečnostních incidentů ÚOOÚ a subjektu údajů;
- předchozí konzultace s ÚOOÚ;
- jmenování pověřence.

(Nezmar, 2018, s. 30)

2.4.1 Vytvoření záznamů o činnostech

Jak píše Janečková (2018, s. 27) *„jedná se v podstatě o podrobný popis zpracování, které probíhá u jednotlivých správců a zpracovatelů“*. Díky této nové povinnosti dosáhnou jak správci, tak i dozorový úřad úplného přehledu. Záznamy musejí splňovat určitá kritéria, která jsou vypsána výčtem v nařízení.

Oznamovací povinnost, která byla zrušena dle Obecného nařízení, tak vykompenzovaly záznamy o činnostech. Správci a zpracovatelé jsou, jak již zákon říká, povinni vést s určitými informacemi záznamy a těmito záznamy mohou podložit práci v souladu s Obecným nařízením. (Nezmar, 2018, s. 31)

2.4.2 Posouzení vlivu na ochranu osobních údajů (DPIA)

Jak uvádí Evropská unie (2016) v čl. 35 Obecného nařízení je nutné provést Data Protection Impact Assessment (DPIA), tedy posouzení vlivu na ochranu osobních údajů u takového druhu zpracování, u kterého se může vyskytnout vysoké riziko pro práva a svobody fyzických osob. Může se tak stát např. v důsledku použití nových technologií, při rozsáhlém automatizovaném zpracování včetně profilování, při zpracování zvláštních kategorií údajů nebo systematického monitorování veřejných prostor.

„DPIA je proces, jehož cílem je popsat zpracování, posoudit nezbytnost a přiměřenost zpracování a napomoci zvládnutí rizik pro práva a svobody fyzických osob vyplývající ze zpracování osobních údajů“, jak uvedl Nezmar (2017, s. 99) ve své publikaci.

Správce je v takové situaci povinen provést posouzení vlivu daného zpracování na ochranu údajů. Při procesu posouzení vlivu si správce zažádá o posudek od pověřence pro ochranu osobních údajů, pokud byl jmenován. Mohou existovat i seznamy obsahující druhy zpracování osobních údajů, u kterých je nutné provést posouzení vlivu a naopak seznamy operací, u kterých posouzení vlivu není nutností. Takový seznam sestavuje dozorový úřad.

Posouzení vlivu na ochranu osobních údajů by mělo obsahovat přinejmenším:

- systematický popis zamýšlených operací zpracování a účely zpracování;
- posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
- posouzení rizik pro práva a svobody subjektů údajů;
- plánovaná opatření k řešení těchto rizik.

Obrázek 2 Proces provedení posouzení vlivu na ochranu osobních údajů (Žůrek, 2018, s. 126)

2.4.3 Předchozí konzultace s ÚOOÚ

Tato povinnost se týká správce, který musí provést konzultaci s ÚOOÚ ohledně zpracování osobních údajů, v případě, kdy předpokládáme, že daný druh zpracování údajů povede k vysokému riziku, jestliže správce neučiní vhodné opatření ke zmenšení tohoto rizika. To znamená, že se konzultace povede v případě, jestliže i po přijetí opatření ke snížení rizika trvá hrozba vysokého rizika. Cílem této povinnosti je ovládat a zmírňovat případná velká rizika. (ÚOOÚ, © 2013)

2.4.4 Změny v povinnostech

Jak uvádí Navrátil et al. (2018, s. 65- 66), Obecné nařízení není úplně novým právním předpisem, ale navazuje na již zavedenou legislativu zaměřenou na ochranu osobních údajů. Některé záležitosti vzhledem ke staré právní úpravě mění, ruší či zakládá nové. Zde jsou dvě hlavní změny ze starého na nový zákon:

- správci a zpracovatelé se již nemusejí povinně registrovat u ÚOOÚ, tato povinnost se tedy ruší, ale nahrazuje ji povinnost nově vzniklá, tj. musejí vést předběžné konzultace s ÚOOÚ;
- dále se nemusí vypracovávat „projekt ochrany osobních údajů“ podle zákona č. 101/2000 Sb., tj. další rušící se povinnost, ale tuto povinnost nahrazuje jiná, což je posouzení vlivu na ochranu osobních údajů.

2.5 Práva subjektu údajů

Subjektem údajů stanovuje Obecné nařízení fyzickou osobu, která má svá práva, nerozdílně od zákona č. 101/2000 Sb. Ovšem Obecné nařízení posiluje práva subjektů a podle ÚOOÚ (© 2013) je *„jejich účelem vybalancovat vztah mezi správcem a subjektem údajů“*.

Subjekty údajů disponují několika právy, my si zde zmíníme jen ty nejdůležitější, např. právo na informace o zpracovávání jejich osobních údajů a zpřístupnění těchto údajů či právo na opravu údajů či výmaz neboli „právo být zapomenut“. Všechna práva se rozdělují do dvou kategorií. První kategorie je ta, kdy informace získáme přímo od subjektu údajů, a druhá obsahuje informace, které správce získal jiným způsobem než od subjektu údajů, např. od jiného správce. (ÚOOÚ, © 2013)

2.5.1 Právo být informován a mít přístup k osobním údajům

Právo subjektu údajů na informace se považuje za základní právo, kterým subjekt disponuje a naplňuje se tak zásada transparentnosti. Toto právo má vést subjekt údajů k patřičné informovanosti o využívání a zpracovávání informací o něm. Mezi tzv. minimum poskytovaných informací patří např. totožnost a kontaktní údaje na správce a pověřence (pokud byl jmenován), účely a právní důvody zpracování, informace o příjemci údajů, doba, po kterou budou údaje evidovány, atd. Informovanost patří mezi pasivní práva subjektu, jelikož by se subjekt tohoto práva neměl domáhat správce, ale poskytování informací o zpracování by mělo být automatické.

Jelikož poskytované informace subjektům jsou mnohdy hodně obsáhlé, musí správce najít vhodný způsob jakým je zpřístupňovat, aby dodržel postuláty a zároveň byly informace srozumitelné a jednoduché, což je kolikrát velmi obtížné v důsledku objemnosti dat, jak uvádí Žůrek (2018, s. 132 – 135).

Přístupem k osobním údajům se rozumí dle Nezmara (2017, s. 36 – 37) povinnost správce umožnit získání informací subjektu údajů o tom, zda se osobní údaje o jeho osobě nacházejí v procesu zpracování či nikoliv. Subjekt je oprávněn získat zpracovávané údaje držené správcem. Jestliže se jeho údaje zpracovávají, má právo vědět mimo jiné i další informace týkající se daného zpracování, které jsou vypsané v předcházejícím odstavci vzhledem k informovanosti. Navíc má právo na opravu či výmaz osobních údajů, na vznesení námitky nebo stížnosti u dozorového úřadu. V opačném případě, kdy správce nijak neoperuje

s osobními údaji subjektu, dá mu informace o tom, že údaje subjektu nejsou předmětem zpracování ze strany správce.

Jedná se o aktivní právo subjektu, protože pro zpřístupnění osobních údajů musí subjekt požádat správce a v tom okamžiku, se to pro správce stává povinností, s čímž by měl počítat a být na to připraven. Aby mohl subjekt o přístup zažádat, potřebuje od správce potvrzení o zpracování jeho osobních údajů. (Žůrek, 2018, s. 135 – 136)

2.5.2 Právo na opravu, doplnění a výmaz osobních údajů

Jak stanovuje Evropská unie (2016) čl. 16 první věty, má subjekt údajů právo na to, aby správce při zjištění či na základě žádosti subjektu, opravil nepřesné, zastaralé a již nepravdivé informace, které eviduje, protože to ovlivňuje zpracování osobních údajů a není to v souladu se zásadou přesnosti.

Na základě druhé věty čl. 16 Obecného nařízení je subjekt údajů oprávněn na základě své dobré vůle poskytnout dodatečné informace a doplnit tak své osobní údaje, které správce vede v evidenci. Jedná se avšak o informace, které se vztahují k účelu zpracování údajů.

Právo na výmaz neboli „právo být zapomenut“ popisuje Evropská unie (2016) jako povinnost správce vůči subjektům údajů, kteří mají právo se domáhat vymazání jejich osobních údajů a ukončení tak jejich evidování. Toto právo vzniká, jestliže již pominula potřebnost pro stanovený účel zpracování, v situaci, kdy subjekt svůj souhlas se zpracováním osobních údajů odvolal, v případě vznesení námitky proti manipulaci s jeho osobními údaji, anebo se správce dopustil protiprávního jednání a zpracovával osobní údaje v rozporu s Obecným nařízením a další legislativou. Podle Navrátila a kolektivu (2018, s. 75 – 76) je „právo být zapomenut“ velice důležité, zejména z hlediska mladistvé nerozvážnosti. Jedná se zejména o internetové stránky, kdy se může stát, že jako mladistvý uložil subjekt údajů souhlas se zpracováním svých osobních údajů a později toho litoval, protože v té době netušil, jaké to může mít následky v budoucnosti. Subjekt údajů tedy odvolá souhlas se zpracováním a žádá o odstranění veškerých informací, které se ho týkají. V této situaci je povinen správce, který údaje zveřejnil, kontaktovat správce, který tyto údaje zpracovává, aby odstranil veškeré vazby, kopie či repliky osobních údajů konkrétního subjektu.

2.5.3 Právo vznést námitku proti zpracování osobních údajů

Na základě čl. 21 Evropské unie (2016) platí, že za patřičného odůvodnění plynoucího ze stávající situace subjektu, má právo vznést námitku proti zpracování jeho osobních údajů.

V takovém případě nesmí správce dále zpracovávat konkrétní data, a to až do okamžiku, jestliže nedokáže na základě oprávněných argumentů, že tyto důvody převyšují zájmy subjektu.

Pokud jde o přímý marketing, jakožto oblast zpracování osobních údajů, může subjekt taktéž kdykoli vznést námitku proti zpracování jeho údajů pro účely přímého marketingu. V takové situaci správce přestává a má zákaz zpracovávat osobní údaje subjektu, který vznesl námitku.

2.6 Pověřenec pro ochranu osobních údajů

Ministerstvo vnitra (2018) charakterizuje pověřence, neboli Data Protection Officer (DPO), jako *„důležitého pomocníka a konzultanta v systému ochrany osobních údajů“*, který má specifické postavení. Pozici pověřence může vykonávat jak fyzická osoba, např. pracovník obce či externista, tak i právnická osoba, např. advokátní kancelář. V momentě, kdy si obec vybere právnickou osobu, musí být zároveň zvolena konkrétní fyzická osoba vystupující pod danou právnickou osobou, která bude odpovědná za roli pověřence. Aby jej mohl kdokoliv kontaktovat ve věcech ochrany a zpracování osobních údajů, musí na něj být zpřístupněný kontakt s údaji a to nejlépe na úřední desce a zároveň v elektronické podobě a musí se sdělit dozorovému úřadu.

2.6.1 Úkoly a náplň práce

Prací pověřence pro ochranu osobních údajů je poskytování možnosti poradenství v oblasti povinností a dalších věcí jak pro správce, tak pro zpracovatele včetně jejich zaměstnanců, kteří zpracovávají osobní údaje. Dále je pověřenec povinen sledovat zpracování osobních údajů a hodnotit harmonii mezi zpracováním a Obecným nařízením, zda nedochází k protiprávnímu jednání, které je v rozporu s daným právním rámcem. Mezi jeho další náplně práce patří vlastnost kontaktní osoby, tzn. je ve spojení s dozorovým úřadem, pro území ČR se jedná o ÚOOÚ, dále je kontaktní osobou i pro samotné jedince, neboli pro subjekty osobních údajů, kterých se informace týkají. Všechny tyto osoby se mohou pověřence dotazovat v záležitostech týkajících se zpracování a ochrany osobních údajů subjektů včetně vymáhání jejich práv bez nijakého omezení.

Úlohou je tedy podporovat již zmíněné osoby při aplikaci Obecného nařízení v praxi a tím zajišťovat naplnění souladu reality s Obecným nařízením a další právní úpravou. Úkolem

pověřence je i školení pracovníků a celkové řízení oblasti interní ochrany dat. (Ministerstvo vnitra, 2018)

I když pověřenec radí správci a zpracovateli, nenese za následné zpracování údajů správce či zpracovatele podle poskytnutých rad odpovědnost. Odpovědnost nesou za provedené postupy nadále jednotlivé obce a kraje, neboli správci a zpracovatelé. Ti musejí být schopni v případném dotazu dokázat, že osobní údaje zpracovávají správně v rámci zákonu, jak správně uvádí Nulíček et al. (2017, s. 332).

2.6.2 Jmenování

Jmenovat pověřence pro ochranu osobních údajů má právo správce se zpracovatelem jak stanovuje Evropská unie (2016). Ti jmenují fyzickou osobu do funkce pověřence v případě, kdy orgán veřejné moci či veřejný subjekt provádí zpracování (kromě soudů, ty disponují svými pravomocemi), nebo v situaci, jestliže hlavní náplní práce správce či zpracovatele je zpracování, u kterého je nutné rozsáhlé pravidelné monitorování subjektů údajů včetně rozsáhlého zpracování zvláštních kategorií osobních údajů. Pověřenec ovšem nemusí být vždy jen a pouze jmenován, ale může být i tzv. ustanoven či může být konkrétní osobě svěřena funkce pověřence.

Pokud se jedná o orgán veřejné moci, tak vzhledem k jejich organizační struktuře a velikosti, může být jmenován jen jeden pověřenec pro více takových orgánů, jak je stanoveno v čl. 37 odst. 3 Obecného nařízení.

Nicméně nařízení již nedefinuje, jakou odbornou způsobilost by pověřenec měl mít, jen říká, že musí mít určitou profesní kvalitu a odborné vědomosti a praxi z oblasti práva a ochrany osobních údajů. Pokud takových znalostí a zkušeností nabývá, neměl by být pro něj problém plnit svou práci nezávisle na jiných osobách, což popisuje Janečková (2018, s. 39) ve své publikaci.

3 DEFINOVÁNÍ ZÁKLADNÍCH POJMŮ SOUVISEJÍCÍCH S GDPR

Než se člověk ponoří do samotného Obecného nařízení, je nutné, aby rozuměl základním pojmům, které používá. Proto je jedna kapitola teoretické části věnována definování základního pojmosloví, které se vyskytuje v Obecném nařízení, a které se objevuje v textu bakalářské práce.

3.1 Osobní údaj

Vzhledem k problematice, je právě pojem osobní údaj nejvíce zmiňovaným a skloňovaným ve všech pádech. Evropská unie (2016) definuje tento pojem v čl. 4 odst. 1, kdy se jedná o *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě“*. Oproti zákonu č. 101/2000 Sb. nebyl nijak změněn význam pojmu osobní údaj.

Aby byla osoba identifikovaná či identifikovatelná, jak definuje Žůrek (2018, s. 42 – 43), musíme být schopni tuto osobu přímo či nepřímo identifikovat, dle stanovených identifikátorů nebo základě jednoho či více prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity osoby. Jedná se např. o jméno, číslo, lokační údaje či síťový identifikátor.

3.2 Citlivý údaj

Citlivost údajů se posuzuje z hlediska základních práv a svobod subjektu. Podle Evropské unie (2016) skupinu „citlivých údajů“ řadí mezi zvláštní kategorii osobních údajů, které spadají pod zvláštní ochranu. Zvláštní ochrana proto, že při zpracování takových údajů hrozí vznik rizika pro základní práva a svobody.

Nařízení do oblasti citlivých údajů zahrnuje osobní údaje o *„národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filosofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu, sexuálním životě a také biometrické nebo genetické údaje“* coby definováno dle Maštalky (2008, s. 23 – 24).

3.3 Subjekt údajů

Evropská unie (2016) považuje za subjekt údajů identifikovanou nebo identifikovatelnou fyzickou osobu, ke které se vztahují osobní údaje. Calder (2016, s. 26) říká, že zákon tuto definici nijak dále nerozvádí, ani neomezuje, což znamená, že subjektem osobních údajů může být jakákoliv fyzická osoba, která se vyskytuje kdekoliv na světě, ovšem za předpo-

kladu, že je identifikovatelná. Subjektem může být ovšem jen výhradně fyzická osoba, např. obchodní společnost nebo jiné právnické osoby nemohou být subjektem údajů a tudíž informace o nich nespadají pod ochranu.

3.4 Zpracování osobních údajů

Zpracováním můžeme dle Nezmara (2017, s. 31) označit jakoukoli aktivitu či soubor aktivit, které se dotýkají osobních údajů. Tyto operace mohou probíhat automatizovaně či nikoliv a řadíme mezi ně např. shromažďování, uspořádání, uchovávání, pozměnění, vyhledání, zpřístupnění, blokování či likvidaci a mnoho dalších.

Všechny osobní údaje ovšem nespadají pod ochranu, ale pouze ty, které jsou zpracovávány. Tudíž můžeme říci, že bez zpracování neexistuje ochrana dat a naopak. Mezi hlavní operace s osobními údaji můžeme zařadit:

- shromažďování – takové informace, které získáváme k uložení, včetně operací, které mají za cíl takovou úpravu informací, aby byly vhodné k uchování;
- uchovávání – založení informací např. do kartotéky či databáze, které umožňují následné zpřístupnění dat;
- zpřístupňování – příjemce informací musí mít oprávnění k získání a použití konkrétních osobních údajů. Formou zpřístupnění je zveřejnění, kdy osobní údaje získají všichni, aniž by museli dokazovat jakoukoli skutečnost;
- blokování – osobní údaj znepřístupníme na určitou dobu, po kterou je posuzována např. z důvodu ověřování její přesnosti. Po dokončení posuzování je informace vrácena zpět do procesu nebo naopak může být zlikvidována;
- likvidaci – znamená úplné vymazání informace z databáze a z dalšího používání, či odstranění formou anonymizace.

(Maštalka, 2008, s. 26 – 28)

3.5 Správce

Právě správce osobních údajů patří podle Žůrka (2018, s. 89) k těm důležitějším pojmům a subjektům z hlediska problematiky Obecného nařízení. Tuto důležitost si zasloužil z důvodu, že je tím hlavním, který stanovuje účel a prostředky zpracování osobních údajů. Jak je uvedeno v publikaci Nezmara (2017, s. 150) se jedná zejména o případy rozhodnutí ve věcech:

- kategorie shromažďovaných osobních údajů;
- kdo data shromažďuje;
- zda je potřeba souhlas subjektu;
- jak dlouho budou data shromažďována;
- zda a jakým způsobem bude subjekt informován;
- jak budou data zabezpečena;
- jaké je případné riziko pro subjekty plynoucí ze zpracování.

Ať už se jedná o vlastní rozhodování nebo rozhodování ve spolupráci s jinými subjekty. Bez správce by samotné zpracování ani nemohlo začít. Evropská unie (2016) definuje, že správcem může být *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt“*. Správcem je i vybraný městský úřad, na který je bakalářská práce zaměřena.

Za zpracování osobních údajů nese správce odpovědnost a to i v případě, že jmenuje pověřence. *„Správce může pro zpracování využít jiný subjekt, přičemž tento pověřený subjekt se nazývá zpracovatel.“* To jest situace, kdy za chyby pověřence nese následky správce, který mu radí a pomáhá v mnoha záležitostech, popisuje Žůrek (2018, s. 90).

3.6 Zpracovatel

Žůrek (2018, s. 91) popisuje pozici zpracovatele coby subjekt, který pomáhá se zpracováním osobních údajů pro svého správce, a to jen v případě, že jej správce daným úkolem pověří. Správce nemusí vždy služby zpracovatele využít, pouze když chce.

Rozdíl mezi správcem a zpracovatelem definuje Ministerstvo vnitra (2018) *„zpracovatel v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen“*.

3.7 Profilování

Evropská unie (2016) uvádí definici profilování jako *„jakoukoli formu automatizovaného zpracování osobních údajů“*, které jsou založeny na jejich aplikaci k hodnocení některých osobních údajů, a které se týkají fyzické osoby, a to především k analýze či předvídání aspektů souvisejících ať už s výkonem fyzické osoby v zaměstnání, ekonomickou situací, zdravotním stavem, osobní preferencí, zájmy, spolehlivostí, chování či místa, kde se fyzická osoba nachází nebo pohybuje. Podle těchto informací se postupně vytváří profil dané

osoby. Při profilování osobních údajů musejí být informovány subjekty, kterých se to týká, a musejí s tím souhlasit. (Calder, 2016, s. 30 - 31)

3.8 Anonymizace, pseudonymizace

Pseudonymizované údaje musíme dle Matouškové (2008, s. 32 – 33) odlišovat od anonymních údajů. Anonymní informace nedokážeme spojit s konkrétní fyzickou osobou, ke které by dané informace příslušely. Tato neurčitelnost může být již od počáteční podoby, tj. anonymní údaj nebo až po zpracování, které klasický osobní údaj upraví a změní na anonymní, tzv. anonymizace. Z hlediska procesu zpracování, rozlišujeme úplnou a částečnou anonymizaci. Úplná znamená, že anonymní údaje již nelze přiřadit zpět k subjektu údajů. Při částečné anonymizaci lze za dodržení určitých podmínek spojit údaje k subjektu a to za předpokladu, že subjekt údajů sám k sobě anonymní údaj vztáhne.

Pseudonymizované informace, na rozdíl od anonymních definuje Žůrek (2018, s. 44 – 45) tak, že je lze přiřadit k subjektu údajů, jedná se o tzv. dodatečné informace, na které se musíme dívat jako na osobní údaje.

Přesnou definici pseudonymizace nám říká Evropská unie (2016), kterým se rozumí *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“*.

Pro lepší představení, jak pseudonymizace funguje, jsem uvedla příklad pseudonymizovaných dat, který je zobrazen na následujících obrázcích. Konkrétní data subjektu údajů se od sebe oddělí do dvou různých databází s tím, že mají stejný jeden prvek (v tomto případě ID), díky kterému má uživatel možnost určit, komu data patří, avšak pouze v případě, že má přístup k oběma souborům.

Jméno	Příjmení	Rodné číslo	Telefon
Petr	Vomáčka	560214/134	241 252 252
Karel	Bludička	720516/456	602 789 466
Jana	Nová	875712/9871	774 569 336

Obrázek 3 Data bez pseudonymizace (Nezmar, 2017, s. 115)

ID	Jméno	Příjmení
1	Petr	Vomáčka
2	Karel	Bludička
3	Jana	Nová

ID	Rodné číslo	Telefon
1	560214/134	241 252 252
2	720516/456	602 789 466
3	875712/9871	774 569 336

Obrázek 4 Pseudonymizovaná data (Nezmar, 2017, s. 116)

3.9 Dozorový úřad

Žůrek (2018, s. 173) píše, že pro naplnění ochrany osobních údajů při jejich zpracování jsou důležitým prvkem jednotlivé dozorové úřady členských zemí EU, jež dohlížejí na dodržování Obecného nařízení se snahou *„chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů“*. Dozorové úřady spolupracují mezi s sebou, protože musejí dbát na zásadu jednotnosti.

Úřad pro ochranu osobních údajů, založený jako dozorový úřad v České republice, je „nezávislým orgánem, který:

- provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů;
- vede registr povolených zpracování osobních údajů;
- přijímá podněty a stížnosti občanů na porušení zákona;
- poskytuje konzultace v oblasti ochrany osobních údajů.“

(ÚOOÚ, © 2013)

3.10 Souhlas subjektu údajů

Podle Evropské unie (2016) se souhlasem subjektu údajů rozumí *„jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*.

Abychom mohli souhlas označit jako řádný, musí splňovat několik stanovených podmínek, které jsou často pozměňovány. Správce, zpracovatel nebo kdokoliv jiný, který zpracovává jakýmkoliv způsobem osobní údaje, musí být schopný předložit oprávnění, neboli souhlas subjektu údajů, tyto informace zpracovávat.

II. PRAKTICKÁ ČÁST

4 PŘÍKLADY ODCIZENÍ OSOBNÍCH ÚDAJŮ

4.1 Facebook & Cambridge Analytica

Před více než rokem jsme mohli zaznamenat počátek velké kauzy ohledně zneužití osobních dat z celosvětově známé sociální sítě Facebook. Jak jsem již zmiňovala, technologie nynější doby, jako je internet, o nás neustále sbírají a uchovávají informace. Toto platí i o Facebooku, který toho značně využil v situaci, kdy poskytl informace o svých uživatelích, které uchovával, datové firmě Cambridge Analytica. Poskytla mu neomezený přístup k datům zhruba 87 milionů uživatelů, kteří o tom nevěděli. Tato data měla ovlivnit několik voleb, např. prezidentské volby v USA, ve kterých vyhrál Donald Trump. Po výzkumu a vyšetřování této kauzy se odhalila skutečnost, jak došlo k ovlivnění voleb „ukradenými" osobními údaji z Facebooku. Počátkem bylo vytvoření testu osobnosti „OCEAN", který sloužil pro uživatele k posouzení svého psychologického profilu. Tam museli ovšem uvést souhlas s přístupem aplikace k jejich profilu. Po nějaké době, získala aplikace i profily všech přátel dané osoby, která uvedla souhlas. A právě tato aplikace byla spojena velkou částí s projektem „Project Alamo", který sloužil jako volební kampaň pro nynějšího prezidenta USA Donalda Trumpa. (Isaak, Hanna, 2018)

4.2 Marriott International, Inc.

O něco novější kauza z oblasti kybernetický útoků a odcizení osobních údajů, se stala na podzim loňského roku. V tomto případě se jedná o ubytovací společnost, jejíž působnost je celosvětová, protože přes 6700 ubytovacích zařízení této společnosti, se vyskytuje v téměř 130 zemích a oblastech po celém světě. I přes její 90 let starou tradici, se prozatím nesetkala s tak velkým problémem. (Marriott, © 2019)

Oproti předešlému příkladu Cambridge analytica a Facebooku je tato situace mnohem větší, co se čísel týče, protože v tomto případě byly odcizené informace o zhruba 500 milionů klientů. Začalo to v září 2018, kdy se společnost Marriott dozvěděla, nejen že došlo, ale docházelo již od r. 2014 k neoprávněnému přístupu do sítě Starwood a během celé této doby docházelo k úniku dat. Odcizené byli informace o klientech zejména v podobě jména, poštovní adresy, telefonního čísla, e-mailové adresy, čísla pasu, informací o účtu Starwood, datum narození, informace o příjezdu a odjezdu, datum rezervace a komunikační preference. Ne u každého klienta byly ukradeny všechny tyto typy informací, ale jednalo se o různé kombinace. Unikly taktéž čísla platebních karet a datum vypršení platnosti platební

karty. Marriott ovšem uvádí, že platební karty byly zašifrovány, ale prozatím nemůže vyloučit, že klíč k dešifraci nebyl ukraden také. (O'Flaherty, 2018)

Došlo i k vyčíslení ztráty, která by se měla pohybovat mezi 200 a 600 miliony dolarů, ale je to prozatím pouze odhad, jak uvedla společnost AIR Worldwide. Marriott se snaží alespoň nějakým způsobem napravit tuto závažnou situaci a pomoci svým klientům, např. tím, že jim proplatí výměnu platební karty, vytvořili call centrum a webové stránky, na kterých se mohou klienti informovat o dané situaci, a získat veškeré potřebné informace.

Je zde prozatím mnoho otazníků, ať už ohledně vyčíslení škody, kolik přesně lidí to zasáhlo, zda mezi nimi byly i osoby z EU a tím pádem by se jednalo o porušení Všeobecného nařízení o ochraně osobních údajů, na základě kterého by mohla být vyčíslena pokuta až do astronomických výší. Ale jedno je jasné, tento případ úniku osobních údajů se považuje za největší po obří kauze odcizení dat ze společnosti Yahoo. (Insurance Journal, 2018)

5 CHARAKTERISTIKA OBCE S ROZŠÍŘENOU PŮSOBNOSTÍ

Vybraný městský úřad (dále jen „vybraný MěÚ“), který jsem analyzovala z hlediska implementace Obecného nařízení na jeho činnost a hospodaření, je obcí s rozšířenou působností (dále jen „ORP“). Před definováním ORP je zapotřebí definovat základní stavební kámen tohoto pojmu. Jedná se o obec. Jak stanovuje zákon č. 128/2000 Sb. o obcích, obec je základní územní samosprávný celek, jedná se o společenství občanů, jež je vymezeno svým územím. (ČESKO, 2000) Pomocí svých orgánů, jak definuje Hendrych et al. (2016, s. 105 - 106) vykonávají obce své činnosti, napomáhají k vnitřní a vnější organizaci samosprávného celku. Jak píší Kopecký, Průcha, Havlan a Janeček (2016, s. 16 – 18) obec se dle své působnosti rozděluje na obec vykonávající svou činnost v samostatné a přenesené působnosti. Při výkonu samostatné působnosti má obec ve svém rozhodování určitou míru autonomie. Věci a situace, ve kterých může samostatně rozhodovat, jsou stanovené zákony, přičemž i rozsah tohoto rozhodování je dán zákonem. Naopak v přenesené působnosti jsou na obce na základě zákona delegovány určité otázky a činnosti státní správy. Všechny obce nevykonávají stejný rozsah přenesené působnosti, jak uvádí Malast (2016, s. 279 – 281) ve své publikaci, ale rozlišujeme obce dle jejich rozsahu výkonu státní správy v přenesené působnosti na obce se základním rozsahem (zde patří všechny obce ČR) a širším rozsahem, přičemž do širšího rozsahu patří ty obce, které dělají něco navíc než ty obce se základním rozsahem. Obce rozdělujeme do následujících kategorií obcí:

Tabulka 1 Kategorie obcí (Malast, 2016, s. 280)

Kategorie	Počet
obec se základní působností	6259
obec s pověřeným obecním úřadem	388
obec s rozšířenou působností	205
obce s matričním úřadem	1230
obce se stavebním úřadem	618
obce jako kontaktní místo veřejné správy (CzechPOINT)	5800

Obce s matričním úřadem, se stavebním úřadem a obce, které jsou kontaktními místy pro veřejnou správu (tzv. CzechPOINT) se řadí do zvláštní skupiny obcí při jejich rozdělování

do jednotlivých kategorií. Při tomto rozdělení může nastat také situace, kdy obec nevykonává povinnost z hlediska vykonávání státní správy v přenesené působnosti. Pokud je schopna danou povinnost plnit, ale neplní, má možnost zasáhnout obec, která je „nadřazená“ (má vyšší působnost), ovšem pouze v případě, že obec spadá do jejího obvodu. Obce, které nemohou vykonávat svou povinnost v tomhle ohledu, mohou uzavřít s jinou obcí veřejnoprávní smlouvu, pomocí které dané činnosti deleguje.

5.1 Obecní úřad s rozšířenou působností

Tyto obecní úřady můžeme označit dle Malasta (2016, s. 279 – 281) za jakýsi mezičlánek přeneseného výkonu státní správy mezi krajskými úřady a obecními úřady. ORP disponují oproti „obyčejným“ obecním úřadům činnostmi navíc, které mají v působnosti nejen pro svou obec, ale často i pro okolní obce, které pod ORP spadají.

V případě vybraného MěÚ se jedná o následující oblasti:

- evidence obyvatel;
- vydávání cestovních a osobních dokladů, řidičských průkazů, technických průkazů;
- živnostenské oprávnění;
- sociálně-právní ochrana dětí;
- péče o staré a zdravotně postižené;
- vodoprávní řízení, odpadové hospodářství a ochrana životního prostředí;
- státní správa na úseku lesů, myslivosti a rybářství;
- vybraná problematika v dopravě a silničním hospodářství.

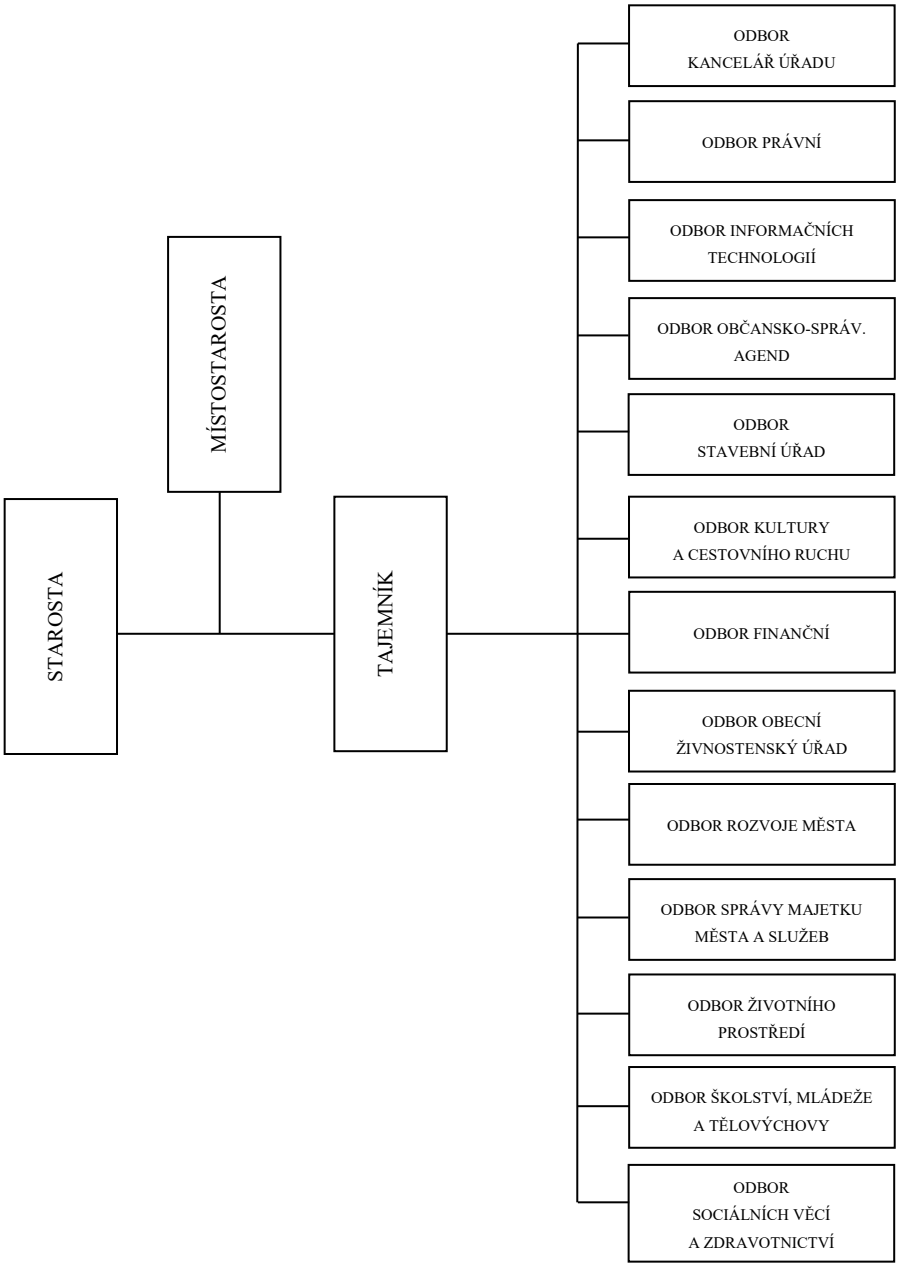
5.2 Organizační struktura

Hlavním představitelem organizace vybraného MěÚ je starosta, který je zastupován místostarosty. Je přímý nadřízený tajemníku úřadu a všem dalším zaměstnancům. Hlavními úkoly tajemníka je řízení a kontrola činnosti zaměstnanců úřadu a zároveň plní funkci nadřízené osoby pro vedoucí odborů a samostatných úseků. Z výsledků své činnosti je tajemník odpovědný svému přímému nadřízenému – starostovi. Pod úsek tajemníka patří oddělení personální, mzdové a vzdělávací, tiskový mluvčí, dále pak asistenti starosty a místostarostů a jako poslední agenda projektu Zdravého města. Všichni tito zaměstnanci se zodpovídají za svou práci tajemníkovi úřadu.

Vedoucí jednotlivých odborů řídí a kontrolují činnost zaměstnanců, kteří jsou součástí daného odboru. Za výsledky své činnosti jsou vedoucí odborů odpovědni tajemníkovi úřadu. Vedoucí každého oddělení vykonávají stejnou funkci jako vedoucí odborů jen s tím rozdílem, že mají na starost své oddělení se zaměstnanci. Jedná se o odbory a související oddělení vybraného MěÚ:

- odbor kancelář úřadu - oddělení organizace a řízení úřadu, kam patří sekretariát, oblast krizového řízení a BOZP, PO, taktéž oblast podpory řízení a oblast provozní a hospodářské správy;
- odbor právní - oddělení majetkoprávního, který se zabývá právními úkoly vyplývající z činnosti města a MěÚ;
- odbor informačních technologií – nemá žádná oddělení, v samostatné působnosti např. zabezpečuje správu licencí MěÚ, zajišťuje provoz a bezpečnost informačních systémů MěÚ, provádí digitalizaci spisů odboru Stavební úřad;
- odbor občansko-správních agend - oddělení správních agend, oddělení matriky, oddělení občansko-správních přestupků a oddělení dopravy a silničního hospodářství;
- odbor Stavební úřad – oddělení územního rozhodování a stavebního úřadu společně s oddělením územního plánování a státní památkové péče;
- odbor kultury a cestovního ruchu – nespadají zde samostatná oddělení, odbor se rozděluje pouze na dvě oblasti, tj. oblast kultury a oblast propagace a cestovního ruchu (např. zajišťuje tvorbu a distribuci propagačních materiálů města);
- odbor finanční - oddělení finanční účtárny a rozpočtu a současně oddělení místních poplatků a vymáhání pohledávek;
- odbor Obecní živnostenský úřad – oddělení registrace živností a oddělení kontrolní a správní (např. živnostenské kontroly fyzických a právnických osob);
- odbor rozvoje města - oddělení strategického rozvoje města, které analyzuje dlouhodobé potřeby města a oddělení investic, které mimo jiné věcně a časově řídí výstavbu města, rekonstrukce atd.;
- odbor služeb – není nadřízen žádnému oddělení, např. zajišťuje označení ulic;
- odbor životního prostředí – oddělení ochrany vod a prostředí (vodoprávní úřad);
- odbor školství, mládeže a tělovýchovy – není rozděleno na oddělení, zajišťuje podmínky pro předškolní vzdělávání, plnění školní docházky a školní stravování ve městě, zabezpečuje konkurzní řízení na obsazení pracovních míst ředitelů škol, spravuje školy a školská zařízení, které město zřídilo, atd.;

- odbor sociálních věcí a zdravotnictví - je nadřízený oddělení sociálně právní ochrany dětí, která vyhledává ohrožené děti a mládež, vede jejich evidenci atp. a oddělení sociální práce, které se mimo jiné podílí na pomoci občanům při překonávání nepříznivé životní situace.



Obrázek 5 Organizační struktura (vybraný MěÚ)

6 ANALÝZA DOPADŮ IMPLEMENTACE OBECNÉHO NAŘÍZENÍ

V praktické části bakalářské práce jsem analyzovala jednotlivé kroky, které musel vybraný MěÚ podstoupit, aby dosáhl souladu s Obecným nařízením, a v jakém rozsahu to mělo dopad na jeho činnost a hospodaření. Analýzu jsem provedla na základě uskutečněného rozhovoru s pověřencem pro ochranu osobních údajů, vedoucím personálního oddělení a s pracovníkem mající na starosti vzdělávání jednotlivých úředníků. Pokládala jsem jim otázky spojené s implementací Obecného nařízení do činnosti vybraného MěÚ. Následně byly zhodnoceny jednotlivé dopady a vyhodnoceno nákladové zatížení implementace, které bylo porovnáno s dalšími MěÚ prostřednictvím získaných informací přes zákon č. 106/1999 Sb. o svobodném přístupu k informacím. Jako poslední jsem podala návrh na zdokonalení práce a dosažení tak vyššího souladu s požadavky Obecného nařízení.

6.1 Pověřenec pro ochranu osobních údajů

Vybranému MěÚ bylo jasné již z jejich velikosti, jelikož se jedná o ORP, že budou muset ustanovit osobu na pozici pověřence pro ochranu osobních údajů (dále jen „pověřenec“). Nedosadili do funkce pověřence jen jednu osobu, ale rovnou dvě. Jeden pověřenec se zabývá záležitostmi pro vybraný MěÚ a druhý pověřenec má na starosti příspěvkové organizace, které město zřizuje. Příspěvkové organizace totiž požadovaly, aby pro ně vybraný MěÚ zabezpečil funkci pověřence, a tak mezi sebou uzavřeli smlouvu o spolupráci. Tato práce je však zaměřena na pověřence výkonného pro potřeby vybraného MěÚ.

Na pozici pověřence nebylo vypsané výběrové řízení, protože se rozhodli využít možnosti interního řešení a tuto funkci svěřili osobě z řad svých zaměstnanců, který byl dříve na pozici interního auditora. Pověřenec byl ustanoven ke dni 1. 5. 2018, a to úpravou stávající pracovní smlouvy na plný úvazek, kterou již měl uzavřenou. Byl vypracován a přiložen pouze dodatek k pracovní smlouvě a upravena pracovní náplň zaměstnance. S ustanovením funkce pověřence plyne vybranému MěÚ další povinnost z hlediska požadavků Obecného nařízení, a to zveřejnění kontaktu na pověřence a sdělení jeho údajů ÚOOÚ včetně příslušných orgánů dozoru, což provedli téměř okamžitě.

Změna pracovní náplně měla za důsledek zvýšení odpovědnosti této osoby, a proto musela být osoba pověřence zařazena do vyšší kategorie platové třídy, aby jeho pozice a s ní související odpovědnost a vzdělanost odpovídala ohodnocení vykonávané práce. Při určování platové třídy se řídili nařízením vlády č. 341/2017 Sb., o platových poměrech zaměstnanců

ve veřejných službách a správě. Nyní je pozice pověřence zařazena do 11. platové třídy, kdy výše platu záleží dále na počtu let započitatelné praxe, jak můžeme vidět v následující tabulce.

Platový stupeň	Počet let započitatelné praxe	Platová třída															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	do 1 roku	9200	9990	10830	11720	12710	13800	14960	16230	17600	19110	20720	22470	24350	26420	28700	31120
2	do 2 let	9530	10350	11230	12170	13190	14310	15530	16830	18290	19820	21520	23330	25280	27430	29780	32280
3	do 4 let	9910	10750	11650	12640	13710	14840	16110	17490	18970	20580	22330	24210	26250	28460	30920	33500
4	do 6 let	10270	11150	12110	13120	14230	15420	16720	18130	19690	21350	23170	25120	27230	29540	32080	34760
5	do 9 let	10660	11580	12550	13590	14770	15990	17350	18830	20430	22180	24020	26040	28260	30650	33270	36080
6	do 12 let	11080	12000	13040	14140	15320	16620	18010	19550	21200	23030	24950	27050	29320	31820	34540	37450
7	do 15 let	11490	12480	13540	14660	15910	17240	18680	20270	22010	23880	25900	28060	30430	33010	35840	38840
8	do 19 let	11930	12960	14030	15210	16500	17880	19400	21030	22830	24770	26860	29130	31590	34270	37190	40300
9	do 23 let	12390	13440	14580	15810	17150	18560	20140	21820	23700	25730	27890	30210	32760	35550	38600	41840
10	do 27 let	12850	13950	15110	16380	17780	19260	20910	22660	24600	26690	28940	31360	34010	36890	40030	43400
11	do 32 let	13340	14480	15690	17000	18460	19990	21710	23510	25510	27690	30030	32550	35280	38290	41550	45040
12	nad 32 let	13840	15050	16320	17640	19160	20720	22550	24400	26500	28750	31170	33780	36620	39720	43130	46740

Obrázek 6 Stupnice platových tarifů podle platových tříd a stupňů (Nařízení vlády č. 341/2017 Sb.)

Dále se měla funkce pověřence začlenit do organizační struktury a organizačního řádu vybraného MěÚ, což bylo uskutečněno, ale jen částečně. Začlenění provedli pouze na místě fyzicky, kdy na organizační tabuli v přízemí dané budovy přidal cedulku pověřence, ale v organizačním řádu funkci pověřence nenajdeme.

Avšak v druhé části nové vnitřní směrnice s názvem „Systém zpracování ochrany osobních údajů“, je pozice pověřence definována podrobněji. Pověřenec uchovává dle směrnice 2 typy záznamů:

- záznamy o účelech zpracování – shrnutí jednotlivých procesů;
- spolupráce s ÚOOÚ – vede veškerou dokumentaci a komunikaci s tímto úřadem.

Osoba pověřence je povinna dle směrnice také poskytovat informace a poradenství starostovi města, tajemníkovi úřadu, vedoucím pracovníkům a dalším oprávněným zaměstnancům úřadu. Dále je pak povinen vydávat doporučení vzhledem ke zpracování a ochrany osobních údajů zaměstnancům vybraného MěÚ ať už poradenstvím na požádání, nebo trvalou kontrolou nových informací z ÚOOÚ a dalších zdrojů a následné předání informací zainteresovaným osobám a další. Do jeho povinností je zařazena taktéž kontrola souladu práce s Obecným nařízením a souvisejícími předpisy, a v neposlední řadě spolupráce s dozorovým úřadem, tedy s ÚOOÚ, atd.

6.2 Vstupní analýza požadavků Obecného nařízení

Prvním krokem po platnosti Obecného nařízení bylo pro vybraný MěÚ zvolení cesty, jakou budou vstupní analýzu zpracovávat, zda to zvládnou interními silami pomocí interních zaměstnanců úřadu, či investují finanční prostředky do externího dodavatele, který za ně celou analýzu zpracuje. Rozhodli se však analyzovat situaci pomocí vlastních sil, interních zaměstnanců, a došlo tak k sestavení odborného týmu, jež se skládal z následujících členů:

- právníci úřadu;
- pověřenec;
- starosta;
- tajemník;
- vedoucí jednotlivých odborů.

Tento projektový tým měl na starosti provedení vstupní a rozdílové analýzy požadavků Obecného nařízení a následně vydefinování návrhů na uskutečnění potřebných kroků pro dosažení souladu s Obecným nařízením. Zpracování bylo zahájeno na přelomu července a srpna roku 2017.

Projektový tým nejdříve vypracoval přehled, jaké procesy na vybraném MěÚ mají, kdo za jaké procesy má odpovědnost, jaké kategorie osobních údajů jsou shromažďovány a z jakého důvodu jsou tyto informace sbírány. To znamená, že u každého procesu stanovili účel zpracování, což je velmi důležitá otázka v souvislosti s navázáním na legitimní titul Obecného nařízení neboli otázka legálního získání osobních údajů. Z hlediska vymezení účelu zpracování se taktéž dotazovali, zda některé účely již nezanikly, či není potřeba zavedení nových účelů zpracování v některých oblastech. Při vyhotovení rozdílové analýzy projektový tým detekoval necelých 130 účelů zpracování.

Tyto účely zpracování odrážejí činnost vybraného MěÚ ať už v přenesené či samostatné působnosti, tj. 1 účel = 1 proces. Následuje příklad z živnostenského odboru:

1. účel zpracování: ohlášení živnosti
2. účel zpracování: kontrolní činnost orgánu vůči živnostníkům
3. účel zpracování: ukončení živnosti

Pro každý proces, který vybraný MěÚ vykonává, našli specifiský účel zpracování.

Tabulka 2 Kategorie zpracovávaných osobních údajů (vlastní zpracování)

Kategorie	Osobní údaj
Obecné	Jméno, příjmení, tituly, pohlaví, věk, datum narození, osobní stav, číslo občanského průkazu
Organizační	Telefonní číslo, e-mailová adresa
Adresné	Adresa trvalého bydliště
Zvláštní (citlivé)	Členství v odborových organizacích, zdravotní stav, trestní delikty/pravomocná odsouzení, exekuce, národnost

Pro každý účel zpracování se evidují rozlišné kategorie osobních údajů. V některých případech zpracovávají o subjektu jen minimum údajů, např. u registrovaných k různým soutěžím, ale v jiných případech evidují o subjektu většinu jmenovaných kategorií, tj. u zaměstnanců a v sociálních oblastech.

Osobní stav zpracovávají pouze v případě, kdy to subjekt sám dobrovolně uvede v dotazníku (vybraný MěÚ to nevyžaduje), nebo se vdá/ožení a tím pádem musí uvést změnu v příjmení, tudíž automaticky vědí, že se změnil osobní stav, nebo v případě žádosti uplatnění slevy na dani na manželku. Telefonní číslo a e-mailovou adresu vedou v systému pro usnadnění komunikace, ale pouze se souhlasem subjektu údajů, který může kdykoliv vyslovit nesouhlas a v ten moment nesmí vybraný MěÚ pokračovat ve zpracování. U některých subjektů zpracovávají údaj o členství v odborových organizacích, jelikož příspěvek za členství se sráží ze mzdy. Zdravotní stav vyžadují pouze z pohledu způsobilosti k práci a konkrétní pracovní pozici, taktéž zaměstnanci podstupují pravidelné zdravotní prohlídky, které jsou dané ze zákona, a vybraný MěÚ uchovává tyto posudky, jež říkají, zda je jedinec způsobilí k práci či nikoliv. Ohledně trestních deliktů a pravomocných odsouzení je zaměstnanec povinen sám informovat vybraný MěÚ. Informace o exekucích zpracovávají z toho důvodu, že konkrétní osobě, která je podrobena exekuci, strhávají část dluhu ze mzdy.

Během zpracovávání vstupní analýzy postupně zjišťovali, co všechno budou muset upravit, aby byly dané věci v souladu s Obecným nařízením. Patří sem zde např. zveřejňování osobních údajů na úřední desce ať už ve fyzické či elektronické podobě, kontrola a zajištění fyzického a současně elektronického zabezpečení osobních údajů, zavedení pravidel-

ných kontrol neboli revizi všech záznamů o účelech zpracování, změny se dotkly i výběrových řízení vypsaných pro obsazení pracovního místa.

Po dokončení vstupní a rozdílové analýzy v lednu minulého roku, předal odborný tým zpracovaný dokument externí firmě, která se zabývá implementací Obecného nařízení. Ta po necelých 2 měsících vlastní práce navštívila vybraný MěÚ s tím, že provedla kontrolu a ve spolupráci s interními posuzovateli záznamů rozebírala každý jednotlivý záznam a současně poskytla poradenské služby, tj. vypracovala a následně poslala doporučení, na případné změny, dle kterých vybraný MěÚ opravil analýzu do finální podoby. Po těchto 4 měsících intenzivní každodenní práce, kterou věnovali interní zaměstnanci vstupní a rozdílové analýze, a po dosažení požadovaného výsledku, se dále zabývali záznamy o činnostech příspěvkových organizací. Ty již probíhaly bez spolupráce s externí firmou, ryze vlastními silami, což zabralo další 2 měsíce.

6.2.1 Zdroje osobních údajů a jejich pořízení

Vzhledem ke zpracovávaným osobním údajům rozdělil projektový tým zdroje těchto informací na dvě skupiny:

- samotné subjekty osobních údajů – jedná se o zaměstnance a občany města, uzavřením nové pracovní smlouvy, či podání žádosti ze strany občana, ve které uvede dobrovolně své osobní údaje;
- ostatní – používání základních registrů, informace od institucí, se kterými vybraný MěÚ spolupracuje (kontrolních orgány, soudy, kraje, apod.).

A na jakém základě vybraný MěÚ pořizuje osobní údaje? Všech 130 účelů zpracování osobních údajů musí být na legální rovině. Ve většině případů se jedná o zákonný důvod zpracování. Druhým nejčastějším způsobem získání osobních údajů je plnění smlouvy či na základě úkonů předcházejících uzavření smlouvy. Vybraný MěÚ eviduje již o dost menší počet oprávněných zájmů a jen 3 případy pořízení osobních údajů na základě souhlasu. Jeden souhlas je např. uzavřen mezi vybraným MěÚ a městskou policií pro případy žádosti ze strany občana o opatření cyklistického kola syntetickou DNA, jedná se o ochranný prvek pro snadnější nalezení ukradeného kola. V tomto případě občan o sobě poskytne mnoho osobních údajů, které se dále zpracovávají a uchovávají pro případnou snadnou budoucí identifikaci.

6.3 Vnitřní směrnice

Vybraný MěÚ nechal vypracovat vnitřní směrnici s názvem „Systém zpracování ochrany osobních údajů“ (dále jen „směrnice“) v návaznosti na platnost a pozdější účinnost Obecného nařízení. Tuto směrnici vypracovával opět projektový tým, který se skládal také z interních zaměstnanců, konkrétně se jednalo o:

- tajemníka;
- pověřence;
- vedoucí odborů;
- interního auditora.

Projektový tým vypracovával novou směrnici v součinnosti s externí odbornou firmou, se kterou již byla uzavřená smlouva v návaznosti na dopracování vstupní a rozdílové analýzy a další spolupráce týkající se vzorových potřebných dokumentů, např. souhlas se zpracováním osobních údajů. Obsah interní směrnice znázorňuje následující tabulka č. 3.

Tabulka 3 Obsah vnitřní směrnice (Vybraný MěÚ, 2018)

Část	Článek
Úvodní ustanovení	Základní ustanovení, základní pojmy, hlavní cíle ochrany osobních údajů, zásady zpracování a ochrany, bezpečnost, vymezení odpovědnosti
Povinnosti při zpracování a ochraně osobních údajů	Pověřenec, vedoucí zaměstnanci, oprávněné osoby
Vybrané oblasti zpracování osobních údajů	Zpracování a ochrana osobních údajů pro pracovněprávní agendu, materiály určené k projednání v orgánech města, kamery MěÚ
Výkon práv subjektů	Společná ustanovení, právo na přístup k osobním údajům, na opravu nepřesných osobních údajů, na výmaz, na omezení zpracování, na přenositelnost, právo vznést námitku
Závěrečná ustanovení	Porušení bezpečnosti osobních údajů, závěrečná ustanovení

Směrnice zahrnuje opravdu všechny důležité aspekty Obecného nařízení. Definici základních pojmů pro zjednodušení orientace ve směrnici pro čtenáře, vymezení kompetencí a povinností pro roli pověřence, vedoucí odborů a oprávněné zaměstnance úřadu, včetně vymezení odpovědnosti těchto osob. Podrobně je zde vymezena funkce pověřence. Dále směrnice pojímá také popis procesů, např. postup přijetí žádosti od občana či situace jak postupovat v případě bezpečnostního incidentu, taktéž stanovuje kontrolní činnost souladu s Obecným nařízením a mnohé další.

Součástí směrnice jsou také přílohy. Jedná se o vzorové dokumenty, které vypracoval na zakázku již zmiňovaný externí specialista a projektový tým si je upravil po designové stránce pro vybraný MěÚ. Jedná se o přílohy:

- podklad pro záznam o činnosti zpracování;
- souhlas se zpracováním osobních údajů;
- záznamový list k žádosti subjektu údajů;
- zápis o kontrole dodržování stanovených technických a organizačních opatření k zajištění ochrany osobních údajů.

Dokument jako celek byl schválen Radou vybraného města dne 17. 5. 2018 a účinná byla směrnice od 25. 5. 2018, což je shodné datum s účinností Obecného nařízení. Směrnice je platná pro celý vybraný MěÚ.

6.4 Úprava smluv

Před nástupem Obecného nařízení měli v pracovních smlouvách zakomponovaný souhlas se zpracováním osobních údajů, což bylo jistou mírou nemístné, jelikož ze zákona víme, aby vznikl nový pracovní poměr, musí daná osoba poskytnout své osobní údaje. To znamená, že k úpravám pracovních smluv mezi vybraným MěÚ a jeho zaměstnanci došlo, a to takovým způsobem, že původní souhlas se zpracováním osobních údajů vyňaly ze smlouvy a použili zvlášť dokument, který zpracovali přímo na tento požadavek nového souhlasu. Stávající zaměstnanci byli informováni o úpravě smlouvy a o podepsání nového platného souhlasu. Nově příchozí zaměstnanci dostanou k podepsání již opravenou verzi smlouvy a nový dokument k souhlasu se zpracováním osobních údajů.

Vzhledem k tomu, že vybraný MěÚ má několik zpracovatelů osobních údajů, i když jich není mnoho, jelikož ve většině činností sám působí jakožto zpracovatel, tak i s nimi má uzavřené smlouvy. Tyto smlouvy taktéž musely projít určitou úpravou, aby odpovídali

požadavkům Obecného nařízení. Jednalo se o vypracování dodatku k jednotlivým smlouvám, přičemž předmětem dodatků bylo vyjasnění vztahů, práv a povinností zúčastněných stran. Úpravu uzavřených smluv zvládli vykonat pomocí vlastních sil, interních zaměstnanců, nevyužili tedy žádného externího specialistu.

6.5 Organizační opatření

Mezi další opatření, která se musela realizovat, řadíme zejména odborná školení zaměstnanců, jež Obecné nařízení považuje jako nutnou součást vzdělávání správců, zpracovatelů a dalších. První školení proběhla již v roce 2017, v měsíci červen se zúčastnili odborného školení starosta s tajemníkem vybraného MěÚ a následně v říjnu byla na školení osoba, která byla později ustanovena do funkce pověřence. Na začátku roku 2018 byla zajištěna dvě školení pro vedoucí pracovníky a následně další dvě školení pro budoucího pověřence, aby prohloubil svou kvalifikaci, znalosti a přehled v oblasti Obecného nařízení. Všechna tato vyjmenovaná školení proběhla mimo území vybraného MěÚ, tedy byla zajištěna externím dodavatelem, který se na danou oblast specializuje.

Dvě velká školení, která byla organizována pro všechny zaměstnance vybraného MěÚ na téma Obecné nařízení, proběhla v červnu roku 2018 na území úřadu pomocí externího dodavatele. V prvním případě šlo o školení, které se zaměřovalo na obecnější informace, jelikož se jej zúčastnili všichni zaměstnanci, přičemž ne všichni měli povědomí o této problematice. Jednalo se o představení Obecného nařízení a pomoci zorientovat se v něm. Výsledkem prvního školení bylo pochopení obsahu a účelu zavedení Obecného nařízení ze strany zaměstnanců, současně s tím proběhlo seznámení se s případnými riziky pro vybraný MěÚ při nedodržení legislativy či při zneužití dat. Druhé školení, které bylo připraveno pro všechny zaměstnance na téma Obecné nařízení, proběhlo také v červnu, přičemž již bylo odbornější a vztahovalo se přímo na implementaci Obecného nařízení do činností vybraného MěÚ a veřejné správy jako takové. Kladla se důležitost na vysvětlení specifik pro tuto oblast s konkrétními příklady z praxe na jednotlivé činnosti vybraného MěÚ, což zaměstnancům pomohlo při pochopení celé problematiky. Dále se od realizace odborných školení, která již proběhla a která teprve proběhnou, očekává zlepšení schopnosti zaměstnanců rozpoznat porušení dat.

V druhé polovině roku 2018 proběhlo jedno větší školení pro vedoucí zaměstnance úřadu a pověřence, což bylo v srpnu na území vybraného MěÚ, následně v říjnu a prosinci se

uskutečnila školení na základě individuální potřeby pověřence mimo úřad externím dodavatelem.

V letošním roce 2019 se prozatím žádné odborné školení neorganizovalo. Účast na školení, tj. prezenční listinu s obsahem školení, by měli příslušní pracovníci vybraného MěÚ evidovat a uchovávat, aby mohli prokázat, že podstoupili všechny kroky k zabezpečení souladu s Obecným nařízením.

6.6 IT opatření

Důležitou součástí implementace Obecného nařízení do úřadů je i zajištění bezpečnosti po stránce IT. Vybraný MěÚ prozatím zajistil dvě opatření v této oblasti. Jedná se o zavedení tzv. soukromého tisku u multifunkčních zařízení, které se nacházejí v chodbách budovy. Toto opatření funguje na základě osobního pokynu k tisku. Zaměstnanci odešlou dokument z počítače do tiskárny (multifunkčního zařízení), ale ta dokument vytiskne až v momentě, kdy daný zaměstnanec k tiskárně přijde a přiloží svou čipovou kartu. Dokument je tedy po celou dobu pod relativním dohledem a je chráněn před přečtením či odcizením dalších osob, které se po úřadě pohybují. Dalším krokem bylo provedení kontroly přístupových hesel do jednotlivých stolních počítačů, či notebooků a systémů v nich. Z kontroly byl zjištěn nevyhovující stav, kdy zaměstnanci používali jednoduchá hesla, která by byla snadno rozluštitelná. Proto bylo zavedeno zpřísnění požadavků na tvorbu a používání přístupových hesel tak, aby situace odpovídala potřebné ochraně osobních údajů.

6.7 Skutečně vynaložené náklady na implementaci Obecného nařízení

Vybraný MěÚ musel provést určité kroky, které vedly k zajištění souladu činnosti úřadu s Obecným nařízením, do kterých musel investovat určitou výši finančních prostředků. Tyto vynaložené finanční prostředky jsem rozdělila dle pravidelnosti jejich evidování (placení), tj. na náklady jednorázové, a naopak na náklady, které vybraný úřad platí pravidelně.

Tabulka 4 Jednorázové náklady (vlastní zpracování)

Položka	Částka
Smlouva s externí firmou	145.300 Kč
Vzorová dokumentace od externí firmy	42.350 Kč
Klíčová politika	150.000 Kč

Prvním jednorázovým nákladem, který vybraný MěÚ zaregistroval, byl spjatý s dokončením zpracování vstupní a rozdílové analýzy požadavků Obecného nařízení, protože se rozhodli, že sice tento dokument zpracují vlastními silami a ušetří tak, ale pro jistotu jej nechali zkontrolovat externím dodavatelem specializujícího se na tuto oblast, zda je vypracován v souladu s Obecním nařízením a současně využili jejich poradenských služeb při přípravě a následnému zhotovení doporučení změn v činnostech vybraného MěÚ. Všechny tyto činnosti byly obsahem uzavřené smlouvy s externím dodavatelem. V návaznosti na zjištění ze vstupní a rozdílové analýzy i z doporučení externisty provedl vybraný MěÚ další kroky. Zjistil, že klíčová politika je již zastaralá a nevyhovující, tudíž jako další náklad bylo zaevidování výměny veškerých klíčů včetně zámků na dveřích do kanceláří a na skříních, ve kterých se uchovávají osobní údaje, zabezpečení odpovídajících trezorů pro vedoucí odborů, pořízení potřebných uzamykatelných skříní, tam, kde chyběly či nakoupení visaček ke klíčům. Dalším krokem bylo objednání od téže externího dodavatele zpracování vzorové dokumentace, která je v souladu s Obecným nařízením. Do objednané dokumentace můžeme zařadit souhlas se zpracováním osobních údajů, podklad pro záznam o činnosti zpracování, záznamový list k žádosti subjektu údajů a zápis o kontrole dodržování stanovených technických a organizačních opatření k zajištění ochrany osobních údajů.

Tabulka 5 Pravidelné náklady (vlastní zpracování)

Položka	Částka
Odborné školení zaměstnanců úřadu za rok: • 2017 • 2018 • 2019	 5.800 Kč 80.238 Kč 0 Kč
Plat pověřence*	21.480 Kč

**uveden v měsíční částce*

Prvním pravidelným nákladem, který vybraný MěÚ eviduje každý měsíc je ohodnocení pověřence za jeho výkon práce, za který mu náleží plat stanovený tabulkově, přesněji 11. platovou třídou. V současné době jsou měsíční náklady na pověřence 21.480 Kč. Druhým pravidelným nákladem jsou odborná školení zajišťovaná pro zaměstnance vybraného MěÚ, kterých se prozatím v období od 1. 1. 2017 do 1. 5. 2019 uskutečnilo několik menších a dvě velká. V případě menších se jednalo o školení pro vedoucí úřadu, tajemníka

a pověřence. Velká školení byla organizována pro všechny zaměstnance, aby každý věděl, o co se jedná, jak má dále pokračovat ve své práci, zda to bude mít vliv na vykonávání jejich práce či nikoliv. Vybraný MěÚ prozatím nemá stanovenou dobu pro organizaci odborných školení v pravidelných intervalech, i když Obecné nařízení stanovuje pravidelné udržování povědomí ochrany osobních údajů. Náklady na školení jsou individuální, protože každé školení je specifické a zaměřuje se na předem dohodnutou oblast pro určitý počet zaměstnanců, které ovlivňuje výslednou částku.

7 ZHODNOCENÍ DOPADŮ NA CHOD VYBRANÉHO MĚÚ

Z provedené analýzy vyplynulo, že existuje mnoho dopadů na činnost a hospodaření vybraného MěÚ v rámci implementace Obecného nařízení, jelikož v téměř každém úkonu úřadu se manipuluje s osobními údaji a zpracovávají se, což je pro Obecné nařízení bodem číslo jedna. Nejedná se tedy o dva dopady obřích rozměrů, ale více dílčích menších, které dávají povinnost něco změnit, obměnit, vytvořit či zrušit a především chránit osobní údaje.

7.1 Zvýšená odpovědnost správce

Jeden z prvních a podstatných dopadů implementace Obecného nařízení, který byl vyvozen z provedené analýzy, je z širšího pohledu spojen s principem odpovědnosti správce. To znamená, že správce nese odpovědnost za to, jakým způsobem zpracovává osobní údaje a nejen to. Je také odpovědný za zpracování osobních údajů svých zpracovatelů, tudíž musí provádět určitou kontrolu, aby mu případně nehrozily sankce za odchýlení se od zásady zákonnosti, korektnosti a transparentnosti, která udává povinnost dodržování právních předpisů a dbání na zvýšenou péči při vytváření a zavádění činností v oblasti zpracování osobních údajů.

7.2 Personální změny a pověřenec pro ochranu osobních údajů

Obecné nařízení mělo dopad v prvé řadě na personální oddělení. První věc, kterou vybraný MěÚ v tomto směru udělal, bylo rozhodnutí o pozici pověřence, zda jeho výkon zabezpečit interně nebo externě formou nájmu či sdíleného pověřence. Zvítězila možnost zajištění interními silami, jelikož úřad disponuje několika vhodnými stávajícími zaměstnanci na danou pozici. I když pověřence nejmenovali a pouze jej ustanovili (svěřili funkci) neznamená, že porušili Obecné nařízení, ve kterém se píše pouze o jmenování do funkce. S touto povinností a dopadem téže souvisí nárůst mzdových nákladů. Z funkce pověřence vyplývá další povinnost nově stanovená pro správce a zpracovatele a to jsou záznamy o činnostech. V jisté míře jde o nahrazení oznamovací povinnosti, která byla zrušena. Jedná se o zapisování postupů zpracování osobních údajů, které souvisejí s novým přístupem práce Obecného nařízení. Záznamy o činnostech slouží jako důkazní prostředek pro ÚOOÚ, že vybraný MěÚ postupuje v souladu s Obecným nařízením.

Dále v oblasti výběrových řízení, kdy součástí přihlášky o pracovní pozici je i souhlas se zpracováním osobních údajů, ale pouze po dobu průběhu výběrového řízení. V případě úspěšnosti se vede o zaměstnanci osobní spis, který je zavřený v kartotéce, ta je zamčená

na klíč ve skříni, která je taktéž uzamykatelná. Naopak v případě neúspěšnosti se osobě vrátí veškeré fyzické dokumenty a v případě informací v elektronické podobě se trvale odstraní z počítače. Subjekt osobních údajů se buď anonymizuje, nebo se uplatní právo na výmaz. Pokud zaměstnanec odejde z pracovně právního vztahu, tak jeho osobní údaje se převedou do archivu, kde se uchovávají po dobu stanovenou zákonem a následně dochází ke skartaci. V personálním okruhu tedy postupují v souladu s požadavky Obecného nařízení.

7.3 Zabezpečení IT systémů

Mezi taktéž důležité dopady jsem zařadila technickou stránku, tj. zabezpečení IT systémů zpracovávajících osobní údaje a každý jiný IT systém na úřadě, protože přes něj může dojít ke zneužití či odcizení veškerých informací prostřednictvím hackerů a jejich útoků. Jedno z opatření, které se realizovalo v oblasti IT, byla revize a zpřísnění požadavků na tvorbu a používání přístupových hesel do počítačů, či personálního systému, jelikož byly v nevyhovujícím stavu, řada zaměstnanců používala opravdu lehce rozluštitelná hesla, která rozhodně neodpovídala žádoucímu stavu. Následovalo také zavedení tzv. soukromého tisku, aby ochránili převod digitálních informací do tištěné podoby po celý proces a nedošlo ke zneužití nebo odcizení vytištěných dokumentů, které by ležely bez tohoto opatření na tiskárně v chodbě, kde se pohybuje několik cizích lidí či zaměstnanců úřadu každý den.

7.4 Zvýšená pozornost na odborná školení

Obecné nařízení rovněž stanovuje povinnost pravidelného udržování povědomí zaměstnanců o dané problematice. Tuto pravidelnost již dále Obecné nařízení nespecifikuje, tudíž každý si ji může vyložit jinak. Vybraný MěÚ řádně proškolil všechny své zaměstnance a především pověřence, kteří se zúčastnili všech školení organizovaných pro zaměstnance úřadu včetně školení dle individuálních potřeb. Pověřenec průběžně informuje o nových informacích a o změnách jednotlivé zaměstnance, kterých se to týká z hlediska náplni jejich práce plus vedoucí zaměstnance. Prozatím si nestanovili žádnou dobu opakovatelnosti odborného školení do budoucnosti, jak uvádí Obecné nařízení.

7.5 Ostatní dopady na činnost a chod vybraného MěÚ

Mezi další dopady na činnost a chod vybraného MěÚ patří např. omezení zveřejňování osobních údajů na úřední desce, jak ve fyzické, tak i v elektronické podobě. Dříve dle zá-

konu č. 101/2000 Sb. údaje, které vedly k identifikaci subjektu, byly běžně na úřední desce vyvěšeny a nikomu to nevadilo. Oproti tomu Obecné nařízení je přísnější a za takové jednání by hrozilo uvalení sankce. Vybraný MěÚ tedy více dohlíží na anonymizaci veškerých údajů, které by vedly k přímé či nepřímé identifikaci subjektu údajů. S anonymizací souvisí i poskytování informací ze zápisů z jednání obecního zastupitelstva a Rady. Na webových stránkách města je zveřejněn listinný záznam převedený do digitální podoby a audiozáznam, tzn. pouze zvuk bez obrazu. V obou případech je nutná pečlivá anonymizace, aby dodržovali Obecné nařízení.

Další dopad byl po provedené analýze zaregistrován u zajištění fyzického a elektronického zabezpečení osobních údajů, které jsou zpracovávány. V tomto směru provedli revizi klíčové politiky a následně ji uvedli do stavu, který je v souladu s požadavky Obecného nařízení. Pro bezpečnost elektronických osobních údajů realizovali obnovu přístupových hesel do počítačů, nyní jsou složitější a těžší pro dešifrování. Tyto uskutečněné kroky vedou k naplňování principu integrity a důvěry. Vybraný MěÚ se snaží, aby všichni zaměstnanci dbali na zamykání své kanceláře při sebemenší době nepřítomnosti, při konci pracovní doby mají povinnost založit veškeré dokumenty z pracovního stolu do uzamykatelných skříní. Zvýšený dozor a kontrola nad zabezpečením ochrany osobních údajů ve fyzické podobě platí pro všechny zaměstnance, kteří je jakýmkoliv způsobem zpracovávají, což je hlídáno vedoucími zaměstnanci taktéž v rámci Obecného nařízení. Všichni zaměstnanci včetně operátorů podlahových ploch a IT pracovníků, kteří by se mohli dostat k mnoha informacím, jsou vázáni mlčenlivostí, pro případ, že by některý ze zaměstnanců pochybil v již zmíněných krocích potřebných k zabezpečení ochrany osobních údajů nebo proti zneužití svého pracovního postavení.

Aby sledovali soulad výkonu práce s požadavky Obecného nařízení, měli by dělat minimálně jednou ročně kompletní revizi všech záznamů o účelech zpracování, což znamená znovu zkontrolovat, zda je vše platné a aktuální, zda pro kategorie osobních údajů, které shromažďují, mají legitimní podklad a mohou je dále sbírat. Jednotliví vedoucí odborů tak zkontrolují výše popsané a vypracují zprávu, kterou podají pověřenci.

7.6 Nákladové vyhodnocení

Implementace Obecného nařízení do činnosti obcí měla dopady i po ekonomické stránce. Jedná se o finanční prostředky vynaložené na dosažení souladu s Obecným nařízením, přičemž u některých se jednalo o jednorázové platby a naopak v jiných případech se jedná

o pravidelné platby, které musí vybraný MěÚ uhradit (plat pověřence, odborná školení). Pro porovnání byly osloveny další městské úřady prostřednictvím zákona č. 106/1999 Sb. o svobodném přístupu k informacím (viz PŘÍLOHA P IV: Otázky na další městské úřady), které byly vybrány dle zvoleného kritéria, tj. počtu občanů města, aby výsledky odpovídaly co nejlépe vzhledem k velikosti města.

Tabulka 6 Srovnání nákladů s jinými MěÚ (vlastní zpracování)

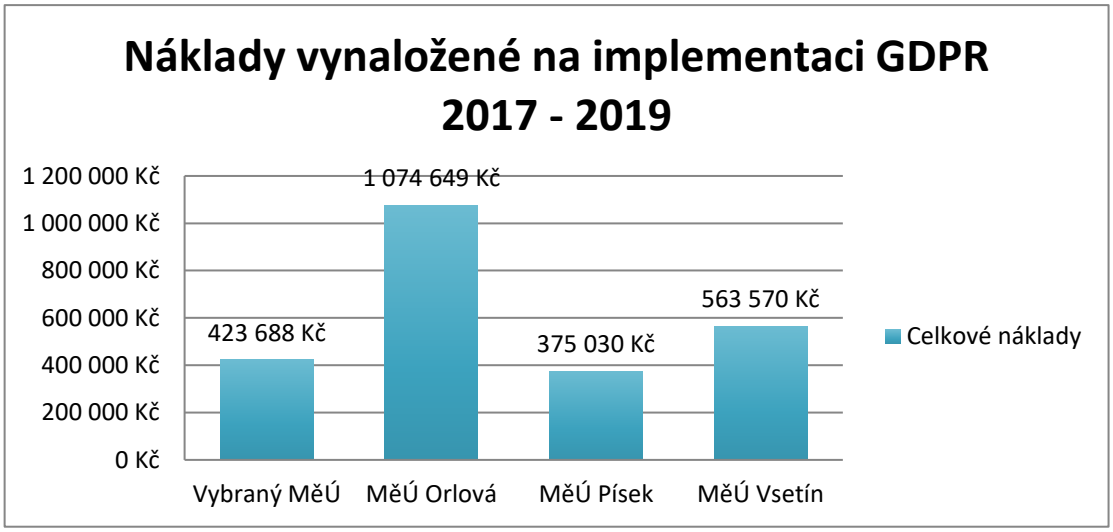
	Vybraný MěÚ	**MěÚ Orlová**	**MěÚ Písek**	**MěÚ Vsetín**
Plat pověřence*	21.480 Kč	21.480 Kč	21.480 Kč	23.630 Kč
Vstupní analýza	145.300 Kč	591.690 Kč	212.000 Kč	320.000 Kč
Odborné školení (2017-2019)	86.038 Kč	64.991 Kč	43.014 Kč	88.000 Kč
Úprava dokumentů	42.350 Kč	173.030 Kč	0 Kč	50.000 Kč
IT opatření	0 Kč	76.229 Kč	44.016 Kč	0 Kč
Klíčová politika	150.000 Kč	168.709 Kč	76.000 Kč	105.570 Kč
Celkové náklady	423.688 Kč	1.074.649 Kč	375.030 Kč	563.570 Kč

**plat pověřence je uveden v měsíční částce*

Vstupní analýzu všechny oslovené městské úřady vypracovávaly pomocí externího dodavatele, za což vynaložili nemalé finanční prostředky. Pouze vybraný MěÚ tuto povinnost splnil pomocí vlastních zaměstnanců ve spolupráci s externí firmou, čímž také ušetřili finanční prostředky. Klíčová politika tyto náklady zvedla oproti ostatním, z čehož vyplývá značná zastaralost klíčů, zámků a souvisejícího zabezpečení nebo jimi nedisponovali. Do celkových nákladů jsem nezapočítala plat pověřence, jelikož každý jej ustanovil k jinému datu a jedná se o měsíční pravidelný výdaj na rozdíl od ostatních výdajů, které nejsou tak pravidelné. Roční náklady na pověřence ve vybraném MěÚ činí 345 398, 40 Kč, tj. superhrubá mzda včetně zdravotního a sociálního pojištění odváděné zaměstnavatelem.

Implementací Obecného nařízení do činnosti vybraného MěÚ došlo tak ke zvýšení mzdových nákladů i ostatních nákladů. Pokud se na tyto vynaložené náklady zaměří vzhledem k celkovému vyhodnocení nákladů na hospodaření MěÚ, tak zjistí, že se nejedná o podstatnou částku, která by jeho chod mohla ohrozit. V případě, že bych veškeré vynaložené výdaje na implementaci od r. 2017 doposud, zaevidovala do roku 2018, kde dle rozpočtu

vybraného MěÚ skutečná výše vyčerpaných výdajů činila 592.917.390 Kč, se jedná opravdu o zanedbatelnou částku, která nečiní ani 1 %. Patří mezi ty, kteří splnili to nejdůležitější, co museli podle požadavků Obecného nařízení, za přijatelné náklady, jak je zobrazeno v následujícím grafu.



Obrázek 7 Porovnání celkových vynaložených nákladů (vlastní zpracování)

Vybraný MěÚ se pohybuje v rozmezí stejném jako ostatní města, pouze město Orlová vystupuje z tohoto rozmezí, což má za následek zaplacení dvakrát vyšší částky za realizaci vstupní a rozdílové analýzy externím dodavatelem. V ostatních výdajích již tak extrémně nevystupuje. Vybraný MěÚ každopádně ušetřil mnoho finančních prostředků využitím vlastních zaměstnanců, kteří se podíleli na značném množství odvedené práce.

8 NÁVRH NA ZDOKONALENÍ SOUČASNÉHO STAVU PRÁCE

Po provedené analýze dopadů a následného vyhodnocení vyplynulo několik bodů, které by vedly ke zlepšení současného stavu práce a zvýšení souladu s požadavky Obecného nařízení, a právě tyto kroky vedoucí kupředu popisuji.

Prvním bodem návrhu a krokem kupředu pro vybraný MěÚ je stanovení doby, po které se bude opakovat odborné školení zaměstnanců v problematice ochrany a zpracování osobních údajů. Jelikož Obecné nařízení nedefinuje rozmezí, po kterém by mělo dojít k odbornému proškolení zaměstnanců, ale stanovuje pouze povinnost pravidelného udržování povědomí, navrhuji, aby odborná školení proběhla vždy jednou za dva roky. Myslím si, že takto zvolená doba je ideální, protože vybraný MěÚ neeviduje nijak zvlášť vysokou fluktuaci, aby školení museli organizovat každý rok nebo dokonce častěji. Pokud by došlo k větším změnám v legislativě či výjimečným situacím, tak by se provedla mimořádná školení. V případě přijetí nového pracovníka v době, kdy se velké odborné školení pro všechny zaměstnance nebude konat, provede individuální školení pověřenec.

Následuje návrh změny v oblasti elektronické spisové služby, ve které by bylo vhodné provést určitá opatření. Prvním opatřením je provedení revize skartačních lhůt, aby tak dodržovali stále zásadu minimalizace dat, případně tyto lhůty ponechat dále nebo upravit na nezbytně dlouhou dobu k uchování osobních údajů. Druhé opatření se týká komunikačních technologií neboli e-mailu. Zde bych navrhla nastavení automatického trvalého odstranění příloh po určité době, protože shromažďováním starých zpráv včetně příloh v e-mailové schránce zaměstnanců se porušuje zásada minimalizace osobních údajů a zároveň zásada omezení uložení, kdy uchovávaná data jsou v e-mailové schránce delší dobu a měla být dávno trvale odstraněna, nehledě na to, že mohou být odcizena.

Dalším návrhem je aktualizace organizačního řádu, který se nachází jako volně přístupný dokument na webových stránkách vybraného MěÚ. Jedná se o začlenění funkce pověřence do tohoto vnitřního předpisu. Pověřenec spadá v případě vybraného městského úřadu pod starostu města, ale v organizačním řádu není tato pracovní pozice nijak zmíněna. Prozatím jej začlenili fyzicky na organizační tabuli v budově úřadu a blíže jej definovali v novém dokumentu s názvem Systém zpracování ochrany osobních údajů.

Zbystřit by měl každý v momentě, kdy se zaměříme na digitální informace a jejich přenos, čímž je myšlen přenos prostřednictvím sítí a internetu nebo přenos mezi mobilními zařízeními, protože právě IT opatření patří mezi ty nejnákladnější jak časově tak i finančně. Prá-

vě bezpečností opatření v této oblasti jsou ve vybraném MěÚ nedostatečné. Pověřenec nedisponuje žádným softwarem nebo programem, který by se specializoval na problematiku Obecného nařízení, a spoléhá se pouze na MS Office, konkrétně na Excel, ve kterém pomocí tabulek zpracovává údaje, které potřebují vědět o procesu, ve kterém probíhá zpracování osobních údajů. Struktura tabulek je daná a jednotliví vedoucí odborů, kteří mají na starosti určitou oblast, je vyplňují. Ovšem mnoho tabulek, mnoho souborů uložených jen tak v počítači pověřence se stávají značně nepřehlednými, navíc dochází k neustálému přeposílání si těchto excelových souborů obsahující záznamy o činnostech přes e-mailovou schránku, protože vyplňování tabulek mají a starosti vedoucí odborů či oddělení. Je to velmi nebezpečné z hlediska toho, že prozatím neprovedli žádná opatření v oblasti e-mailů, jedná se o velmi nepříjemnou situaci, která je velmi nepřehledná a měla by se řešit.

Nový operační systém či program specializující se na práci v souladu s Obecným nařízením by nesmírně ulehčil práci jak pověřenci tak jednotlivým vedoucím odborů a vedoucím oddělení. Na trhu jsou a výběr dvě možnosti, tj. pronajmutí webové aplikace nebo zakoupení speciálního softwaru. V případě první varianty platí kupující za pronájem každý měsíc používání této webové aplikace, jako je GDPR Organizer (© 2018). Nijak se neinstaluje do osobního počítače pověřence, ale spouští se v internetovém prohlížeči. Je zde garantována bezpečnost a zálohování ukládaných dat a zároveň dosažení souladu s Obecným nařízením. Otázkou a značným rizikem pro ochranu osobních údajů při jejich zpracování je v tomto případě zabezpečení internetové sítě vybraného MěÚ, přes kterou by se pověřenec připojoval k webové aplikaci. Proto bych raději doporučila opravdový software, např. YAMACO Software (2015) nebo eDPO od společnosti DataLite (© 2019). V obou případech jde o software sestavený pro běžný provoz úřadů či firem v souladu s Obecným nařízením, který se instaluje přímo do osobních počítačů, tudíž nedochází k přenášení a ukládání osobních údajů prostřednictvím internetové sítě. Oba softwary nabízejí zlepšení organizace práce, protože veškeré potřebné informace jsou umístěny bezpečně na jednom místě, tudíž je i snazší doložit soulad s požadavky Obecného nařízení. Lze si zakoupit již hotový systém, ale můžeme si jeho prostředí upravit dle našich potřeb. YAMACO Software (2015) nabízí základní (omezenou) verzi zdarma, ta ovšem neobsahuje všechny potřebné oblasti a plnou (neomezenou) verzi, která by již pro účely vybraného MěÚ s přehledem stačila. Software eDPO od společnosti DataLite (© 2019) nabízí jednu pouze jednu verzi ke koupi, která je taktéž vhodná pro vybraný MěÚ, ale má navíc velkou výhodu, že prostředí tohoto softwaru si může pověřenec upravit dle svých představ. V obou případech uvedených

softwarů může vybraný MěÚ zde využít přístup z několika počítačů s nastavením správy jednotlivých oblastí a případného šifrování, tudíž nebude již docházet k věčnému přeposílání e-mailů. Potřebné informace si každý najde ve svém počítači bez nutnosti oslovovat další kolegy. Je zde možnost nastavení zákonných důvodů, účelů a lhůt, které nám systém hlídá a upozorní nás, nebo díky němu vyhledáme konkrétní subjekt údajů napříč všemi evidencemi tzv. na jedno kliknutí. Postará se o úplný výmaz osobních údajů subjektu z evidence, umožňuje tvorbu přehledů a poskytuje možnost sledování využívání osobních údajů, taktéž lze docílit principu minimalizace zpracovávaných osobních údajů. V případě softwaru se jedná o vyšší vstupní náklady oproti najmutí aplikace, přičemž se měsíčním placením jednou dostaneme na stejnou částku, kterou zaplatíme za software. Důležité je výrazně nižší riziko ohrožení ochrany shromažďovaných a zpracovávaných osobních údajů, výrazné zjednodušení práce, zlepšení efektivity práce a zvýšení důvěryhodnosti a profesionality.

Jako poslední návrh na zlepšení bych zmínila provádění kompletních revizí záznamů o účelech zpracování. Kontrolu platnosti, aktuálnosti a legitimních podkladů pro sběr osobních údajů bych stanovila jednou za půl roku. Jako obec s rozšířenou působností zpracovávají, které by měly pravidelně kontrolovat, jelikož mohou porušovat některé zásady a principy Obecného nařízení, např. minimalizace údajů, přesnost či omezení uložení.

ZÁVĚR

Bezpečnost a ochrana subjektů a jejich osobních údajů musí být na prvním místě nejen u správců, ale také u všech zpracovatelů, kteří nakládají jakýmkoliv způsobem s osobními údaji. To je ten důvod, proč musejí chtít a činit všechno proto, aby ve své činnosti dosahovali co nejvyššího souladu s Obecným nařízením. Ačkoliv nikdy nebudeme moci říci „právě jsme dosáhli souladu se všemi požadavky Obecného nařízení a nemusíme již nic dělat“. Jedná se o neustálý dlouhodobý proces implementace, zdokonalování, kontrolování, vyhodnocování a opakování některých činností, jak postupně vyplynulo z teoretické a praktické části bakalářské práce.

Obecné nařízení mělo a stále má výrazný dopad na fungování obcí, přičemž mezi dopady v negativním slova smyslu patří jednoznačně zvýšená administrativní náročnost pro úřady a nejen ty. Veškerá činnost úřadů musí být zdokumentovaná, např. musejí vést záznamy o činnostech, museli provést vstupní a rozdílovou analýzu, nejlépe vypracovat a zavést vnitřní směrnici o zpracování a ochraně osobních údajů, byli povinni upravit uzavřené smlouvy a některé dokumenty, formuláře atd., aby nedocházelo k rozporu s Obecným nařízením. Vykonávaná práce musí být taktéž průhledná a okamžitě zjistitelná pro úřady, zejména pro Úřad pro ochranu osobních údajů. Všechny tyto činnosti, které zajistili a musejí je vykonávat i nadále, stálo úřady mnoho úsilí, námahy a času. Z finančního hlediska to není náročné pro větší úřady, pro menší obce to může být náročnější i po výdajové stránce, ale není to likvidační. Na druhé straně v příchodu Obecného nařízení vidím i pozitivní dopady na společnost jako celek. V době, kdy byl účinný na území České republiky pouze zákon č. 101/2000 Sb. o ochraně osobních údajů, na něj mnoho lidí nereflektovalo, nebyl pro lidi až tak důležitý a někteří ani nevěděli o jeho existenci. Oproti tomu povědomí Obecného nařízení se ihned od jeho počátku šířilo společností jako kulový blesk. Prošlo velkou kampaní a mediální masáží, kdy se o něm neustále psalo, mluvilo a diskutovalo napříč celým společenstvím občanů i mimo území České republiky. Pozitivum je v tom, že lidé tomu opravdu věnovali pozornost a neustále se zvyšovala jejich vědomost o Obecném nařízení a tím i znalosti o ochraně osobních údajů, což je nesmírně důležité vzhledem k tomu, co se poslední dobou odehrává po celém světě, ať už se jedná o kybernetické útoky, odcizování osobních údajů včetně jejich zneužívání atd. Dalším pozitivním dopadem je fakt, že byla revidována a ucelena ochrana osobních údajů.

V teoretické části jsou rozepsané základní principy, na kterých je Obecné nařízení postaveno, jaké změny a novinky přineslo, což se dále odráží v činnosti vybraného městského úřadu popsané v praktické části. Ovšem aby se člověk orientoval v problematice ochrany osobních údajů a pochopil, jak funguje, je zapotřebí znát základní pojmy používající se v Obecném nařízení, které jsou definované v poslední kapitole teoretické části.

V praktické části jsou nejprve uvedeny příklady zneužití osobních údajů, které vycházejí ze současné situace ve světě. Dále byla provedena analýza, při které jsem vycházela z poznatků teoretické části, které mne navedly správným směrem při konstruování otázek k rozhovorům s jednotlivými osobami. Po dokončení analýzy byly následně zhodnoceny dopady, které vyplynuly z provedené analýzy a to v souvislosti s teoretickou částí. Jako poslední byl podán návrh pro vybraný městský úřad na zdokonalení současného stavu práce s Obecným nařízením. V návrhu jsem popsala činnosti, ve kterých by měl vybraný městský úřad pokračovat, aby dosáhl vyššího souladu s požadavky Obecného nařízení. Jedná se např. o zvážení pořízení softwaru pro pověřence, který by značně ulehčil práci, ušetřil čas a celkově zlepšil efektivitu práce, opatření v oblasti odborného školení zaměstnanců, aktualizace organizačního řádu či zabezpečení e-mailů. Všechny tyto návrhy jsou pro vybraný městský úřad realizovatelné. Výdaje navíc zaznamenají v případě pořízení softwaru a zajištění pravidelného odborného školení. Ostatní návrhy nepřinášejí výdaje navíc, přičemž díky tomu docílí lepších výsledků práce s Obecným nařízením.

Výsledek bakalářské práce naplnil všechny stanovené cíle. V návaznosti na další rozpracování této práce, by bylo zajímavé se zaměřit na Obecné nařízení v elektronickém prostředí a problematiku cloudových úložišť, které městské úřady také využívají. Výzvou by bylo se celkově věnovat detailněji vztahu Obecného nařízení s informačními technologiemi, protože se v nich pohybuje nespočet osobních údajů, které se zpracovávají a ani o tom nemusíme vědět.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje

CALDER, Alan, 2016. *EU GDPR a Pocket Guide*. 1st ed. United Kingdom: IT Governance Publishing, 96 p. ISBN 978-1-84928-832-3

HENDRYCH, Dušan et al., 2016. *Správní právo: Obecná část*. 9. vyd. Praha: C. H. Beck, 599 s. ISBN 978-80-7400-624-1

JANEČKOVÁ, Eva, 2018. *GDPR Praktická příručka implementace*. 1. vyd. Praha: Wolters Kluwer ČR, 136 s. ISBN 978-80-7552-248-1

KOPECKÝ, Martin, PRŮCHA, Petr, HAVLAN, Petr, JANEČEK Jan, 2016. *Zákon o obcích. Komentář*. 2. aktualizované vydání. Praha: Wolters Kluwer ČR, 380 s. ISBN 978-80-7552-376-1

MALAST, Jan, 2016. *Teoretická východiska obecní samosprávy v České republice*. 1. vyd. Plzeň: Západočeská univerzita v Plzni, 340 s. ISBN 978-80-261-0657-9

MAŠTALKA, Jiří, 2008. *Osobní údaje, právo a my*. 1. vyd. Praha: C. H. Beck, 212 s. ISBN 978-80-7400-033-1

MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav, 2008. *Osobní údaje a jejich ochrana*. 2. doplněné a aktualizované vydání. Praha: ASPI, Wolters Kluwer ČR, 468 s. ISBN 978-80-7357-322-5

NAVRÁTIL, Jiří et al., 2018. *GDPR pro praxi*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 339 s. ISBN 978-80-7380-689-7

NEZMAR, Luděk, 2017. *GDPR: praktický průvodce implementací*. 1. vyd. Praha: Grada, 301 s. ISBN 978-80-271-0668-4

NULÍČEK, Michal et al., 2017 *GDPR: Obecné nařízení o ochraně osobních údajů*. 1. vyd. Praha: Wolters Kluwer ČR, 544 s. ISBN 978-80-7552-765-3

VALENTOVÁ, Tatiana et al., 2018. *GDPR: Všeobecné nariadenie o ochrane osobných údajov, praktický komentár*. 1. vyd. Bratislava: Wolters Kluwer SR, 568 s. ISBN 978-80-8168-852-2

ŽŮREK, Jiří, 2018. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 343 s. ISBN 978-80-7554-152-9

Internetové zdroje

ČESKO, 1993. Zákon č. 2/1993 Sb. ze de 16. prosince 1992 Listina základních práv a svobod, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/1993-2

ČESKO, 2000. Zákon č. 128/2000 Sb. ze dne 15. května 2000 O obcích, ve znění pozdějších předpisů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-128?text=128

DATALITE, © 1997 – 2019. *eDPO* [online]. [cit. 2019-04-30]. Dostupné také z: https://www.edpo.cz/

EVROPSKÁ UNIE, 2016. Nařízení Evropského parlamentu a Rady (EU) č. 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: *Úřední věstník Evropské unie.* Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1524836439071&uri=CELEX:32016R0679

GDPR ORGANIZER, © 2018. *GDPR Organizer* [online]. [cit. 2019-04-30]. Dostupné také z: https://gdpro.online/#

INSURANCE JOURNAL, 2018. AIR Estimates Marriott Cyber Breach Direct Losses Could Reach $600 Million. In: *Insurance Journal* [online]. San Diego: Wells Media Group [cit. 2019-03-11]. ISSN 00204714. Dostupné také z: https://search.proquest.com/docview/2159395993?accountid=15518

ISAAK, Jim, HANNA, Mina J., 2018. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. In: *Computer* [online]. New York, **51**(8), 56-59 [cit. 2019-03-11]. DOI: 10.1109/MC.2018.3191268. ISSN 0018-9162. Dostupné také z: https://search.proquest.com/docview/2117129957/E87A7D73E13C4EF8PQ/1?accountid=15518

KOMÍNKOVÁ, Magda, 2018. Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?. In: *Euroskop* [online]. [cit. 2019-03-01]. Dostupné také z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

KRANČÚNOVÁ, Jaroslava, KUĽHOVÁ, Lívia, 2017. Nový návrh zákona o zpracování osobních údajů: česká adaptace GDPR a dvojí metr při ukládání pokut?. In: *epravo* [online]. [cit. 2019-03-16]. Dostupné také z: https://www.epravo.cz/top/clanky/novy-navrh-zakona-o-zpracovani-osobnich-udaju-ceska-adaptace-gdpr-a-dvoji-metr-pri-ukladani-pokut-106385.html?mail

MARRIOTT, © 2019. About Marriott. In: *Marriott* [online]. [cit. 2019-02-12]. Dostupné také z: https://www.marriott.com/marriott/aboutmarriott.mi

MINISTERSTVO VNITRA, 2017. Přehled dopadů návrhu právního předpisu. Návrh zákona o zpracování osobních údajů. In: *Poslanecká sněmovna České republiky* [online]. [cit. 2019-02-15]. Dostupné také z: http://www.psp.cz/sqw/text/tiskt.sqw?o=8&ct=138&ct1=14

MINISTERSTVO VNITRA, 2018. Metodické doporučení k činnosti obcí: k organizačně-technickému zabezpečení funkce pověřence pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí. In: *Ministerstvo vnitra* [online]. [cit. 2019-01-31]. Dostupné také z: https://www.mvcr.cz/gdpr/clanek/aktualizovana-metodika-k-poverencum-pro-ochranu-osobnich-udaju.aspx

O'FLAHERTY, Kate, 2018. Marriott Breach: What Happened, How Serious Is It And Who Is Impacted?. In: *Forbes* [online]. [cit. 2019-02-12]. Dostupné také z: https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/#258b93b87d25

POSLANECKÁ SNĚMOVNA, 2019. Sněmovní tisk č. 138. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. [cit. 2019-05-02]. Dostupné také z: http://www.psp.cz/sqw/historie.sqw?o=8&t=138

SNĚMOVNÍ TISK (č. 138), 2017. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. [cit. 2019-02-20]. Dostupné také z: http://www.psp.cz/sqw/historie.sqw?o=8&t=138

ÚOOÚ, © 2013. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-03-06]. Dostupné také z: https://www.uoou.cz/

YAMACO SOFTWARE, 2015. *Produkty: problematika GDPR* [online]. [cit. 2019-04-30]. Dostupné také z: https://yamaco.cz/produkty/problematika-gdpr.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP	Bezpečnost a ochrana zdraví při práci
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ES	Evropské společenství
EU	Evropská unie
GDPR	General Data Protection Regulation
ID	Identifikační číslo
Inc.	Incorporated (veřejná obchodní společnost)
IT	Informační technologie
MěÚ	Městský úřad
ORP	Obec s rozšířenou působností
PO	Požární ochrana
Sb.	Sbírka zákonů
Sb.z.s.	Sbírka zákonů soudních
ÚOOÚ	Úřad pro ochranu osobních údajů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OTÁZKY K ROZHOVORU S POVĚŘENCEM PRO OCHRANU OSOBNÍCH ÚDAJŮ

1. Jaké kategorie osobních údajů zpracováváte?
2. Jaké zdroje osobních údajů evidujete?
3. Na jakém základě jsou osobní údaje pořizovány?
4. Jaký je účel zpracování osobních údajů?
5. Jakým způsobem jste zařadili Obecné nařízení do stávajících procesů?
6. Zpracovali jste vnitřní předpis o ochraně osobních údajů? V případě, že ano:
    a. Jakým způsobem byl zpracován (interně, externě)?
    b. Kdy byl vytvořen?
    c. Co je jeho obsahem?
7. Vyhodnotili jste si sami (jakožto MěÚ) situaci Obecného nařízení a udělali průzkum osobních údajů?
8. Ke kterému datu a jakým způsobem byl jmenován pověřenec pro ochranu osobních údajů?
9. Na základě jaké smlouvy/dohody/… je vykonávaná pozice pověřence?
10. Jakým způsobem sledujete soulad práce s Obecným nařízením? Jak se provádí případná kontrola?
11. Jaké záznamy uchovává pověřenec?
12. Jak dlouho probíhala implementace ochrany osobních údajů?
13. Došlo na městském úřadě k nějakému úniku či znehodnocení dat?
14. Jakým způsobem vedete záznamy o zpracování osobních údajů?
15. Co nesmíte zveřejňovat na úřední desce ve fyzické a elektronické podobě?
16. Jak ovlivnilo Obecné nařízení zveřejňování osobních údajů při výkonu samosprávy (poskytování informací z jednání Zastupitelstva obce a Rady)?
17. Co znamenalo pro městský úřad zavedení Obecného nařízení do své činnosti po ekonomické stránce?
18. Došlo ke zvýšení mzdových nákladů v návaznosti na Obecné nařízení, příp. ostatních nákladů? Jakých a v jaké výši?
19. Došlo k úpravě uzavřených smluv se zpracovateli osobních údajů? Co je obsahem těchto smluv?

PŘÍLOHA P II: OTÁZKY K ROZHOVORU S VEDOUCÍM PERSONÁLNÍHO ODDĚLENÍ

1. Jaké osobní údaje zpracováváte?
2. Jaké subjekty zpracování osobních údajů evidujete?
3. Jakým způsobem uchováváte a kde umisťujete osobní údaje?
4. Máte osobní údaje ve fyzické podobě zabezpečeny? Jak?
5. Jakým způsobem máte zabezpečený počítač, ve kterém se nacházejí osobní údaje?
6. Jak máte zabezpečenou kancelář, ve které se nacházejí osobní údaje?
7. Co děláte s nepotřebnými dokumenty?
8. Museli jste do pracovních smluv zakomponovat dodatek ohledně Obecného nařízení?

PŘÍLOHA P III: OTÁZKY K ROZHOVORU S ÚŘEDNÍKEM PRO VZDĚLÁVÁNÍ

1. Byli zaměstnanci úřadu odborně proškoleni o Obecném nařízení?
2. V případě, že ano:
    a. Kolik školení již proběhlo?
    b. Jakým způsobem byla školení zabezpečena (interně, externě)?
    c. Jaké bylo rozmezí jejich realizace?
    d. Pro jaké účastníky byla odborná školení určena?
    e. Jaká byla výše nákladů na zajištění odborných školení zaměstnanců?
3. Jakým způsobem budete nadále zabezpečovat odborná školení, která souvisejí s povinností stanovenou Obecným nařízením, tj. pravidelné udržování povědomí?

PŘÍLOHA P IV: OTÁZKY NA DALŠÍ MĚSTSKÉ ÚŘADY

1. Jak Vaše organizace zajišťuje výkon osoby pověřené ochranou osobních údajů?
2. Jaká výše odměny byla sjednána s pověřencem?
3. Jak jste řešili tzv. GAP analýzu GDPR (revizi osobních údajů)? V jaké cenové relaci byly nabídky?
4. Kolik korun Vaše organizace vynaložila v letech 2017, 2018 a 2019 (tj. od 1. 1. 2017 do dne obdržení této žádosti o informace) na uvedení Vaší organizace do souladu s GDPR?
5. Kolik činily (z celkové částky podle odpovědi na otázku č. 4):
    a. náklady Vaší organizace na školení týkající se GDPR (ať již v rámci zvyšování kvalifikace či jiných);
    b. náklady Vaší organizace na sepis a přípravu právní dokumentace, která je v souladu s GDPR;
    c. náklady Vaší organizace na IT produkty a služby (s uvedením o jaké produkty a služby se jednalo);
    d. ostatní náklady Vaší organizace (s uvedením o jaké náklady se jednalo).