Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Změny ve fungování obcí po zavedení směrnice o ochraně osobních údajů (GDPR)

Adam Škranc

Bakalářská práce

2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Adam Škranc**
Osobní číslo:	**E16065**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Změny ve fungování obcí po zavedení směrnice o ochraně osobních údajů (GDPR)**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je zmapovat nutné změny po zavedení směrnice o ochraně osobních údajů na úrovni obcí. Součástí práce bude případová studie dokumentující nutné změny na příkladu vybrané obce.

Osnova:
- Podstata ochrany údajů na základě GDPR
- Nutné změny fungování obcí po zavedení GDPR
- Případová studie

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-765-3.
MORÁVEK, Jakub. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7478-139-1.
JELÍNKOVÁ, Jitka. Zákon o svobodném přístupu k informacím. Praha: Wolters Kluwer, 2017. ISBN 978-80-7552-859-9.
MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana: knížka pro praxi. Praha: ASPI, 2003. ISBN 80-86395-50-2.
MATES, Pavel a Karel NEUWIRT. Právní úprava ochrany osobních údajů v ČR: znění zákona č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů. Praha: IFEC, 2000. ISBN 80-86412-02-4.
Eu Gdpr: A Pocket Guide. Velká Británie: IT GOVERNANCE, 2016. ISBN 9781849288316.

Vedoucí bakalářské práce: **Ing. Hana Kopáčková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

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

L.S.

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

V Pardubicích dne 3. září 2018

PROHLÁŠENÍ

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

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2019 Adam Škranc

PODĚKOVÁNÍ:

Rád bych poděkoval své vedoucí práce Ing. Haně Kopáčkové, Ph.D., za odbornou pomoc a rady, které mi poskytla během našich konzultací. Dále bych rád poděkoval Romanu Satrapovi, starostovi obce Radiměř, za poskytnuté informace, které mi pomohly vypracovat tuto bakalářskou práci.

ANOTACE

Tato bakalářská práce se zabývá převážně ochranou osobních údajů (GDPR) z pohledu obce. Z úvodu je práce zaměřená na objasnění základních pojmů v GDPR. Následně nás seznamuje s pravidly, které s sebou toto nařízení přináší. Dále v práci najdeme základní postup při všeobecném zavádění a poté při zavádění v určité obci. V analytické části jsou zpracovány postupy a změny, kterými musela vybraná obec projít pro úspěšné zavedení GDPR. Zejména se jedná o změny v systému práce, zveřejňování osobních údajů, výběr pověřence a zabezpečení osobních údajů.

KLÍČOVÁ SLOVA

Osobní údaje, zabezpečení, pověřenec

TITLE

Changes in the functioning of municipalities after the introduction of the data protection directive (GDPR)

ANNOTATION

This bachelor thesis deals mainly with the protection of personal data (GDPR) from the perspective of the municipality. The introduction is focused on clarification of basic terms in GDPR. Afterwards, it brings us to the rules, which are included in the previously mentioned regulation.. Next, we find the basic procedure for general introduction and then for introduction in a particular village. The analytical part deals with the procedures and changes that the selected municipality had to go through to successfully implement the GDPR. In particular, these are changes in the work system, disclosure of personal data, selection of credentials and security of personal data.

KEYWORDS

Personal data, security, data protection officer

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK A ZNAČEK

ČR	Česká republika
EU	Evropská unie
Sb.	Sbírka zákonů
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
IT	Informační technologie
DPIA	Vliv na ochranu osobních údajů
Odst.	Odstavec
Č.	Číslo
ÚOOÚ	Úřad pro ochranu osobních údajů

Obsah

ÚVOD

Hlavním tématem bakalářské práce je GDPR (zkratka z angl.. General Data Protection Regulation) a jeho zavedení na úrovni obcí. Toto Nařízení nabylo účinnosti 25. 5. 2018 a v této práci se zaměřím na GDPR jako takové a jeho postupné zavádění na úrovni obcí.

Důvodem k zavedení tohoto nařízení je, že z osobních dat se stal zdroj pro podnikání a dále pro obchodování. V této práci se, ale nebudu zabývat zpracováním dat ve veřejných společnostech, ale ve veřejné správě. Díky tomuto nařízení dostali občané do rukou mnoho práv ohledně zpracování jejich osobních údajů. Na druhou stranu společnostem, ale také úřadům ve státní sféře vzniklo mnoho povinností. Je nutné zmínit, že toto Nařízení platí po celé Evropské unii.

Jednotlivě budou vysvětleny všechny důležité pojmy, které jsou klíčové ke správnému pochopení fungování zpracování osobních údajů po zavedení nařízení GDPR. Stručně zde budou popsány jednotlivá práva subjektů údajů a také zde budou povinnosti subjektů, které provádí zpracování osobních údajů. Také budou všeobecně popsány etapy, které vedou k úspěšnému zavedení tohoto nařízení. Obecně popíši, jak se jednotlivé obce musely připravit na příchod tohoto nařízení. Pro obce byly vydávány návody a průvodce zejména od ministerstva vnitra a také od Úřadu pro ochranu osobních údajů.

Proto ve vybrané obci zanalyzujeme postup při zavádění GDPR. Tedy jak postupovaly krok po kroku při jeho zavádění. Jedná se tedy o to, jak zpracovávaly osobní údaje dříve a jak to dělají dnes. Jaká bezpečnostní opatření musely zavést, aby osobní údaje dostatečně ochránily.

1 GDPR

Jak jsem již zmínil v úvodu, GDPR je zkratka pro General Data Protection Regulation. V dnešní době jsou osobní údaje velmi cenné. Čím dál tím více se informace stávají přístupnější, a to díky novým technologiím. V dnešní době není problém si najít spoustu informací o ostatních na internetu. Firmy taktéž tento fenomén využívají a vstupují do našeho soukromého života a naše osobní údaje byly pak pro spousty lidí přístupné. Proto přišel tento nový právní rámec ochrany osobních údajů. Tato právní úprava se týká Evropské unie a jejich členských států. Cílem je, aby nedocházelo k neoprávněnému zacházení s osobními údaji. [1]

Nové nařízení nabylo účinnosti 25. 5. 2018. Úpravu ochrany osobních údajů můžeme nalézt už v Listině základních lidských práv a svobod, kde je uvedeno, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužívání údajů o své osobě. Přitom se nejedná se o žádnou revoluci v oblasti ochrany osobních údajů. Mnoho zákonů již ukládá povinnosti, které slouží k ochraně osobních údajů. Toto nařízení vychází z platné směrnice 95/46/ES, kde většina povinností je totožná. Zpracování osobních údajů je umožněno realizovat jen na základě zákonných titulů, které musí být dostatečně určité tedy zákonné, korektní a transparentní. Tyto tři zásady musí být splněny, aby mohlo dojít k zpracování osobních údajů. Jestliže není zákonný důvod nalezen nebo pomine, je povinností osobní údaj zcela zlikvidovat. Pokud od samého začátku není žádný právní důvod, jedná se o nelegální zpracování osobních údajů. Zásada zákonnosti nám tedy určuje důvod zpracování, a proto je základním kamenem ke zpracování osobních údajů. Zásada zákonnosti nám také stanovuje, že nesmí dojít k protiprávnímu zpracování. [1]

1.1 Aplikováni GDPR v České republice

GDPR bylo schváleno již v dubnu 2016 a v květnu 2018 začalo být již účinné. Doba mezi tím byla určena k přípravě. V této době museli ti, kterých se to týká, upravit svoje informační systémy a postup zpracování a nakládání s osobními údaji. Během tohoto období musely přijmout členské státy EU prováděcí zákon, který měl upřesnit více než padesát bodů, které GDPR přenechává do jejich národních pravomocí. Hlavním dozorčím orgánem u nás je Úřad pro ochranu osobních údajů. Tento úřad je nyní částečně podřízen Evropskému sboru pro ochranu osobních údajů.[2]

1.2 Osobní údaje

Podle znění článku 2 písm. a) Úmluvy 108 je osobním údajem každá informace týkající se identifikované nebo identifikovatelné fyzické osoby (subjektu údajů) a dle článku 2 písm. e) směrnice 95/46 „*veškeré informace o identifikované nebo identifikovatelné osobě. Za identifikovatelnou se považuje osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity. Identifikace osoby tedy znamená její jednoznačné rozlišení od jiných osob, možnost rozpoznat konkrétní jednotlivce*“.

V českém právním řádu je definice obsažena v ustanovení §4 písm. a) zákona o ochraně osobních údajů, dle kterého „*osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“.* Definici osobního údaje je převzata z mezinárodních dokumentů, zejména z Úmluvy 108, respektive směrnice 95/46.[1]

1.3 Správce a zpracovatel

Správce je fyzická nebo právnická osoba, která určuje účely a prostředky zpracování osobních údajů a také za jeho zpracování zodpovídá. Správce zpracovává osobní údaje pro účely zahrnující jeho činnost nebo také pro vlastní účely, ale ty nesmí převyšovat zájem ochrany základních práv a svobod fyzických osob.[4]

Zpracovatel je ten, koho si správce najímá, aby pro něj zpracovával osobní údaje a prováděl další zpracovatelské úkony. Správce nemá povinnost si najmout zpracovatele, takže zpracovatel není nutný k zpracování osobních údajů. Zpracovatel může provádět jen takové zpracování dat, které mu určil správce.[9]

1.4 Souhlas se zpracováním osobních údajů

Vyjádření souhlasu se zpracováním osobních údajů je jedna ze základních zásad zpracování osobních údajů, protože tímto zpracováním dochází k zásahu do soukromí jejich nositele. Podle definice obsažené v § 4 písm. n) zákona o ochraně osobních údajů je souhlasem svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení se zpracováním osobních údajů. Správce má povinnost, po celou dobu zpracování osobních údajů, prokázat vědomý souhlas subjektu se zpracováním osobních údajů. Tím pádem nese důkazní břemeno správce nikoliv

subjekt. Správce musí prokázat, že subjekt souhlasil se zpracováním a souhlas splňoval všechny náležitosti. Subjekt údajů musí být obeznámen během udílení souhlasu, za jakým účelem poskytuje své osobní údaje, jaké osobní údaje poskytuje, jakému správci je poskytuje a na jak dlouhou dobu. Nová právní úprava v zásadě parametry souhlasu nemění, pouze je rozšiřuje. [1]

Souhlas se zpracováním osobních údajů by měl splňovat několik vlastností. Mezi hlavní patří vyjádření svobodné vůle při souhlasu se zpracováním. Dále by měl být souhlas konkrétní a musí obsahově splňovat všechny náležitosti. Takže jaké osobní údaje budou zpracovány, za jakým účelem budou zpracovány, jak dlouho budou zpracovávány, kdo je bude zpracovávat a práva které má poskytovatel osobních údajů. Souhlas je nutné prokázat po celou dobu zpracování. [1]

1.5 Práva subjektů údajů

S GDPR se značně posílily práva občanů tzv. subjektů údajů. Nejzásadnější práva jsou právo na výmaz, právo na opravu a doplnění, právo přístupu k osobním údajům a právo vznést námitku. Ve zkratce občané v EU získávají kontrolu nad svými osobními údaji. Nyní také musí být o svých právech důkladně informováni. Nyní musí být subjekty údajů informováni, že došlo k úniku jejich osobních údajů. Dříve tuto povinnost správci neměli. [1]

Právo na výmaz

Toto právo můžeme nalézt v článku 17 Nařízení, podle kterého má subjekt právo na to, aby bez zbytečného odkladu správce zlikvidoval veškeré osobní údaje, které se daného subjektu týkají. Správce má za povinnost veškeré osobní údaje ihned vymazal. [1]

Právo na přístup k osobním údajům

Můžeme ho nalézt v článku 15 Nařízeni. Subjekt má právo zjistit, jestli jsou jeho osobní údaje správcem zpracovávány, a pokud tomu tak je, je jeho právem získat k těmto údajům přístup. Subjekt má právo získat kopii osobních údajů. Pokud požádá o více kopií, tak mu může správce účtovat přiměřený poplatek. [1]

Právo na opravu a doplnění

Toto právo nalezneme v článku 16 Nařízení. Říká nám, že subjekt údajů má právo na to, aby správce ihned opravil nepřesné osobní údaje, které se ho týkají. Toto právo úzce souvisí s povinností správce, vést přesně zpracované osobní údaje. [1]

Právo na přenositelnost

Toto právo je uvedeno v článku 20 Nařízení. Subjekt ve své podstatě umožňuje používat své údaje pro své účely pro různé služby. Toto právo umožňuje snadno přesouvat, kopírovat nebo předávat osobní údaje mezi různými informačními prostředími. Osobní údaje musí být předány v běžně strukturovaném a strojově čitelném formátu. [1]

Právo vznést námitku

Podle článku 21 Nařízení má subjekt údajů právo vznést námitku pro zpracování osobních údajů. Správce dále údaje nezpracovává, pokud nedokáže závažný oprávněný důvod k jejich zpracování, který převažuje nad zájmy nebo právy a svobodami subjektu údajů. Jestli subjekt údajů vznese námitku proti zpracování pro přímý marketing, osobní údaje nesmí být nadále zpracovávány. [1]

Nové povinnosti pro správce

Správcem osobních údajů může být fyzická osoba nebo právnická osoba. Provádí shromažďování, zpracování a uchování osobních údajů. Správce je primárně zodpovědný za zpracování osobních údajů. Základním předpokladem je to, že správce musí disponovat řádným právním důvodem, proč zpracovává dané osobní údaje. Také musí údaje dostatečně zabezpečit. Správce tedy odpovídá za dodržování zásad zpracování, dodržování povinností upravených nařízením a zabezpečení údajů.[3]

Vytvoření záznamů o činnostech

Záznam o činnostech obsahuje podrobný popis zpracování, které provádí jednotliví správci a zpracovatelé. Tento záznam umožňuje dozorčím úřadům získat dokonalý přehled o tom, jak je s osobními údaji nakládáno a jak jsou zpracovávány. Mimo jiné umožňuje získat přehled i samotnému správci. Záznam musí obsahovat například:[1]

- jméno a kontaktní údaje správce, jeho zástupce a pověřence pro ochranu osobních údajů
- účel zpracování
- popis kategorií subjektů a kategorií osobních údajů
- seznam příjemců, kterým budou osobní údaje zpřístupněny
- obecný popis bezpečnostních opatření
- plánované lhůty pro výmaz

Záznam je tedy určen k doložení činností zpracovatele a správce s Nařízením. Povinnost vést tento záznam mají, jak správce údajů, tak i zpracovatele údajů. Záznamy musí být vedeny v takové podobě, aby byly při případné kontrole snadno doložitelné. [1]

1.5.1 Povinnost zabezpečení a hlášení bezpečnostních incidentů

Správci a zpracovatelé mají povinnost chránit osobní údaje během jejich zpracovávání, ale také i po jejím ukončení, kdy v zákoně není stanovena žádná časová hranice. Osobní údaje chrání před úmyslném, ale také i nedbalostním jednáním, stejně tak i před přírodními vlivy, které by mohly umožnit zneužití osobních údajů. Tato povinnost je stanovena jako absolutní, proto lze chápat tuto povinnost zároveň i jako podmínku pro zpracování. Správce a zpracovatel jsou tedy povinní za zajištění náležitých opatření vylučují veškerá rizika, která by mohla vést k jejich zneužití. [1]

Posouzení vlivu

Povinnost vzniká tehdy, kdy je pravděpodobné, že při zpracovaní osobních dat za použití nových technologií, dojde k omezení či porušení práv a svobod fyzické osoby. Proto správce musí před zpracováním provést posouzení vlivu. Správce by měl hlavně vyhodnotit původ, zvláštnost, závažnost a povahu tohoto rizika. [1]

Jmenování pověřence

Pověřenec pro ochranu osobních údajů musí být jmenován na základně jeho zkušeností a kvalit, které se týkají jejich ochrany. Mezi jeho hlavní vědomosti by měla patřit národní a evropská legislativa. Mimo jiné praxe v oboru ochrany osobních údajů. [1]

Jmenování pověřence pro ochranu osobních údajů neboli DPO (Data Protection Officer). Jeho hlavním úkolem je monitorování zpracování osobních údajů, aby byly v souladu s povinnostmi vyplívajícími z nařízení. DPO by měl být schopen plnit své povinnosti a úkoly nezávislým způsobem, ať už je zaměstnancem firmy nebo funguje jako externista. Pověřenci nenesou osobní odpovědnost za nesprávné dodržování GDPR. Nařízení stanoví, že jsou to správci nebo zpracovatelé, kteří nesou zodpovědnost a musí být schopni doložit správnost zpracování osobních údajů.[12]

1.6 Sankce

Za porušení, nezavedení nového nařízení hrozí velmi vysoké pokuty, které mohou být ve spoustě případů až likvidační. GDPR totiž zavádí několikanásobně vyšší pokuty, než které byly

doposud. Strop pokuty je dvacet milionů euro nebo 4 % z celkového ročního obratu společnosti a závisí na mnoha faktorech, které jsou např. povaha, závažnost a délka porušování, počet poškozených občanů a míra škody, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, kategorie osobních údajů a mnoho dalších. Mimo udělení pokuty mohou být správci nebo zpracovatelé osobních údajů vystaveni žalobám podaným fyzickými osobami. Společnosti se pak taktéž vystavují rizikům způsobeným nesprávným zacházením s osobními údaji.[4]

1.7 Role ÚOOÚ

Úřad pro ochranu osobních údajů je ústředním správním úřadem pro oblast ochrany osobních údajů. Mezi jeho hlavní úkoly patří monitorovat a vymáhat uplatňování obecného nařízení a jiných předpisů upravujících některé otázky ochrany osobních údajů. Úřad také poskytuje zástupcům odborných, profesních a průmyslových sdružení konzultace ohledně aplikace GDPR. Zaměřuje se na konkrétní návrhy postupů při plnění povinností uložených v Nařízení. Všechny využitelné výstupy z konzultační činnosti zveřejňuje ÚOOÚ na svých webových stránkách.[5]

Úřad je také jediným dozorovým úřadem s obecnou působností podle GDPR v České republice. Úřad se zabývá stížnostmi dotčených subjektů a následně provádí kontroly podle kontrolního řádu. Dále sleduje činnosti zpracování osobních údajů a neustále zkvalitňuje a prohlubuje ochranu osobních údajů v evropském hospodářském prostoru.[5]

WP29

Jedná se o nezávislý orgán na ochranu dat a soukromí. Je složena z dozorových zástupců všech členských zemí Evropské unie. Od 25. května 2018 se změnila na Evropský sbor pro ochranu osobních údajů. Úkolem tohoto sboru je zajišťování souladu GDPR a za tím účelem tedy monitorovat jeho uplatňování a vydávat doporučení, pokyny a postupy.[13]

1.8 Předávání osobních údajů do jiných zemí

Aby mohl správce předat osobní údaje jinému správci, tak musí mít právní důvod, protože předání dat patří taktéž mezi zpracování osobních údajů. Pokud chce správce předat osobní údaje do jiného státu mimo Evropskou unii, tak musí být zajištěna institucionální ochrana. To znamená, že v daném státě, kam putují osobní údaje, musí být zajištěná dostatečná právní ochrana těchto údajů. V těchto případech rozhoduje komise, zda země zajišťuji potřebnou ochranu osobních údajů. Pokud rozhodne, že ano, tak se nevyžaduje žádná speciální povolení pro předání osobních údajů a nejsou kladeny žádné překážky. Pokud komise nevydala

rozhodnutí k dané zemi, tak osobní údaje mohou být předány do třetí země pouze v případě, kdy přijímací správce dal dostačující záruky a za podmínky, že práva subjektů údajů budou vymahatelná.[6]

Standartní smluvní doložky

Standartní smluvní doložky jsou nástrojem, díky kterému lze předávat osobní údaje do zemí mimo Evropskou unii, o kterých se rozhodlo, že poskytují dostatečnou právní ochranu subjektů údajů. Jde o text, kde se správce, který přijímá osobní údaje, zavazuje, že bude dodržovat pravidla o zpracování osobních údajů podle pravidel, které platí v Evropské unii.[6]

1.9 Porušení zabezpečení

Je povinností ohlašovat všechny porušení zabezpečení, které by mohly mít za následek porušení práv subjektů údajů. Může jít o útok na počítač, kde jsou uloženy osobní údaje, nebo jít o ztrátu či odcizení listinných dokumentů, které obsahují osobní údaje. Případy, kde je velice nepravděpodobné riziko pro subjekty údajů, se nemusí nahlašovat. Jde například o momentální nedohledatelnost listinných dokumentů, kdy jde třeba o špatné založení do kartotéky. Správce musí zaslat ohlášení dozorovému úřadu, který je v našem případě Úřad pro ochranu osobních údajů. Správce nebo zpracovatel musí zaslat toto ohlášení nejpozději do 72 hodin od okamžiku, kdy se o porušení zabezpečení dozvědí. Musí také informovat subjekty údajů, kterých se únik dat týká.[13][1]

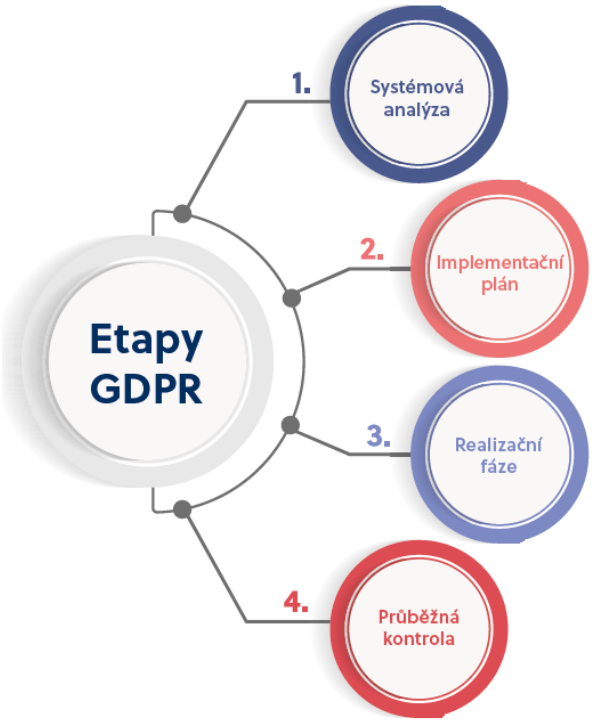
V některý případech správce nemusí informovat subjekty údajů a to ve 3 případech:

- Data byla zašifrována
- Správce přijal taková opatření, že vysoké riziko pro subjekty údajů se pravděpodobně již neprojeví
- V případě, kdy by to vyžadovalo úsilí nepřiměřené k jeho riziku, a proto jsou informováni pomocí veřejného prohlášení

Jestliže správce subjekty údajů neinformoval o porušení zabezpečení jejich údajů, může požádat správce, aby to provedl.[10]

2 GDPR V PRAXI

Pro úspěšné zavedení Nařízení je potřeba provést přípravu. Tato příprava by se dala rozdělit do 4 etap. Každá etapa na sebe navazuje a po jejich dokončení můžeme říct, že jsme připraveni. Jako první provedeme důkladnou analýzu postupu zpracování dat, zabezpečení dat a jeho právní stránku. Po důkladné analýze se přesuneme k implementačnímu plánu. V této etapě vyhodnotíme výstup z analýzy. Po vyhodnocení se můžeme posunout k realizaci. V realizaci začneme upravovat zabezpečení, právní stránku a všechny kroky zpracování tak, aby vyhovovaly Nařízení a splňovaly všechny náležitosti a povinnosti. V poslední fázi už provádíme monitoring a případné audity. Ty nám slouží k zajištění bezpečnosti zpracování dat. Jednotlivé etapy a jejich pořadí můžeme vidět na Obrázku 1. [1]



Obrázek 1 Jednotlivé etapy zavedení GDPR

Zdroj:[8]

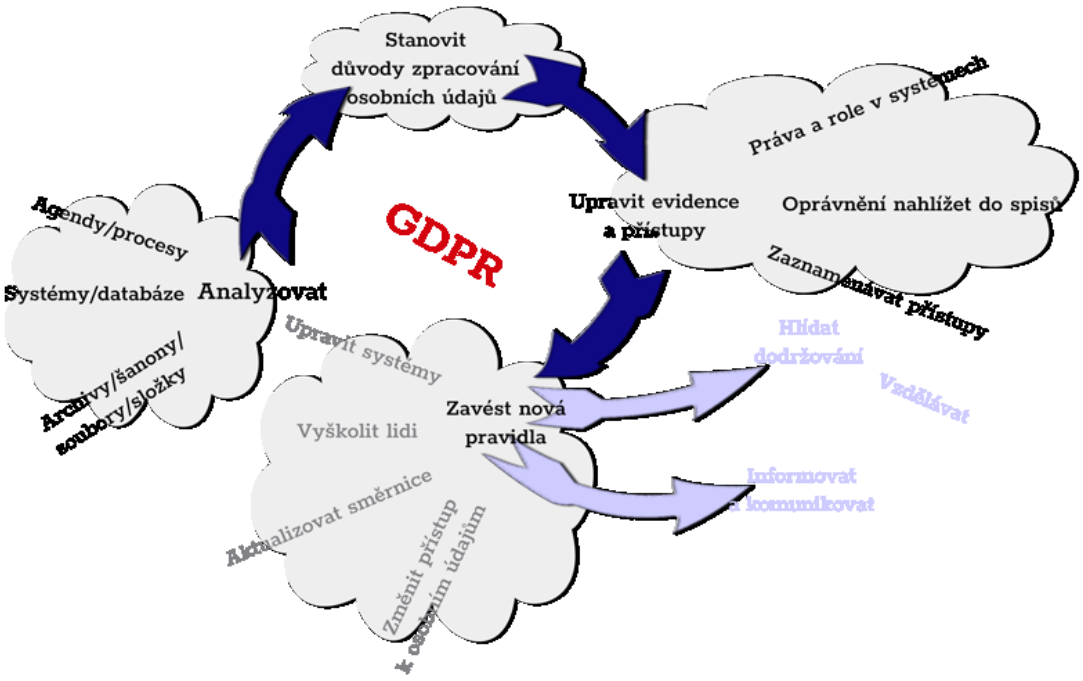
2.1 Systémová analýza

Jako první krok pro úspěšné zavedení GDPR je nutné provést analýzu zpracování osobních dat. Musíme zjistit, jaké osobní údaje správce zpracovává a v jakém rozsahu. Jestli již má zpracovány některé právní dokumenty, které se dříve věnovaly zpracování těchto dat například směrnice, bezpečností dokumentace a jaký je jejich obsah. Cílem této vstupní analýzy je objasnit a vyhodnotit rozsah zpracování osobních údajů, úroveň jejich zabezpečení, zpracování

a způsob plnění povinností podle zákona. Tím vytvoříme výchozí bod, od kterého se můžeme odrazit a začít implementovat Nařízení. [1]

V první etapě zpracování dat je potřeba určit základní parametry zpracování osobních údajů. Jde hlavně o určení:

- Kategorií osobních údajů a jejich rozhas zpracování
- Účely zpracování
- Zákonný důvod
- Kategorie subjektů údajů
- Kategorie příjemců
- Předávání osobních údajů do třetí země
- Doba uchování
- Zdroj (subjekt údajů)
- Prostředky zpracování osobních údajů



Obrázek 2 Promítnutí požadavků ochrany osobních údajů do firemního prostředí

Zdroj:[7]

2.2 Implementační plán

Po vypracování analýzy se dostáváme k implementačnímu plánu. Zde vyhodnotíme analýzu. Ve vyhodnocení zjistíme rozsah a potřebnost zpracování osobních údajů. Zjistíme, zda souhlas

ke zpracování osobních údajů obsahuje všechny náležitosti a zda plníme informační povinnost. Výstupem bude také vyhodnocení zpracování dat jako celek a zda jsou zajištěny všechny povinnosti vůči subjektům údajů a zda jsme efektivně schopni vyhovět jejich požadavkům v rámci jejich práv podle Nařízení. Tedy jestli jsme schopni například smazat jejich osobní údaje, zpřístupnit jim všechny osobní údaje, které jsou zpracovávány. Posoudíme, zda je ochrana osobních údajů v listinné a elektronické podobě dostačující. Vyhodnotíme zabezpečení kamerových záznamů, které také zpracovávají naše osobní údaje. A jako poslední, vyhodnotíme kontrolní činnosti vůči zaměstnancům správce. [1]

2.3 Realizační fáze

V této fázi máme v ruce již implementační plán, dle kterého zjistíme, na které oblasti se musíme zaměřit a upravit. Na konci této fáze budeme již osobní údaje zpracovávat tak, že budou v souladu s Nařízením. V této části je potřeba se zaměřit na záznamy o činnostech, které jsou velmi důležité. Musí být také správně zpracován souhlas se zpracováním osobních údajů, úprava smluv se zpracovateli a v neposlední řadě je potřeba zajistit vyhovující zabezpečení osobních údajů[1][12]

2.3.1 Záznamy o činnostech zpracování

Nahrazení, oznamovací povinnosti úzce souvisí vytváření záznamů o činnostech zpracování osobních údajů. Tyto záznamy můžeme využít jako náhradu za oznamovací povinnost. Obsahují totiž obdobné informace, jako které byly v oznamovací povinnosti. Správci a zpracovatelé, mají povinnost vést tyto záznamy o činnostech zpracování osobních údajů, pokud se jich netýká nějaká výjimka. Tyto záznamy pak slouží jako prostředek pro dokázání, že zpracování probíhá v souladu s nařízením. Záznamy o činnostech si může vyžádat kontrolní úřad, který je v našem případě úřad pro ochranu osobních údajů. Záznamy musí být vedeny písemně a nezáleží, jestli v listinné podobě nebo elektronické.[13]

Záznamy musí obsahovat tyto informace:

- Kontaktní údaje správce nebo zpracovatele a pověřence
- Účel zpracování
- Kategorie subjektů údajů a jejich popis
- Příjemci, kterým budou osobní údaje zpřístupněny, včetně příjemců třetích zemích
- Plánované lhůty pro výmaz, pokud je to možné
- Popis organizačních, technických a bezpečnostních opatření

Záznamy by měly teda ve zkratce obsahovat kdo je správce či zpracovatelem osobních údajů. Zda má správce nebo zpracovatel určeného pověřence a kontakt na něj. Za jakým účelem jsou osobní údaje zpracovávány a jaké údaje jsou zpracovávány. Podle důvodu zpracovávání se ukládají další povinnosti či se zvětšuje nebo zmenšuje rozsah práv subjektu údajů. Z důvodu zpracování osobních údajů, můžeme určit na jak dlouho budou údaje zpracovávány a kdy mohou být vymazány. A v neposlední řadě musí obsahovat to, jak je zajištěna bezpečnost těchto osobních údajů. [1]

2.3.2 Úprava smluv se zpracovateli

Jak jsem již dříve napsal, tak zpracovatelem je fyzická či právnická osoba, agentura nebo orgán veřejné moci. V článku 28 Nařízení je dáno, že správce může využít pouze zpracovatele, kteří mu poskytnou veškeré záruky, že zpracování osobních údajů probíhá, tak že splňuje všechny požadavky tohoto Nařízení. Tím, že správce uzavře se zpracovatelem smlouvu, tak se nezbavuje odpovědnosti. Odpovědnost vždy leží na bedrech správce, i když se dokáže že pochybil zpracovatel. Správce může být konfrontován z důvodu, že zvolil špatného zpracovatele, který nebyl příliš věrohodný a špatně si ho prověřil. Smlouva, kterou mezi sebou uzavírají, musí být v písemné formě. Smlouva nemusí být uzavírána zcela samostatně. To znamená, že může být obsahem jiné smlouvy např. mandátní nebo příkazní smlouvy. Nařízení jasně udává, jaké náležitosti musí smlouva mít. Pokud tyto náležitosti nemá, tak smlouva není neplatná, ale jednalo by se o jinou smlouvu o zpracování. To by znamenalo, že zpracovatel a správce nemají vhodný právní titul, což by mohlo mít negativní důsledky. [13][18]

Smlouva musí obsahovat tyto náležitosti:

- Předmět a doba trvání po kterou je prováděno zpracování osobních údajů
- Povahu a účel zpracování
- Kategorie subjektů údajů a osobní údaje, které budou zpracovávány
- Práva a povinnosti správce
- Činnost na základě pokynů správce
- Závazek mlčenlivosti
- Povinnost údaje zabezpečit
- Zákaz řetězení zpracovatelů
- Součinnost zpracovatele

Správce může využít služeb více zpracovatelů, kdy zpracování je složité a má více částí. Se všemi zpracovateli musí mít uzavřenou smlouvu o zpracování. Smlouvu o zpracování může uzavřít pouze správce se zpracovatelem nikoli zpracovatel s jiným zpracovatelem. Zpracovatel si může určit pouze pověřence.[18]

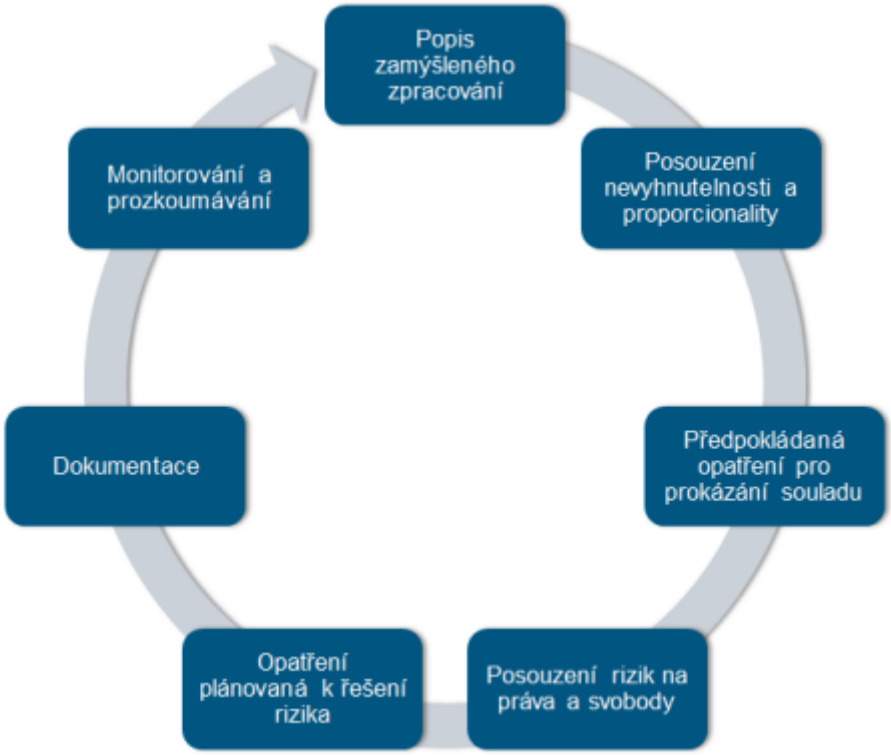
2.3.3 Úprava souhlasů se zpracováním

Souhlas se zpracováním osobních údajů je pouze jedním ze zákonných důvodů, které Nařízení udává. Pro správce je ale lepší, když si najdou jiný zákonný podklad, díky kterému mohou údaje zpracovávat, protože souhlas může být kdykoliv odvolaný a je tedy i nestabilní. Ke každému zpracování osobních údajů musí být dán účel zpracování a k němu tedy právní základ. Avšak tento právní základ nesmí být během zpracování nikterak upraven nebo změněn. Správce se tedy ještě před zpracováním osobních údajů musí rozhodnout, jaký právní základ uplatní. Pokud vyjde z analýzy, že souhlas je jediným nenahraditelným zákonným důvodem ke zpracování, tak se musí zajisti to, že tento souhlas splňuje všechny náležitosti. Jak jsem psal výše, tak souhlas musí být svobodný, konkrétní, informovaný a jednoznačný projev vůle. Vyjádřením svobodný, se myslí, že subjekty údajů mají kontrolu nad svým rozhodnutím. Pokud bude subjekt údajů k souhlasu donucen, tak je tento souhlas neplatný. Za odvolání souhlasu nesmí nést ani žádné sankce, jinak tento souhlas bude taktéž nesvobodný.[13][1]

2.3.4 Posouzení vlivu

Posouzení vlivu patří k novinkám, které s sebou přináší GDPR. Posouzení vlivu se provádí v případech, kdy se ve velkém zpracovávají osobní údaje za pomoci informačních technologií a toto zpracování má vysoké riziko porušení práv a svobod subjektů údajů. Typickým příkladem je profilování. Při vyhodnocování osobních údajů subjektů, dochází k analyzování osobnosti a chování fyzické osoby. Toto vyhodnocování je prováděno automaticky využitím výpočetních technik. Druhým případem, kdy se provádí posouzení vlivu na ochranu osobních údajů, je případ, kdy je prováděno obrovské zpracování osobních údajů, které jsou pro subjekty údajů citlivé nebo pokud se jedná o osobní údaje týkajících se rozsudků v trestních věcech. Dalším případem, kdy se musí provést posouzení vlivu na ochranu osobních údajů, je případ, kdy dochází k monitorování veřejných prostor. V dnešní době je totiž možné rozeznat osobu podle rozpoznávání obličeje a nejen to. Dnešní technologie dokáží rozeznat fyzickou osobu i podle chůze, chování a dalších věcí. Posouzení vlivu nemusí být provedeno jen v těchto třech případech. Je doporučeno pro společnosti, které mají více jak 250 zaměstnanců, aby se posouzení vlivu na ochranu osobních údajů udělaly a předešly tak zbytečným komplikacím

ohledně ochrany osobních údajů. Posouzení vlivu by mělo hlavně obsahovat analýzu stavu správy, zpracování a ochrany osobních údajů. To znamená, že musí být popsané systematické operace zpracování osobních údajů a účely zpracování. Musí být posouzena nezbytnost a přiměřenost operací zpracování. Posouzení rizik pro práva a svobody subjektů údajů. Plán opatření, která povedou k odstranění těchto rizik.[12]



Obrázek 3 Výkladová stanoviska WP29 pro DPIA

Zdroj:[15]

2.4 Zabezpečení zpracování

Zajištění zabezpečení osobních údajů je jednou z nejdůležitějších záležitostí. Aby správce mohl korektně zareagovat včas a správně, musí vědět co je porušení zabezpečení osobních údajů. Podle nařízení porušení zabezpečení je takové porušení, které by mohlo vést k náhodnému či protiprávnímu zničení, ztrátě nebo neoprávněnému poskytnutí a zpřístupnění přenášených osobních údajů. Správce proto musí disponovat takovým systémem, který bude dostatečně chránit osobní údaje. Pro zhodnocení bezpečnosti se zohledňují často tři rizika. První rizikem může být náhodné nebo protiprávní zničení. Druhým rizikem může být ztráta osobníc údajů. V tomto případě data pořád existují, ale správce nad nimi ztratil kontrolu. V třetím případě se jedná o pozměňování, nebo neoprávněné zpřístupnění předávaných osobních údajů. Abychom

zajistili bezpečnost musíme revidovat procesy a odebírat přístupy lidem, kteří nemusí mít přístup k těmto datům. Je potřeba zajistit kybernetickou bezpečnost, aby nedošlo k nabourání do databáze a k odcizení osobních údajů, které by mohly být posléze zneužity. Nařízení ukládá, aby správce a zpracovatel disponovali vyhovujícími technickými a organizačními opatřeními, aby zajistili dostatečnou úroveň zabezpečení. [1][10]

Tabulka 1 – Seznam porušení zabezpečení

Porušení	Nutnost nahlásit dozorovému úřadu	Nutnost nahlásit subjektu údajů	Lhůta
Porušení nepředstavující riziko	Ne	Ne	Ne
Porušení představující riziko	Ano	Ne	72 hodin od okamžiku, kdy se správce o porušení dozvěděl
Porušení představující vysoké riziko	Ano	Ano	Bez zbytečného odkladu

Zdroj: [1]

2.4.1 Bezpečnost IT systémů

Obecné Nařízení neukládá konkrétní opatření, která by měla být aplikována. Při zavedení opatření se bere v potaz stav techniky, veškeré náklady na přijetí opatření a jednotlivá organizační opatření. Nařízení požaduje, že nově vyvíjené systémy by měly co nejvíce respektovat soukromí. To znamená, aby byly zpracovávány pouze osobní údaje, které ke své činnosti nutně potřebují. K těmto systémům, a hlavně k jeho datům by měl být výhradně omezený přístup.[12]

Tyto systémy, které slouží ke zpracování dat by měly obsahovat:

- Pseudonymizace (není povinná)
- Šifrování (není povinné, ale vysoce doporučené)
- Zajištění odolnosti, dostupnosti a integrity systému

Pseudonymizace

Jedná se o zamezení přístupu k osobním údajům v hlavní databázi systému. Ostatní systémy, které následně pracují s osobními údaji, už nepoužívají přímá data, která by vedla k jasné identifikaci subjektu údajů, ale pouze náhodné pseudonymy, které se odkazují na jinak nedostupná data. Hlavní databáze je tedy po celou dobu zpracování, provozována za velmi vysokého zabezpečení. [12]

Šifrování dat

Toto opatření je v rámci ochrany osobních údajů velice doporučeno, ale není nijak povinné. Šifrování lze definovat jako metodu, při které se z dat stanou údaje nečitelné pro všechny, kteří k nim nemají oprávněný přístup. Tento bezpečností krok je účinný proti hackerským útokům, protože i po ztrátě či odcizení dat jsou nečitelné, tedy je bez klíče nelze přečíst. Nevýhodou je, že s daty se nedá pracovat, pokud nejsou odšifrovány.[12]

2.5 Výhody GDPR

Výhody GDPR pocítí hlavně subjekty údajů, tedy lidé jejichž údaje se zpracovávají. Dostávají totiž do ruky nová práva. Tyto práva jim přináší možnost, aby byly informování o rozsahu a účelu zpracování dat nebo možnost, aby jejich osobní údaje byly vymazány z jejich evidence. Dále, aby mohly být osobní údaje zpracovány, tak musí mít zpracovatel či správce souhlas se zpracováním. Souhlas musí být jasně doložitelný a musí dokazovat, že je projevem svobodné vůle.

2.6 Možné nevýhody GDPR

Mezi jasné nevýhody GDPR patří finanční zátěž, která je na straně podnikatelů. Firmy si často najímají externisty, kteří zajistí a nastaví správný chod zpracování dat podle Nařízení nebo se stanou správci dat za nějaký paušální poplatek, který se odvíjí podle rozsahu a náročnosti zpracování dat. Jednou z variant je i ta, že si GDPR firma chce pohlídat sama a své zaměstnance nechá proškolit. Musí vytvořit nový tým lidí, kteří budou za toto zodpovědní. Mezi další nevýhody pro podnikatele jsou, že nespokojený zaměstnanec může udat svého zaměstnavatele například, že osobní údaje chrání nedostatečně, nebo je nezákonně zpracovává. Tyto obvinění může využít i konkurence, která bude těžit z toho, kdy pokuta rivala oslabí, protože pokuty jsou opravdu vysoké, jak jsem se zmiňoval již dříve. Problémem je i to, že pokuty bude úředník udělovat takřka subjektivně, podle míry a rozsahu provinění. Bohužel může v tomto ohledu nastoupit na scénu i korupce, která se bude snažit o ovlivnění výše pokut pro jednotlivé firmy.

3 GDPR NA OBCÍCH

Od 25. května 2018 vstoupilo v platnost obecné Nařízení ve všech členských státech Evropské unie. Pro obce to znamená, že všechny musí mít pověřence pro ochranu osobních údajů a jsou povinny plnit další povinnosti, které přináší toto Nařízení. Obec musíme brát jako orgán veřejné moci, který má za povinnost zařídit funkci veřejného pověřence. Mezi orgány veřejné moci můžeme ale také zařadit školy ve formě právnické osoby. Povinnost mít pověřence je i pro subjekty, které zpracovávají osobní údaje ve velkém měřítku. [10]

3.1 Pověřenec

Pro obce má pověřenec fungovat jako pomocník a konzultant v systému ochrany osobních údajů. Jeho hlavní činností tedy bude poskytování poradenství správcům a zpracovatelům, kteří nějakým způsobem zpracovávají osobní údaje. Jeho dalším úkolem je monitorování zpracování osobních údajů, což obnáší monitorování, sledování a vyhodnocování souladu zpracování s Nařízením a souvisejícími právními předpisy. Pověřenec se navíc stává kontaktní osobou pro dozorový orgán, kterým je v České republice Úřad pro ochranu osobních údajů. ÚOOÚ se může obrátit na pověřence ve všech záležitostí tykajících se zpracování osobních údajů. Avšak odpovědným subjektem jsou nadále jednotlivé obce či kraje, protože oni jsou správci nebo zpracovatelé osobních údajů, kteří mají povinnost vše doložit a prokázat, že zpracování je prováděno korektně podle Nařízení. Pověřenec musí vykonávat jeho úkoly zcela nezávislým způsobem. Obec tedy nemůže udílet pověřenci žádné úkoly. Obec je též povinna, aby zajistila, že pověřenec nebude ve střetu zájmů. Pověřence tedy nelze sankciovat, pokud zastává jiný názor než správce nebo zpracovatel osobních údajů. Nařízení také požaduje, aby mezi vedením a obce a pověřencem nebyl žádný prostředník. Nařízení nezadává povinnost, aby každá obec měla svého vlastního pověřence. Proto připouští, aby více obcí využívalo služeb jednoho pověřence. Sdílení pověřence využijí zejména menší obce, které nezpracovávají osobní údaje ve velké míře. Samozřejmě pověřenec nemusí být schopný zastávat svoji funkci ve více jak 10 obcích, proto se doporučuje maximálně toto číslo. Samozřejmě záleží na obci, zda určí jestli je daný pověřenec schopný zvládnout tuto funkci i v jejich obci. Obec zjišťuje, zda má pověřenec dostatek času a jiných předpokladů pro plnění této funkce. Obce mají tři způsoby, jak zajistit spolupráci s jinými obci při sdílení pověřence.[10]

Více obcí uzavře smlouvu s jediným pověřencem

Jedná se o nejjednodušší cestu, kdy každá obec uzavře samostatně smlouvu s jediným správcem. Pokud se jedná o zaměstnance jedné obce, který vykonává funkci pověřence a jeho služeb chtějí využít i další obce, tak musí mít tento úředník písemní souhlas územního samosprávného celku, u kterého je zaměstnán. Toto ustanovení nalezneme v § 304 odstavec 1 zákoníku práce. [10]

Obec uzavře s jinou obcí smlouvu o spolupráci, která pro ni pověřence zajistí

Obec tedy může uzavřít smlouvu o spolupráci, která zajistí, že jiná obec zajistí plnění úkolů pověřence. Jedná se o koordinační veřejnoprávní smlouvu mezi jednotlivými obcemi. Jiná obec bude tedy v postavení pověřence a bude danou službu smluvně zabezpečovat. V dané obci bude nutné určit zaměstnance, který bude úkoly pověřence vykonávat. [10]

Dobrovolný svazek s obcí

Jedná se o uzavření smlouvy vedoucí k vytvoření dobrovolného svazku obcí. V tomto případě se stává svazek pověřencem a jednotlivé obce již nemusí jednotlivě uzavírat smlouvy s pověřencem. Ale i v tomto případě musí být určena fyzická osoba, kterou bude možno zkontaktovat. [10]

Pověřencem pro obec může tedy být buď její zaměstnanec, kdy ale obec musí zajistit jeho nezávislost nebo externí fyzická či právnická osoba, která splňuje požadavky na to být pověřencem. Pokud se bude jednat o právnickou osobu, musí se v její organizaci jmenovitě určena fyzická osoba, která bude funkci pověřence vykonávat. Kontaktní údaje pověřence musí být veřejné, aby byl dosažitelný. Obec může jmenovat i více pověřenců k dosažení větší efektivnosti. Všichni tito pověřenci v organizaci musí však splňovat kvalifikační předpoklady pro výkon této funkce. Pověřencem se nemůže stát zastupitel obce na základě jeho funkce, ale pokud obec uzavře pracovní smlouvu s tímto zastupitelem je již možné, aby se jím stal. Žádný právní předpis totiž zatím nezakazuje, aby zastupitel plnil i roli pověřence. Tato osoba musí být, ale dostatečně zkušená v profesní znalosti ochrany osobních údajů. V krátké nepřítomnosti pověřence není nutné zavádět jakákoliv opatření, ale pokud půjde o dlouhodobou nepřítomnost je nutné ustanovit náhradního pověřence. Náhradní pověřenec musí také splňovat kvalifikační podmínky pro výkon této funkce. [10]

4 ZAVEDENÍ GDPR V OBCI RADIMĚŘ

V této kapitole se zaměřím na zavedení Nařízení do obce Radiměř. Celé zavádění a jak probíhalo jsem probíral se starostou této obce, který mi byl velice nápomocný. V následujících kapitolách uvedu, jak se změnilo zpracování osobních údajů před a po zavedení Nařízení. Jak se přímo dotklo dané obce a jak postupovala při jeho zavádění. Na obci pracují dvě úřednice a samozřejmě pan starosta.

Tato obec má zhruba 1100 obyvatel, takže se řadí mezi středně velké obce. Nachází se v okrese Svitavy. Je součástí svazku obcí v mikroregionu Svitavsko. Tento mikroregion zabírá zhruba 20 % okresu Svitavy. V tomto svazku se nachází celkem 16 obcí. Svazek byl založen v roce 2000. Cílem tohoto svazku je rozvoj v oblasti ekonomického rozvoje, rozvoje venkova, kvality života a ochrany životního prostředí regionu.

Tabulka 2 – Seznam obcí v mikroregionu Svitavsko

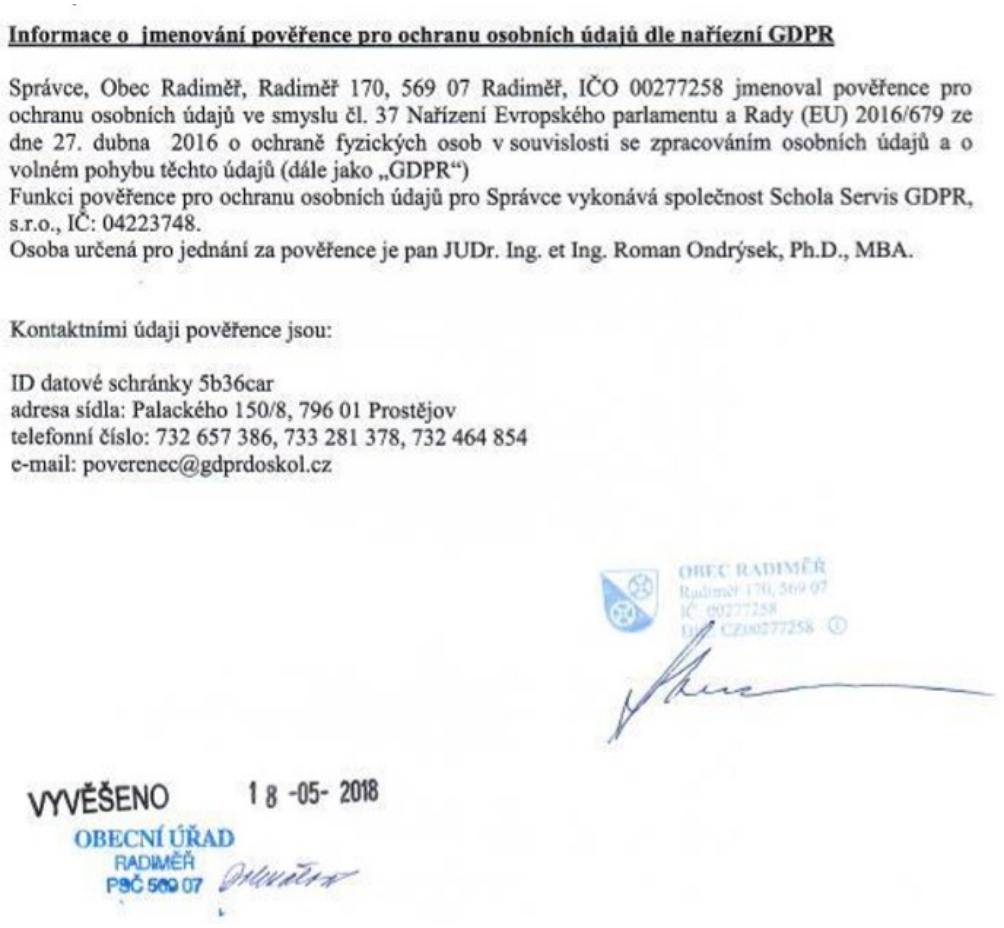
Název obce	Počet obyvatel (2018)
Březová nad Svitavou	1666
Dětřichov	329
Hradec nad Svitavou	1693
Javorník	404
Kamenná Horka	305
Karle	394
Koclířov	710
Kukle	78
Mikuleč	235
Opatov	1152
Opatovec	685
Pohledy	312
Radiměř	1114
Sklené	227
Svitavy	16937
Vendolí	964

Zdroj:[16]

Jak je vidět z tabulky, tak obec patří k těm větším v tomto mikroregionu. Proto je patrné, že zpracovává větší množství osobních údajů.

4.1 Postup při zavedení GDPR na obci

Jak jsem již psal výše, každá obec si dle nového Nařízeni musí zajistit pověřence. Tento pověřenec má fungovat jako jejich poradce, který jim řekne, jak mají přesně zpracovávat osobní údaje. Jeho dalším úkolem bude monitorování a kontrola zpracování osobních údajů, zda vše dělají v souladu s Nařízením. Takže logicky bylo prvním krokem obce, si tohoto pověřence zajistit. Díky tomu, že jsou členy svazku obcí v mikroregionu Svitavsko, tak poptávku vydal tento svazek. Podařilo se tedy zajistit lepší cenu pro jednotlivé obce. Následně byl vybrán vítěz s nejnižší cenou. Obce si pak mohly dobrovolně vybrat, jestli si zajistí pověřence sami nebo využijí nabídky, kterou jim zajistil tento svazek. Samozřejmě všechny obce si vybraly stejného pověřence, který vyšel z jejich společného úsilí ve svazku. Pověřencem se tedy stala firma Schola Servis GDPR, s kterou obec uzavřela smlouvu o poskytování služeb pověřence pro ochranu osobních údajů. Jelikož se jedná o právnickou osobu, tak musela ještě přímo jmenovat fyzickou osobu, jak jsem se již zmiňoval výše. Obec následně vyvěsila na úřední desku dokument o jmenování pověřence pro ochranu osobních údajů.



Informace o jmenování pověřence pro ochranu osobních údajů dle nařiezní GDPR

Správce, Obec Radiměř, Radiměř 170, 569 07 Radiměř, IČO 00277258 jmenoval pověřence pro ochranu osobních údajů ve smyslu čl. 37 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jako „GDPR")
Funkci pověřence pro ochranu osobních údajů pro Správce vykonává společnost Schola Servis GDPR, s.r.o., IČ: 04223748.
Osoba určená pro jednání za pověřence je pan JUDr. Ing. et Ing. Roman Ondrýsek, Ph.D., MBA.

Kontaktními údaji pověřence jsou:

ID datové schránky 5b36car
adresa sídla: Palackého 150/8, 796 01 Prostějov
telefonní číslo: 732 657 386, 733 281 378, 732 464 854
e-mail: poverenec@gdprdoskol.cz

OBEC RADIMĚŘ
Radiměř 170, 569 07
IČ 00277258
DIČ CZ00277258

VYVĚŠENO 18 -05- 2018
OBECNÍ ÚŘAD
RADIMĚŘ
PSČ 569 07

Obrázek 4 Obsah dokumentu o jmenování pověřence

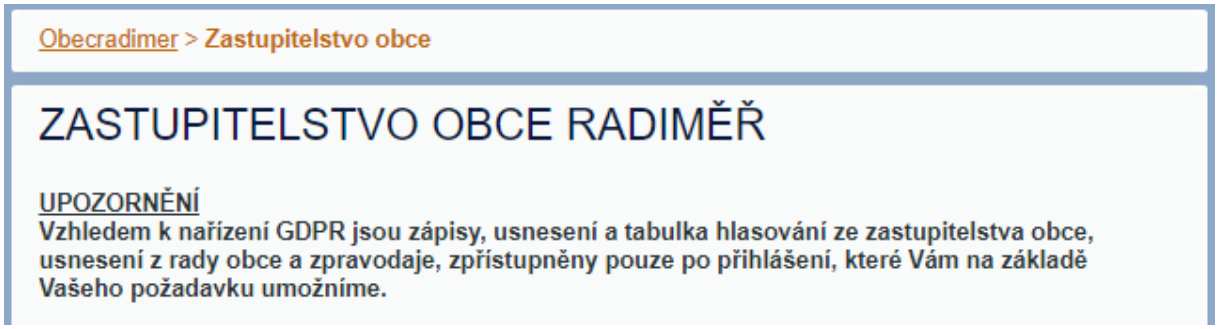
Zdroj:[13]

Jako první musel pověřenec provést analýzu, jejíž účelem je řádně připravit a upřesnit poskytování služeb a získat informace o postupech, procesech a systémech, v nichž je prováděno zpracování osobních údajů. Tím pádem mohl pověřenec zajistit úspěšné a efektivní plánování provedení služeb pověřence. Dále mohl seznámit klienta, tedy obec, s nadcházejícím průběhem realizace služeb. Obě strany se tedy zavázaly upřesnit rozsah informaci, tak aby došlo k úspěšnému a efektivnímu zavedení Nařízení. Obec tedy musí seznámit pověřence se všemi informacemi ohledně zpracování osobních údajů. Tyto informace se musí být pravdivé a nesmí pověřenci nic zamlčet. Ceny služeb byly jasně dány při podpisu smlouvy a jsou pevné a konečné. Pověřenec taktéž není v postavení zaměstnance a obec musí respektovat jeho nezávislost. Všechny informace, které se pověřenec dozví v rámci provádění a poskytování jeho služeb jsou důvěrné, a proto se pověřenec zavazuje mlčenlivostí. Proto pověřenec nesmí dále šířit údaje subjektů údajů, tedy jejich osobní údaje. S těmito údaji je nakládáno jako s obchodním tajemstvím. Pověřenec si s sebou přivádí realizační tým, proto se pověřenec zavazuje, že členové realizačního týmu splňují kvalifikační požadavky Nařízení. Jména jednotlivých členů realizačního týmu byla sdělena obci.

Následně byla sepsána směrnice pro zacházení s osobními údaji. Tato směrnice je samozřejmě v souladu s Nařízením. Došlo k proškolení zaměstnanců obce a také došlo k zajištění zabezpečení na samotném úřadě v obci. Zaměstnanci byli proškoleni, jak správně pracovat na počítačích ve smyslu bezpečnosti, aby se nedostal do jejich počítače škodlivý software.

Velkou změnu, kterou pocítili i občané obce, je úprava obecního zpravodaje. V tomto zpravodaji bylo zvykem, že se zde objevovaly osobní údaje. Oblíbenou rubrikou byl seznam lidí, kteří slaví v daném měsíci narozeniny. Jelikož v obsahu bylo příjmení a věk dané osoby, jedná se jednoznačně o osobní údaje. Proto se tento seznam již v obecním zpravodaji nenachází. Zpravodaj vychází jinak každý měsíc. Dále v něm byli napsaní i zesnulí občani této obce, jenže bez jejich souhlasu nelze uvést jejich jméno ve zpravodaji. Proto často starší občané obce chodili na obecní úřad a vyjadřovali svůj nesouhlas s těmito kroky. Obec je velice dlouhá a lidé z obou konců obce se setkávali zřídka, a proto vnímali tyto informace ve zpravodaji velice kladně, protože věděli, co se zhruba děje na druhém konci obce. Protože staré zpravodaje nesplňovaly náležitosti, které vyžaduje GDPR, musely být z obecních stránek částečně staženy. K přístupu do těchto zpravodajů je zapotřebí zajistit si povolení od obce. Když je přístup schválen, vytvoří se přihlašovací údaje do archivu a následně je přístup povolen, ale je také monitorován.

Zápisy z jednání zastupitelstva obce taktéž obsahují osobní údaje, proto k jejich zpřístupnění potřebujete souhlas obce. Obec Vám následně poskytne přihlašovací údaje, pod kterými se k těmto zápisům dostanete.



Obrázek 5 Upozornění na nutnost oprávnění k nahlédnutí do spisu

Zdroj:[15]

Zaměstnanci obce mají za povinnost zachovávat mlčenlivost o všech skutečnostech, které se týkají osobních údajů, s nimiž v rámci výkonu své práce přichází do styku. Taktéž nesmí nikde šířit, jaká bezpečností opatření se zavedla pro ochranu osobních údajů. Tato mlčenlivost platí i na dobu po ukončení pracovněprávního vztahu. Této mlčenlivosti mohou být zbaveni, ale pouze na pokyn orgánu veřejné moci v zákonem předvídaných situací. Dále není dovoleno uchovávat datové nosiče, u kterých uplynula doba archivace a údaje již nebudou nadále využívány.

4.2 Prohlášení o ochraně osobních údajů

Toto prohlášení obec uveřejnila na svých webových stránkách. Obsah prohlášení obsahuje kontaktní údaje pověřence. Tímto dokumentem správce plní svoji informační povinnost, kterou mu ukládá Nařízení. Správce poskytuje subjektům údajů informace o činnostech zpracování, které jsou nezbytné pro subjekty údajů, aby mohly uplatňovat jejich práva.

4.2.1 Účel a doba zpracování

V prohlášení, které obec vydala, je vysvětleno, jaké osobní údaje obec shromažďuje, z jakého důvodu a na základě jakého právního titulu. Dále obsahuje, k čemu tyto informace využívá, po jakou dobu je nakládáno s těmito informacemi, kdo může do osobních údajů nahlížet a jaká práva mají subjekty údajů.

Vyřizování žádostí a poskytování informací

Aby obec mohla zahájit a řádně ukončit řízení o poskytnutí informace, musí zpracovávat osobní údaje. Obec za tímto účel zpracovává:

- Jméno
- Příjmení
- Datum narození
- Trvalé bydliště
- Adresu pro doručování
- ID datové schránky

Obec archivuje tyto osobní údaje po dobu, která je stanovená ve spisovém a skartačním řádu obce. V případě poskytování informací ze zákona se jedná o dobu 5 let.

Evidence obyvatel obce

Obec v rámci své zákonné působnosti vede evidenci obyvatel. Vedení této evidence je prakticky plnění zákonem uložené povinnosti, která se nachází v 6 odst. 1 písm. C) GDPR- plnění právní povinnosti. Za účelem vedení evidence obyvatel obce osobní údaje archivuje po dobu, která je stanovená ve spisovém a skartačním plánu obce. V případě např. rozhodnutí o zrušení trvalého pobytu je doba stanovena 5 let

V rámci této činnosti obec zpracovává následující osobní údaje:

- Jméno
- Příjmení
- Datum narození
- Rodné číslo
- Trvalý pobyt
- Doručovací adresa
- Číslo občanského průkazu

Mohou být zpracovány i další osobní údaje uvedené v § 3 odst. 3 zákona č. 133/2000 Sb.

Prezentace obce pro občany

Účelem tohoto zpracování je informování občanů o dění v obci a prezentace obce. Právní důvod pro zpracování osobních údajů v tomto případě najdeme v 6 odst. 1 písm. F) GDPR – nezbytnost pro účely oprávněných zájmů obce. Tedy v případě prezentace obce může být uveřejněna fotografie, která obsahuje podobiznu z veřejně konaných akcí obce, zachycující atmosféru obce. Tyto osobní údaje mohou být uveřejněny jen po dobu nezbytně nutnou pro naplnění deklarované účelu.

Obec zde tedy informuje, že pro některé zveřejňované fotografie a videozáznamy nepotřebuje souhlas se zpracováním osobních údajů. Dále zde zmiňuje, že pokud někdo nesouhlasí s uveřejněnými fotografiemi nebo záznamy, má se obrátit na pověřence nebo správce, který pak rozhodne o jejich stažení.

Poplatková agenda

Řádný výběr stanovených poplatků vykonávání zákonem dovolené činnosti, a to na základě zákona č. 128/2000 Sb., o obcích. Právním důvodem zpracování osobních údajů je článek 6 odst. 1 písm. c) GDPR – plnění právní povinnosti.

V rámci této činnosti obec zpracovává následující osobní údaje:

- Jméno
- Příjmení
- Titul
- Adresa bydliště
- Rodné číslo
- Bankovní spojení

Za účelem vedení poplatkové agendy obec archivuje po dobu, která je taktéž stanovená ve spisovém a skartačním plánu obce. V případě daní a poplatků je doba archivace stanovena 10 let.

Zajištění knihovních služeb v obci

Obec, jak je podle nadpisu zřejmé, zajišťuje knihovní služby v obci a provádí ochranu knihovního fondu. Zákonný rámec k uvedené činnosti poskytuje zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných a knihovnických služeb. Právním důvodem zpracování osobních údajů je článek 6 odst. 1 písm. c) GDPR – plnění právní povinnosti a článek 6 odst. 1 písm. c) GDPR – plnění smluvní povinnosti, protože návštěvník knihovny, pokud využívá knihovních služeb, uzavírá s obecní knihovnou smlouvu o poskytování služeb, která nemusí být v písemné podobě.

Obec v rámci knihovních služeb zpracovává zejména následující údaje:

- Jméno
- Příjmení
- Datum narození
- Bydliště

- Podpis

Za tímto účelem obec archivuje tyto osobní údaje po dobu, která je uvedena ve spisovém a skartačním plánu obce. V tomto případě je to na 5 let.

Hospodářská činnost a účetnictví

Aby byl zajištěn řádný chod obce, musí obec provádět činnosti s tím spojené jako je např. zajištění účetnictví, provoz telefonů, IT sítě, ale i běžná údržba veřejných budov. Za tímto účelem jsou uzavírány různé soukromoprávní smlouvy ať už s fyzickými osobami nebo s dodavateli služeb a zboží. Tyto smlouvy obsahují osobní údaje smluvních partnerů – nejčastěji se jedná například o tyto osobní údaje:

- Jméno
- Příjmení
- Titul
- datum narození
- Trvalý pobyt
- Bydliště
- E-mail nebo telefon
- Podpis

S těmito osobními údaji obec zachází převážně za účely plnění uzavřené smlouvy. Což je tedy i právním důvodem. Plnění zákonných povinností nastává typicky v případě, kdy na základě uzavřené smlouvy musí obec evidovat v rámci účetnictví faktury nebo jiné daňové doklady. Smlouvy jsou obcí uchovávány nejdéle 10 let, protože mohou být vyžadovány při kontrole nadřízenými správními orgány.

Zajištění volební agendy

Za účelem řádného zajištění voleb obec shromažďuje osobní údaje. V případě kandidátních listin a souvisejících dokumentů je doba archivace stanovena na 10 let, pro ostatní dokumenty je to na 5 let.

Personální agenda

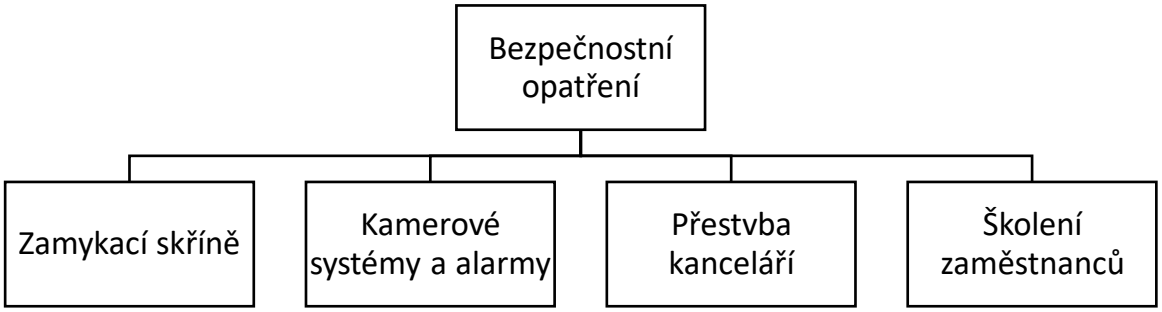
Osobní údaje zaměstnanců správce, tedy obce, jsou zpracovány pro účely vedení personálních dokumentů zaměstnanců a plnění pracovněprávních povinností obce a zaměstnance. Jde tedy například o provádění mzdového účetnictví zaměstnanců, plnění ohlašovací povinnosti zaměstnavatele apod.

4.1 Zabezpečení osobních údajů

Obec nejvíce zasáhly změny v tomto bodě. Zabezpečení je totiž jedním z nejdůležitějších bodů v implementaci GDPR. Aby obec mohla osobní údaje zpracovávat, tak musí zajistiti jejich bezpečí.

Proto pro zajištění souladu s Nařízením, musely být částečně přestavěny i kanceláře přímo na obci. Kanceláře byly nevyhovující z hlediska bezpečnosti, kdy návštěvníci obce měli snadný přístup po celé kanceláři a mohli cokoliv odcizit nebo se dostat do kontaktu s dokumenty, které mohly obsahovat osobní údaje. Z tohoto důvodu byla vybudována přepážka, kde jsou vyřizovány veškeré žádosti, se kterými přijdou lidé na obecní úřad.

Do místnosti, kde jsou uchovávány listiny, které obsahují osobní údaje, byly zakoupeny nové bezpečnostní skříně. Také zde byly instalovány bezpečnostní zařízení, jako jsou alarmy, kamerové systémy a detekce pohybu. Tedy na všechny listinné dokumenty, kde jsou vedené fyzické osoby, se vztahuje tato ochrana. Dokumenty jsou uzavřeny v zamykacích skříní nebo zásuvkách. Musí být také v uzavřené místnosti, která je po celou dobu uzamčená za předpokladu, že se tam nenachází osoba, která s těmito dokumenty aktuálně nepracuje. Kamerové systémy uchovávají záznamy po dobu několika dnů, avšak pokud dojde k nějakému incidentu, jsou tyto kamerové záznamy uchovávány po dobu nezbytně nutnou. Správcem takových osobních údajů je vždy městská police nebo policie České republiky. Archiv záznamů je v souladu s doporučením Úřadu pro ochranu osobních údajů.



Obrázek 6 Souhrn bezpečnostních opatření

Zdroj: vlastní zpracování

Údaje v počítačích jsou zaheslovány a mají k nim přístup jen oprávněné osoby, což jsou dvě úřednice, které na úřadě pracují spolu se starostou. Přístup k osobním údajům mají tedy pouze

zaměstnanci obce, kteří disponují příslušným oprávněním a prověřením. Musí tedy spadat do náplně práce těchto zaměstnanců.

4.2 Náklady

Obec musela provést kroky, které vedou k dostatečnému zabezpečení a zajištění vhodného zpracování osobních údajů. Nejdražší položkou v seznamu pro ni byla renovace kanceláří. Do této renovace jsou započítány nové zamykací skříně, vybudování přepážky, nové bezpečnostní dveře a další náklady spojené s renovací kanceláře. Dále jsou na seznamu bezpečností systémy jako je alarm a kamerový systém. Poslední položkou je cena analýzy, kterou prováděl pověřenec.

Tabulka 3 Náklady na implementaci GDPR

Položky	**Cena**
Přestavba kanceláře	171 385,00 Kč
Alarm	15 000,00 Kč
Kamerový systém	10 000,00 Kč
Cena analýzy	18 000,00 Kč
Celkové náklady	**214 385,00 Kč**

Zdroj: vlastní zpracování

Obec taktéž platí paušální částku 2.700,- Kč, která je placena každý měsíc. Tato částka se platí pověřenci za jeho služby obci.

4.3 Shrnutí

Obec se již řídila zákonem č. 101/2000 Sb., který je v platnosti již od roku 2000, proto změny v obci nebyly tak rozsáhlé. Když jsem na toto téma diskutoval se starostou obce, tak zmínil, že ze začátku měl obavy ze zavedení tohoto Nařízení. Domníval se, že implementace bude velice náročná, jak z finanční stránky, tak i ze stránky právnické. Ministerstvo vnitra však vydalo několik metodik, jak postupovat k úspěšnému zavedení GDPR. Ve zkratce zde byla obec vedena k tomu, aby si zajistila pověřence, který zajistí vše potřebné. Řekne, kde se co musí změnit, které údaje jsou zpracovávány nad míru a co se kde již nesmí uvádět.

Příkladem v této obci je jasně obecní zpravodaj, kde se často uváděly osobní údaje. Dalším příkladem jsou obecní stránky, kde největší změnou prošel archiv obecního zpravodaje a zápisy ze zasedání zastupitelstva, které již nejsou přístupné veřejnosti bez souhlasu obce.

Největší změny pro obec jsou změny v oblasti zabezpečení. To si vyžádalo největší náklady na zajištění. Kanceláře musely být částečně přestaveny. Byly zde nainstalovány kamerové systémy další zabezpečovací prostředky.

Největší změny GDPR přineslo pro obce hlavně v ochraně informací a informační povinnosti. Jinak, pokud se obec řídí zákonem č. 101/2000 Sb., tak změny pro obce nebyl nijak rozsáhlé. Obce nyní mají za sebou pomyslný bič ze strany ÚOOÚ, který funguje jako dozorový úřad a může ukládat vysoké pokuty. Nad svými osobními údaji mohou dohlížet taktéž i subjekty údajů, protože GDPR jim přinesla spoustu práv v tomto ohledu.

POUŽITÁ LITERATURA

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

[2] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.

[3] Co je GDPR a jak bude aplikováno v Česku?. *GDPR.cz* [online]. Praha, 2016 [cit. 2019-01-05]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[4] Správce osobních údajů. *GDPR* [online]. Praha: Mgr. Eva Škorničková, 2016 [cit. 2019-03-11]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/

[5] Jaké sankce hrozí firmám, které budou GDPR ignorovat. *GDPR* [online]. Praha: Mgr. Eva Škorničková, 2006 [cit. 2019-03-13]. Dostupné z: https://www.gdpr.cz/gdpr/sankce/

[6] Role ÚOOÚ. *Úřad pro ochranu osobních údajů*[online]. Praha: Úřad pro ochranu osobních údajů, 2018 [cit. 2019-03-13]. Dostupné z: https://www.uoou.cz/role-uoou/ds-4726/archiv=0&p1=3938

[7] Předávání osobních údajů do jiných zemí. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, 2017 [cit. 2019-03-14]. Dostupné z: https://www.uoou.cz/10-p-edavani-osobnich-udaj-do-jinych-zemi/d-27284

[8] Naplnění požadavků ochrany osobních údajů v organizacích. In: *PDQM* [online]. Praha: PDQM, 2017 [cit. 2019-03-14]. Dostupné z: http://www.pdqm.cz/services/executive/zavedeni-GDPR

[9] Etapy GDPR. In: *Czechinvest* [online]. Praha: Czechinvest, 2018 [cit. 2019-03-14]. Dostupné z: https://www.czechinvest.org/cz/Sluzby-pro-male-a-stredni-podnikatele/GDPR

[10] Nejdůležitější pojmy. *Úřad pro ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2017 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293

[11] Porušení zabezpečení. *Úřad pro ochranu osobních údajů* [online]. Praha: ÚOOÚ, 2017 [cit. 2019-03-17]. Dostupné z: https://www.uoou.cz/poruseni-zabezpeceni/ds-5020/p1=5020

[12] MLSNA, Petr. MINISTERSTVO VNITRA. *Metodické doporučení k činnosti obcí*. Praha, 2017, 23 s. Dostupné také z: https://www.helpgdpr.cz/rstsp/clanky.nsf/i/gdpr_metodicke_doporuceni_k_cinnosti_obci_17120608_81377890

[13] NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.

[14] Informace o jmenování pověřence pro ochranu osobních údajů dle nařízení GDPR. In: *Úřední deska - Obec Radiměř* [online]. Radiměř: OÚ Radiměř, 2018, 2018-05-18 [cit. 2019-04-24]. Dostupné z: http://radimer.imunis.cz/edeska/file.asp?id=12721&ts=RjqLAKb6CLjLu0RVw8O8W5ZKAEBOvhs%3D

[15] ZASTUPITELSTVO OBCE RADIMĚŘ. In: *Obec Radiměř* [online]. Radiměř: OÚ Radiměř, 2018, 2018-05-11 [cit. 2019-04-24]. Dostupné z: https://www.obec-radimer.cz/zastupitelstvo-obce/

[16] Průvodce pro přípravu obcí na požadavky GDPR. In: AKADEMIE GDPR – SVAZ PRŮMYSLU A DOPRAVY ČR. *Ministerstvo vnitra* [online]. Praha: Ministerstvo vnitra, 2018, 2018 [cit. 2019-04-24]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/gdpr-modelove-situace-pruvodce-pro-pripravu-obci-na-gdpr.aspx

[17] *Databáze demografických údajů za obce ČR*. Praha, 2018. Dostupné také z: https://www.czso.cz/csu/czso/databaze-demografickych-udaju-za-obce-cr

[18] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013. Právní rukověť (Wolters Kluwer ČR). ISBN 978-80-7478-139-1.