Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

GDPR z pohledu místních samospráv

Martina Machová

Bakalářská práce
2018

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martina Machová**
Osobní číslo:	**E15866**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Název tématu:	**GDPR z pohledu místních samospráv**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je zhodnotit pozitivní a negativní důsledky zavádění GDPR v obcích regionu (kraje). Popsat jaké změny a povinnosti pro obce přináší, jaký má vliv na informační systémy v obcích, jak je celý proces řešen a jak zatěžuje rozpočty obcí.
Osnova:
- Zásady a popis GDPR
- Nové povinnosti plynoucí z GDPR
- Sběr dat a dotazník
- Vyhodnocení a závěry.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

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).
MVČR - Ochrana osobních údajů (online). Praha: MVČR. ?2018. Poslední změna 27.04.2018, (cit. 27.07.2018). Dostupné z: http://www.mvcr.cz/gdpr/
JANEČKOVÁ, E. GDPR - Praktická příručka implementace, 1. vydání, Praha: Wolters Kluwer, 2018, 136 s. ISBN 978-80-7552-248-1.
NULÍČEK, M. a kol. GDPR / Obecné nařízení o ochraně osobních údajů. Praktický komentář. 1. vydání, Praha: Wolters Kluwer, 2017, 525 s. ISBN 978-80-7552-765-3.
ŽŮREK, J. Praktický průvodce GDPR, 1. vydání, Olomouc: ANAG, 2017, 223 s. ISBN 978-80-7554-097-3.

Vedoucí bakalářské práce: **Ing. Pavel Jirava, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **9. května 2018**

Termín odevzdání bakalářské práce: **13. prosince 2018**

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

L.S.

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

V Pardubicích dne 9. května 2018

PROHLÁŠENÍ

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

Byla jsem seznámena 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 12.12.2018 .....

Martina Machová

PODĚKOVÁNÍ

Ráda bych poděkovala svému vedoucímu práce Ing. Pavlu Jiravovi Ph.D., za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Všem paním starostkám a pánům starostům, kteří mi byli nápomocní u realizace vyplnění dotazníků v Pardubickém kraji.

ANOTACE

Tato bakalářská práce se zabývá ochranou osobních údajů (GDPR) z pohledu místních samospráv. Úvodní část práce objasňuje pojmy jako základy a zásady GDPR. Dále seznamuje s obecnými pravidly. Práce má za cíl zhodnotit pozitivní a negativní důsledky zavádění GDPR (General Data Protection Regulation) v obcích regionu (kraje). Analytická část zpracovává dotazníkové šetření, kterým popisuje, jaké změny a povinnosti pro obce přináší, jaký má vliv na informační systémy v obcích, jak je celý proces řešen a jak zatěžuje rozpočty obcí.

KLÍČOVÁ SLOVA

Ochrana, osobní údaje, rizika, zabezpečení

TITLE

GDPR from the point of view of local authorities

ANNOTATION

This bachelor thesis deals with the protection of personal data (GDPR) from the local authorities' point of view. The introductory part of the thesis clarifies concepts as the foundations and principles of GDPR. It also introduces general rules.
The work aims to evaluate the positive and negative consequences of introducing the General Data Protection Regulation (GDPR) in the municipalities of the region. Analytical part deals with the questionnaire survey, which describes the changes and responsibilities for the municipalities, the influence on the information systems in the municipalities, the way the whole process is solved and what it means for the municipal budgets.

KEYWORDS

protection, personal data, risks, security

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

DPIA	Vliv na ochranu osobních údajů
EU	Evropská unie
GDPR	General Data Protection Regulation
Sb.	Sbírka zákonů
ÚOOÚ	Úřad pro ochranu osobních údajů

ÚVOD

Tato bakalářská práce se zabývá problematikou tzv. GDPR (zkratka z angl. General Data Protection Regulation), neboli ochranou osobních údajů, které aktuálně přináší do českého právního řádu 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), jehož název je zpravidla zkracován na Obecné nařízení o ochraně osobních údajů nebo GDPR (General Data Protection Regulation, dále také jen „Nařízení" či „Nařízení GDPR") a které je vnímáno jako dosud nejvíce ucelený soubor pravidel na ochranu osobních údajů na světě.

Evropské nařízení je právní předpis schválený na půdě Evropské unie, který je závazný pro všechny státy Evropské unie i všechny soukromé subjekty, adresáty práva (fyzické i právnické osoby).

Problematika GDPR by pak v této práci měla být zpracovávána jednak z obecného hlediska a jednak z pohledu místních samospráv. Postup práce tedy bude od obecného ke konkrétnímu.

Smysl této práce vidím ve skutečnosti, že problematika GDPR reflektuje aktuální stav, v němž rozsah zpracovávaných osobních údajů se stále zvětšuje a stále více zasahuje do všech oblastí lidského života. Díky dokonalejším a dostupnějším technologiím se shromažďování obrovského množství údajů stává snadnější a přístupnější více lidem. Bez ohledu na případnou polemiku o nutnosti zakotvit ochranu osobních údajů právním předpisem či o vhodnosti zvoleného řešení, je však nutné respektovat fakt, že existuje právní úprava, kterou je zapotřebí implementovat a řídit se jí. Touto právní úpravou je především nařízení GDPR.

Úpravu ochrany osobních údajů je třeba hledat již v Listině základních práv a svobod, kde je v článku 10 odst. 3 uvedeno, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Ochrana osobních údajů je tedy právem ústavním, jinak řečeno, je to právo s nejvyšší silou.

GDPR se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu. Nařízení míří na firmy, instituce i jednotlivce, kteří zacházejí s osobními údaji fyzických osob, ať již zaměstnanců, žáků, studentů, zákazníků, klientů a jiných. Zasáhne i ty, kteří sledují

či analyzují chování uživatelů na webu při používání chytrých technologií. V neposlední řadě pak GDPR zasáhne i orgány veřejné správy, orgány místních samospráv z toho nevyjímaje.

Cílem práce je zhodnotit pozitivní a negativní důsledky zavádění GDPR v obcích regionu (kraje). Práce popisuje, jaké změny a povinnosti pro obce GDPR přináší, jaký má vliv na informační systémy v obcích, jak je celý proces řešen a jak zatěžuje rozpočty obcí.

1 ZÁKLADY, ZÁSADY A POJMY GDPR

Soubor zavádí nová pravidla pro ochranu osobních údajů, které přináší do českého právního řádu Nařízení Evropského parlamentu a Rady.

1.1 Právní stav

Evropské nařízení je právní předpis schválený na půdě Evropské unie, který je závazný pro všechny státy Evropské unie. Na rozdíl od častější směrnice však není potřeba jeho implementace do jednotlivých právních řádů členských států, jelikož evropské nařízení je aplikovatelné automaticky bez dalšího. Evropské nařízení se použije přednostně před českými zákony. V České republice tak nahradí současnou právní úpravu ochrany osobních údajů v podobě zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Zákon o ochraně osobních údajů bude již upravovat jen některé aspekty týkající se Úřadu pro ochranu osobních údajů (např. jeho ustavení, organizaci atd.) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou obecným nařízením upraveny nebo které obecné nařízení umožňuje upravit na vnitrostátní úrovni. [5]

Příslušným orgánem pro provádění kontrol a ukládání pokut je stejně jako doposud Úřad pro ochranu osobních údajů. Přibydou mu ale pravomoci odrážející závažnost celé reformy a zároveň bude částečně podřízen Evropskému sboru pro ochranu osobních údajů. Evropský sbor pro ochranu osobních údajů bude plnit především koordinační funkci a dohlížet na to, že GDPR je uplatňováno v celé EU stejným způsobem. Provádění kontrolních řízení se bude řídit samotným GDPR a dále vnitrostátními předpisy, tedy zejm. kontrolním řádem.

GDPR se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů, včetně společností a institucí mimo území EU, které působí na evropském trhu. Nařízení míří na firmy, instituce i jednotlivce, kteří zacházejí s osobními údaji fyzických osob, ať již zaměstnanců, žáků, studentů, zákazníků, klientů, nebo jiných osob.

GDPR zasáhne i ty, kteří sledují či analyzují chování uživatelů na webu při používání chytrých technologií. Nezáleží na tom, jestli je organizace soukromá, nebo veřejná. GDPR se vztahuje na obě dvě. Veřejným subjektům ukládá zpravidla více povinností než soukromým. [5]

Typicky školy a školská zařízení jsou veřejnými subjekty a vedle toho sbírají velké objemy osobních údajů o žácích a nezanedbatelný objem osobních údajů o zaměstnancích. Není tedy pochyb o tom, že se budou muset podřídit nové úpravě GDPR. [5]

1.2 Základní zásady

Některé základní povinnosti, z nichž většinu již správci a zpracovatelé osobních údajů znají, vyplývají ze zásad zpracování osobních údajů, které jsou uvedeny v článku 5 Nařízení.

Každá z těchto zásad odpovídá některé z povinností, jak je zná zákon o ochraně osobních údajů. Základní zásady jsou samy o sobě nejvýznamnějšími povinnostmi, které určují, jak může správce zpracovávat osobní údaje. Zároveň jsou však také do určité míry obecnými klauzulemi, pod které lze rozřadit většinu konkrétních povinností v Nařízení.

1.2.1 Zásada zákonnosti, korektnosti a transparentnosti

Zásada zákonnosti, korektnosti a transparentnosti vyjadřuje premisu, že ke zpracování osobních údajů musí vždy být minimálně jeden z důvodů uváděných v Nařízení. V případě, že zákonný důvod není nalezen nebo pomine, je nezbytné osobní údaje zlikvidovat. Jestliže od počátku neexistoval řádný právní důvod zpracování, jedná se o nelegální zpracování a tento nedostatek nelze zhojit bezvadným plněním ostatních povinností stanovených Nařízením. Zásada zákonnosti, tj. přítomnost právního důvodu zpracování, je tedy základním předpokladem, aby bylo možné hovořit o zpracování osobních údajů jako o zákonném. [18]

1.2.2 Zásada účelového omezení

Zásada účelového omezení vyjadřuje, že osobní údaje je možné zpracovávat pouze pro určité, výslovně vyjádřené a legitimní účely. Je tedy nepřípustné, aby správce shromáždil osobní údaje k určitému účelu a následně je on sám nebo zpracovatel zpracoval k účelu jinému, což by pravděpodobně znamenalo, že subjekt údajů zůstane bez informace o tomto novém účelu. Tímto ustanovením se současně vylučuje možnost obcházení právní úpravy a zároveň je kladen limit libovůli správců.

Je zde výrazně zohledněno základní pravidlo zpracování osobních údajů, a to že subjekt údajů je tím, kdo by měl mít plnou informaci o zpracování svých osobních údajů a v mezích možností rozhodovat, jak s jeho údaji bude naloženo. [7]

1.2.3 Zásada minimalizace údajů

Zásada minimalizace údajů odráží myšlenku, že zpracování musí být přiměřené, relevantní, omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány. Správce má povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu. Splnění této povinnosti bude tedy vyžadovat přesné vymezení minimálního rozsahu konkrétních osobních údajů, které budou v daném případě k naplnění stanoveného účelu skutečně potřebné. [7]

1.2.4 Zásada přesnosti

Zásada přesnosti znamená, že správce osobních údajů je povinen aktualizovat údaje, které zpracovává. Je-li to nezbytné, osobní údaje aktualizuje. Musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny. [1]

Dlužno dodat, že pořizování a uchovávání kopií nejrůznějších druhů osobních dokladů a jiných listin je velmi častým zjištěním Úřadu pro ochranu osobních údajů v souvislosti s výkonem dozoru dle zákona. Ačkoliv kopie sama o sobě není svým významem adekvátní originálnímu dokladu nebo dokumentu, je pořizování a uchovávání kopií osobních dokladů nebo veřejných listin považováno za zpracování osobních údajů, které by mělo stejně jako jiné druhy zpracování probíhat pouze v jeho mezích a v souladu s platným zvláštním právním předpisem. [1]

1.2.5 Zásada omezení uložení

Zásada omezení uložení zakotvuje povinnost správce vymazat nebo anonymizovat osobní údaje, které již nepotřebuje pro účel, za kterým byly shromážděny (s výjimkou pro další zpracování).

Čím vyšší je (jakékoli) riziko plynoucí z nepřesnosti některého ze zpracovávaných osobních údajů, tím větší jsou nároky na mechanismy aktualizace osobních údajů.

U zásady omezení uložení tento přístup předepisuje již samotná formulace zásady. Rovněž uzpůsobení každého zpracování zásadě korektnosti musí přihlížet k rizikům pro práva a svobody lidí. [1]

1.2.6 Zásada integrity a důvěrnosti

Zásada integrity a důvěrnosti znamená, že osobní údaje musí být zabezpečeny před hrozbami uvnitř organizace i vně organizace, a to ve všech podobách zpracování (automatizované i papírové). Tato zásada je v podstatě stanovením povinnosti údaje zabezpečit, což je základní povinností při zpracování osobních údajů. [1]

Podle článku 5 odst. 1 písm. f) Nařízení musí být osobní data zpracovávána způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“). [1]

1.2.7 Zásada odpovědnosti

Zásada odpovědnosti nakonec ukládá správci povinnost zajistit soulad se všemi výše uvedenými zásadami a být schopen tento soulad prokázat. Povinnost prokazovat soulad je přitom v Nařízení nová. Pro dodržení této povinnosti bude správce muset uchovávat důkazy ohledně všech opatření, která přijal s cílem zajistit soulad s Nařízením, jako jsou např. různá posouzení, dokumentace systémů zpracování, popisy bezpečnostních opatření, důkazy o udělených souhlasech se zpracováním či splnění informační povinnosti. Zásadu blíže rozvádí zejména čl. 24 a 25 Nařízení, projevuje se ale v mnoha konkrétních institutech Nařízení. [12]

Podle těchto ustanovení má správce povinnost zavést s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována. Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uplatňování vhodných koncepcí v oblasti ochrany údajů správcem. [12]

1.3 Základní pojmy

Základní pojmy jsou obsaženy v čl. 4 odst. 1 Nařízení GDPR. V této kapitole jsou tedy obsaženy legální definice.

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno,

identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. [9]

Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. **Chyba! Nenalezen zdroj odkazů.**

Zpracování ve smyslu Nařízení však nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky. [9]

Profilováním se rozumí jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu. [9]

Pseudonymizací je 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. [9]

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě, jelikož Nařízení vylučuje svoji působnost na údaje o zesnulých osobách. [9]

Správcem je subjekt, nerozhoduje jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv), ale může je zpracovávat i pro vlastní určené účely např. pro své oprávněné zájmy, pokud tyto zájmy nepřevyšují zájem na ochraně základních práv a svobod fyzických osob. [9]

Příjemcem je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování. [9]

Evidencí je jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska. [9]

Třetí stranou je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů. [9]

Souhlasem subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. [9]

Porušením zabezpečení osobních údajů je porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. [9]

Genetickými údaji jsou osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby. [9]

Biometrickými údaji jsou osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje. [9]

Údaji o zdravotním stavu jsou osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu. [9]

Podnikem je jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost. [9]

Závaznými podnikovými pravidly jsou koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost. [9]

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že 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. [9]

1.4 Nové přístupy

Lze hovořit o dvou nových přístupech, na kterých je Obecné nařízení založeno. Novými přístupy jsou princip odpovědnosti správce a přístup založený na riziku.

1.4.1 Princip odpovědnosti

Princip odpovědnosti znamená odpovědnost správce za dodržení zásad zpracování, které jsou uvedeny v článku 5 odst. 1 Nařízení a zároveň musí správce být schopen tento soulad doložit. K dokládání souladu budou mimo jiné sloužit kodexy, osvědčení či certifikace, případně záznamy o činnostech zpracování. [17]

S povinnostmi správce a rovněž s ústředním principem odpovědnosti správce, jak ostatně napovídá samotné označení tohoto ustanovení, úzce souvisí čl. 24 Nařízení, dle jehož odst. 1 „s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.“ [9]

Z citovaného ustanovení je zřejmé, že povinností správce bude nejprve náležitě posoudit konkrétní a specifické okolnosti zpracování konkrétních osobních údajů a současně zvážit rizika tohoto zpracování pro základní práva a svobody subjektu údajů.

V návaznosti na takto provedenou důkladnou analýzu pak správce zavede vhodná technická i organizační opatření, jejichž cílem je zajištění zpracování osobních údajů v souladu s GDPR. Správce je současně povinen doložit soulad zpracování osobních údajů

s GDPR, přičemž tento bude dokládán zejména adekvátní dokumentací vyhotovenou pro příslušný účel a vytvořením koncepce na ochranu osobních údajů. Obecné nařízení nepředkládá konkrétní vodítko pro obsah dokumentace, ovšem lze usuzovat na to, že jejím obsahem by mělo být především vyhodnocení rizik pro základní práva a svobody subjektů údajů, doložení právního titulu pro zpracování osobních údajů, způsob řešení žádostí subjektů údajů k uplatnění jejich práv, konkretizace technických a organizačních opatření sloužících k zajištění souladu zpracování osobních údajů s GDPR atd. [17]

1.4.2 Přístup založený na riziku

Nařízení se vyznačuje přístupem založeným na riziku. V důsledku toho jsou některé povinnosti správce vázány pouze na riziková či vysoce riziková zpracování, tudíž bude záviset na okolnostech konkrétního zpracování, zda bude muset některé povinnosti plnit či nikoliv. [8]

Přístup založený na riziku v širším slova smyslu znamená, že správce je již od počátku zpracování osobních údajů povinen respektovat povahu, rozsah, účel zpracování a dbát možných rizik zásahu do chráněných subjektivních práv fyzických osob. Nařízení v tomto ohledu stanoví, že s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření. [8]

Znamená to, že v prvé řadě je nezbytností vyhodnotit rizika, následně pak rizika posoudit a rozhodnout o přijetí opatření ke snížení a eliminaci rizika nebo riziko přijmout. Pro riziko existuje celá řada definic. Riziko je nejčastěji definováno jako součin velikosti následků nežádoucí události a pravděpodobnosti, že k uvedené nežádoucí události dojde. Analýzu rizik je možné zpracovat ve vztahu k základním právům a svobodám subjektu údajů, kterými jsou např.: ochrana identity, právo na informace, právo na ochranu osobních údajů, právo na duševní a tělesnou integritu, právo na soukromí atd. [3]

1.5 Nové povinnosti

Novou povinností správce je jeho odpovědnost za soulad zpracování osobních údajů se zásadami zpracování a schopnost tento soulad prokázat. K tomu jim mají napomáhat mimo jiné i kodexy, osvědčení (pečetě, známky) a záznamy o činnostech zpracování. Kodexy mají správcům, zejména na sektorové úrovni, sloužit jako vodítko správné praxe při zpracování

osobních údajů právě s ohledem na specifičnost daného sektoru (např. bankovnictví, telekomunikace, internetové obchody, zdravotnictví). Osvědčení má sloužit k prokázání souladu zpracování s Obecným nařízením. Záznamy o činnostech zpracování obsahují informace o prováděném zpracování, což správci umožní lehčí orientaci ohledně zpracování, která provádí. Tato povinnost je stanovena v článku 30 Obecného nařízení, přičemž někteří správci jsou vyňati z nutnosti vést záznamy o činnostech zpracování. Dokládání souladu zpracování však nelze omezit pouze na shora uvedené možnosti, ale dokládání souladu je komplexní činnost, zahrnující dílčí činnosti, mezi které lze zařadit nejen shora uvedené kodexy, osvědčení a záznamy o činnostech zpracování, ale například i zveřejňování informací, které Obecné nařízení ukládá správci zveřejňovat, vyhotovením vnitřních předpisů až po řádnou spolupráci s příslušným dozorovým úřadem. [10]

Je nutné zdůraznit, že základní zásady, principy a klíčové instrumenty zůstávají de facto neměnné, resp. byly detailněji pouze rozpracovány a zpřesněny (např. nutnost disponovat pro zpracování právním důvodem, zabezpečení osobních údajů, transparentnost vůči subjektu údajů atd.). Obecné nařízení na těchto základech přináší nástavbu spočívající v dodatečných nových povinnostech, které pro české správce budou nové. Jde zejména o tyto nové povinnosti:

- povinnost vést záznamy o činnostech zpracování;
- posouzení vlivu na ochranu osobních údajů;
- předchozí konzultace s Úřadem pro ochranu osobních údajů;
- ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů, a oznamování případu porušení zabezpečení osobních údajů subjektu údajů;
- ustavení pověřence pro ochranu osobních údajů. [11]

Kromě povinnosti vést záznamy o činnostech zpracování a ustanovit pověřence, jsou ostatní nové povinnosti založeny na přístupu založeném na riziku, tj. jejich uplatnění je vázáno na přítomnost rizika či vysokého rizika pro práva a svobody subjektu údajů. Avšak byť u povinnosti ustanovit pověřence není přímo pracováno s pojmy riziko či vysoké riziko, odráží se v této povinnosti do určité míry též přístup založený na riziku, jelikož pro určitá zpracování, resp. určité subjekty, je povinností ustanovit pověřence pro ochranu osobních údajů. [11]

1.5.1 Povinnost vést záznamy o činnostech zpracování

Povinnost vést záznamy o činnostech zpracování je novou povinností, která částečně nahrazuje zrušenou oznamovací povinnost (§ 16 zákona o ochraně osobních údajů). Jedná se v podstatě o podrobný popis zpracování, které probíhá u jednotlivých správců a zpracovatelů. Tento popis umožní získat dokonalý přehled správci, ale i dozorovému úřadu. Nařízení stanoví přesný obsah těchto záznamů. Z této povinnosti existuje výjimka, jejíž výklad není zcela jasný. Povinnost vytvořit záznamy o činnostech se netýká podniku nebo organizace zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. [7]

Není nutné zaznamenávat každé jednotlivé zpracování osobních údajů konkrétního člověka. Jinými slovy, správce má záznam o činnostech zpracování nazvaný „personální agenda", v němž je obecně popsáno, se kterými údaji zaměstnanců se pro tento účel pracuje. Při přijetí nového zaměstnance se nový záznam o činnostech zpracování připravovat nebude, nicméně by správce osobních údajů měl postupovat v souladu se záznamem o činnostech zpracování. Záznam o činnostech zpracování je jakousi náhradou za oznamovací povinnost vůči Úřadu pro ochranu osobních údajů, která byla Nařízením zrušena. Záznamy je nutné na žádost zpřístupnit Úřadu pro ochranu osobních údajů. Záznam totiž primárně slouží ÚOOÚ jako vodítko k tomu, aby se zorientoval v tom, jak v dané organizaci probíhá zpracování osobních údajů. ÚOOÚ bude také posuzovat, zda faktické zpracování v organizaci probíhá tak, jak je popsáno v záznamech o činnostech zpracování. Záznamy o činnostech zpracování je nutné vést písemně, přičemž za písemnou podobu se považují i záznamy vedené v elektronické podobě. Záleží tedy na správci osobních údajů, zda se rozhodne tyto záznamy mít uložené elektronicky nebo je mít vytištěné a založené v pořadači. [4]

1.5.2 Posouzení vlivu na ochranu osobních údajů

Co se týče posouzení vlivu na ochranu osobních údajů (tzv. „DPIA“), pak ve smyslu ustanovení článku 35 a recitálů 89 a 90 je nutné provádět toto posouzení pouze za předpokladu, že se jedná o zavádění nového zpracování či při jeho podstatné změně či zavádění nových technologií. Dle výkladového stanoviska pracovní skupiny WP 29 je však toto posouzení doporučeno i tam, kde započalo zpracování před účinností Nařízení, a to zejména v případě, kdy je zpracování vysoce rizikovým; v tomto stanovisku jsou i výslovně jako příklad uvedeny nemocnice a jejich informační systémy. Na straně druhé

je v současné době v legislativním procesu nový zákon na ochranu osobních údajů (tzv. adaptační zákon) v gesci Ministerstva vnitra, kdy je navrhováno, že posouzení vlivu na ochranu osobních údajů není potřeba dělat, pokud je zpracování stanoveno právním předpisem. [2]

DPIA je důležitým nástrojem pro eliminaci odpovědnosti, neboť pomáhá správcům nejen splňovat požadavky Nařízení, ale také prokazuje, že byla přijata vhodná opatření k zajištění souladu s Nařízením.

Posouzení by mělo obsahovat alespoň 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 a plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s nařízením. [2]

1.5.3 Konzultace s Úřadem pro ochranu osobních údajů

Stejně jako jmenování pověřence není ani posouzení vlivu na ochranu osobních údajů a předchozí konzultace s Úřadem pro ochranu osobních údajů povinností obecně platnou, týká se těch, kdo hodlají provádět s osobními údaji rozsáhlé rizikové operace, spočívající například v rozsáhlém profilování lidí prostřednictvím internetu, při kterém jsou pro marketingové účely získávány podrobné informace o jejich soukromém životě, nebo rizikovost spočívá ve využití nových technologií používaných, např. na velké množství údajů o zdravotním stavu pacientů. Seznam těchto operací bude Úřadem pro ochranu osobních údajů zveřejněn. [6]

Institut konzultace s Úřadem pro ochranu osobních údajů slouží k zesílení ochrany osobních údajů a k minimalizaci pravděpodobnosti zásahu do práv subjektů údajů, v pochybnostech o závažnosti rizika se proto doporučuje z preventivních důvodů vždy ke konzultaci s Úřadem pro ochranu osobních údajů přistoupit. Úřad pro ochranu osobních údajů bude dále v této věci postupovat v souladu s čl. 36 odst. 2 Nařízení, a to ve stanovených lhůtách. [6]

1.5.4 Ohlašování případu porušení zabezpečení osobních údajů

Podle čl. 33 odst. 1 Nařízení má správce povinnost ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu. Porušením zabezpečení osobních údajů (dále jen „porušení zabezpečení“) se rozumí porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Ohlášení je správce

povinen provést bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Ohlášení správce není povinen provádět, pokud je nepravděpodobné, že by porušení mělo za následek riziko pro práva a svobody fyzických osob, vždy je však povinen porušení zabezpečení zdokumentovat. [2]

Stejnou povinnost má zpracovatel vůči správci a takové ohlášení musí obsahovat přinejmenším popis povahy daného případu porušení zabezpečení osobních údajů včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů, jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, popis pravděpodobných důsledků porušení zabezpečení, popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení, včetně případných opatření ke zmírnění možných nepříznivých dopadů. Správce má navíc povinnost veškeré případy porušení zabezpečení, skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření dokumentovat. [2]

1.5.5 Ustavení pověřence pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů je institut přejatý z německého práva, kde funguje již od roku 2009. Zjednodušeně se jedná o poradce organizace v oblasti ochrany osobních údajů. Pověřenec má na starosti poskytovat informace a poradenství správcům osobních údajů (tedy školám) a monitorovat soulad s GDPR. Další jeho povinností je spolupracovat s Úřadem pro ochranu osobních údajů a zároveň pro tento úřad působit jako kontaktní místo. Nicméně pověřenec není odpovědný za dodržování GDPR a jiných předpisů, odpovědným subjektem zůstává vždy správce. [16]

Subjekty, které musejí jmenovat pověřence pro ochranu osobních údajů, jsou definovány v čl. 37 odst. 1 GDPR. Jedná se o (i) orgány veřejné moci či veřejné subjekty s výjimkou soudů jednajících v rámci svých soudních pravomocí, (ii) subjekty, jejichž hlavní činnost spočívá v takovém zpracování osobních údajů, jež vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů, nebo (iii) subjekty, jejichž hlavní činnost spočívá v rozsáhlém zpracování citlivých údajů a osobních údajů týkajících se rozsudků v trestních věcech. Pověřenec nemusí mít žádné formální vzdělání. Nicméně existují faktory, které by měl ředitel při výběru pověřence vzít v potaz: znalosti práva a praxe v oblasti ochrany osobních údajů, znalost IT a bezpečnosti dat a znalost procesů v dané organizaci. [16]

2 DOTAZNÍKOVÉ ŠETŘENÍ

Cílem této části práce je zhodnotit pozitivní a negativní důsledky zavádění GDPR v obcích regionu (kraje). Práce popisuje, jaké změny a povinnosti pro obce GDPR přináší, jaký má vliv na informační systémy v obcích, jak je celý proces řešen a jak zatěžuje rozpočty obcí.

Tohoto cíle je dosaženo mimo jiné také za pomoci vyhodnocení šetření. Analýza byla vytvořená z dat získaných od respondentů za pomoci dotazníkového šetření.

2.1 Cíl šetření

Účelem výzkumu je analyzovat získaná data z dotazníkového šetření, a následně poskytnout takové odpovědi, které by naplnily cíl praktické části práce, tj. vyhodnotit, zhodnotit pozitivní a negativní důsledky zavádění GDPR v obcích regionu.

2.2 Metodika šetření

V analytické části práce budou popsány metody šetření, kterými zhodnotíme důsledky zavádění GDPR v obcích.

2.2.1 Techniky sběru dat

Jak bylo naznačeno výše, sběr dat byl proveden za pomoci dotazníkového šetření (Příloha A). Tato metoda je jednou z nejčastěji používaných metod získávání dat. Je obzvláště vhodná k použití ke zkoumání názorů, postojů a řešení v rámci zavádění nových organizačních změn, kterými GDPR na úrovni obcí beze sporu jsou.

Pomocí dotazníkového šetření byla provedena analýza zvoleného vzorku respondentů, splňujícího předem stanovená kritéria, přičemž každý z dotazovaných měl povinnost vyplnit dotazník samostatně.

2.2.2 Popis zúčastněného vzorku respondentů

Celkem bylo osloveno 10 respondentů. Veškeří respondenti budou nadále charakterizováni jako právnické osoby (obce), přestože fyzicky dotazníky vyplňovaly statutární orgány (starostové) či jiní jimi pověření zaměstnanci.

Respondenti mají společné to, že jsou obcemi z Pardubického kraje, konkrétně pak z okresu Pardubice. Jedná se o obce menšího rozsahu. Bylo pamatováno na skutečnost, že skupina vybraných respondentů musí být nutně konfrontována s vybraným problémem.

V následující tabulce je výčet oslovených obcí s počtem obyvatel.

Tabulka 1 – Seznam dotazovaných obcí

Obec	Počet obyvatel
Břehy	1010
Dříteč	445
Horní Ředice	1043
Hrobice	212
Kunětice	318
Němčice	606
Ráby	549
Rokytno	882
Staré Hradiště	1829
Starý Mateřov	599

Zdroj: vlastní zpracování

2.2.3 Dotazník

Dotazník zahrnuje 8 otázek. Jejich řazení bylo sestaveno od jednodušších po složitější a zároveň tak, aby postupně směřovalo od obecných otázek ke specializovanějším. Byl koncipován tak, aby začínal zajímavými a jednoduchými otázkami, na které respondent snadno nalezne odpověď a postupem času se nad dalšími otázkami musel hlouběji zamyslet.

Aby byla zajištěna dostatečná vypovídací hodnota vytěžených dat, byl dotazník rozvržen tak, aby respondentům kladl jednak standardizované otázky (a nabízel standardizované odpovědi) a jednak i otevřené otázky, které umožnily respondentům se blíže vyjádřit. Dotazník tak má jakožto celek polostrukturovaný charakter. Převažují otázky dichotomické, případně polytomické.

První otázka se dotazovala respondentů, jakým způsobem bude obec jmenovat pověřence pro ochranu osobních údajů. Jako odpověď byly na výběr stavěny čtyři možnosti:

a) Obec jej bude zaměstnávat pro svou výlučnou potřebu;
b) Obec bude využívat služby nezávislého profesionála (outsourcing);
c) Pověřenec bude vykonávat svou pravomoc na úrovni svazku obcí, jíž je obec členem;
d) Jinak – uveďte jak.

Druhá otázka zjišťovala, zda mají oslovení představu, v jaké míře bude zavedení GDPR znamenat zátěž pro obecní rozpočet. Na výběr byly dány dvě odpovědi:

a) Ano – uveďte odhadnuté roční náklady;
b) Ne.

Třetí otázka dotazníku zkoumala, zda obec zavedla či bude zavádět v souvislosti s GDPR nové informační systémy. Jako odpověď byly na výběr dány dvě možnosti:

a) Ano – uveďte jaké (název, účel);
b) Ne.

Čtvrtá otázka se dotazovala, zda obec zavedla či bude zavádět v souvislosti s GDPR jiné nová technická a organizační opatření. Jako odpověď byly na výběr dány dvě možnosti:

a) Ano – uveďte jaká (název, účel);
b) Ne.

Pátá otázka zjišťovala, jak dlouho se obec organizačně připravovala na nabytí účinnosti GDPR. Jako odpověď byly na výběr dány čtyři možnosti:

a) Dva roky;
b) Rok;
c) Méně než rok;
d) Vůbec.

Šestá otázka zkoumala, jak bude obec provádět posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, pokud určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Jako odpověď byly na výběr dány čtyři možnosti:

a) Prostřednictvím pověřence pro ochranu osobních údajů;
b) Vlastními silami;
c) Nebudeme provádět;
d) Zatím nemáme představu, budeme řešit, až nastane tato potřeba.

Sedmá otázka dotazníku se dotazovala respondentů, jaké prvky zabezpečení používá obec v souvislosti s ochranou osobních údajů? Jako odpověď bylo na výběr dáno pět možností:

a) Uzamykatelné dveře a skříně;
b) Alarm;
c) Střežení bezpečnostní agenturou / dozorčím / strážníky obecní policie;
d) Silné heslo v PC, kde jsou soustředěny databáze osobních údajů;
e) Jiné – uveďte jaké.

Osmá se zaměřovala na otázku, zda obec prováděla tzv. analýzu GDPR (inventarizace a identifikace rizik za účelem jejich budoucí minimalizace), případně s jakým výsledkem. Jako odpověď byly na výběr dány čtyři možnosti:

a) Ano – rizika byla shledána žádná či minimální;
b) Ano – rizika byla shledána závažná, nepřijali jsme však zatím žádná opatření;
c) Ano – rizika byla shledána závažná, přijali jsme opatření – uveďte jaká;
d) Neprováděla.

2.2.4 Organizace sběru dat

Samotnému dotazníkovému šetření předcházela tzv. testovací fáze, v jejímž rámci testoval tazatel jednotlivé otázky z dotazníku na náhodně vybraných osobách, přičemž si tím ověřoval jednak to, zda jsou otázky dostatečně srozumitelné a jednak sbíral zpětnou vazbu od takto testovaného vzorku cvičných respondentů, zda oni považují otázky za přínosné vzhledem ke stanoveným cílům práce.

Respondenti byli dopředu vybráni z blízkého okolí města Pardubic, byli typizováni podle požadovaného počtu obyvatel, přičemž toto stanovené kritérium mělo rozpětí 200 až 2000 obyvatel. Následně byli respondenti kontaktováni, zda jsou ochotni se dotazníku zúčastnit.

Dotazník byl některým respondentům distribuován elektronickou poštou (email). Vzhledem k nevelké návratnosti dotazníků byli další respondenti kontaktováni osobně. Vyplnění dotazníků při osobní návštěvě proběhlo stoprocentně.

2.2.5 Metody zpracování získaných dat

Shromážděná data byla vyhodnocována pomocí vybraných metod statistické analýzy, konkrétně vybranými charakteristikami popisné statistiky.

Aritmetický průměr je statistická veličina, která v jistém smyslu vyjadřuje typickou hodnotu popisující soubor mnoha hodnot. rozpočtu obcí.

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i n_i \qquad (1)$$

kde: n je rozsah výběru.

Výběrový rozptyl je nazýván střední kvadratickou odchylkou a je používán ve statistice. Ukazuje, jak jsou hodnoty ve statistickém soubory rozptýleny.

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2 n_i \qquad (2)$$

kde: n je rozsah výběru;

$\bar{x}$ aritmetický průměr.

Směrodatná odchylka, analogicky jako rozptyl, určuje, jak se hodnoty rozptylují či odchylují od průměru hodnot. Rovná se odmocnině z rozptylu. Vypovídá o tom, nakolik se od sebe navzájem typicky liší jednotlivé případy v souboru zkoumaných hodnot.

Medián rozděluje řadu vzestupně seřazených výsledků na dvě stejně početné poloviny. Jeho hodnota se nalézá uprostřed seznamu.

Modus je hodnota, která se v daném souboru vyskytuje nejčastěji (největší relativní četnost). [13]

Aplikovat statistické metody a postupy znamená zaznamenávat data o jevech a zpracovávat je, tj. třídit, vyhodnocovat a interpretovat. Statistika informaci z dat získává a převádí ji do srozumitelné formy. Úkolem uživatele statistické analýzy je informaci poté správně interpretovat, převést na znalost a případně na základě této znalosti jednat. Kvalitní statistická analýza se nepokouší informaci z dat získat pouze přesně a úplně, ale snaží se ji převést do takové podoby, aby ji uživatel mohl pochopit a aby mu byla užitečná. K tomu slouží celá škála statistických metod od nejjednodušších popisných statistik až po komplexní modely vícerozměrné statistické analýzy. Důležitou součástí analýzy jsou grafy pro přehledné zobrazení jak základních vztahů v datech, tak i výsledků modelování. [13]

Ve fázi analýzy je použita popisná statistika. V ní dochází ke kvantifikaci získaných dat pomocí absolutních i relativních četností a následnému grafickému znázornění za pomoci výsečových grafů. Z výsledků popisné analýzy lze hledat mezi proměnnými různé vztahy a kauzality. Kruhový diagram nebo výsečový graf je způsob grafického znázornění struktury sledovaného souboru. Plocha kruhu představuje celý soubor, který je rozdělený do jednotlivých výsečí.

Kromě popisné statistiky jsou data zpracována i za pomoci analýzy závislosti. Zatímco obecně lze říct, že v rámci analýzy závislostí jsou předmětem zkoumání závislosti (souvislosti) mezi dvěma a více jevy a jedná se o proniknutí do vztahů mezi sledovanými jevy a tím i přiblížení k tzv. příčinným, tj. kauzálním souvislostem, cílem analýzy rozptylu

je rozhodnout, zda pozorovaná data hovoří ve prospěch hypotézy o nezávislosti, či zda lze s vysokou spolehlivostí tvrdit, že znak X ovlivňuje znak Y. V analýze rozptylu nám tedy jde o zjištění, zda mezi proměnnými X a Y existuje nějaká závislost, a případně jakou těsnost tato závislost vykazuje. [15]

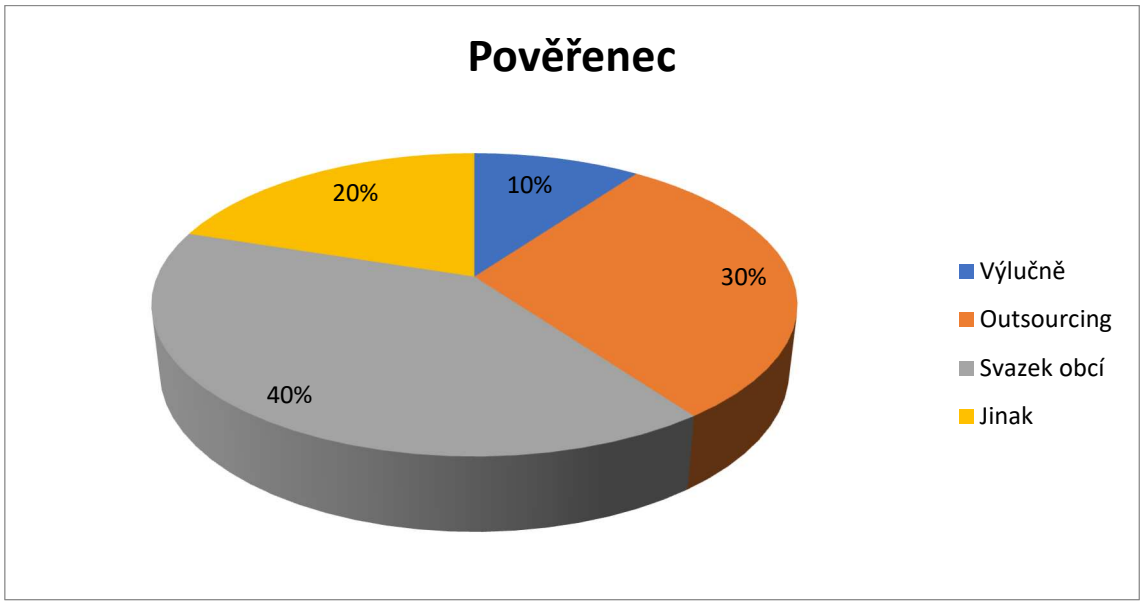
2.3 Výsledky – statistická analýza

Otázka č. 1:

Jakým způsobem bude vaše obec jmenovat/jmenovala pověřence pro ochranu osobních údajů?

Odpovědi:

- Obec jej bude zaměstnávat pro svou výlučnou potřebu – 1 (10%);
- Obec bude využívat služby nezávislého profesionála (outsourcing) – 3 (30%);
- Pověřenec bude vykonávat svou pravomoc na úrovni svazku obcí, jíž je obec členem – 4 (40%);
- Jinak – 2 (20%).



Obrázek 1 – Graf rozložení odpovědí na otázku č. 1

Zdroj: vlastní zpracování

Poznámka: U odpovědi „Jinak“ uvedly dvě obce, že hodlají využívat služby společnosti SHS služby s.r.o. Veškeré kategorie odpovědí, které respondenti uvedli, jsou v souladu

se zásadami GDPR. Nejvíce odpovědí (40 %) bylo zaznamenáno u možnosti „Pověřenec bude vykonávat svou pravomoc na úrovni svazku obcí, jíž je obec členem“.

Otázka č. 2:

Máte představu, v jaké míře bude zavedení GDPR znamenat zátěž pro obecní rozpočet?

Odpovědi:

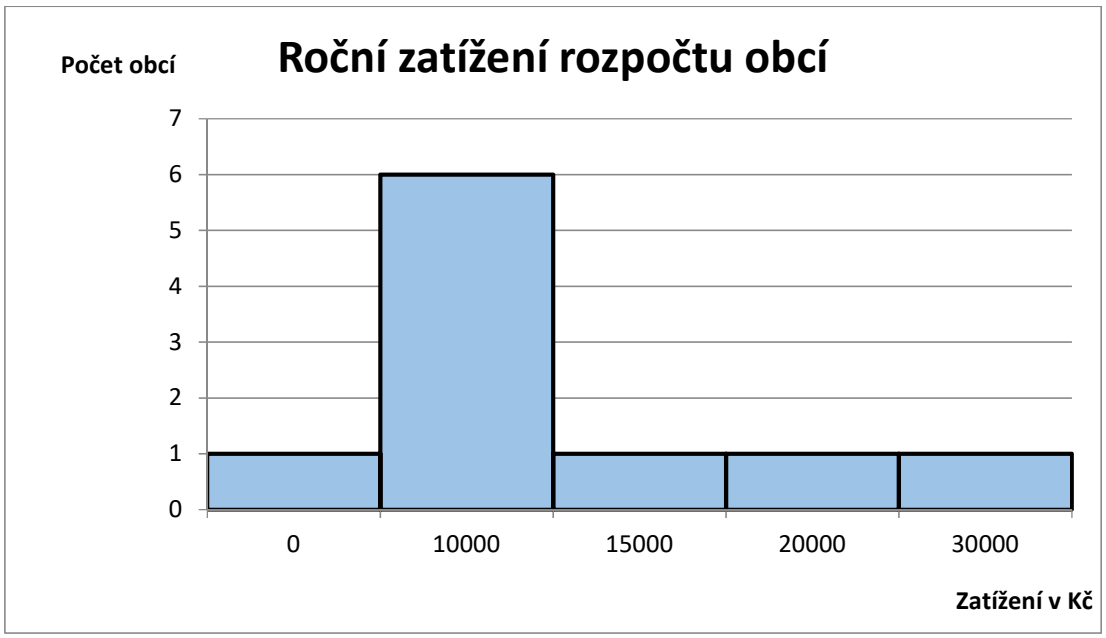
- Ano (30 000 Kč) – 1 (10%);
- Ano (20 000 Kč) – 1 (10%);
- Ano (15 000 Kč) – 1 (10%);
- Ano (10 000) – 6 (60%);
- Ne – 1 (10%).

Tabulka 2 – Rozdělení četností ročních nákladů

Roční náklady (v Kč)	Absolutní četnost	Relativní četnost	Kumulativní absolutní četnost	Kumulativní relativní četnost
0	1	0,1	1	0,1
10000	6	0,6	7	0,7
15000	1	0,1	8	0,8
20000	1	0,1	9	0,9
30000	1	0,1	10	1

Zdroj: vlastní zpracování

Poznámka: Rozpočet jedné obce zatěžuje GDPR nulovými náklady. Zcela převažují odpovědi v kategorii 10 000 Kč. Samotná tato skutečnost napovídá, že obce nebyly ochotny investovat do komplexnějšího či náročnějšího systému (včetně informačního systému) ochrany osobních údajů – což odpovídá také skutečnostem, uvedeným v rámci odpovědí na otázku č. 3. Zásady GDPR nepředepisují žádné povinnosti ohledně objemu financí, které by subjekty byly povinny investovat do (lepšího) zabezpečení. Do jakých oblastí obce investovaly, napovídají odpovědi na otázky č. 4 a případně i č. 7 výzkumu.



Obrázek 2 – Histogram ročního zatížení rozpočtu obcí

Zdroj: vlastní zpracování

Tabulka níže (Tabulka 3) znázorňuje výsledky základních charakteristik ročního zatížení rozpočtu obcí. Aritmetický průměr byl spočítán pomocí vzorce (1).

Dotázané obce jsou v průměru zatížené částkou 12 500 Kč ročně.

Pro výběrový rozptyl byl použit vzorec (2) a směrodatná odchylka je odmocninou z rozptylu.

Všechny výsledky jsou zobrazeny v tabulce 3. Roční zatížení 10 000 Kč ročně je prostřední i nejčastější hodnotou.

Tabulka 3 – Vybrané charakteristiky ročního zatížení rozpočtu obcí

Průměr	12 500,00 Kč
Rozptyl	62 500 000,00 Kč
směrodatná odchylka	7 905,69 Kč
Medián	10 000,00 Kč
Modus	10 000,00 Kč

Zdroj: vlastní zpracování

Otázka č. 3:

Zavedla/bude zavádět obec v souvislosti s GDPR nové informační systémy?

Odpovědi:

- Ne – 10 (100%);
- Ano – 0 (0%).

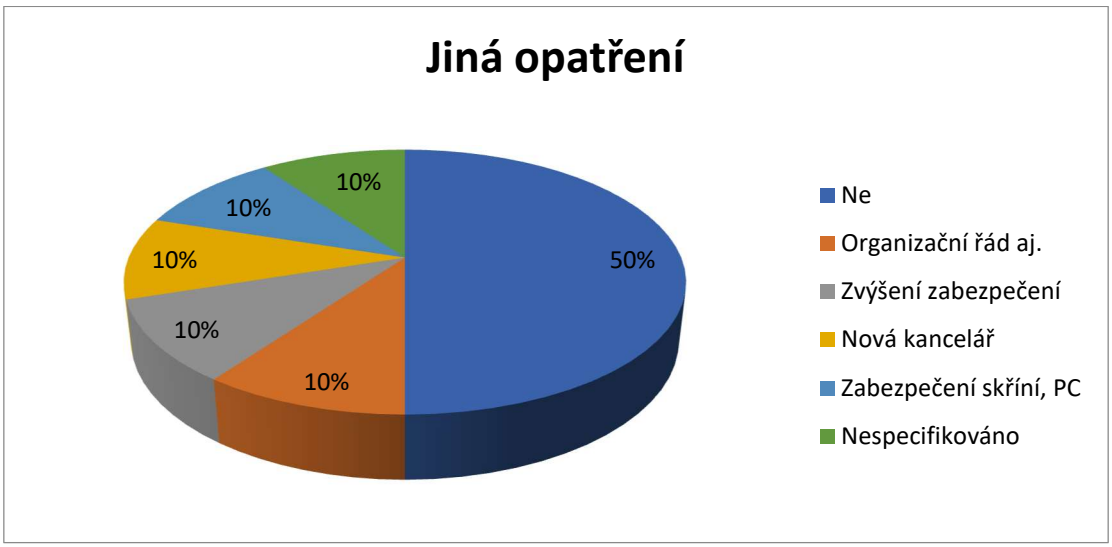
Poznámka: Vnímání zavádění nových informačních systémů (či obecně technologií), které by napomohly větší bezpečnosti osobních údajů v databázích obcí, jakožto zbytných věcí, může nasvědčovat nízké prioritě, kterou starostové ochraně osobních údajů přikládají. Ještě spíše tato skutečnost nasvědčuje omezeným možnostem obecních rozpočtů, které si nemohou dovolit vynakládat výdaje na nový informační systém spojený s každou agendou, které jsou obce povinny se věnovat. Zásady GDPR nepředepisují povinnost střežit kyberneticky uchovávané osobní údaje za pomoci specializovaných informačních systémů, tudíž lze mít za to, že respondenti zde žádné své povinnosti neporušují. Odkazuje se zde skutečnosti uvedené u otázky č. 4 výzkumu.

Otázka č. 4:

Zavedla/bude zavádět obec kromě informačních systémů v souvislosti s GDPR jiná nová technická a organizační opatření?

Odpovědi:

- Ne – 5 (50%);
- Ano – nový Organizační řád, nový Provozní řád výpočetní techniky, Seznam osob s přístupem k osobním datům, pravidelné změny hesel na PC – 1 (10%);
- Ano – zvýšení zabezpečení ochrany osobních údajů – 1 (10%);
- Ano – nová kancelář, zabezpečení dokumentů – 1 (10%);
- Ano – zabezpečení skříní, PC – 1 (10%);
- Ano – nespecifikováno – 1 (10%).



Obrázek 3 – Graf rozložení odpovědí na otázku č. 4

Zdroj: vlastní zpracování

Poznámka: Výsledky tohoto šetření jsou zajímavé s odkazem na odpovědi na otázku č. 3 výzkumu (viz také odpovědi na otázku č. 7). Souhrn výpovědí totiž napovídá tomu, že ač nebudou v obcích zaváděny nové informační systémy, přesto hodlají některé obce přistoupit k lepšímu zabezpečení dat shromažďovaných za pomoci výpočetní techniky. Odpověď „Ne" nevypovídá nic o tom, zda považují obce své dostatečné zabezpečení za dostatečné, či zda respondenti nechtějí v tomto směru investovat.

Otázka č. 5:

Jak dlouho se vaše obec organizačně připravovala na nabytí účinnosti GDPR?

Odpovědi:

- Dva roky – 0 (0%);
- Rok – 0 (0%);
- Méně než rok – 10 (100%);
- Vůbec – 0 (0%).

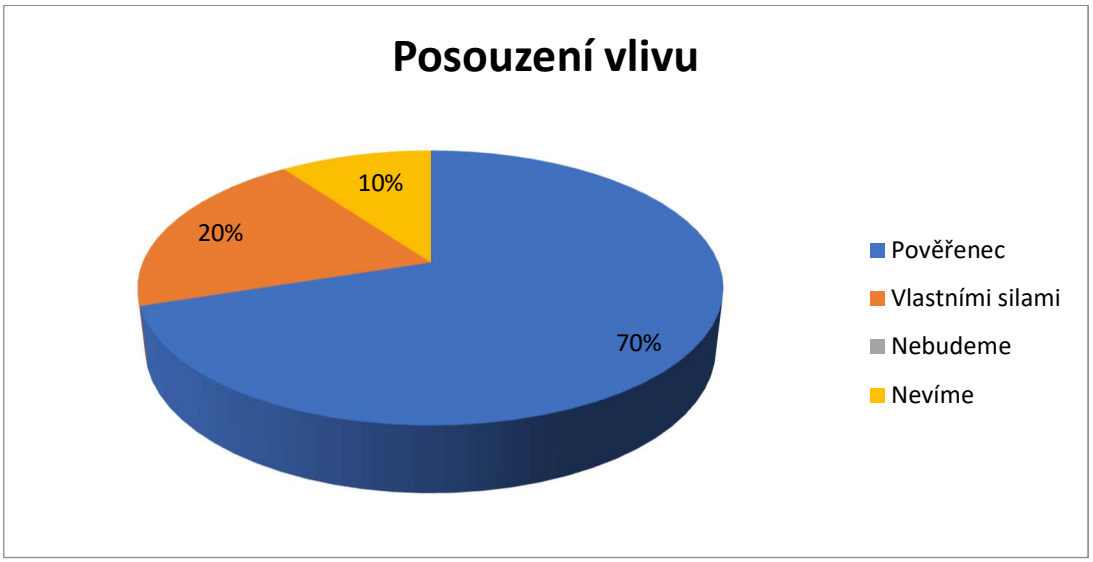
Poznámka: Skutečnost, že všichni dotázaní respondenti věnovali problematice GDPR méně než rok, může znamenat alarmující fakt, že se obce nepřipravují na přechod na novou podobu ochrany osobních údajů dostatečně svědomitě. Lze tak usuzovat s poukazem na názory předních odborníků na ochranu osobních údajů, podle kterých je 1 rok nedostatečně dlouhá doba přípravy. [12] Tato skutečnost ovšem oficiálně není v rozporu se zásadami GDPR.

Otázka č. 6:

Jak budete provádět posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, pokud určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob?

Odpovědi:

- Prostřednictvím pověřence pro ochranu osobních údajů – 7 (70%);
- Vlastními silami – 2 (20%);
- Nebudeme provádět – 0 (0%);
- Zatím nemáme představu, budeme řešit, až nastane tato potřeba – 1 (10%).



Obrázek 4 – Graf rozložení odpovědí na otázku č. 6

Zdroj: vlastní zpracování

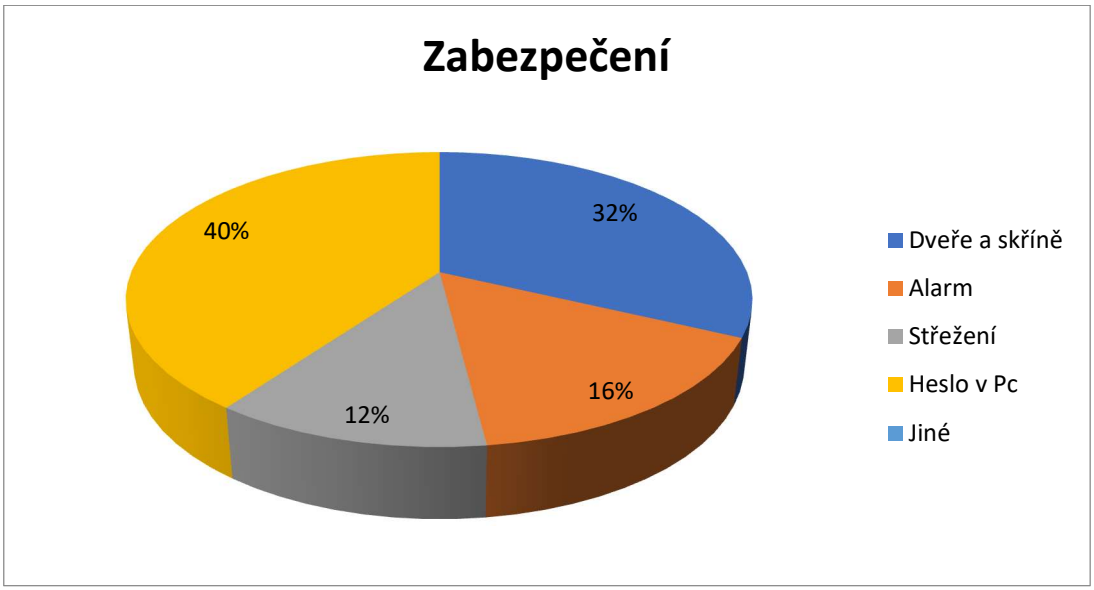
Poznámka: Posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů je natolik specifickým a specializovaným postupem, že je možno se podivit nad skutečností, že představitelé malých obcí se hodlají pokoušet do takovýchto operací vlastními silami. Pokud to zvládnou, není jejich volba v rozporu se zásadami GDPR.

Otázka č. 7:

Jaké prvky zabezpečení používá vaše obec v souvislosti s ochranou osobních údajů? (je možno uvést více odpovědí)

Odpovědi:

- Uzamykatelné dveře a skříně – 8 (32%);
- Alarm – 4 (16%);
- Střežení bezpečnostní agenturou / dozorčím / strážníky obecní policie – 3 (12%);
- Silné heslo v PC, kde jsou soustředěny databáze osobních údajů – 10 (40%);
- Jiné – uveďte jaké – 0 (0%).



Obrázek 5 – Graf rozložení odpovědí na otázku č. 7

Zdroj: vlastní zpracování

Poznámka: Díky komplexnímu spektru odpovědí na tuto otázku si lze utvořit představu, že obce přistupují k ochraně osobních údajů poměrně zodpovědně, neboť prvky zabezpečení osobních údajů v uspokojivé míře kombinují a nespoléhají se pouze na jedinou úroveň ochrany. Za poměrně efektivní lze považovat kombinaci fyzické, osobní a kybernetické ochrany. Ohledně uvedených odpovědí nic nenapovídá skutečnosti, že by obce v této záležitosti postupovaly v rozporu se zásadami GDPR

Kombinace prvků zabezpečení byly u jednotlivých obcí kombinovány v pozoruhodných variacích. Všechny obce mají zabezpečeny PC. Pouhých osm obcí uvedlo, že má data zabezpečena pomocí uzamykatelných dveří a skříní, byť se dá logicky předpokládat, že minimálně uzamykatelnou kanceláří disponují veškeré objekty (kanceláře), kde jsou data

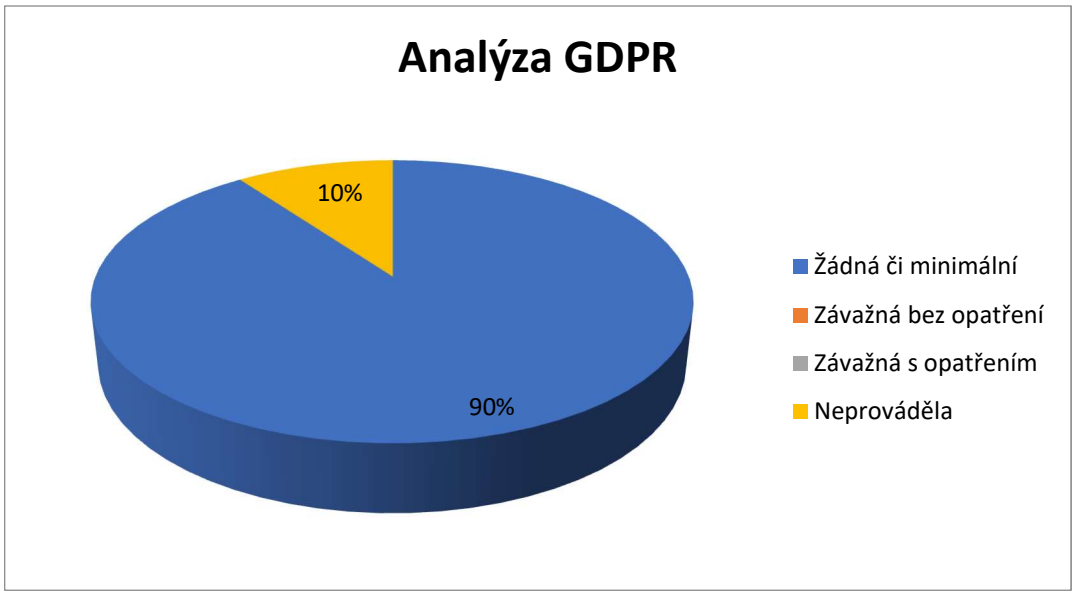
osobních údajů uložena. Mezi respondenty jsou dva případy, kdy obce zabezpečují osobní údaje pouze prostřednictvím zabezpečených PC; takové zabezpečení by bylo nutno zřejmě vyhodnotit jako nedostatečné. Oproti tomu jen jediná obec používá všechny čtyři (dotazníkem nabízené) možnosti zabezpečení. Pět obcí používá tři složky zabezpečení, a dvě obce používají pouze dvě složky zabezpečení. Je nezodpovězenou otázkou, proč obce neuvedly žádné další prvky zabezpečení (otevřená odpověď), když se nabízí například možnosti střežení za pomoci bezpečnostních kamer či za pomoci elektronické požární signalizace.

Otázka č. 8:

Prováděla vaše obec tzv. analýzu GDPR (inventarizace a identifikace rizik za účelem jejich budoucí minimalizace)? S jakým výsledkem?

Odpovědi:

- Ano – rizika byla shledána žádná či minimální – 9 (90%);
- Ano – rizika byla shledána závažná, nepřijali jsme však zatím žádná opatření – 0 (0%);
- Ano – rizika byla shledána závažná, přijali jsme opatření – uveďte jaká – 0 (0%);
- Neprováděla – 1 (10%).



Obrázek 6 – Graf rozložení odpovědí na otázku č. 8

Zdroj: vlastní zpracování

Poznámka: Ve faktu, že jedna z obcí vůbec neprováděla analýzu GDPR, lze sledovat rozpor se zásadami GDPR. Tato otázka č. 8 by si zasloužila další šetření s otázkou: za jakých

podmínek, jakými prizmaty jakými nástroji byla prováděna předmětná inventarizace a identifikace rizik za účelem jejich budoucí minimalizace? Výstupy z odpovědí na předmětnou otázku by mohly napomoct posoudit, zda byla analýza dostatečná či nikoliv.

2.4 Výsledky – analýza závislostí

Analýza závislosti by měla pomoci ověřit hypotézu: čím má obec více obyvatel (přihlášených k trvalému pobytu), tím lépe je obcí zajištěna ochrana osobních údajů (kvalita zabezpečení je poměřována počtem prvků ochrany, které obec k ochraně osobních údajů zajišťuje, tj. více prvků ochrany = lepší ochrana). Hypotéza vychází z předpokladu, že větší obec disponuje lepšími kapacitami a většími materiálními prostředky, ale musí také spravovat větší objem osobních údajů.

Na základě výstupů z výzkumu byla provedena analýza, konkrétně pak za pomocí výsledků šetření – odpovědí na otázku č. 7: „Jaké prvky zabezpečení používá vaše obec v souvislosti s ochranou osobních údajů?“

Tabulka 4 – Počet prvků ochrany

Jméno obce	Počet obyvatel	Počet prvků ochrany
Hrobice	212	1
Kunětice	318	3
Dříteč	445	2
Ráby	549	3
Starý Mateřov	599	2
Němčice	606	1
Rokytno	882	3
Břehy	1010	3
Horní Ředice	1043	4
Staré Hradiště	1829	3

Zdroj: vlastní zpracování

Závislost byla ověřena pomocí korelační analýzy. Pro měření lineární závislosti se používá Pearsonův korelační koeficient (vzorec 2)

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \qquad (2)$$

kde: r je hodnota Pearsonova korelačního koeficientu;

$\bar{x}$ aritmetický průměr vysvětlující proměnné;

$\bar{y}$ aritmetický průměr vysvětlené proměnné. [16]

Hodnota Pearsonova koeficientu r = 0,4969 byla použitá při výpočtu testu významnosti koeficientu korelace (vzorec 3)

$$t = r\sqrt{\frac{n-2}{1-r^2}} \tag{3}$$

kde: *t* je hodnota testovací statistiky;

r Pearsonův korelační koeficient;

n rozsah výběru. [16]

Hodnota testovací statistiky t = 1,6193 byla na hladině významnosti α = 0,05 porovnána s kritickou hranicí t = 2,306. Protože testovací statistika neleží v kritické oblasti, nelze nulovou hypotézu o nezávislosti zamítnout. Na hladině významnosti 0,05 neexistuje statisticky významná závislost mezi počtem obyvatel v obcích a počtem prvků ochrany.

Hypotézu se potvrdit nepodařilo. Lze sledovat fakt, že jedna ze dvou obcí, která používá pouze jediný prvek ochrany zabezpečení osobních údajů, je shodou okolností obcí nejmenší a čtyři největší obce používají tři až čtyři prvky ochrany. Nicméně pouze v těchto ohledech by zjištěná data do jisté míry nasvědčovala nastíněné hypotéze. Neplatí však, že by zdaleka největší obec (Staré Hradiště) používala nejvíce prvků ochrany, stejně jako neplatí, že by s rostoucím počtem obyvatel lineárně rostl počet prvků ochrany. Potvrzení hypotézy brání pak zejména skutečnost, že obec Němčice (pátá největší) používá pouze jediný prvek ochrany, zatímco obec Kunětice (druhá nejmenší) zabezpečuje tři prvky ochrany.

2.5 Diskuse

Výsledky výzkumu v první řadě ukázaly, že malé obce se problematice ochrany osobních údajů v souvislosti s nabytím účinnosti nařízení GDPR svědomitě věnovaly a věnují. Jak nasvědčují odpovědi na otázku č. 5, přípravy obcí byly prováděny spíše na poslední chvíli, ve všech případech trvaly méně než 1 rok. A to i přesto, že nařízení GDPR bylo platné už více jak dva roky před nabytím jeho účinnosti. I tak lze kladně zhodnotit zodpovědný přístup obcí, neboť žádná z nich očividně přípravy na nabytí účinnosti nařízení GDPR nezanedbala, přípravy proběhly u všech dotázaných respondentů. Zvláště pak je třeba brát na zřetel, že malé obce mají ve srovnání k velikému počtu povinností, které musí zvládnout, pouze omezené množství kapacit a personálu. Problematika ochrany osobních údajů malé obce poměrně značně zatěžuje a dokonce je nezřídka vnímána jako zbytečná a nepříjemná součást úřadu.

Z výsledků výzkumu je jasně vidět, že obce přistupovaly s implementací nařízení GDPR do místních podmínek přiměřeně s přihlédnutím ke své velikosti, rozsahu agend, počtu institucí, ale hlavně i k individuálním potřebám. Je to patrné například na otázce č. 1 výzkumu, která se dotázala na způsob řešení potřeby jmenovat pověřence pro ochranu osobních údajů. Pouze jediná obec zvolila řešení, že bude pověřence zaměstnávat pro svou výlučnou potřebu, kdežto všechny ostatní zvolily řešení vnější osobou. Omezené možnosti jsou pak patrné i na zatížení obecního rozpočtu (ve většině případů je to v míře do 10 000 Kč ročně) či v otázce zavádění nových informačních systémů (žádná z obcí nepociťuje potřebu zavádět nové informační systémy).

Za jeden z největších přínosů, které vidím ve výsledcích výzkumu, jsou odpovědi na otázku č. 4, která se dotazovala, zda obec zavedla kromě informačních systémů v souvislosti s nařízením GDPR jiná nová technická a organizační opatření. Polovina obcí odpověděla negativně, zbytek pak uvedl poměrně variabilní odpovědi, které vypovídají o tvůrčím individuálním řešení zabezpečení osobních údajů.

Omezené odborné kapacity ochrany osobních údajů jsou z výsledků průzkumu v odpovědích na otázku č. 6 zřejmé. 70% respondentů uvedlo, že posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, pokud určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, bude provádět prostřednictvím pověřence pro ochranu osobních údajů. Pouze 20% dotázaných uvedlo, že toto bude provádět vlastními silami. Tyto výsledky svědčí o tom, že vysoce specializované činnosti nechává většina obcí na profesionálech, neboť na ně samy z pochopitelných důvodů nestačí. Podle mého názoru je třeba nebrat tyto procesy na lehkou váhu a je třeba si pokládat otázku, zda obce skutečně vlastními silami tento úkol zvládnou.

Velikou variabilitu odpovědí přinesly odpovědi na otázku č. 7, která se dotazovala na prvky zabezpečení, které používá obec v souvislosti s ochranou osobních údajů. Silné zastoupení měly všechny vyjmenované alternativy, tedy prvky ochrany fyzické (uzamykatelné dveře a skříně), elektronické (alarm, heslo v PC) i personální (střežení bezpečnostní agenturou / dozorčím / strážníky obecní policie). Tyto výsledky svědčí o vysoké prioritě, kterou respondenti přikládají zabezpečení osobních údajů a také o náležitě zodpovědném přístupu obcí. Analýzou závislosti vyšlo najevo, že neexistuje statisticky významná závislost mezi počtem obyvatel a jejich mírou ochrany osobních údajů.

Za zajímavé lze považovat odpovědi na 8. otázku, přičemž 90% respondentů přiznalo, že byla rizika, v rámci inventarizace a identifikace rizik za účelem jejich budoucí

minimalizace, shledána žádná či minimální. Tyto výsledky by mohly být teoreticky v rozporu s odpověďmi na otázku č. 4, které svědčí o tom, že polovina dotázaných pociťovala potřebu zavést nová technická a organizační opatření k ochraně osobních údajů. Tato skutečnost by mohla nasvědčovat tomu, že rizika v rámci jejich inventarizace a identifikace mohla být zastoupena ve vyšší míře nežli je žádná či minimální.

Jako celek na mne výsledky působí tak, že obce se snažily vypořádat se svými úkoly ohledně zavedení GDPR do praxe jen v té míře, v jaké jim na tento úkol stačily síly. Je zcela zřejmé, že ochrana osobních údajů se netěší být v malých organizačních celcích velké popularitě a není v ní ani spatřována priorita. Jinak řečeno: obce ze své podstaty zřejmě naplňují vůči svým občanům jiné funkcionality, nežli jsou otázky ochrany osobních údajů.

ZÁVĚR

Tato práce se zaměřuje na ochranu osobních údajů v souvislosti s nařízením GDPR, které aktuálně nabylo účinnosti. V prvé řadě popisuje, jaké změny a povinnosti pro obce nařízení GDPR přináší, jaký má vliv na informační systémy v obcích, jak je celý proces řešen a jak zatěžuje jejich rozpočty. Velkými změnami jsou nové přístupy: princip odpovědnosti a princip založený na riziku.

Vzhledem k novým povinnostem zůstaly základní zásady, principy a klíčové instrumenty oproti předchozímu stavu neměnné. Nařízení GDPR přineslo obcím některé nové povinnosti, mezi které patří: povinnost vést záznamy o činnostech zpracování, posoudit vliv na ochranu osobních údajů, ohlašovat případy jejich porušení zabezpečení subjektu údajů a Úřadu pro ochranu osobních údajů a také povinnost ustanovení pověřence pro ochranu osobních údajů.

Z šetření vyplynulo, že vliv na informační systémy v obci do dvou tisíc obyvatel je nulový. Žádná z obcí, které se zúčastnily výzkumu, nevyhodnotila zavedení nových informačních systémů jako důležité a neimplementovala je do praxe. Tuto skutečnost je, dle mého názoru, třeba brát vážně, neboť může představovat bezpečnostní rizika. Polovina dotázaných neidentifikovala náležitá rizika, přesto zavedla nová technická a organizační opatření k ochraně osobních údajů.

Dopad na rozpočty obcí považuji za zanedbatelný, neboť ve všech případech čítá řádově roční náklady desítky tisíc korun (pouze v jednom případě až 30 000 Kč ročně). Tento závěr lze učinit s vědomím toho, že vzhledem k různým servisním řešením zabezpečení ochrany osobních údajů, která lze dohledat v komerčních nabídkách specializovaných agentur, mohly být dopady na implementaci nařízení GDPR hypoteticky nepoměrně vyšší.

Cílem práce bylo porovnat pozitivní a negativní důsledky zavádění nařízení GDPR v obcích do dvou tisíc obyvatel v pardubickém kraji. Toto zhodnocení lze generalizovat i přesto, že výzkum byl prováděn v omezených podmínkách jednoho kraje.

Za pozitivní důsledky zavádění nařízení GDPR v obcích považuji vyšší zabezpečení osobních údajů, přičemž nezamýšlenou přidanou hodnotou tohoto stavu je nejen zabezpečení osobních údajů, ale i ostatních agend, které se společně s nosiči osobních údajů v chráněných objektech obecních úřadů nalézají. Za další pozitivní dopad považuji vyšší profesionalizaci ochrany osobních údajů, která by měla být zajištěna zejména díky působení pověřence

s aktivní účastí při vlastní implementaci nařízení GDPR a vyjádřena v procesu uvádění do souladu k dílčím skutečnostem ochrany osobních údajů.

Za negativní důsledky považuji především zvýšení byrokracie, kterou nové povinnosti spojené s ochranou osobních údajů v režimu nařízení GDPR nutně přibydou. Nejtíživěji ji ponesou právě malé organizace (obce). Dalším negativním důsledkem jsou zvýšené náklady, byť nejsou nijak katastrofické.

Na úplný závěr je třeba podotknout, že dotazníkového šetření se zúčastnilo pouze deset obcí, jejichž výsledek lze sice generalizovat na poměry všech malých obcí v celé republice nikoli však na obce s různým počtem obyvatel. Přesto se domnívám, že výsledky šetření mají svou vypovídající hodnotu.

POUŽITÁ LITERATURA

[1] BĚLECKÝ, Miroslav. Pravidla pro vedení evidence odborně způsobilou osobou, *Bezpečnost a hygiena práce*, 2012, č. 2.

[2] DIBLÍK, Jan, JAROŠ, Ján. Povinnosti správců a zpracovatelů ve světle obecného nařízení o ochraně osobních údajů (GDPR), *Komorní listy*, 2017, č. 4.

[3] DUŠEK, Ladislav a kol. *Jak implementovat GDPR v ambulantní sféře*, publikováno v Automatizovaném systému právních informací dne 26. 1. 2018, ASPI ID: LIT246480CZ.

[4] FRÝBOVÁ, Alice. GDPR v otázkách a odpovědích, *Otázky a odpovědi v praxi*, 2018, č. 4.

[5] FRÝBOVÁ, Alice, URBANOVÁ, Eva. GDPR – úvod do problematiky, *Školní poradenství v praxi*, 2018, č. 1.

[6] *GDPR stručně* [online]. [cit. 2018-07-11]. Dostupné z: https://www.uoou.cz/gdpr-strucne/ds-4843/archiv=0&p1=5005.

[7] JANEČKOVÁ, Eva. *GDPR – Praktická příručka implementace*, 1. vydání, Praha: Wolters Kluwer, 2018, 136 s. ISBN 978-80-7552-248-1.

[8] JAROŠ, Ján, DIBLÍK, Jan. Povinnosti správců a zpracovatelů ve světle obecného nařízení o ochraně osobních údajů (GDPR), *Komorní listy*, 2017, č. 4.

[9] 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)

[10] NEZMAR, Luděk. GDPR: *Praktický průvodce implementací*, 1. vydání, Praha: Grada Publishing, 2017, 304 s. ISBN 978-80-2710-920-3.

[11] *Nové přístupy a povinnosti* [online]. [cit. 2018-07-11]. Dostupné z: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=1091.

[12] NULÍČEK, Michal a kol. *GDPR / Obecné nařízení o ochraně osobních údajů. Praktický komentář.* 1. vydání, Praha: Wolters Kluwer, 2017, 525 s. ISBN 978-80-7552-765-3.

[13] *Statistická analýza dat* [online]. [cit. 2018-11-29]. Dostupné z: https://acrea.cz/sluzby/statisticka-analyza-dat.html

[14] ŠKALOUDOVÁ, Alena. Korelační analýza. *Katedra psychologie* [online]. Univerzita Karlova, 2014 [cit. 2018-11-21]. Dostupné z: http://kps.pedf.cuni.cz/skalouda/pokrocili/korelacni.htm

[15] *Téma 5: Analýza závislostí* [online]. [cit. 2018-11-29]. Dostupné z: https://k101.unob.cz/~neubauer/pdf/Analyza%20zavislosti.pdf

[16] URBANOVÁ, Eva, FRÝBOVÁ, Alice. Pověřenec pro ochranu osobních údajů, *Řízení školy*, 2018, č. 3.

[17] ZEMANOVÁ ŠIMONOVÁ, Hana. Reforma ochrany osobních údajů v EU z pohledu pracovněprávních vztahů, *Bulletin advokacie*, 2017, č. 9.

[18] ŽŮREK, Jiří. *Praktický průvodce GDPR*, 1. vydání, Olomouc: ANAG, 2017, 223 s. ISBN 978-80-7554-097-3.

PŘÍLOHA A: DOTAZNÍK

1) Jakým způsobem bude vaše obec jmenovat pověřence pro ochranu osobních údajů?

a) Obec jej bude zaměstnávat pro svou výlučnou potřebu;

b) Obec bude využívat služby nezávislého profesionála (outsourcing);

c) Pověřenec bude vykonávat svou pravomoc na úrovni svazku obcí, jíž je obec členem;

d) Jinak – uveďte jak.

2) Máte představu, v jaké míře bude zavedení GDPR znamenat zátěž pro obecní rozpočet?

a) Ano – uveďte odhadnuté roční náklady;

b) Ne.

3) Zavedla/bude zavádět obec v souvislosti s GDPR nové informační systémy?

a) Ano – uveďte jaké (název, účel);

b) Ne.

4) Zavedla/bude zavádět obec kromě informačních systémů v souvislosti s GDPR jiná nová technická a organizační opatření?

a) Ano – uveďte jaká (název, účel);

b) Ne.

5) Jak dlouho se vaše obec organizačně připravovala na nabytí účinnosti GDPR?

a) Dva roky;

b) Rok;

c) Méně než rok;

d) Vůbec.

6) Jak budete provádět posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, pokud určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob?

a) Prostřednictvím pověřence pro ochranu osobních údajů;

b) Vlastními silami;

c) Nebudeme provádět;

d) Zatím nemáme představu, budeme řešit, až nastane tato potřeba.

7) Jaké prvky zabezpečení používá vaše obec v souvislosti s ochranou osobních údajů?

a) Uzamykatelné dveře a skříně;

b) Alarm;

c) Střežení bezpečností agenturou / dozorčím / strážníky obecní policie.;

d) Silné heslo v PC, kde jsou soustředěny databáze osobních údajů;

e) Jiné – uveďte jaké.

8) Prováděla vaše obec tzv. analýzu GDPR (inventarizace a identifikace rizik za účelem jejich budoucí minimalizace)? S jakým výsledkem?

a) Ano – rizika byla shledána žádná či minimální;

b) Ano – rizika byla shledána závažná, nepřijali jsme však zatím žádná opatření;

c) Ano – rizika byla shledána závažná, přijali jsme opatření – uveďte jaká;

d) Neprováděla.