ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

GDPR – Vyhodnocení dopadů GDPR na podniky v České republice

GDPR – Evaluation of the Impacts of GDPR on Businesses in the Czech Republic

Bc. Markéta Maňourová

Plzeň 2019

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma GDPR – Vyhodnocení dopadů GDPR na podniky v České republice vypracovala samostatně pod odborným dohledem vedoucího diplomové práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni dne …….. ……...

podpis autora

Poděkování

Chtěla bych tímto poděkovat panu Ing. Martinu Januškovi, Ph.D. za pomoc při realizaci práce. Také bych chtěla poděkovat všem respondentům, kteří si našli chvíli ze svého času a zúčastnili se dotazníkového šetření. V neposlední řadě bych ráda poděkovala své rodině, která mě po dobu celého studia neustále podporovala.

Obsah

Úvod

Tato diplomová práce se zabývá tématem General Data Protection Regulation, implementací změn v rámci ochrany osobních údajů do organizací a vyhodnocením dopadů Nařízení na organizace v České republice.

Práce se zaměřuje na charakteristiku problematiky GDPR a hlavním cílem práce je analyzovat dopady GDPR na organizace, které vznikají v průběhu implementace Nařízení do organizací.

Teoretické poznatky obsažené v práci vycházejí z dostupné literatury, která se zabývá problematikou GDPR. Pro následné získávání empirických dat je použito dotazníkové šetření.

V první části práce je představeno Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Druhá část se zabývá základními pojmy, které jsou pro Nařízení důležité a také pojmy, které jsou v rámci práce používány. Následná, tedy třetí, část se zabývá implementací GDPR do organizací. Ve čtvrté části je představeno dotazníkové šetření a poslední, pátá část, obsahuje vyhodnocení a analýzu dotazníkového šetření.

1 General Data Protection Regulation

S rozvojem nových technologií bylo nutné, aby Evropská unie na tento pokrok reagovala. Ať už se jedná o nové technologie v internetovém obchodování, sociální sítě či internetové služby, ve všech případech dochází k rozsáhlému sběru osobních informací, k jejich zpracovávání, monitorování a profilování fyzických osob či chování zaměstnanců a další. Díky takto rozsáhlému sběru a zpracovávání dat je nutné zavést nová organizační a technická opatření, která povedou k ochraně nejen osobních údajů, ale také subjektů údajů. (Navrátil 2018)

GDPR, nebo také celým názvem General Data Protection Regulation, označuje obecné označení pro obecné nařízení o ochraně osobních údajů. Konkrétně se však jedná o ***Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob*** v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. V České republice *Nařízení* nahrazuje zákon č. 101/2000 Sb., o ochraně osobních údajů.

Díky tomu, že se jedná o nařízení Evropské unie, je tento dokument právně zavazující a platný v celém svém rozsahu v celé Evropské unii. *Nařízení* je jednotné pro všechny členy EU. Vzhledem k mezinárodnímu pohybu informací se jedná o velmi důležitý dokument, prostřednictvím kterého se zjednodušuje nejen cestování, ale také pohyb osob a zboží v zahraničí. (Navrátil 2018, Evropská unie, ©2019)

1.1 Cíle GDPR

Nařízení GDPR si klade následující cíle:

- *„přizpůsobení právní regulace ochrany osobních údajů poměrům dnešní doby,*
- *Sjednocení práva ochrany osobních údajů ve všech zemích Evropské unie a dalších zemích, na které dopadá,*
- *posílení práv v oblasti ochrany osobních údajů všech osob, které jsou subjekty údajů a dosáhnout sjednoceného výkladu GDPR dozorovými úřady jednotlivých zemí Evropské unie,*
- *posílit důvěryhodnost Evropské unie a jejích členských zemí (i dalších zemí, které pod GDPR spadají) pro jiné země, které mají zájem na rozvoji obchodu s Evropskou unií a s tím souvisícím předáváním osobních údajů mezi zeměmi.“* (Navrátil 2018, s. 30)

1.2 Platnost GDPR

Nařízení vešlo v platnost 27. dubna 2016, avšak ve všech členských státech Evropské unie nabývá účinnosti 25. května 2018. Od tohoto dne se podle tohoto *Nařízení* řídí ochrana osobních údajů a taktéž od tohoto dne je *Nařízení* vymahatelné. Od 27. dubna 2016 do 25. května 2018 probíhala legisvakační lhůta. Tato lhůta označuje dobu, během které měli všichni, kteří osobní údaje zpracovávají, uvést nejen toto zpracovávání, ale také správu osobních údajů v souladu s *Nařízením* GDPR. (Navrátil 2018, s. 31)

1.3 Přístupy k osobním údajům

V souvislosti s *Nařízením* je ochrana osobních údajů je nově založena na dvou principech. Jedná se o princip odpovědnosti správce a přístup založený na riziku.

1.3.1 Princip odpovědnosti správce

Princip odpovědnosti správce, který označuje zodpovědnost správce za dodržování zásad pro zpracovávání osobních údajů. Dodržování zásad *Nařízení* je správce povinen také doložit.

1.3.2 Přístup založený na riziku

Úřad pro ochranu osobních údajů definuje přístup založený na riziku následovně:

„Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů.“ (Úřad pro ochranu osobních údajů, ©2018)

Taktéž ÚOOÚ dále uvádí: *„V pojetí obecného nařízení tento přístup navíc znamená aplikaci dodatečných povinností pro některé správce, kdy zpracování osobních údajů či porušení zabezpečení představuje riziko či vysoké riziko pro práva a svobody fyzické osoby a je tedy důvodné aplikovat tyto povinnosti. Mezi tyto nové povinnosti, o kterých nelze hovořit, že se plošně vztahují na všechny správce či zpracovatele patří:*

- *záznamy o činnostech zpracování,*
- *jmenování pověřence pro ochranu osobních údajů,*
- *posouzení vlivu na ochranu osobních údajů,*

- *předchozí konzultace s dozorovým úřadem,*
- *povinnost ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů.“* (Úřad pro ochranu osobních údajů, ©2018)

1.4 Struktura Nařízení

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů je ve svém znění členěno do jedenácti kapitol. Jednotlivé kapitoly *Nařízení* se zabývají následujícím:

- V první kapitole jsou uvedena obecná ustanovení, definice, cíle a působnost Nařízení.
- Druhá kapitola se týká zpracovávání osobních údajů.
- Třetí kapitola se zaměřuje na práva subjektu údajů.
- Čtvrtá kapitola se zabývá správcem a zpracovatelem.
- V páté kapitole se řeší předávání osobních údajů do třetích zemí nebo mezinárodním organizacím.
- V šesté kapitole se Nařízení zaměřuje na podmínky, pravidla, úkoly a pravomocemi nezávislých dozorových úřadů.
- Sedmá kapitola je zaměřena na spolupráci a jednotnost mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady.
- Osmá kapitola se zabývá právní ochranou, odpovědností a sankcemi.
- V deváté kapitole jsou představena zvláštní ustanovení, které se týkají zvláštních situací, ke kterým dochází při zpracování.
- Desátá kapitola se zabývá akty v přenesené pravomoci a prováděcími akty.
- Jedenáctá kapitola obsahuje závěrečná ustanovení. (DonauMedia 2018)

Nařízení se však netýká každého. V článku 18 je uvedeno následující:

(18) Toto nařízení se nevztahuje na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností. Činnosti osobní povahy nebo činnosti v domácnosti by mohly zahrnovat korespondenci a vedení adresátů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi. Toto nařízení se však

vztahuje na správce nebo zpracovatele, kteří tyto činnosti osobní povahy či činnosti v domácnosti poskytují prostředky pro zpracování osobních údajů. (Evropský parlament a Rada Evropské unie 2016, s. 3)

2 Pojmy z oblasti GDPR

V oblasti GDPR a zpracovávání osobních údajů se jedná s mnoha pojmy, které je nutné si nejprve představit. Tato kapitola se zaměřuje právě na pojmy z oblasti GDPR, které jsou důležité nejen pro ochranu osobních údajů, ale také pro další části práci.

2.1 Osobní údaje

V rámci celého *Nařízení* se jedná o zpracovávání osobních údajů. *Nařízení* definuje osobní údaje následujícím způsobem:

„Osobní údaje jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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.“ (Evropský parlament a Rada Evropské unie 2016, s. 33)

Osobní údaje označují obecný pojem a je možné je rozdělit do čtyř následujících kategorií:

- ***adresní a identifikační údaje*** – do této kategorie patří například: jméno, příjmení, datum narození, rodinný stav, rodné číslo a další;
- ***citlivé údaje*** – například údaje o rasovém nebo etnickém původu, genetické údaje, údaje o náboženském přesvědčení, zdravotním stavu a další
- ***popisné údaje*** – tato kategorie označuje údaje, které se týkají vzdělání, zaměstnání, odborné způsobilosti a dovedností, počtu dětí a podobně;
- a ***údaje o jiné osobě*** – tato kategorie osobních údajů se týká údajů o členech rodiny. (Matoušková a Hejlík 2008)

2.2 Subjekt údajů

„Subjektem údajů je fyzická osoba, které 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 obecné nařízení

vylučuje svoji působnost na údaje o zesnulých osobách. (Ministerstvo vnitra České republiky, ©2019)

Dle GDPR mají subjekty údajů šest základních práv. Tato práva jsou zobrazena na obrázku č. 1.

Obrázek č. 1: Základní práva subjektů údajů

Zdroj: HelpGDPR.cz, ©2017

2.2.1 Právo na přístup

Prostřednictvím tohoto práva mají subjekty údajů možnost získat od správce potvrzení, zda jsou jejich osobní údaje zákonně zpracovány. Díky tomuto právu mají subjekty právo získat informace o:

- *„účelech zpracování,*
- *kategoriích dotčených osobních údajů,*
- *příjemcích a kategoriích příjemců, kterým budou nebo byly osobní údaje zpřístupněny,*
- *době, po kterou budou osobní údaje uloženy,*

- *existenci práva požadovat od správce opravu nebo výmaz osobních údajů či právo vznesení námitky,*
- *Právu podat stížnost u dozorového úřadu,*
- *veškerých dostupných informacích o zdroji osobních údajů, pokud nebyly získány od subjektu údajů,*
- *skutečnosti, zda dochází k automatizovanému rozhodování, včetně profilování.“* (Žůrek 2017, s. 129)

2.2.2 Právo na opravu

V případě, kdy má subjekt údaje podezření, že údaje jsou nesprávné, má právo na pořádat společnost o opravu. V rámci tohoto práva může subjekt také osobní údaje doplnit.

2.2.3 Právo na výmaz

Toto právo taktéž může být nazýváno „právo být zapomenut“. V rámci tohoto práva má správce povinnost osobní údaje bez zbytečného odkladu vymazat v případě, že existuje jeden z následujících důvodů:

- *„osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány,*
- *subjekt údajů odvolá souhlas, na základě, kterého byly osobní údaje zpracovávány, a současně neexistuje žádný další právní důvod pro zpracování,*
- *subjekt údajů vznese námitky proti zpracování a neexistují převažující oprávněné důvody pro zpracování,*
- *osobní údaje byly zpracovány protiprávně,*
- *osobní údaje musí být vymazány ke splnění právní povinnosti vztahující se na správce.“* (Žůrek 2017, s. 132)

2.2.4 Právo vznést námitku

Subjekt údajů má právo kdykoliv vznést námitku proti zpracování osobních údajů. „*Správce pak osobní údaje dále nezpracovává, pokud neprokáže oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.“* (GUARD7, ©)

2.2.5 Právo na omezení zpracování

Pokud se subjekt údajů domnívá, že jeho osobní údaje jsou zpracovávány v rozporu s legislativou, případně, že by zpracování jeho osobních údajů mohlo omezit jeho práva a svobody, má právo vznést námitku pro omezení zpracování těchto údajů.

V rámci *Nařízení* je uvedeno následující:

„Subjekt údajů má právo na to, aby správce omezil zpracování, pokud:

- *subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k* tomu, *aby mohl správce přesnost osobních údajů ověřit,*
- *je zpracovávání protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho omezení jejich použití,*
- *správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků,*
- *subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.“* (Evropský parlament a Rada Evropské unie 2016, s. 44)

2.2.6 Právo na přenositelnost

Toto právo umožňuje subjektu údajů *„získat osobní údaje, jež poskytl správci a které se ho týkají, ve strukturovaném, běžně používaném a strojově čitelném formátu a zároveň tyto údaje předat jinému správci, a to i prostřednictvím původního správce, a to v případě, že zpracování je založeno na souhlasu subjektu údajů nebo na smlouvě a provádí se automatizovaně.“* (Žůrek 2017, s. 136)

2.3 Správce

V rámci zpracovávání osobních údajů je definován také pojem *správce*. Tento pojem označuje subjekt, který určuje účel zpracovávání osobních údajů a použité prostředky pro toto zpracovávání. Taktéž je za zpracování primárně zodpovědný. Zpracovávání osobních údajů vyplývá z činnosti správce, avšak ten může osobní zpracovávat i pro vlastní určené účely v případě, že jeho zájmy pro zpracování údajů nepřesahují ochranu základních práv a svobod fyzických osob.

Každého správce se *Nařízení* dotýká jiným způsobem, neboť každý správce zpracovává různé údaje a taktéž zpracování provádí různými způsoby. V souvislostí s tím také musí odpovídat přípravy každého správce na splnění požadavků obecného nařízení. Správce by si před přistoupením k zavedení změn měl vypracovat analýzu zpracování, které provádí, čímž zjistí povinnosti, které se na něj vztahují. Součástí této analýzy by také mělo být vytipování slabých míst správce, ať už se jedná o slabá místa v zabezpečení či provedení revize právních důvodů zpracování osobních údajů a mnoho dalších.

V případě, že správce plnil povinnosti, které v České republice vyplývaly z předešlého zákona č. 101/2000 Sb., o ochraně osobních údajů, *Nařízení* by pro nej nyní nemělo představovat výrazné komplikace

Při nakládání s osobními údaji je správce odpovědný za:

- dodržování zásad zpracování,
- dodržování povinností upravených Nařízením a
- zabezpečení údajů. (Obecné nařízení o ochraně osobních údajů prakticky ©)

Správce má také ve své činnosti určité povinnosti. Jedná se například o povinnost:

- aplikovat záměrnou a standardní ochranu osobních údajů,
- jmenovat pověřence pro ochranu osobních údajů (tato povinnost se však netýká všech správců),
- posuzovat vliv na ochranu osobních údajů a provádět předchozí konzultace s dozorovým úřadem,
- ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznamovat případy porušení zabezpečení osobních údajů subjektu osobních údajů a
- vést záznamy o zpracovávání osobních údajů (taktéž se netýká všech správců). (Obecné nařízení o ochraně osobních údajů prakticky ©)

2.4 Zpracovatel

„Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace.“ (Úřad pro ochranu osobních údajů, ©2013)

Zpracovatelem může být jakákoliv fyzická osoba, orgán veřejné moci, agentura či jiný subjekt. Nezáleží tedy o jakou právní formu se jedná.

Činností zpracovatele jsou pouze takové zpracovatelské operace, které vyplývají ze zpracovatelské smlouvy. Operace, jež vykonává jsou tedy operace, kterými jej správce pověří.

ÚOOÚ uvádí povinnosti zpracovatele následovně: *„Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce. Zpracovatel musí postupovat podle smlouvy nebo právního předpisu, které jej zavazují vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Osobní údaje musí být adekvátně zabezpečeny i u zpracovatele. Zpracovatel nesmí zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. Zpracovatel je povinen dodržovat další povinnosti uvedené zejména v článku 28 GDPR.“* (Úřad pro ochranu osobních údajů, ©2018)

2.5 Zpracovávání osobních údajů

Nařízení ve svém znění jedná také o zpracovávání osobních údajů. Zpracování označuje jakoukoliv operaci či soubor operací s osobními údaji, které mohou být vykonávány s pomocí či bez pomoci automatizovaných postupů. Jedná se například o shromažďování, zaznamenání, uspořádávání, ukládání, přizpůsobení nebo pozměnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Zpracování je však nutné chápat jako provádění operací s osobními údaji za nějakým účelem a je tak prováděno systematicky.

Nařízení stanovuje principy, které je nutné při zpracovávání osobních údajů dodržovat. Jedná se o následující principy:

- ***zákonnost, korektnost a transparentnost,***
- ***účelovost,***
- ***minimalizace,***
- ***přesnost,***

- ***omezenost,***
- ***integrita a důvěrnost***.

Dodržování výše zmíněných zásad je pro správce zásadní nikoliv jen z důvodu, že se jedná o jeho povinnost, ale také proto, že správce musí být schopen doložit dodržování těchto povinností. Tato povinnost již byla krátce zmíněna v předchozí kapitole, tzv. princip odpovědnosti správce. Pro doložení dodržování těchto povinností slouží záznamy o činnostech zpracování ale také kodexy a osvědčení.

2.5.1 Zákonnost, korektnost a transparentnost

Zákonnost zpracování osobních údajů znamená, že zpracovávání musí probíhat v souladu s právními předpisy. Aby toto zpracovávání probíhalo v souladu s těmito předpisy, musí probíhat buďto na základě souhlasu subjektu údajů nebo na základě právního důvodu. (Nulíček 2018)

Korektnost označuje poctivé zpracovávání osobních údajů. Při zpracovávání osobních údajů je nutné zohlednit zájmy a očekávání dotčených osob a nesmějí se přehlížet případně mylných představ dotčených osob využívat. (Nulíček 2018)

Zásada *transparentnosti* udává, že všechny informace a sdělení určená ke zpracování osobních údajů budou přístupné a srozumitelné. (Nulíček 2018)

2.5.2 Účelovost

Zásada účelovosti doplňuje výše zmíněnou zásadu transparentnosti. Subjekt údajů musí být informován, k jakému účelu budou získané informace použity již při samotném sběru dat. (Navrátil 2018)

2.5.3 Minimalizace

Vzhledem k účelu zpracovávání musejí být získávané osobní údaje přiměřené a relevantní. *„Tato zásada se skládá ze tří požadavků. Za prvé, data musí být pro sledovaný účel podstatná. Za druhé, musí být pro sledovaný účel potřebná, tedy zpracování údaj musí být omezeno na nutnou míru odpovídající sledovanému účelu. Za třetí musí být takové omezení přiměřené.“* (Navrátil 2018, s. 42)

2.5.4 Přesnost

Zásada přesnosti označuje, že osobní údaje musejí být správné. Pokud toto nesplňují, je nutné je okamžitě vymazat, případně musejí být opraveny. K této zásadě také náleží aktuálnost osobních údajů, je-li to potřebné.

2.5.5 Omezenost

Tato zásada se zabývá omezením uložení osobních údajů. *„Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.“* (Navrátil 2018, s. 43)

2.5.6 Integrita a důvěrnost

Při zpracovávání osobních údajů musí být zajištěna jejich bezpečnost. Tato bezpečnosti znamení *„ochranu před neoprávněným nebo nezákonným zpracováním a před nezamýšleným ztracením, zničením nebo poškozením dat“*. Pro zajištění bezpečnosti dat je nutné přijmout vhodná organizační a technická opatření. (Navrátil 2018, s. 43)

2.6 Právní důvody zpracovávání osobních údajů

Jak již bylo uvedeno v předchozí části práce, pro zpracovávání osobních údajů musí existovat právní důvody, které správce k této činnosti opravňují. Správce může osobní údaje zpracovávat pro různé účely, avšak pro každý účel je nutná existence právního důvodu.

Dle *Nařízení* lze osobní údaje zpracovávat, pokud je přítomen alespoň jeden z následujících právních důvodů:

- *„subjekt údajů udělil souhlas pro jeden či více konkrétních účelů;*
- *zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
- *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;*
- *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*

- *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
- *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů.“* (Evropský parlament a Rada Evropské unie 2016, s. 36)

V případě, že správce pozbude poslední právní důvod ke zpracování osobních údajů, nastává jeho povinnost osobní údaje o subjektu či subjektech zlikvidovat.

Zpracování osobních údajů se souhlasem subjektu údajů

„Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným potvrzením své svolení ke zpracování svých osobních údajů. Jde o aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen.“ (Úřad pro ochranu osobních údajů, ©2018)

V případě, že správce provádí zpracování osobních údajů subjektu údajů na základě jeho souhlasu, musí být schopen tento souhlas také doložit.

Souhlas subjektu údajů je však odvolatelný, ačkoliv odvolání souhlasu nutně neznamená pro správce nutnost osobní údaje zlikvidovat. (Úřad pro ochranu osobních údajů, ©2018)

Balanční test

Balanční test se používá pro prokázání, zda jeho oprávněné zájmy převyšují zájmy či základní práva a svobody subjektů údajů. V případě získání kladného výsledku z tohoto testu, správce je oprávněn osobní údaje zpracovávat na základě oprávněného zájmu.

Oprávněný zájem

Na základě oprávněného zájmu je možné zpracovávat osobní údaje pouze v případě, že se to nezbytně nutné a to *„za účelem ochrany práv či právem chráněných zájmů správce, příjemce či jiné dotčené osoby“* (Nulíček 2018, s. 135). Aby mohl být využit oprávněný zájem zpracovávání osobních údajů, je nutné tyto údaje zpracovávat pro účely:

- *„zamezení podvodům,*

- *přímého marketingu,*
- *předávání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely,*
- *oznámení trestných činů či hrozeb pro veřejnou bezpečnost a předání dotčených osobních údajů příslušnému orgánu,*
- *zajištění bezpečnostní sítě a informací k zabánění neoprávněného přístupu k nim, šíření škodlivých kódů a zamezení útokům a škodám na počítačových systémech a systémech elektronických komunikací."* (Kuchař, ©2018)

2.7 Technická a organizační opatření

Pro dodržován zásad *Nařízení* a zabezpečení osobních údajů je nutné zavést v organizaci technická a organizační opatření. Jejich cílem je snížení pravděpodobnosti vzniku rizika případně snížení negativních dopadů, které souvisejí se vznikem rizika. (Staňková 2018)

Správce je povinen zavést opatření v závislosti na povaze, rozsahu, kontextu a účelům zpracování osobních údajů, ale také v závislosti na možných rizicích, které mohou v při práci s osobními údaji nastat. Zajištění těchto opatření musí být správce také schopen doložit.

Nařízení také zmiňuje některé technické či organizační opatření. Jedná se o následující:

- *„pseudonymizace a šifrování osobních údajů,*
- *schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,*
- *schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických nebo technických incidentů,*
- *proces pravidelného testování, posuzován a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracován."* (Evropský parlament a Rada Evropské unie 2016, s. 51)

Lucie Staňková ve své publikaci GDPR snadno a přehledně uvádí následující:

„Obecně lze za technická a organizační opatření považovat:

- ***integritu*** *– zaručení pravosti a nenarušenosti osobních údajů (opatření, která zajistí, že nedojde k úmyslné nebo náhodné změně osobních údajů při jejich zpracování),*
- ***důvěrnost*** *– taková opatření, která zajistí, že se k údajům nedostane nepovolaná osoba (např. pseudonymizace, šifrování, povinnost mlčenlivosti nebo správa přístupových práv),*
- ***transparentnost*** *– zajištění používání dostatečných opatření (především zpracovatel musí správci prokázat, že skutečně používá opatření, ke kterým se zavázal),*
- ***izolovanost*** *– opatření, která zajistí, že nedojde ke sloučení nebo záměně souborů osobních údajů (např. zpracovatel musí zaručit, že nedojde ke sloučení nebo záměně osobních údajů, která zpracovává pro různé správce),*
- ***součinnost*** *– jedná se především o zabezpečení výkonu práv subjektů údajů,*
- ***odpovědnost*** *– zaručení efektivního dodržování zásad ochrany osobních údajů daným Nařízením GDPR (např. sankce a další postihy vůči zaměstnancům a pracovníkům, kteří poruší své povinnosti).“* (Staňková 2018, s. 107)

Zavedená opatření nikdy nebudou pro všechny organizace stejná, neboť každá organizace je jiná, zpracovává různé osobní údaje za různými účely. Při volbě technických a organizačních operací je tedy nutné brát ohled na:

- velikost organizace,
- množství zpracovávaných osobních údajů,
- povahu zpracovávaných osobních údajů,
- rizika zpracovávaných osobních údajů,
- účel zpracování,
- předávání osobních údajů,
- dobu zpracování a jiné. (Staňková 2018, s. 107)

2.7.1 Technická opatření

Technická opatření pro zabezpečení osobních údajů označují zavedení technologií, které zajistí větší fyzickou bezpečnost osobních údajů, ale také zabezpečení informačních systémů, která zabrání poškození dat, jejich ztrátě případně neoprávněnému přístupu.

Mezi technická opatření lze například zařadit:

- identifikace a autentizace osob,
- hesla,
- PIN,
- antivirová ochrana,
- dvoufázové ověření přihlášení,
- pseudonymizace,
- anonymizace,
- šifrování,
- uzamykatelné místností/stoly/skříně,
- oprávnění k přístupu na základě otisku prstu a další. (Know Your Compliance, ©2018)

Anonymizace, šifrování, pseudonymizace

Jak již bylo zmíněno, anonymizace, šifrování i pseudonymizace patří mezi technická opatření pro ochranu osobních údajů při jejich zpracovávání. I přesto, že tato opatření vedou ke snížení možného rizika, nejedná se o opatření pro správce ani zpracovatele povinná.

Anonymizace označuje proces, prostřednictvím kterého dojde k odstranění či nahrazení veškerých osobních údajů prostřednictvím kterých by mohla být daný osoba identifikována v budoucnosti. V případě anonymizace se jedná o nevratný proces. Díky tomu, že po anonymizaci údajů již není možné zpětně identifikovat osoby, nevztahuje se již na tato data Nařízení GDPR.

Šifrováním dat se rozumí znemožnění nepovolaným osobám data přečíst. Jedná se o zakódování dat, přičemž pro rozluštění dat je nutné mít dešifrovací klíč. Pouze pro vlastníka šifrovacího klíče jsou tedy data čitelná.

Posledním pojmem v této části je *pseudonymizace*. Jedná se o proces, při kterém se skrývá identita subjektu. Při pseudonymizaci osobních údajů se jménu a příjmení subjektu přiřadí unikátní kód. Klíč pro rozšifrování unikátního kódu, tedy k přiřazení dat k určité osobě, musí být uložen odděleně od všech ostatních údajů.

(Staňková 2018)

2.7.2 Organizační opatření

Na rozdíl od technických opatření, organizační opatření se zaměřují na procesy, kompetence a odpovědnosti. Díky těmto opatřením dochází k minimalizaci spravovaných údajů, minimalizaci oprávnění konkrétních osob, které mohou s osobními údaji nakládat, ale také je díky těmto opatřením nastavená maximální auditovatelnost všech operací a přístupů.

Mezi organizační opatření se řadí například:

- směrnice,
- záznamy o činnostech zpracování,
- školení zaměstnanců,
- analýza rizik,
- pověřenec na ochranu osobních údajů,
- posouzení vlivu na ochranu osobních údajů,
- konzultace s dozorovým úřadem,
- opakované kontroly a aktualizace zavedených opatření pro ochranu osobních údajů,
- spolupráce s dozorovým úřadem a mnoho dalších. (Know Your Compliance, ©2018)

2.7.2.1 Záznamy o činnostech zpracování

Vedením záznamů o činnostech zpracování správce může dokládat soulad s *Nařízením* GDPR. Vedení těchto záznamů však není povinné pro všechny správce či zpracovatele. Podle *Nařízení* nemusejí záznamy o činnostech zpracování vést podniky či organizace, které zaměstnávají méně než 250 osob. Avšak i pro podniky s méně než 250 zaměstnanci existují výjimky. Záznamy o činnostech zpracování musejí vést i jiné než velké organizace v případě, že:

- *„zpracování osobních údajů, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů,*
- *zpracovávání osobních údajů není příležitostné,*

- *zpracovávání osobních údajů zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.“* (Staňková 2018, s. 111)

Záznamy o činnostech zpracování musí být aktuální a zároveň je v *Nařízení* vymezeno, co musejí tyto záznamy musejí obsahovat. Jedná se o následující údaje:

- *jméno a kontaktní údaje správce*
- *účely zpracování osobních údajů,*
- *rozsah zpracovávaných osobních údajů,*
- *informace o příjemcích daných osobních údajů,*
- *informace o případném předávání údajů do třetích zemí,*
- *lhůty pro výmaz jednotlivých kategorií údajů a*
- *popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů.* (Obecné nařízení o ochraně osobních údajů prakticky ©)

2.7.2.2 Pověřenec pro ochranu osobních údajů

„Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je specifickou funkcí, kterou musí dle Nařízení zřídit a obsadit část správců a zpracovatelů. Pověřenec dohlíží na soulad zpracování s Nařízením a radí správci ohledně různých skutečností spojených s ochranou osobních údajů. Pověřenec zároveň slouží jako kontaktní místo pro subjekty údajů a dozorový úřad ohledně záležitostí týkajících se zpracování osobních údajů.“ (Nulíček 2018, s. 361)

Jmenování pověřence však není povinné pro všechny správce či zpracovatele. Povinnost jmenovat pověřence mají organizace, které splní alespoň jednu z podmínek uvedených v *Nařízení*. Pověřence tedy musejí organizace jmenovat v případě, že:

- *zpracování provádí orgán veřejné moci nebo veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudní pravomocí;*
- *hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů;*

- *hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů uvedených v článku 9 Nařízení nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 Nařízení.* (Nulíček 2018, s. 362)

Organizace, které nemají povinnost jmenovat pověřence, se mohou k tomuto úkonu rozhodnout dobrovolně. Také však musejí povinně jmenovat pověřence správce či zpracovatelé zastupující kategorie správců nebo zpracovatelů, pokud to vyžaduje právo Evropské unie nebo členského státu. (Staňková 2018)

„Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:

- *poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů,*
- *monitorování souladu s Nařízením GDPR, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,*
- *poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35 Nařízení GDPR,*
- *spolupráce s dozorovým úřadem,*
- *působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení, a případně vedení konzultací v jakékoliv jiné věci.“* (Staňková 2018, s. 124)

Pověřencem pro ochranu osobních údajů nemusí být pouze externí pracovník. *Nařízení* dává správcům a zpracovatelům možnost pověřit touto funkcí také pracovníka interního. Interní pracovník vykonávající funkci pověřence představuje pro organizaci nižší náklady na jeho vzdělávání a také jeho alokaci. Pro jmenování externího pověřence se může organizace rozhodnout například v případě nedostatku interních kapacit. Pro externího pověřence je však charakteristické, že oproti internímu nedisponuje detailními znalostmi organizace a jejích procesech. (Nulíček 2018)

Pověřenec pro ochranu osobních údajů musí být přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele. Toto však neznamená, že se jedná o organizační postavení. Jedná se o podmínku, kdy má pověřenec přímý přístup k vedení organizace – mezi pověřencem a vedením organizace se nenachází další mezičlánek a pověřenec se tak kdykoliv může v záležitostech ochrany osobních údajů obrátit na vedení organizace.

2.7.2.3 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů, taktéž známé pod zkratkou DPIA (Data Protection Impact Assessment) patří mezi organizační ochranná opatření, které zajišťuje soulad s *Nařízením*. Toto posouzení je povinné v případě, kdy je pravděpodobné, že zpracování osobních údajů přináší vysoká rizika pro práva a svobody fyzických osob, a to zejména při využívání nových technologií pro zpracování.

„Účelem posouzení vlivu na ochranu osobních údajů je především eliminace rizik, která vysoce rizikové zpracování pro práva a svobody subjektu údajů představují." (Žůrek 2017, s. 117)

Článek 35 Nařízení uvádí příklady, kdy je nutné provést posouzení vlivu. Jedná se o následující příklady:

- *„systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,*
- *rozsáhlé zpracování zvláštních kategorií osobních údajů uvedených v článku 9 Nařízení nebo osobních údajů týkajících se rozsudků v trestních věcech a trestních činů uvedených v článku 10 Nařízení,*
- *rozsáhlé systematické monitorování veřejně přístupných prostorů."* (Evropský parlament a Rada Evropské unie 2016, s. 53)

Lucie Staňková ve své publikaci uvádí následující: *„Proces posouzení vlivu by se měl skládat alespoň z těchto kroků:*

1. *charakteristika posuzovaného zpracování osobních údajů,*

2. *identifikace rizik pro práva a svobody subjektů údajů,*
3. *identifikace a určení vhodných opatření pro snížení rizika na přijatelnou úroveň,*
4. *dokumentace výsledků, rozhodnutí a zbytkových rizik,*
5. *aktualizace a opakování posouzení vlivu.“* (Staňková 2018, s. 127)

Dokument posouzení vlivu na ochranu osobních údajů by měl obsahovat alespoň následující náležitosti:

- *systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce,*
- *posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů,*
- *posouzení rizik pro práva a svobody subjektu údajů,*
- *plánování opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s Nařízením GDPR, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.* (Staňková 2018, s. 128)

2.8 Dozorový úřad

Článek 51 Nařízení uvádí: *„Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování tohoto nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie (dále jen „dozorový úřad“). Každý dozorový úřad přispívá k jednotnému uplatňování tohoto nařízení v celé Unii. Dozorové úřady za tímto účelem spolupracují mezi sebou.“* (Evropský parlament a Rada Evropské unie 2016, s. 65)

V České republice je dozorovým úřadem Úřad pro ochranu osobních údajů. Tento úřad dohlíží na dodržování povinností při zpracovávání osobních údajů, řeší stížnosti občanů, ale také poskytuje konzultace týkající se ochrany osobních údajů. (Obecné nařízení o ochraně osobních údajů prakticky ©)

Mezi úkoly dozorového úřadu patří dle znění Nařízení následující:

- *„monitoruje a vymáhá uplatňování nařízení,*

- *zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s článkem 80 nařízení, a ve vhodné míře prošetřuje předmět stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření,*
- *provádí šetření o uplatňování nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci.“* (Úřad pro ochranu osobních údajů ©)

Pravomoci dozorového úřadu jsou:

- *vyšetřovací* – úřad je touto pravomocí zmocněn ke kontrole zpracování osobních údajů, ale také ke kontrole ve vztahu k osvědčení o ochraně údajů či pečetí a známek;
- *nápravné* – prostřednictvím nápravné pravomoci může úřad udělovat nápravná opatření;
- *povolávací a poradní* pravomoc dává úřadu možnost poskytovat poradenství, povolovat zpracování, pokud je státem vyžadováno, schvalovat návrhy kodexů a další. (Nulíček 2018)

Kontroly dozorového úřadu spočívají především v kontrole předložených dokumentů, ale také mohou obsahovat pohovory se správcem, jeho zaměstnanci a dalšími. Ke kontrolám přistupuje úřad na základě stížností či podnětů fyzických či právnických osob, případně dle vlastního plánu kontrol. Dozorový úřad se při svých kontrolách zaměřuje nejčastěji na:

- rozsah a formu zpracovávání osobních údajů – především se zaměřuje na kategorii citlivých osobních údajů a také, zdali jsou anonymizované či předávané třetím stranám,
- evidenci a oprávněnost přístupů k osobním údajům,
- existenci souhlasů se zpracováním osobních údajů,
- náležitosti zpracovatelských smluv. (Staňková 2018)

2.9 Porušení zabezpečení

„Tímto pojmem se dle článku 4 odstavce 12 Nařízení rozumí porušení zabezpečení zpracovávaných osobních údajů, které následně vede k náhodnému nebo protiprávnímu

zničení, ztrátě nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uchovávaných nebo jinak zpracovávaných údajů. K těmto porušením může dojít jak činností zvenčí organizace, tak činností zevnitř organizace, a to jak úmyslně, tak z nedbalosti.“ (Nulíček 2018, s. 95)

Jednotlivá porušení zabezpečení je možné rozdělit do třech základních kategorií:

- *porušení důvěrnosti* – při tomto porušení se jedná o bezpečnostní incident, při kterém došlo k neoprávněnému či náhodnému poskytnutí či zpřístupnění osobních údajů,
- *porušení dostupnosti* – toto porušení označuje náhodnou či neoprávněnou ztrátu přístupu či zničení osobních údajů,
- *porušení integrity* – porušení tohoto typu představuje neoprávněné nebo náhodné pozměnění osobních údajů. (Staňková 2018)

Nařízení ukládá povinnost správcům a zpracovatelům ohlásit porušení zabezpečení osobních údajů s výjimkou porušení zabezpečení, kdy je nepravděpodobné, že by došlo k omezení práv a svobod fyzických osob.

V případě porušení zabezpečení je nutné posoudit velikost rizika. Při tomto posuzování je nutné vzít v úvahu následující:

- o jaký typ porušení se jedná,
- povahu, citlivost a objem zpracovávaných osobních údajů, u kterých došlo k porušení zabezpečení,
- snadnost identifikace jednotlivců,
- závažnost důsledků pro jednotlivce,
- zvláštní charakteristiky jednotlivce,
- počet dotčených jednotlivců, zvláštní charakteristiky správce a
- obecné zkušenosti.

V článku 33 Nařízení je dáno následující: *„Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody*

fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.“ (Evropský parlament a Rada Evropské unie 2016, s. 52)

V ohlášení porušení zabezpečení, které je zasíláno dozorovému úřadu, je nutné poskytnout následující informace:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, 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 kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení, včetně případných opatření ke zmírnění možných nepříznivých dopadů. (GDPR solutions, ©2019)

2.10 Sankce

Sankce jsou ukládány adresátům za účelem donucení chovat se podle stanovených pravidel.

Uložení sankce musí být účinné, přiměřené, ale zároveň odrazující. U každého jednotlivého případu se hodnotí okolnosti, až následně se rozhoduje o způsobu uložení postihu. Porušení zabezpečení však nemusí automaticky představovat uložení pokuty.

Pokud dozorové orgány rozhodnou, že došlo k porušení *Nařízení* a začnou přistoupí k rozhodování, zda uložit správní pokutu, případně o jakou výši pokuty by se jednalo, musejí být řádně zohledněny všechny okolnosti porušení:

- *„povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena,*
- *zda došlo k porušení úmyslně nebo z nedbalosti,*
- *kroky podniknuté ke zmírnění škod způsobených subjektům údajů,*

- *míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedených podle článku 25 a článku 32 Obecného nařízení,*
- *veškerá relevantní předchozí porušení správce či zpracovatele,*
- *míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků,*
- *kategorie osobních údajů dotčených daným porušením,*
- *způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře,*
- *v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v článku 58 odstavce 2 Obecného nařízení, splnění těchto opatření,*
- *dodržování schválených kodexů chování nebo schváleného mechanismu pro vydávání osvědčení,*
- *jakákoliv jiná přitěžující nebo polehčující okolnost, jako je finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.“* (Žůrek 2017, s. 179)

„Při ukládání pokut, případně i při jejich vyměřování, musejí dozorové úřady respektovat následující principy:

1. *Porušení nařízení by mělo mít za následek uložení rovnocenných sankcí.*
2. *Stejně jako všechna nápravná opatření zvolená dozorovými úřady by i správní pokuty měly být “účinné, přiměřené a odrazující“.*
3. *Příslušný dozorový úřad provede posouzení „v každém jednotlivém případě“.*
4. *Harmonizovaný přístup ke správním pokutám v oblasti ochrany údajů vyžaduje aktivní spolupráci dozorových úřadů a výměnu informací mezi nimi.“* (Nulíček 2018, s. 517)

Doktor Žůrek ve své publikaci následně uvádí, že místo či současně s pokutou je možné udělit také nápravná opatření. Jím uvedená opatření jsou:

- *„upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují Obecné nařízení,*

- *udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily Obecné nařízení,*
- *nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle Obecného nařízení,*
- *nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s Obecným nařízením, a to případně předepsaným způsobem ve stanovené lhůtě,*
- *nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,*
- *uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu,*
- *Nařídit opravu, výmaz nebo omezení zpracování a ohlašování takových opatření příjemcům,*
- *odebrat osvědčení nebo nařídit, aby jej subjekt oprávněný k vydávání osvědčení odebral nebo nevydal,*
- *uložit správní pokutu podle článku 83 Obecného nařízení vedle či namísto dalších nápravných opatření, podle okolností každého jednotlivého případu,*
- *nařídit přerušení toků údajů příjemci ve třetí zemi nebo mezinárodní organizaci.“* Žůrek 2017, s. 180)

Výše pokut je v *Nařízení* rozdělena do dvou skupin, a to dle porušení, kterého se správce dopustil. První skupina pokut má maximální výši pokuty 10 000 000 EUR (případně 2 % celkového ročního celosvětového obratu) a druhá skupina má maximální výši pokuty 20 000 000 EUR (případně 4 % celkového ročního celosvětového obratu). Rozdělení pokut do svou skupin odráží důležitost porušení povinností správce. Skupina s vyšší sazbou označuje porušení zabezpečení, u kterého se očekává vyšší intenzita zásahu do práv na ochranu osobních údajů. „*V nižší kategorii se například může jednat o porušení ustanovení týkají se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, zatímco ve vyšší kategorii je například zahrnuto porušení povinností upravující zásady a zákonnost zpracování, podmínku souhlasu se zpracováním osobních údajů a podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů.“* (Staňková 2018, 67)

Pro lepší přehled doktor Žůrek ve své publikaci uvádí výčet porušení, pro který bude pokuta z nižší kategorie (viz tabulka č. 1) a pro který bude pokuta z kategorie vyšší (viz tabulka č. 2).

Tab. č. 1: Výčet porušení pro pokutu z nižší kategorie

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

Zdroj: Praktický průvodce GDPR, 2017

Tab. č. 2: Výčet porušení pro pokutu z vyšší kategorie

20 000 000 EUR nebo, jde-li o podnik, 4 % z obratu za porušení:	
Správce a tam, kde připadá v úvahu i zpracovatel	zásad a zákonnosti zpracování
	podmínek vyjádření souhlasu
	podmínek pro zpracování zvláštních kategorií osobních údajů
	práv subjektu údajů
	podmínek pro předávání osobních údajů do třetích zemí

	povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které Obecné nařízení umožňuje upravit na vnitrostátní úrovni
	povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle článku 58 odstavce 2 Obecného nařízení nebo neposkytnutí přístupu v rozporu s článkem 58 odstavce 1 Obecného nařízení
	nesplnění příkazu dozorového úřadu podle článku 58 odstavce 2 Obecného nařízení (nápravné pravomoci) nebo poskytnutí přístupu při uplatnění dozorové pravomoci

Zdroj: Praktický průvodce GDPR, 2017

3 Implementace Nařízení

Tato kapitola práce se zabývá zaváděním Nařízení do organizací. V rámci této kapitoly bude představen proces implementace.

Implementaci Nařízení do organizace nelze označit jako jednoznačný proces, který ve všech organizacích probíhá stejným způsobem a má přesně daný postup.

Lucie Staňková ve své publikaci uvádí základní kroky, prostřednictvím kterých dochází k implementaci pravidel Nařízení do organizací. Zmíněné kroky v publikaci jsou následující:

1. *krok* – „*Proces provedený před zavedením Nařízení GDPR“*
2. *krok* – „*Zjištění a hodnocení hrozeb pro osobní údaje“*
3. *krok* – *„Zavádění GDPR“* (Staňková 2018, s. 18)

3.1 Proces provedený před zavedením Nařízení GDPR (1. krok)

První krok procesu se zaměřuje na analýzu současného stavu v organizaci. Zjišťuje se, zdali organizace splňuje požadavky *Nařízení* a také jakým způsobem.

V tomto kroku si organizace musí udělat jakýsi audit zpracovávání osobních údajů. V rámci tohoto auditu dochází k následujícímu:

- zjištění jaké kategorie osobní údaje organizace zpracovává,
- zjištění účelu zpracovávání osobních údajů, zdali existuje zákonný důvod zpracovávání,
- zjištění jakým způsobem a od koho jsou data získávána,
- zjištění jakým způsobem a kde jsou data uložena, ale také kdo k nim má přístup,
- zjištění samotného zpracovávání dat, tedy co se s daty děje. (Horn, ©2018)

3.2 Zjištění a hodnocení hrozeb pro osobní údaje (2. krok)

V rámci druhého kroku firma analyzuje, jaká rizika k osobním údajům existují. U všech zjištěných rizik je nutné, aby došlo k jejich eliminaci. Posuzuje se tedy, jaká je nutná provést opatření v závislosti na zjištěných rizikách. V tomto kroku také mikropodniky,

malé podniky a střední podniky hodnotí, zdali se jejich společnosti týká výjimka z povinnosti vést záznamy o činnosti zpracování. Taktéž dochází k posouzení, zdali organizace má povinnost jmenovat pověřence pro ochranu osobních údajů. V případě, že tuto povinnost organizace má, měla by jej jmenovat již v této fázi, tedy před samotným zaváděním GDPR do organizace. Pověřenec pak bude moci organizaci dávat rady k plánovaným opatřením a dohlížet, zdali zaváděné změny v organizaci budou splňovat podmínky a zásady Nařízení. (Staňková 2018)

3.3 Zavádění GDPR (3. krok)

Právě třetí krok označuje samotnou implementaci GDPR do organizace. Zavádí se opatření, která byla navrhnuta v předchozím kroku a zároveň je nutné zdokumentovat tato opatření ve formě vnitřní směrnice o ochraně osobních údajů. Tento dokument může sloužit později k prokázání, že organizace má osobní údaje dostatečně zabezpečené. V rámci implementace dohází k úpravě externí a interní dokumentace, upravují se procesy zpracování osobních údajů. Taktéž dochází k vytvoření plánu, na jehož základě se bude postupovat v případě porušení zabezpečení. (Horn, ©2018)

4 Šetření dopadů GDPR na organizace v České republice

Šetření, které je součástí práce, se zaměřuje na analýzu dopadů GDPR na organizace v České republice. Pro získání dat po posouzení dopadů bylo použito dotazníkové šetření.

4.1 Cíl dotazníkového šetření

Cílem dotazníkového šetření je vyhodnocení dopadů Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES na organizace v České republice.

4.2 Metodologie

Samotné šetření bylo realizováno online. Dotazník byl vytvořen prostřednictvím nástrojů Google Docs, konkrétně prostřednictvím Google Formulářů.
Vyhodnocování získaných dat probíhalo pomocí metod statistické analýzy.

4.3 Distribuování

Distribuování dotazníku mezi organizace proběhlo prostřednictvím e-mailů. V zaslaném e-mailu byly organizace seznámeny s účelem dotazníkového šetření a také osloveny s žádostí o vyplnění dotazníku. Dotazník byl spuštěn od 15. února 2019 do 15. března 2019.

4.4 Respondenti

Po dobu, kdy byl dotazník otevřen, byly získány odpovědi od 223 respondentů. Respondenty jsou podnikatelské subjekty a organizace z České republiky.

4.5 Struktura dotazníku

Použité dotazníkové šetření má strukturovanou formu. Tento typ dotazníku je vyznačen tím, že otázky v něm jsou stanoveny v pevném pořadí. Respondenti tedy museli odpovídat na otázky tak, jak jim byly předloženy a nemohli přeskakovat na různé sekce dotazníku.

Dotazník, který je použit pro výzkum v této práci obsahuje následující typy otázek:

- *otevřené otázky* – v těchto otázkách má respondent prostor k vlastnímu vyjádření k dané otázce;
- *polouzavřené otázky* – pro tyto otázky je typické, že je respondentovi položena uzavřená otázka a následně je požádán o další dovysvětlení, případně se může jednat o typ otázek, které ve svých možnostech umožňují respondentovi označit možnost „jiné“ a mohou dopsat svou vlastní odpověď;
- *uzavřené otázky* – v těchto otázkách má respondent možnost zvolit pouze jednu z nabízených možností. Dotazník obsahuje dva typy uzavřených otázek tedy otázky dichotomické, kdy respondent vybírá ze dvou nabízených odpovědí (nejčastěji z možnosti ano či ne), a také otázky polytomické, ve kterých je respondentovi nabízeno k výběru několik variant. (Eger a Egerová 2017)

Dotazníkové šetření je rozčleněno na více oddílů, ale ve své struktuře odpovídá základní struktuře dotazníku, kterou popisují ve své publikaci Ludvík Eger a Dana Egerová. Základní strukturu dotazníku tvoří:

- *vstupní či úvodní část* – v této části je respondent osloven a informován o účelu výzkumu a taktéž tato část obsahuje žádost o vyplnění dotazníku.
- *Druhá část obsahuje vlastní otázky* – jsou zjišťovány informace, které jsou předmětem šetření, ale také jsou v této části zjišťovány identifikační údaje.
- Poslední částí ve struktuře dotazníku je *závěrečná část/konec dotazníku* – tato část obsahuje poděkování respondentovi. (Eger a Egerová 2017)

Použité dotazníkové šetření pro výzkum dopadů GDPR na organizace v České republice má následující strukturu:

- V ***úvodní části*** šetření je respondent osloven a informován o použití získaných dat a také je zde uvedena samotná žádost o vyplnění dotazníku
- ***Hlavní část*** dotazníku, tedy část obsahující vlastní otázky týkající se šetření, je rozdělena do osmi oddílů. Každý oddíl je zaměřen na určitou problematiku. Oddíly použité v dotazníku jsou následující:

- *Informace o organizaci I.* – jedná se o první oddíl, ve kterém respondent uvádí informace o organizaci, konkrétně tento oddíl se zabývá právní formou organizace.
- *Informace o organizace II.* – v tomto oddílu respondent specifikuje typ organizace a čím se organizace zabývá. Taktéž v tomto oddíle označí velikost organizace a jaké kategorie osobních údajů organizace zpracovává.
- *Implementace GDPR* – tento oddíl se týká již samotné implementace GDPR v organizaci. Respondent zde uvádí délku přípravy na GDPR, způsob přípravy, uskutečněné změny pro splnění povinnosti *Nařízení* a náklady, které musely vynaložit pro plnění povinností a zásad.
- *Nabídky konzultačních společností* – v tomto oddíle jsou od respondenta zjišťovány informace, zdali získal nabídky od konzultačních firem na zavádění GDPR do organizace a co je ovlivnilo při volbě spolupráce s konzultační společností.
- *Komplikace při implementaci GDPR* – v této části dotazníku respondent uváděl, zdali ve vyskytly při implementaci změn do organizace nějaké komplikace.
- *Pověřenec pro ochranu osobních údajů* – v případě, že společnost má pověřence, v tomto oddíle se zjišťuje, kolik se vynakládá na jeho činnost.
- *Ohlašovací povinnost při porušení zabezpečení* – jak již název oddílu napovídá, respondent je v tomto oddíle dotazován na porušení zabezpečení.
- V poslední sekci je respondent dotázán na jeho pracovní pozici v organizaci.

- *Závěrečná část* dotazníku dává respondentovi prostor pro jeho připomínky případně další doplňující informace, které by chtěl respondent zmínit a poté následuje již jen poděkování za jeho spolupráci.

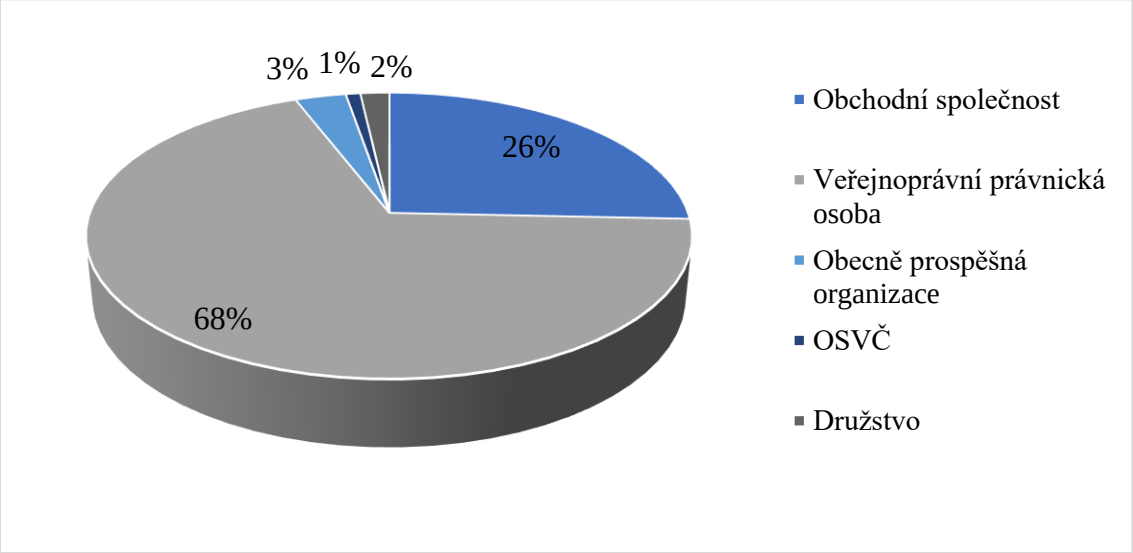
5 Analýza a vyhodnocení dotazníkového šetření

V předchozí části již byla popsána struktura dotazníku. Tato část práce se zaměřuje na analýzu získaných dat. Pro lepší přehlednost je analýza dotazníkového šetření rozdělena do několik částí.

5.1 Právní forma a typy respondentů

Z analýzy vyplývá, kdy byla zjišťována právní forma organizace respondentů, vyplývá, že největší počet respondentů jsou veřejnoprávní právnické osoby, které tvoří 68 % z respondentů. Mezi další respondenty patří obchodní společnosti (26 %), obecně prospěšné organizace (3 %), OSVČ (1 %) a také družstva (2 %).

Obrázek č. 2:Právní forma organizace

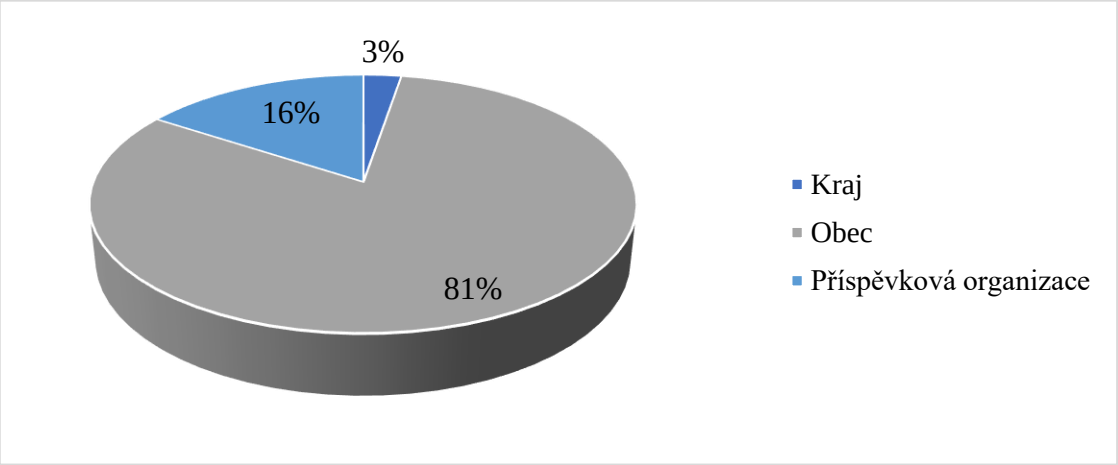


Zdroj: Vlastní zpracování, 2019

Na obrázku č. 2 je uvedeno zastoupení veřejnoprávních právnických osob. Respondenti, kteří jsou z této kategorie, jsou nejčastěji obce, z celkového počtu veřejnoprávních právnických osob se jedná o 81 %. Dalšími respondenty jsou příspěvkové organizace (16 %), ale také kraje, ačkoliv tvoří pouze 3 %.

Příspěvkové organizace jsou v šetření zastoupeny základními školami.

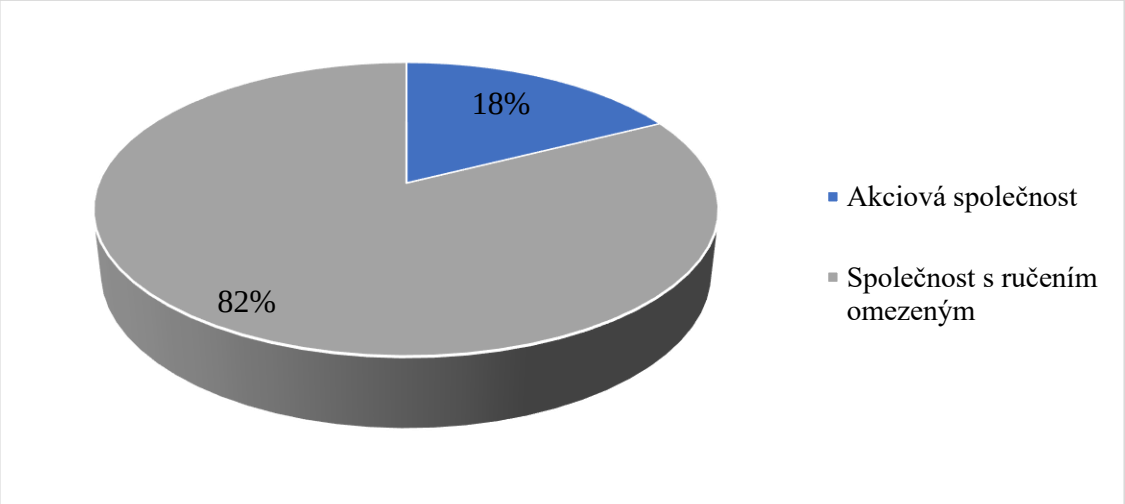
Obrázek č. 3: Zúčastněné veřejnoprávní právnické osoby



Zdroj: Vlastní zpracování, 2019

Následný obrázek č. 3 pak zobrazuje zastoupení obchodních společností, které se šetření zúčastnily. Především se jedná o společnosti s ručením omezeným (82 %), následně pak akciové společnosti (18 %).

Obrázek č. 4: Zúčastněné obchodní společnosti

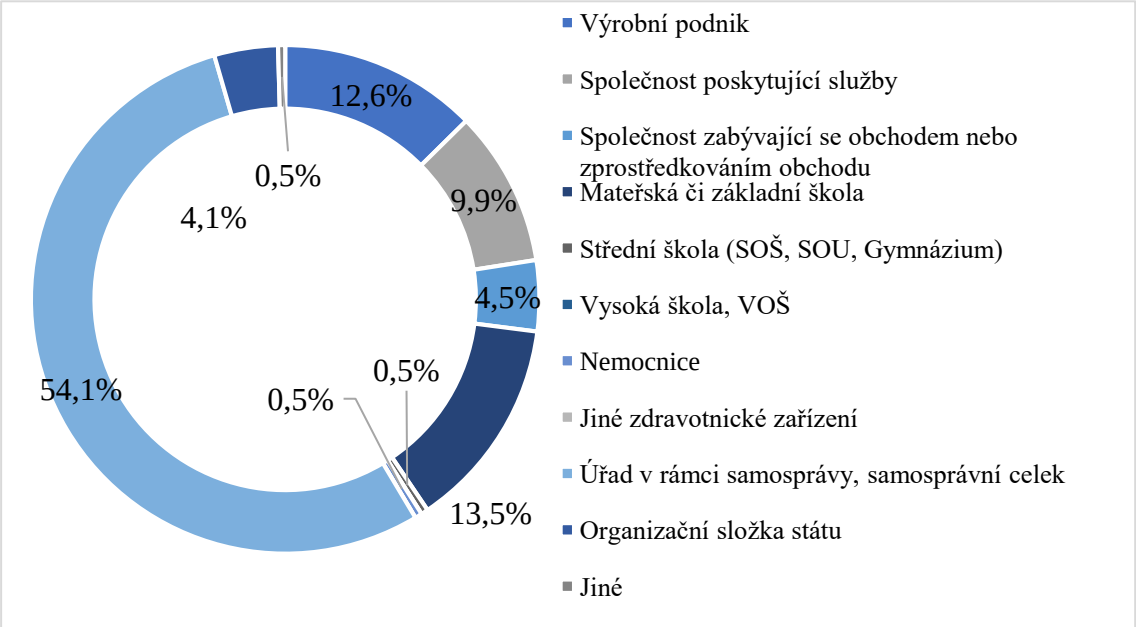


Zdroj: Vlastní zpracování, 2019

Typy organizací, které se zúčastnily dotazníkového šetření jsou zobrazeny na obrázku č. 4. Nejčastěji se dotazníkového šetření zúčastnily úřady v rámci samosprávy či samosprávní celky (54,1 %), základní školy (13,5 %) a výrobní podniky (12,6 %). Dále jsou v šetření zastoupeny společnosti poskytující služby (9,9 %), společnosti zabývající se obchodem či jeho zprostředkováním (4,5 %), organizační složky státu (4,1 %), ale také

střední školy (0,5 %), nemocnice (0,5 %). Z obrázku je patrné, že v dotazníkovém šetření respondenti označili i možnost jiné. Respondent uvedl, že typ jeho organizace je školské zařízení pro děti s nařízenou ústavní výchovou.

Obrázek č. 5: Typy organizací účastnící se šetření



Zdroj: Vlastní zpracování, 2019

5.2 Velikost organizací respondentů

Respondenti dále uváděli velikost své organizace. Na výběr měli z následujících možnosti:

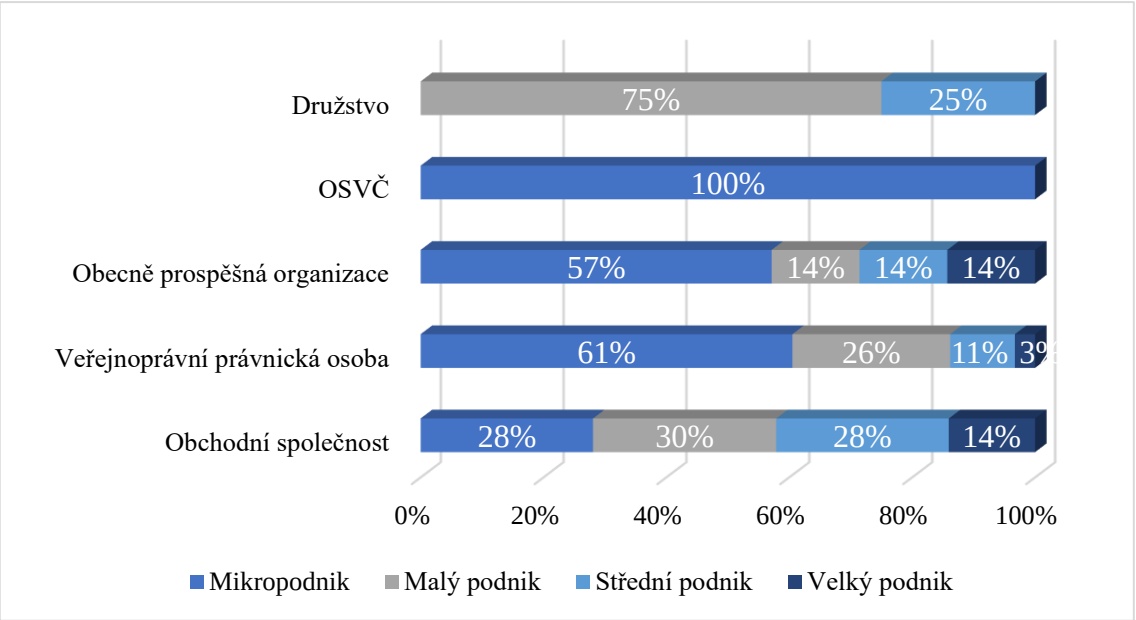
- MIKROPODNIK – organizace zaměstnávající méně než 10 zaměstnanců;
- MALÝ PODNIK – zaměstnává méně než 50 zaměstnanců;
- STŘEDNÍ PODNIK – zaměstnává méně než 250 zaměstnanců;
- VELKÝ PODNIK – má více než 250 zaměstnanců. (Veber a Srpová 2012)

Z šetření vyplývá, že nejčastěji se šetření zúčastnily organizace velikosti mikropodniků, celkem 51 %. Další nejvíce zastoupenou kategorií jsou malé podniky, a to z 27 %. Střední podniky jsou zastoupeny z 15 % a velké podniky pouze ze 6 %.

Na obrázku č. 5 si je následně možné prohlédnout zastoupení velikosti organizace v závislosti na právní formě organizace. Z obrázku je patrné, že družstva jsou zastoupena pouze malými a středními velikostmi. Osoby samostatně výdělečně činné se řadí do

mikropodniků. Naopak veřejnoprávní právnické osoby jsou již zastoupené všemi velikostmi organizací a taktéž je tomu u společností obchodních.

Obrázek č. 6: Podíl velikosti organizací v závislosti na typu organizace



Zdroj: Vlastní zpracování, 2019

5.3 Zpracovávané osobní údaje

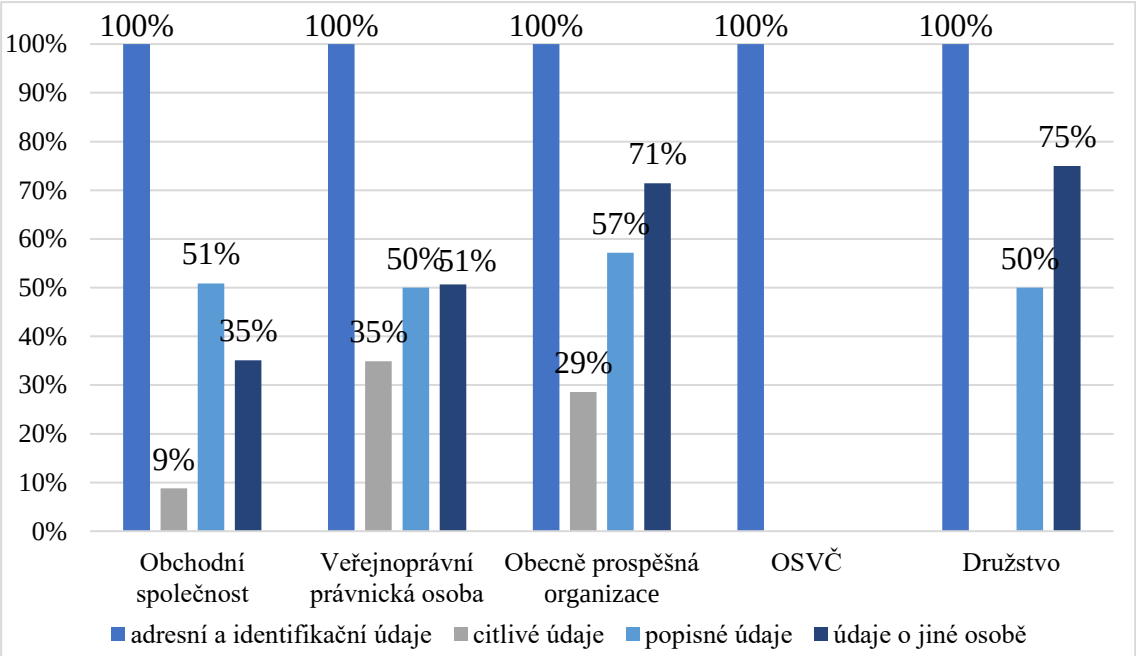
Již v předchozí části práce byly představeny osobní údaje a kategorie, na které je možné je rozlišovat. V rámci šetření byli respondenti dotazováni, které z kategorií jejich organizace zpracovává. Na obrázku č. 6 jsou následně zobrazeny jednotlivé kategorie osobních údajů v závislosti na typu organizace. Z obrázku je patrné, že všechny typy organizací zpracovávají adresní a identifikační údaje. Tento stav byl však již předpokládán před šetřením, neboť každá organizace zpracovává alespoň jméno, příjmení, adresu a kontakt na svého zaměstnance.

Nejméně často organizace zpracovávají citlivé údaje (respondenti typu OSVČ a družstva tyto údaje nezpracovávají vůbec). Nejvíce kategorii citlivých údajů zpracovávají veřejnoprávní právnické osoby (35 %), dále pak obecně prospěšné organizace (29 %) a následně společnosti obchodní (9 %).

Další často zpracovávanou kategorií osobních údajů jsou údaje o jiné osobě. Tyto údaje nejčastěji zpracovávají družstva (75 %) a obecně prospěšné organizace (71 %). Méně často tyto údaje zpracovávají veřejnoprávní právnické osoby (51 %) a obchodní společnosti (35 %). Respondenti typu OSVČ uvedli, že tyto údaje nezpracovávají.

Taktéž popisné údaje jsou relativně často zpracovávanou kategorií. Přibližně polovina respondentů že všech typů organizací, kromě OSVČ, tyto údaje zpracovává.

Obrázek č. 7: Typy zpracovávaných osobních údajů v závislosti na typu organizace



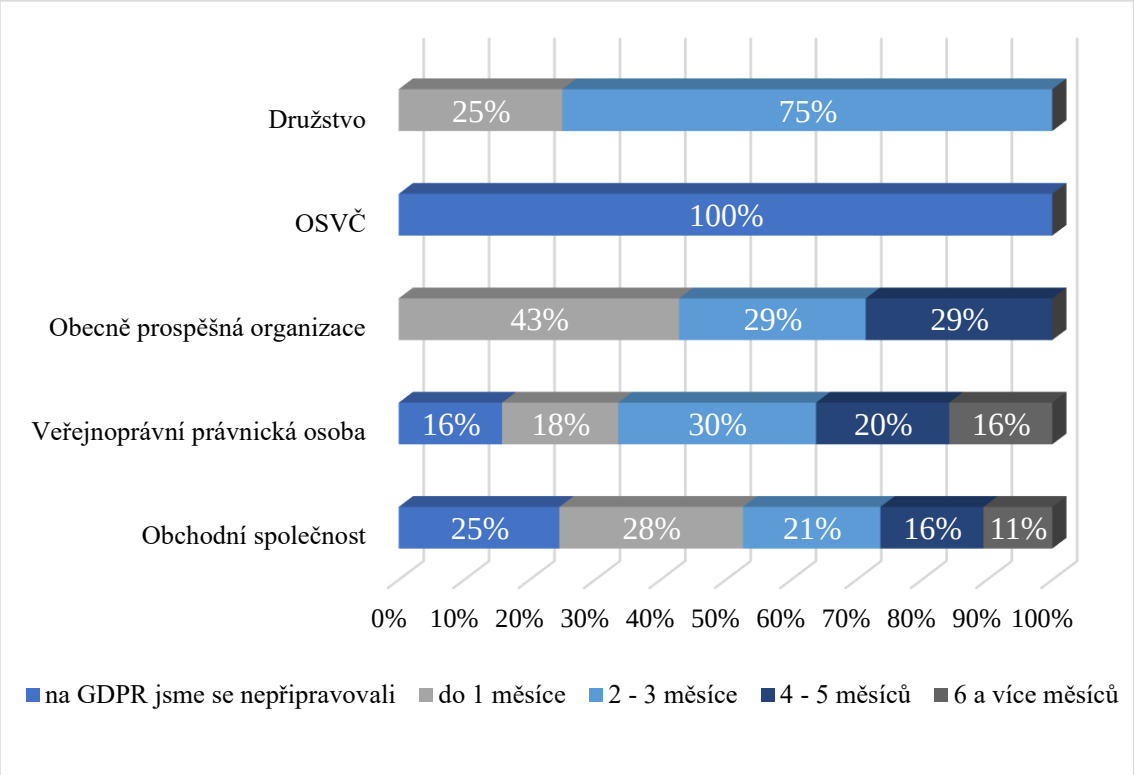
Zdroj: Vlastní zpracování, 2019

Po zjišťování základních informací o organizacích, které se dotazníkového šetření zúčastnily, následovalo zjišťování informací o samotné implementaci změn v rámci organizací.

5.4 Doba přípravy organizací na GDPR

Nejprve se šetření zaměřilo na očekávanou dobu přípravy na GDPR. Nejprve byla očekávaná doba přípravy analyzována v závislosti na velikosti organizace. Tuto dobu pro jednotlivé typy organizací zobrazuje obrázek č. 7. Z tohoto obrázku je patrné, že osoby samostatně výdělečně činné očekávali nulovou přípravu (označily odpověď, že se na GDPR nepřipravovali). Taktéž nulovou přípravu očekávalo 16 % veřejnoprávních právnických osob a 25 % obchodních společností.

Obrázek č. 8: Očekávaná doba přípravy v závislosti na typu organizace

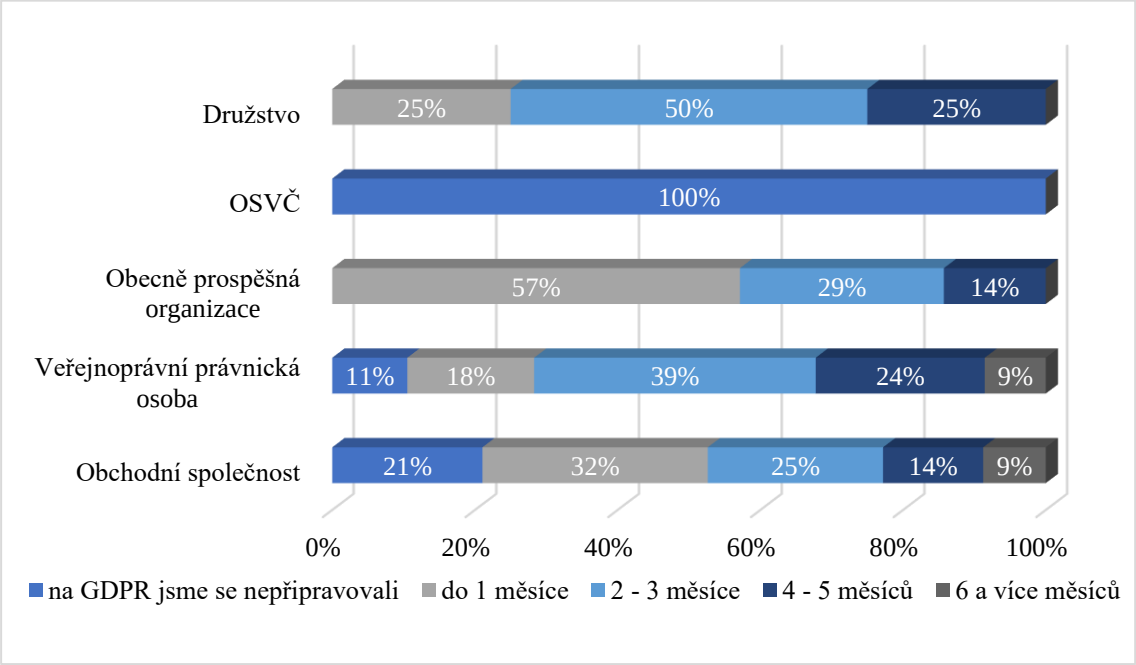


Zdroj: Vlastní zpracování, 2019

V rámci analýzy došlo k porovnání očekávané doby přípravy se skutečnou dobou přípravy v závislosti na právní formě organizace. Skutečné náklady jsou pak zobrazeny na obrázku č. 8.

V porovnáním s očekávanou dobou přípravy došlo k mírným změnám. Snížilo se množství respondentů, které se na GDPR vůbec nepřipravovali (u veřejnoprávní právnické osoby ze 16 % na 11 % a u obchodní společnosti z 25 % na 21 %), ačkoliv by se očekávalo, že pokles bude ve větším množství. To, že se společnosti na GDPR nepřipravovali by mohlo značit, že již před tím, než *Nařízení* vešlo v platnost, společnosti měly osobní údaje dostatečně zabezpečené a nemusely tak zavádět další dodatečné úpravy. Také je však možné, že společnosti, které se na GDPR nepřipravovaly, považovaly tuto aktivitu nadbytečnou a nechtěly provádět dodatečné úpravy pro zabezpečení osobních údajů, které zpracovávají. Pokud tomu tak je, je pravděpodobné, že právě u těchto společností, které nedodržují zásady *Nařízení* GDPR, může dojít k porušení zabezpečení zpracovávaných údajů.

Obrázek č. 9: Skutečná doba přípravy v závislosti na typu organizace



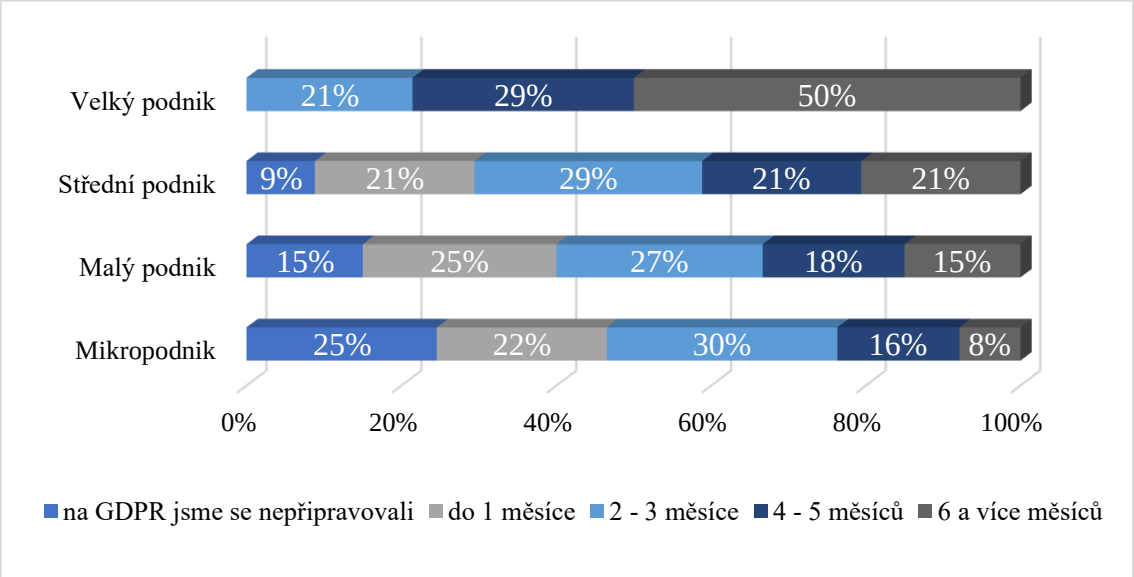
Zdroj: Vlastní zpracování, 2019

Při analýze doby přípravy došlo k analyzování jak očekávané, tak skutečné doby přípravy v závislosti na velikosti organizace.

Na obrázku č. 9 je očekávaný doba přípravy v závislosti na velikosti organizace. Nejdelší očekávanou dobu přípravy, tedy 6 a více měsíců, očekávaly velké podniky (50 %), což se předem očekávalo, neboť právě velké organizace zpracovávají velké množství osobních údajů. Avšak také ostatní velikosti organizací očekávaly takto dlouhou přípravu na GDPR. U středních podniků se jednalo o 21 %, u malých podniků 15 % a u mikropodniků 8 %.

Z průzkumu vyplývá, že organizace, které uvedly, že se na GDPR nepřipravovaly, tedy očekávaly nulovou přípravu, jsou nejčastěji mikropodniky (25 %), následně malé podniky (15 %) a střední podniky (9 %).

Obrázek č. 10: Očekávaná doba přípravy v závislosti na velikosti organizace



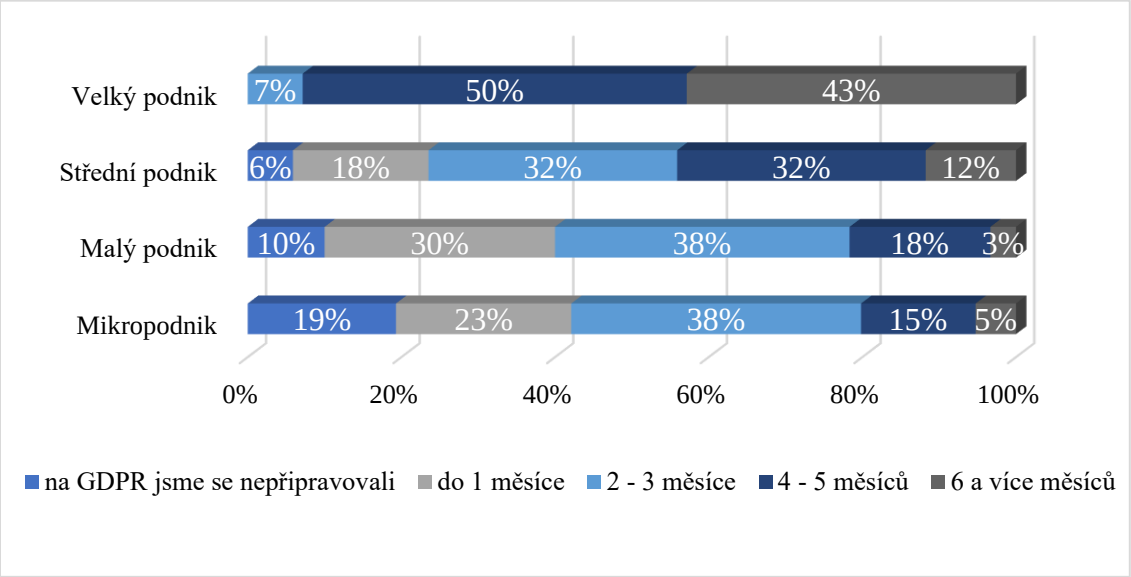
Zdroj: Vlastní zpracování, 2019

Taktéž v případě závislosti doby přípravy na velikosti organizace došlo v rámci analýzy šetření k porovnání očekávané doby s dobou skutečnou.

Z obrázku č. 8 je patrné, že došlo ke snížení počtu respondentů, kteří se ve skutečnosti na GDPR nepřipravovali. U mikropodniků došlo ke snížení z 25 % na 19 %, u malých podniků došlo ke snížení z 15 % na 10 % a u středních podniků z 9 % na 6 %.

Z analýzy také vyplývá mírná změna u všech velikostí organizací v porovnání s očekávanou dobou přípravy. Velké organizace se nejčastěji připravovaly na GDPR 4–5 měsíců (50 %). Taktéž střední organizace se z větší části připravovaly na GDPR 4–5 měsíců (32 %). Pro malé organizace byla nejčastější doba přípravy 2–3 měsíce (38 %) a stejnou dobu přípravy nejčastěji označily také mikro organizace (38 %).

Obrázek č. 11: Skutečná doba přípravy v závislosti na velikosti organizace



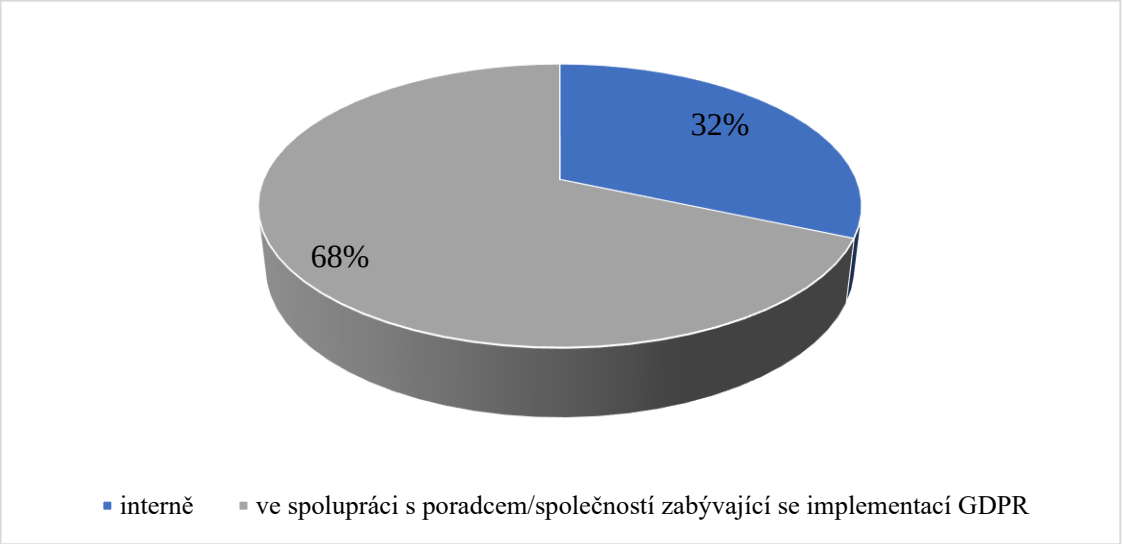
Zdroj: Vlastní zpracování, 2019

5.5 Příprava organizací na GDPR

Pro přípravy na GDPR případně pro implementaci změn v rámci organizací mohli společnosti využít služeb konzultačních společností, případně samotných konzultantů. Z uskutečněného výzkumu vyplývá, že tuto možnost zvolilo 68 % respondentů. Pouze 32 % respondentů se připravovalo na GDPR pouze interně.

Jako dodatek respondenti často uváděli jako přípravu na GDPR účast na školení, které je alespoň teoreticky připravilo na to, co se musí v rámci organizace uskutečnit, aby došlo k dodržování zásad *Nařízení*, případně jak postupovat při implementaci potřebných změn.

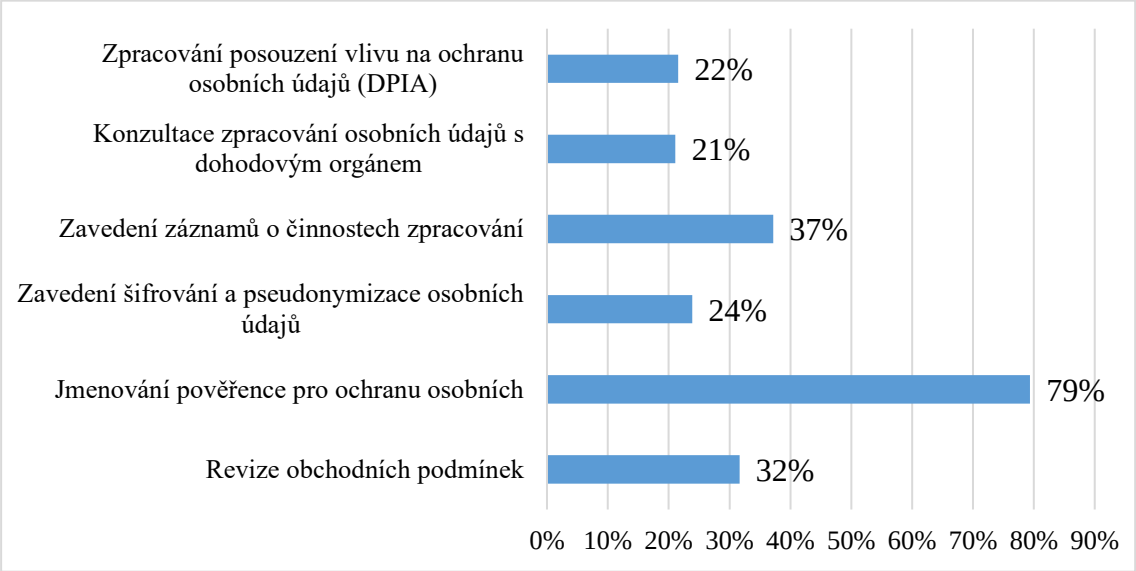
Obrázek č. 12: Příprava na GDPR



Zdroj: Vlastní zpracování, 2019

V rámci přípravy na GDPR museli organizace uskutečnit některé změny, které vedly k dodržování zásad a povinností uváděných v *Nařízení*. Mezi nejčastěji označovanou odpovědí respondentů na změny, které uskutečnily v rámci implementace GDPR, bylo jmenování pověřence pro ochranu osobních údajů (tuto změnu uskutečnilo 79 % respondentů). 22 % respondentů uvedlo, že zpracovávali posouzení vlivu na ochranu osobních údajů, tzv. DPIA. 21 % respondentů konzultovalo zpracovávání osobních údajů s dozorovým orgánem. 37 % organizací zavedlo záznamy o zpracování osobních údajů. 24 % respondentů zavedlo šifrování či pseudonymizaci osobních údajů a 32 % respondentů zrevidovalo obchodní podmínky v rámci organizací.

Obrázek č. 13: Uskutečněné změny v rámci implementace GDPR



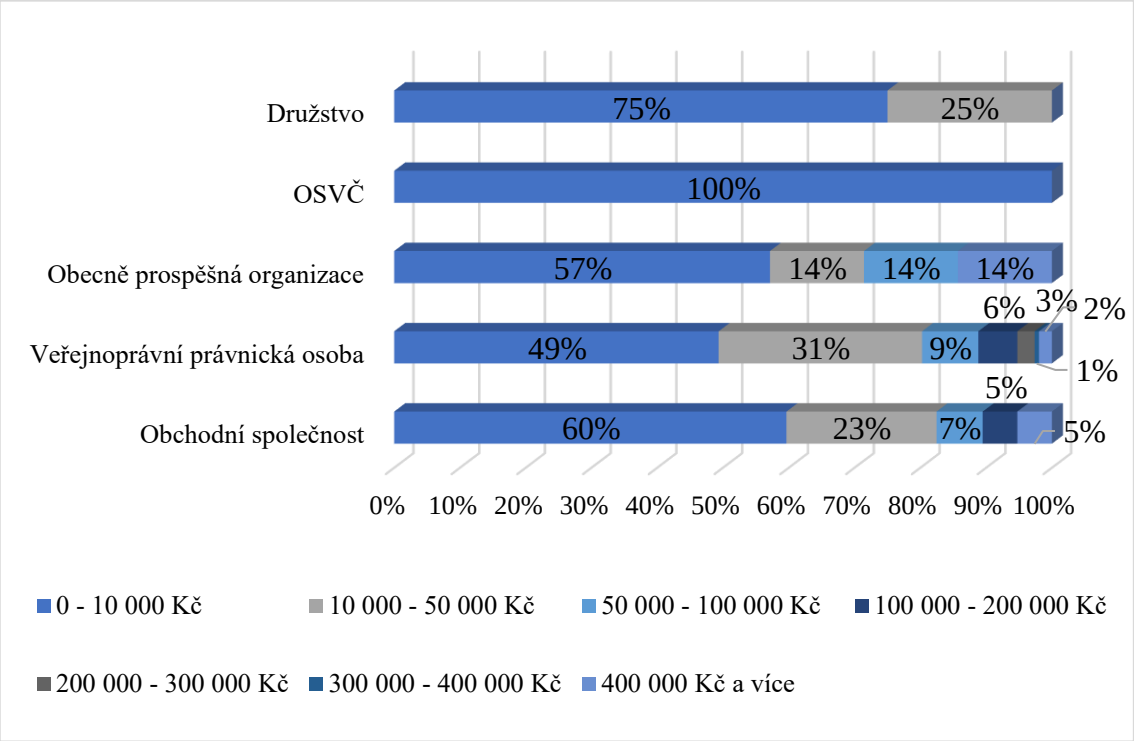
Zdroj: Vlastní zpracování, 2019

5.6 Náklady na GDPR

Na přípravu a uvedení v souladu všechny zásady a povinnosti uvažovaly společnosti určitou výši nákladů, kterou budou muset do této přípravy vložit. V rámci dotazníkového šetření docházelo ke zjišťování těchto očekávaných nákladů, ale následně také nákladů skutečně vynaložených.

V následném vyhodnocování výsledků šetření došlo k analyzování očekávaných nákladů v závislosti na právní formě organizace, přičemž konečné výsledky analýzy jsou shrnuty na obrázku č. 12. Z tohoto obrázku je patrné, že všechny typy organizací nejčastěji očekávaly náklady v rozmezí 0 – 10 000 Kč. Z družstev tyto náklady očekávalo 75 % respondentů, u OSVČ se jednalo o 100 % respondentů, u obecně prospěšných organizací 57 %, u veřejnoprávních právnických osob 49 % a u obchodních společností 60 %.

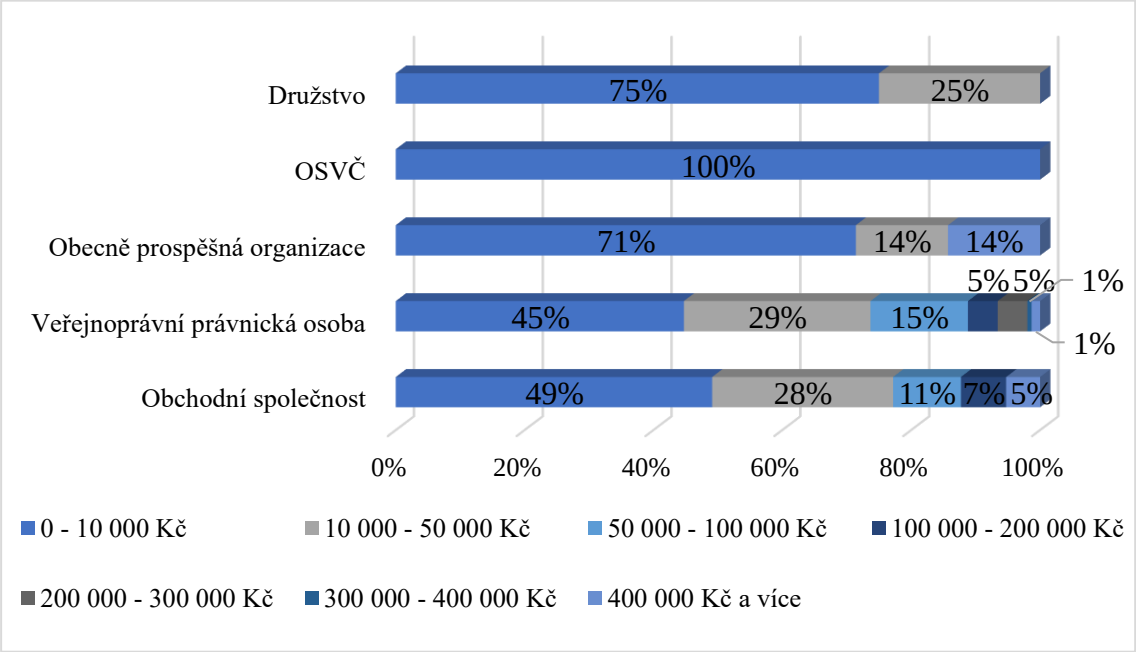
Obrázek č. 14: Očekávané náklady v závislosti na typu organizace



Zdroj: Vlastní zpracování, 2019

Po porovnávání očekávaných a skutečně vynaložených nákladů je však patrné, že došlo k mírným změnám. I u skutečně vynaložených nákladů je nejčastější rozmezí 0 – 10 000 Kč, jak je vidět na obrázku č. 13. Náklady do 10 000 Kč zůstaly stejně o družstva (tedy 75 %) a u OSVČ (100 %). U obecně prospěšných organizací náklady do 10 000 Kč vynaložilo 71 % z respondentů (oproti očekávaným 57 %), u veřejnoprávních právnických organizací 45 % (oproti 49 %) a u obchodních společností 49 % (oproti 60 %).

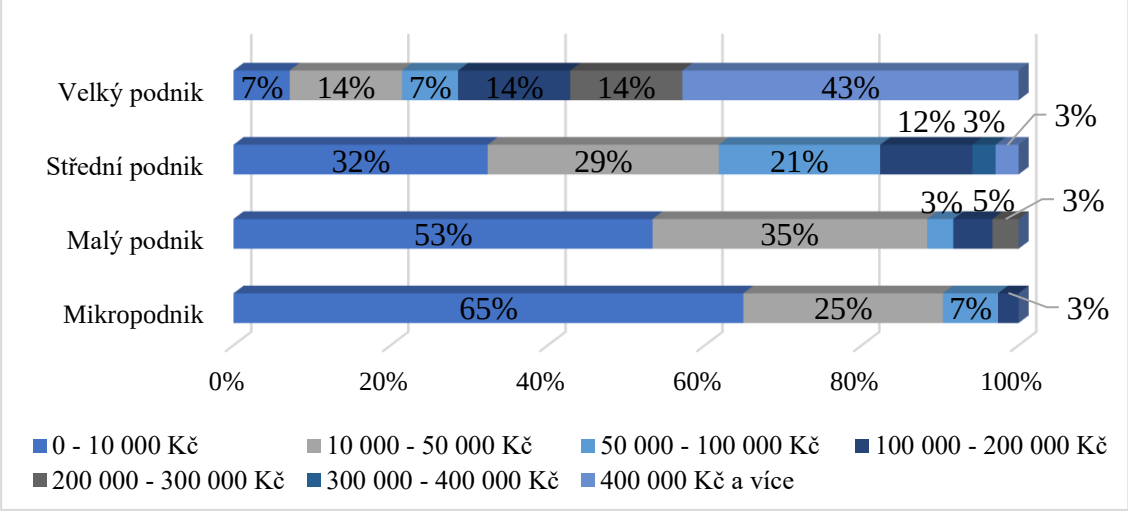
Obrázek č. 15: Skutečné náklady v závislosti na typu organizace



Zdroj: Vlastní zpracování, 2019

V rámci analyzování dotazníkového šetření však nebyly náklady analyzovány pouze v závislosti na právní formě organizace, ale také v závislosti na velikosti organizace. Nejrozličnější odpovědi v rámci očekávaných nákladů byly od respondentů z velkých organizací. Tyto organizace nejčastěji očekávaly náklady ve výši 400 000 a výše (43 %). Ostatní velikosti organizací nejčastěji očekávaly náklady ve výši 0 – 10 000 Kč – střední organizace 32 %, malé organizace 53 % a mikro organizace 65 %.

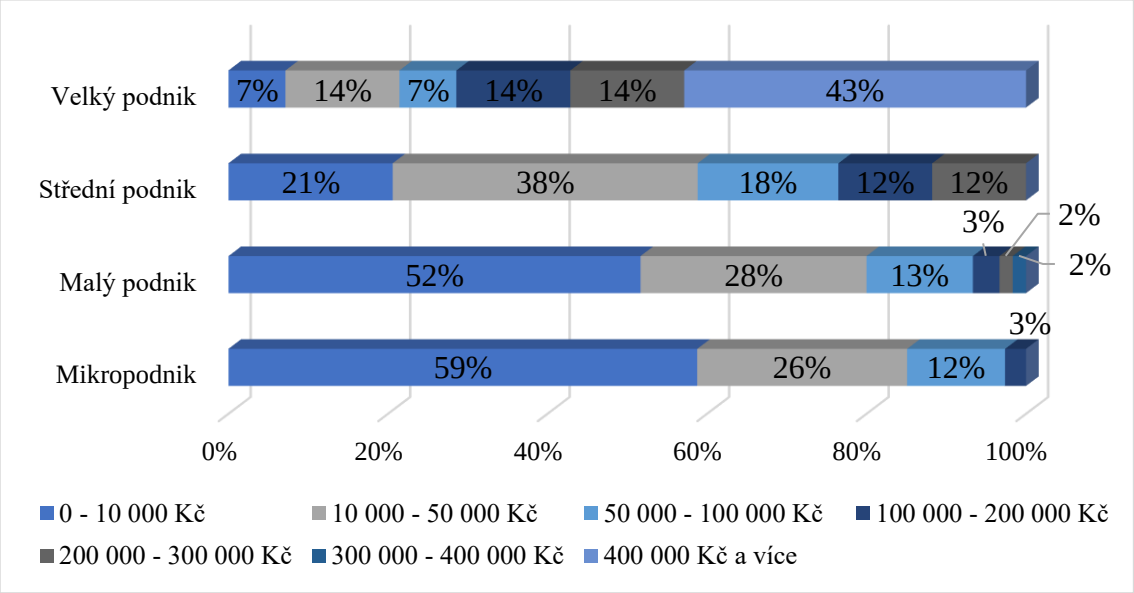
Obrázek č. 16: Očekávané náklady v závislosti na velikosti organizace



Zdroj: Vlastní zpracování, 2019

I v případě závislosti nákladů na velikosti organizace došlo k porovnání očekávaných nákladů a náklady skutečnými. V případě velkých organizací se očekávané a skutečné náklady nelišily, tedy poměry jednotlivých odpovědí respondentů jsou. K mírným změnám došlo u středních organizací, kdy ve skutečnosti největší množství respondentů vynaložilo náklady v rozmezí 10 000 – 50 000 Kč (38 %). U malých organizací došlo k největším změnám v rámci skutečně vynaložených nákladů. 52 % respondentů vynaložilo náklady v rozmezí 0 – 10 000 Kč, 28 % v rozmezí 10 000 – 50 000 Kč, 13 % v rozmezí 50 000 – 100 000 Kč, 3 % v rozmezí 100 000 – 200 000 Kč, 2 % v rozmezí 200 000 – 300 000 Kč a 2 % vynaložilo náklady ve výši 400 000 Kč a výše.

Obrázek č. 17: Skutečné náklady v závislosti na velikosti organizace

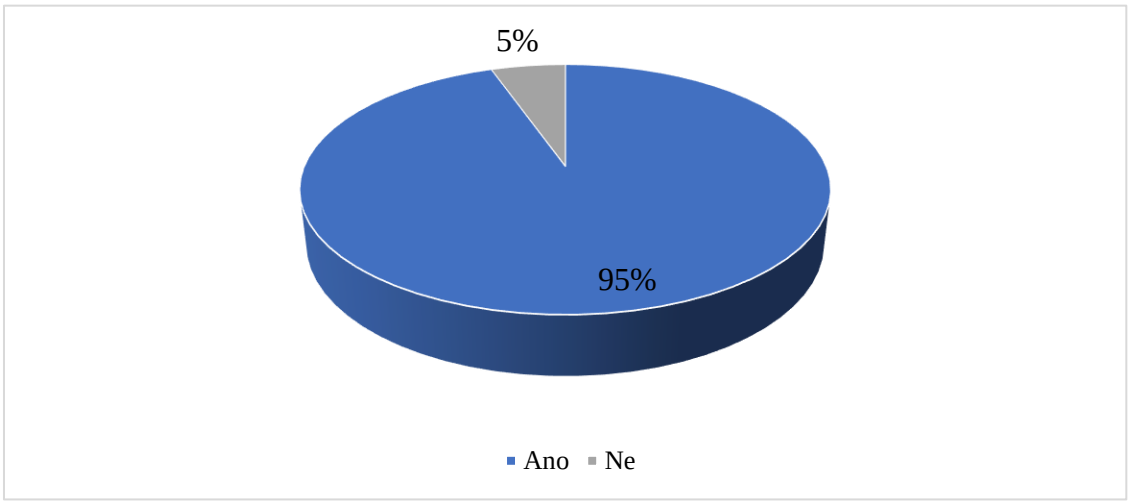


Zdroj: Vlastní zpracování, 2019

5.7 Konzultační společnosti

V době, kdy se blížila účinnost Nařízení, tedy 28. května 2018, se na trhu objevila spousta konzultačních společností a mnoho poradců, kteří společnostem nabízeli pomoc při analýze zpracovávaných údajů v organizaci a při následné implementaci změn pro dosažení souladu s Nařízením. V rámci dotazníkového šetření vyplývá, že 95 % respondentů bylo osloveno s nabídkou spolupráce od konzultační společnosti (viz obrázek č. 16).

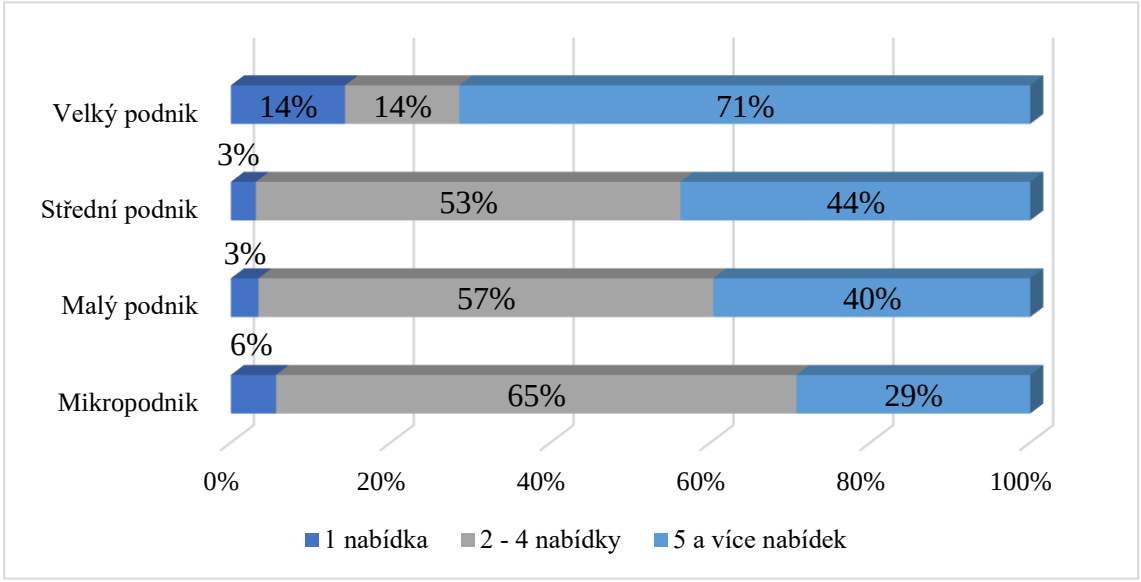
Obrázek č. 18: Nabídky konzultačních společností



Zdroj: Vlastní zpracování, 2019

Nabídky konzultačních společností jsou analyzovány v závislosti na velikosti organizací. Ze získaných dat vyplývá, že nabídky od konzultačních společností obdržely všechny velikosti organizací, viz obrázek č. 17. U velkých organizací se nejčastěji jednalo o 5 a více nabídek (71 %). U ostatních velikostí organizací se jednalo přibližně o 2–4 nabídky (mikro organizace 65 %, malé organizace 57 %, střední organizace 53 %).

Obrázek č. 19: Počet nabídek konzultačních společností v závislosti na velikosti organizace

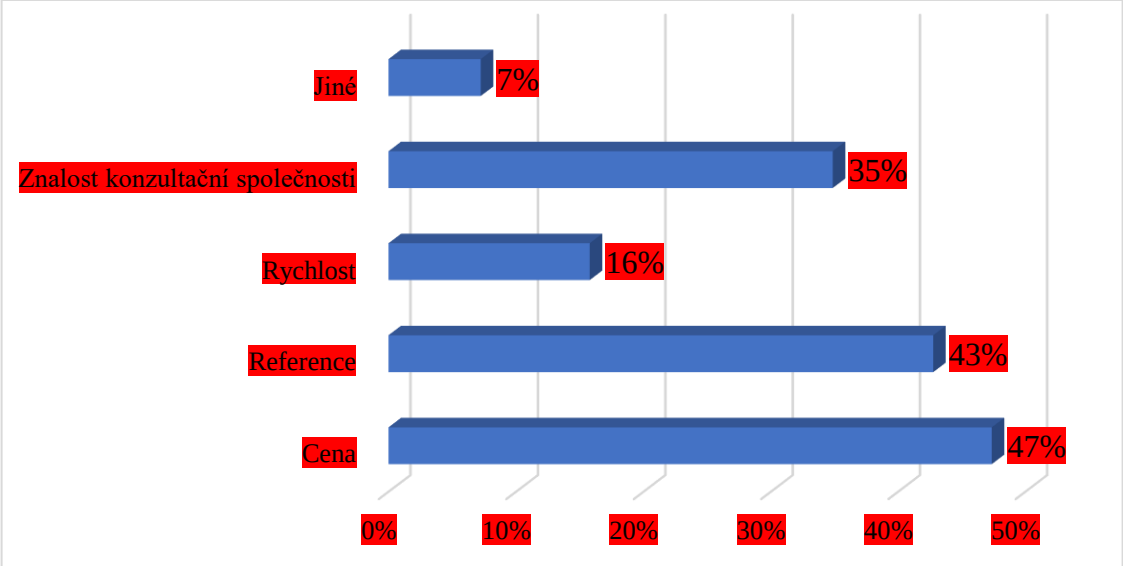


Zdroj: Vlastní zpracování, 2019

V případě, že se organizace rozhodly o využití služeb konzultantů, měly možnost si vybrat z již obdržených nabídek, ale také si mohly vyhledat konzultanty jiné. Při výběru

respondenty nejčastěji ovlivnila cena za nabízené služby (47 %) jak je zobrazeno na obrázku č. 19. Taktéž často volbu konzultační společnosti ovlivnily její reference (43 %) a případná znalost jednotlivých společností (35 %). Některé základní školy, které jsou zřizovány obcemi, v šetření uvedly, že výběr konzultační společnosti byl dán právě jejich zřizovatelem.

Obrázek č. 20: Faktory ovlivňující výběr konzultační společnosti

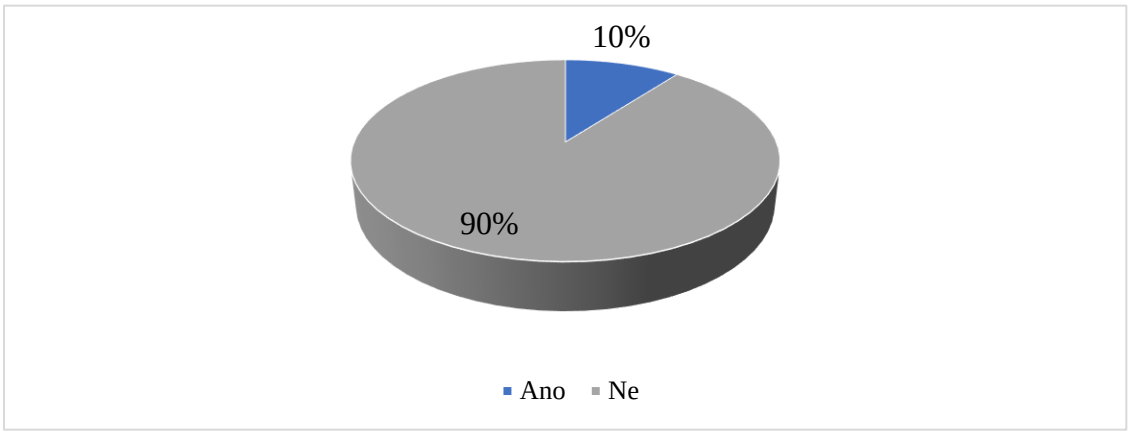


Zdroj: Vlastní zpracování, 2019

5.8 Komplikace při implementaci GDPR

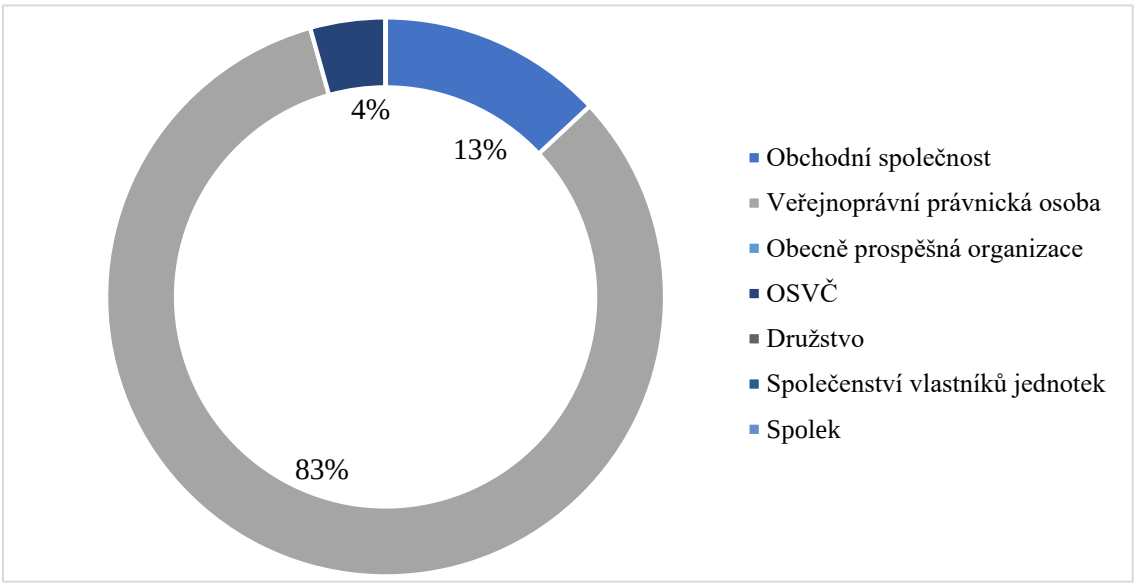
Při zavádění GDPR do organizace je nutné mít na paměti, že se mohou vyskytnout různé komplikace, které mohou implementaci ovlivnit. 90 % respondentům se podle získaných informací komplikace vyhnuly (viz obrázek č. 20). Zbylých 10 % respondentů v šetřen uvedlo, že se při implementaci GDPR do jejich organizací vyskytly komplikace. Z analýzy získaných dat následně vyplynulo, že nejčastěji se komplikace vyskytly u veřejnoprávních právnických osob (viz graf č. 21).

Obrázek č. 21: Výskyt komplikací při implementaci GDPR



Zdroj: Vlastní zpracování, 2019

Obrázek č. 22: Výskyt komplikací

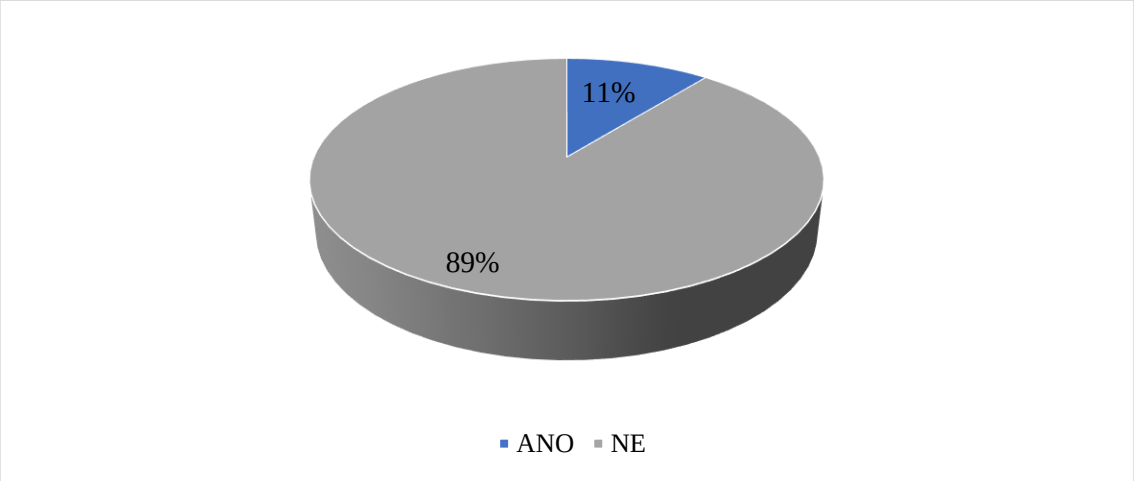


Zdroj: Vlastní zpracování, 2019

V dotazníkovém šetření měli respondenti možnost také uvést, o jaké komplikace se jednalo. Jako nejčastější komplikaci uváděli časovou náročnost, která je nutná pro uvedení zpracovávání osobních údajů v souladu s *Nařízením* do organizace. Nejen však časová zátěž byla velmi častá, ale také administrativní zátěž, která s GDPR vzrůstá. Mezi dalšími byla také uvedena nutnost stavebních úprav pro fyzické zabezpečení osobních údajů či například nedostatečná podpora státních orgánů

Pokud by organizace měly zavádět GDPR znovu s tím, že teď už ví, co tato implementace obnáší, 89 % respondentů by postupovalo stejným způsobem jako doposud. Zbylých 11 % respondentů by v případě znovuzavádění GDPR zvolilo jiný přístup. Jako nejčastější obměnu při znovuzavádění respondenti uvedli rozhodnutí zavádět GDPR do organizace bez pomoci konzultační společnosti.

Obrázek č. 23: Volba jiného přístupu k zavádění GDPR do organizace

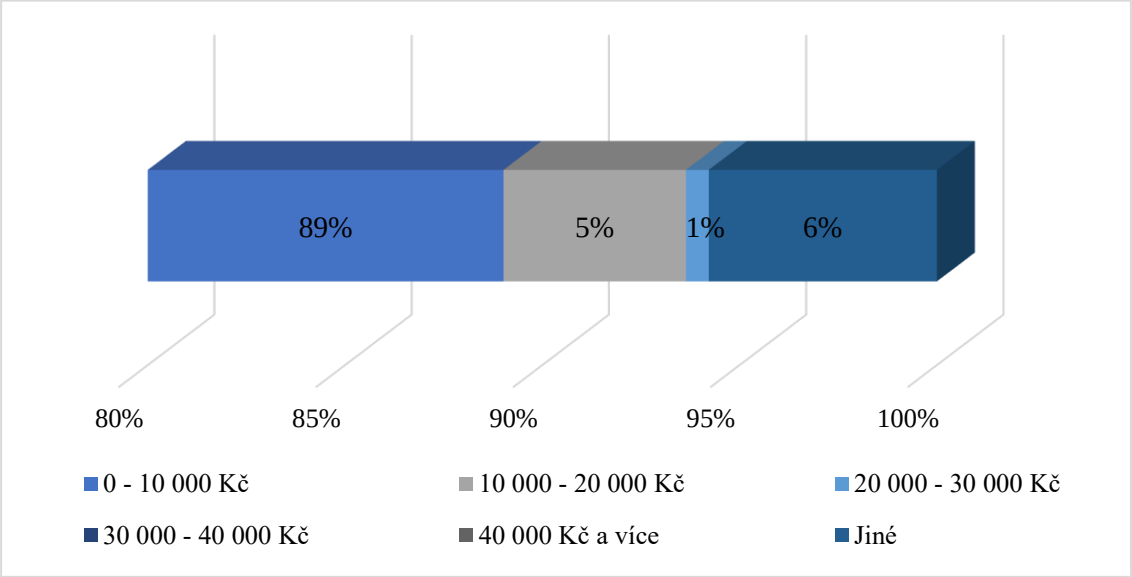


Zdroj: Vlastní zpracování, 2019

5.9 Pověřenec pro ochranu osobních údajů

Jak již bylo zmíněno ve druhé kapitole, jedním z organizačních opatření pro ochranu osobních údajů je jmenování pověřence pro ochranu osobních údajů. Z předchozí analýzy získaných dat z dotazníkového šetření vyplynulo, že toto opatření zavedlo 79 % respondentů. Organizace, které pověřence jmenovaly musejí na jeho činnost vynakládat určité náklady. Vyhodnocení získaných dat týkajících se těchto nákladů je zobrazeno na obrázku č. 23. Z analýzy těchto dat vyplývá, že nejčastěji se náklady na pověřence pohybují v rozmezí 0 – 10 000 Kč. Respondenti, kteří označili možnost *jiné* uvedli, že funkci pověřence vykonává interní zaměstnanec, kterému díky přidání nové funkci byla navýšena mzda. Taktéž někteří respondenti uvedli, že pověřence platí nadřízený orgán.

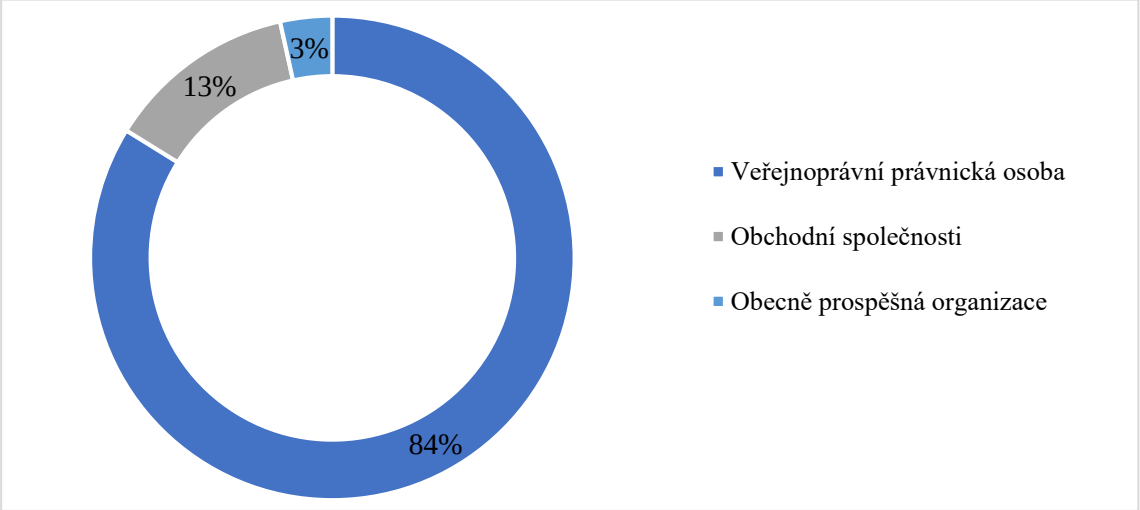
Obrázek č. 24: Náklady na DPO



Zdroj: Vlastní zpracování, 2019

Z analýzy dat od organizací, které jmenovaly pověřence pro ochranu osobních údajů vyplynulo, že mezi nejčastějšími organizacemi, které toto opatření zavedly, jsou veřejnoprávní právnické osoby (84 %, viz obrázek č. 24). Dále jmenovalo pověřence 13 % obchodních společností a 3 % obecně prospěšných organizací.

Obrázek č. 25: Typy organizací, které jmenovaly pověřence

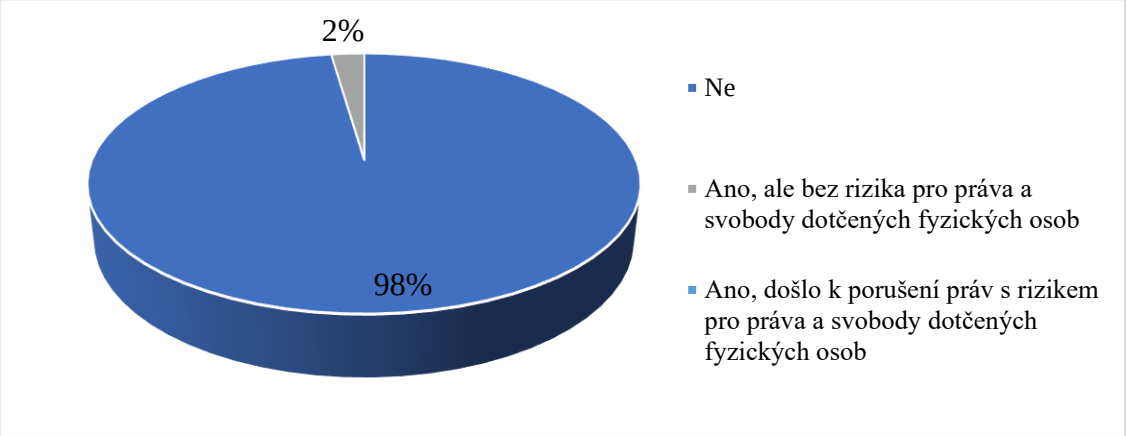


Zdroj: Vlastní zpracování, 2019

5.10 Porušení zabezpečení osobních údajů

Závěr šetření se zabýval porušením zabezpečení osobních údajů. K porušení zabezpečení těchto dat došlo u 2 % respondentů, přičemž podle zjištění se jednalo o porušení, u kterého nehrozilo riziko pro práva a svobody dotčených fyzických osob (viz obrázek č. 22).

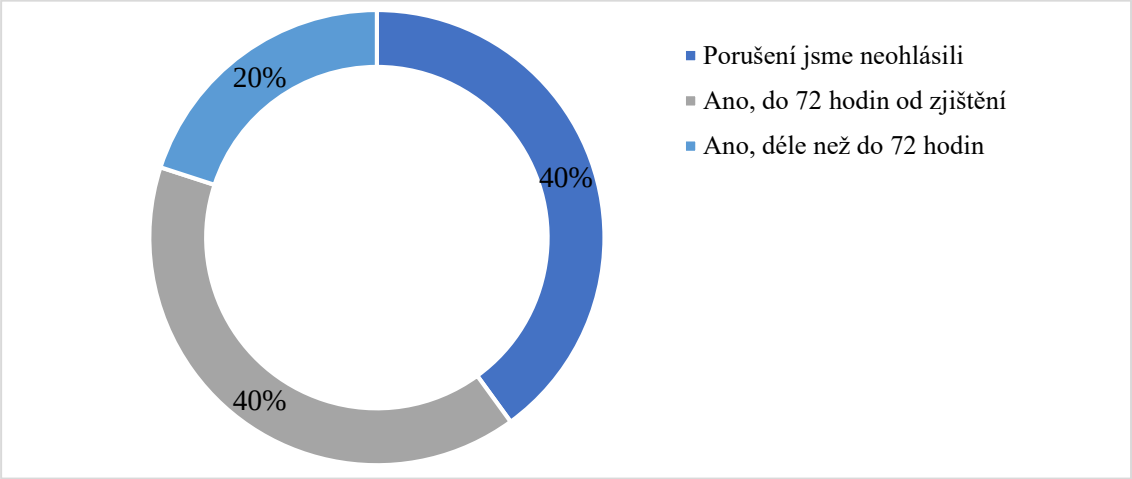
Obrázek č. 26: Výskyt porušení zabezpečení



Zdroj: Vlastní zpracování, 2019

Porušením zabezpečení se zabývala již kapitola 2.8. V případě zjištění porušení zabezpečení je nutné tuto skutečnost posoudit a pokud možno nahlásit dozorovému úřadu do 72 hodin. Z výše zmíněných 2 % respondentů, u kterých došlo k porušení zabezpečení pouze 40 % respondentů nahlásilo tuto skutečnost dozorovému úřadu (viz obrázek č. 23). Dalších 40 % respondentů porušení zabezpečení neohlásili. V případě organizací, které neohlásily porušení je možné se domnívat, že správce ihned po zjištění incidentu přijal nápravná opatření a aktualizoval svá technická či organizační opatření pro ochranu údajů. Zbylých 20 % respondentů ohlásilo porušení zabezpečení po 72 hodinách od zjištění.

Obrázek č. 27: Nahlášení porušení zabezpečení



Zdroj: Vlastní zpracování, 2019

5.11 Připomínky a doplňující informace od respondentů

Před odesláním dotazníku měli respondenti možnost vyjádřit své připomínky případně nějaké doplňující informace týkající se GDPR. Ačkoliv většina respondentů žádné připomínky neuvedla, někteří respondenti tuto možnost využily a podělili se o své názory na problematiku GDPR. Některé z poznámek od respondentů jsou následující:

- *„S ochranou osobních údajů pracuji mnoho let, nenastaly nikdy takové komplikace, aby musely být vynakládány takové náklady na GDPR. Považuji celý tento systém za nadbytečný.“*
- *„Po téměř roce se opět ukazuje, že GDPR je velký humbuk s minimálním účinkem, ale velkým dopadem na práci normálních lidí (institucí), procesy komplikují, prodražují, spamy a telefony nepřestaly, v ČR dosud nemáme zákon, ale všichni "musí" být v souladu.“*
- *„V naší organizaci nikdy v minulosti nebyl registrován žádný přestupek či porušení týkající se problematiky GDPR. Lidstvo se zbláznilo a GDPR v této podobě je jeden z produktů tohoto zbláznění.“*
- *„GDPR jako takové neúměrně zatěžuje chod malé obce, ať finančně, tak po stránce administrativní. Už tak dost zatížené administrativní činností, kterou jsme povinováni ze strany státu a jeho institucí.“*
- *„Další administrativní zátěž pro malé organizace.“*
- *„Jedná se jako vždy v případě ČR o nepochopení principu, a hlavně smyslu právní regulace ze strany EU, která měla podle mne být primárně namířena proti*

nelegálním přeprodejcům osobních údajů za účelem poskytování nevyžádaných nabídek a reklamy, případně proti zneužívání údajů pro kriminální činnost. Místo aby byl zasažen tento problematický sektor, jehož byznys stojí na pololegálním shromažďování a využívání osobních údajů, jsme vyrobili standardní českou cestou vzájemné šikanování orgánů veřejné správy, přičemž veřejná správa měla jako jediná už před nařízením GDPR tyto procesy nastavené podle zák. č. 101. nejlépe. Samozřejmě jde taktéž o obvyklé nafouknutí problému ze strany zejména softwarových a právnických organizací pod heslem: "Vyděsit a vyfakturovat".“

- *„Myslím, že zákon 101 O ochraně osobních údajů byl pro naše účely dostačující, zavádění GDPR je zbytečné, nepromyšlené mrhání prostředků na povel státu. Pro pověřence a firmy, které se toho chopily, je to neskutečný job právě na úkor škol a jiných příspěvkových organizací.“*
- *„Změny v přístupu k osobním údajům jsme nezaznamenali pouze přibylo spoustu mailů a dokladů k podpisu.“*
- *„Myslím, že se to s ochranou osobních údajů přehání, obce to stálo hodně financí, které by mohly použít na prospěšnější účely.“*

5.12 Zhodnocení dotazníkového šetření

Dotazníkového šetření se zúčastnilo celkem 223 respondentů, přičemž získaný data byla validní od 222 organizací. Mezi respondenty šetření bylo 68 % veřejnoprávních právnických organizací, 26 % obchodních společnosti, 3 % obecně prospěšných organizací, 2 % družstev a 1 % OSVČ. Nejčastěji se dotazníkového šetření zúčastnily úřady v rámci samosprávy či samosprávní celky (54,1 %) a následně pak výrobní podniky (13,5 %). V případě porovnávání respondentů dotazníkového šetření dle velikosti, nejčastěji zastoupenou kategorií jsou mikropodniky, a to z 51 %.

Z části dotazníkového šetření, které se týká kategorií zpracovávaných osobních údajů v organizacích vyplývá, že všichni respondenti zpracovávají adresní a identifikační údaje, přičemž OSVČ zpracovávají pouze tyto údaje. Ostatní právní formy organizací zpracovávají i popisné údaje a údaje o jiné osobě. Citlivé údaje zpracovávají pouze obchodní společnosti, veřejnoprávní právnické osoby a obecně prospěšné organizace.

Předtím, než *Neřízení* nabylo své účinnosti, měly organizace a společnosti dostatečné množství času na přípravu a uvedení veškerých povinností zpracovávání osobních údajů

v souladu s *Nařízením*. V části dotazníkového šetření, které se zabývalo očekávanou a skutečnou dobou přípravy na GDPR, došlo následně k analýze doby přípravy v závislosti na právní formě organizace. Z šetření je patrné, že při porovnání obou dob přípravy došlo k mírným změnám. Pro OSVČ byla očekávaná doba přípravy shodná s dobou skutečnou. Družstva ze ¾ očekávala přípravu dlouhou 2–3 měsíce, avšak ve skutečnosti jen ½ respondentů příprava trvala tuto dobu. ¼ respondentů příprava trvala 4–5 měsíců a ¼ do 1 měsíce. Obecně prospěšné organizace nejčastěji očekávaly přípravu do 1 měsíce. I skutečná doba přípravy byla stejné délky, avšak tuto dobu přípravy očekávalo pouze 43 % respondentů, ve skutečnosti byla tato doba pro 57 % respondentů. U veřejnoprávních právnických organizací byla doba přípravy značně diverzifikována, přičemž nejčastěji tato doba bylo 2–3 měsíce, a to pro 30 % respondentů. Diverzifikovaná doba byla taktéž skutečná doba přípravy, přičemž 2–3 měsíce byla pro 39 % respondentů. U obchodních společností byla doba přípravy taktéž diverzifikovaná, ačkoliv u těchto společností došlo ve skutečné době oproti očekávané k nejmenším změnám. Nejčastěji se obchodní společnosti připravovaly do 1 měsíce.

Příprava a implementace GDPR do společností a organizací s sebou přinesla také náklady, které musely být vynaloženy, aby společnosti a organizace uvedly své zpracovávání v souladu s *Nařízením*. Všechny dotazované společnosti a organizace nejčastěji vynaložily náklady ve výši 0 – 10 000 Kč. Družstva a OSVČ náklady v této výši očekávaly, u ostatních respondentů došlo k mírným změnám. 57 % obecně prospěšných organizací očekávalo tyto náklady a ve skutečnosti byla tato výše nákladů pro 71 %. U veřejnoprávních právnických osob tyto náklady očekávalo 49 % a ve skutečnosti je vynaložilo 45 %. Náklady ve výši 0 – 10 000 Kč očekávalo 60 % obchodních společností, přičemž nakonec tuto výši nákladů vynaložilo 49 % obchodních společností.

Neboť v České republice již před *Nařízením* byl zákon o ochraně osobních údajů, očekávalo se, že společnosti a organizace musely vykonat pouze dodatečné povinnosti a nebude docházet při implementaci *Nařízení* k velkým komplikacím. Toto potvrdila i analýza dotazníkového šetření, neboť komplikace se vyskytly u 10 % respondentů. Jako nejčastější komplikaci však respondenti uváděli administrativní zátěž, kterou GDPR přináší.

Jelikož se však najdou i takové společnosti či organizace, které se na GDPR nepřipravovaly, případně byla jejich příprava minimální, může dojít i k porušení

zabezpečení osobních údajů. Z analýzy dotazníkového šetření vyplývá, že k porušení zabezpečení došlo pouze u 2 % respondentů, přičemž nedošlo k porušení práv a svobod dotčených fyzických osob.

Ačkoliv se společnosti a organizace mohly bát sankcí za porušení zabezpečení, dle nejnovějších informací od ÚOOÚ, nedošlo ještě k žádnému uložené pokuty. (Novinky.cz, ©2019)

5.13 Doporučení

Pro dodržování zásad a povinností *Nařízení* je důležité, aby zavedená opatření pro ochranu zpracování osobních údajů byla účinná. Společnostem se doporučuje zavedená opatření kontrolovat, popřípadě aktualizovat, pokud je nutné, v určitých pravidelných intervalech a pokud jsou již opatření zastaralá či neplní správně svoji funkci, opatření je potřeba upravit případně zaměnit za jiné. Tímto organizace zajistí, že v případě jakéhokoliv zpracovávání osobních údajů jsou data chráněna.

Taktéž se doporučuje mít veškerá opatření pro ochranu osobních údajů sepsaná v interní směrnici, pro případnou nutnost doložit plnění zásad a povinností *Nařízení*.

Se zavedenými opatřeními, povinnostmi a zásadami v rámci GDPR by měli být seznámeni i zaměstnanci organizací. Zaměstnanci by měli například absolvovat školení či by se měly konat pravidelné porady, kde by se se zaměstnanci komunikovaly změny v rámci organizace a zpracovávání osobních údajů tak, aby těmto změnám zaměstnanci porozuměli, neboť nejen vedení organizace zpracovává osobní údaje, ale také například personalisté či mzdoví účetní.

Společnosti či organizace by však měly dokumentovat nejen zavedená opatření, ale také všechna porušení zabezpečení, ať už je hlásili dozorovému úřadu či nikoliv. V případě neohlášení porušení tento dokument musí také obsahovat důvod, proč k nahlášení porušení nedošlo. Především však je nutné zdokumentovat jakých kategorií osobních údajů se porušení týká, o jak rozsáhlé porušení se jedná a jaká byla uskutečněna nápravná opatření pro znovu zabezpečení těchto údajů. V případě, že by došlo znovu ke stejnému porušení, mohou tak správci rychleji zrevidovat, jaká byla vykonána nápravná opatření, případně kde byl jejich nedostatek, v závislosti na tom, že k incidentu došlo znovu.

Společnostem ani organizacím se nedoporučuje brát ochranu osobních údajů na lehkou váhu a na GDPR při zpracovávání dat nebrat ohled. Při nezabezpečení osobních údajů

může snadno dojít k porušení zabezpečení. V případě, že dojde k nahlášení tohoto porušení zabezpečení a ve společnosti či organizaci nebudou dodržované zásady zpracovávání osobních údajů, dozorové orgány přihlédnou k i k tomu a může dojít k vyměření pokuty, které jak je uváděno mohou být i ve značné výši.

Závěr

Cílem této diplomové práce byla analýza dopadů GDPR na společnosti a organizace v České republice.

V první části práce došlo k představení Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). V rámci této kapitoly byly představeny cíle tohoto Nařízení, platnost, přístupy k osobním údajům a také je v této kapitole zjednodušeně popsána struktura Nařízení. Druhá kapitola se následně zaměřila na pojmy z oblasti GDPR. Mezi představenými pojmy v této kapitole jsou osobní údaje, subjekt údajů, správce, zpracovatel, zpracovávání osobních údajů, právní důvody zpracovávání osobních údajů, technická a organizační opatření, dozorový úřad, porušení zabezpečení a naposledy sankce. Ve třetí kapitole byl zjednodušeně popsán proces implementace Nařízení do organizací si společností.

V následné, tedy čtvrté, kapitole bylo představeno dotazníkové šetření, které bylo použito pro získání dat pro empirickou část výzkumu. Poslední, pátá, kapitola se zaměřila přímo na analýzu získaných dat z dotazníkového šetření, porovnávání získaných dat dle různých závislostí a následně zhodnocení samotného šetření.

Seznam tabulek

Seznam obrázků

Seznam použitých zkratek

EU	Evropská unie
GDPR	General Data Protection Regulation
Kč	koruny české
Nařízení	Nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
OSVČ	osoba samostatně výdělečně činná
Pověřenec	
ÚOOÚ	Úřad pro ochranu osobních údajů

Seznam použité literatury

Monografické publikace a elektronické monografie

BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací*. Olomouc: ANAG, c2013. Právo (ANAG). ISBN 978-80-7263-811-6.

EGER, Ludvík a Dana EGEROVÁ. *Základy metodologie výzkumu*. 2. přepracované a rozšířené vydání. V Plzni: Západočeská univerzita, 2017. ISBN 978-80-261-0735-4.

Evropský parlament a Rada Evropské unie. (2016). *Nařízení evropského parlamentu a rady (eu) 2016/679*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

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

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana*. 2., dopl. a aktualiz. vyd. Praha: ASPI, 2008. Právní rukověť (ASPI). ISBN 978-80-7357-322-5.

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

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

NULÍČEK, Michal. *GDPR – obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

Praktický manuál GDPR pro každého: vše, co potřebujete vědět o novém nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů v praktickém kompletu s webem, e-bookem a aktualizačním servisem. Bratislava: DonauMedia, 2018. ISBN 978-80-8183-049-5.

STAŇKOVÁ, Lucie. *GDPR snadno a přehledně*. Praha: Mladá fronta, 2018. ISBN 978-80-204-5108-8.

The EU general data protection regulation (GDPR). New York, NY: Springer Berlin Heidelberg, 2017. ISBN 978-3-319-57958-0.

VEBER, Jaromír a Jitka SRPOVÁ. *Podnikání malé a střední firmy*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012. Expert (Grada). ISBN 978-80-247-4520-6.

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

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

Internetové zdroje

2. Nové přístupy a povinnosti. *Úřad pro ochranu osobních údajů* [online]. 5.3.2018 [cit. 2019-04-04]. Dostupné z: https://www.uoou.cz/2-nove-pristupy-a-nbsp-povinnosti/d-27268/p1=4744

Co je GDPR?. *GDPR Pro malé a střední podniky* [online]. [cit. 2019-04-04]. Dostupné z: http://www.gdprbezobav.cz/gdpr/

Dozorová činnost. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-04-04]. Dostupné z: https://www.uoou.cz/dozorova-cinnost/ds-1277/rd=0

GDPR Appropriate Technical and Organisational Measures. *Know Your Compliance* [online]. 8.5.2018 [cit. 2019-04-04]. Dostupné z: https://www.knowyourcompliance.com/gdpr-technical-organisational-measures/

HORN, David. GDPR za dveřmi: pusťte ho dál. *Svět neziskovek* [online]. 4.5.2018 [cit. 2019-04-04]. Dostupné z: https://svetneziskovek.cz/gdpr-za-dvermi-pustte-ho-dal

Jak postupovat při porušení zabezpečení osobních údajů. *GDPR solutions* [online]. [cit. 2019-04-04]. Dostupné z: https://www.gdprsolutions.cz/poruseni-zabezpeceni

KUCHAŘ, Roman. Využití oprávněného zájmu na zpracování osobních údajů podle GDPR. *Epravo.cz*[online]. 2018 [cit. 2019-04-04]. Dostupné z: https://www.epravo.cz/top/clanky/vyuziti-opravneneho-zajmu-na-zpracovani-osobnich-udaju-podle-gdpr-107490.html

Nařízení, směrnice a další právní akty. *Evropská unie* [online]. [cit. 2019-04-04]. Dostupné z: https://europa.eu/european-union/eu-law/legal-acts_cs

Právo na omezení zpracování (Článek 18, GDPR). *Lewik* [online]. [cit. 2019-04-04]. Dostupné z: https://www.lewik.org/term/16364/pravo-na-omezeni-zpracovani-clanek-18-gdpr/

Právo vznést námitku. *GUARD7* [online]. [cit. 2019-04-04]. Dostupné z: http://www.guard7.cz/gdpr/pravo-vznest-namitku

Pseudonymizace osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-04-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju

Subjekt údajů. *HelpGDPR.cz* [online]. 5.9.2017 [cit. 2019-04-04]. Dostupné z: https://www.helpgdpr.cz/rstsp/clanky.nsf/i/subjekt_udaju_17080521_24045167

SVOBODA, Jakub. Obavy z GDPR byly zbytečné, pokuta za něj zatím nepadla. *Novinky.cz* [online]. 30.3.2019 [cit. 2019-04-04]. Dostupné z: https://www.novinky.cz/internet-a-pc/499998-obavy-z-gdpr-byly-zbytecne-pokuta-za-nej-zatim-nepadla.html

Úřad pro ochranu osobních údajů. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-04-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/urad-pro-ochranu-osobnich-udaju

Základní příručka k GDPR. *Úřad pro ochranu osobních údajů* [online]. [cit. 2019-04-04]. Dostupné z: https://www.uoou.cz/zakladni-prirucka/ds-4744/archiv=0&p1=3938

Základní pojmy v GDPR. *Ministerstvo vnitra České republiky* [online]. [cit. 2019-04-04]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

Zpracovatel. *Úřad pro ochranu osobních údajů* [online]. 15.10.2018 [cit. 2019-04-04]. Dostupné z: https://www.uoou.cz/zpracovatel/d-29316/p1=3938

Záznamy o činnostech zpracování. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2019-04-04]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/zaznamy-o-cinnostech-zpracovani

Seznam příloh

Přílohy

Příloha A: Dotazníkové šetření

Dotazníkové šetření

Dobrý den,

prosím Vás o vyplnění následujícího dotazníkového šetření, které se týká problematiky GDPR (General Data Protection Regulation) a implementace Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob.

Vyplnění dotazníku zabere přibližně 10 minut.
Šetření je zcela anonymní a výsledky budou použity pro zpracování diplomové práce na Fakultě ekonomické ZČU.

Předem Vám děkuji za Váš čas.

Markéta Maňourová
m.manourova@gmail.com

DALŠÍ

Strana 1 z 13

Nikdy přes Formuláře Google neposílejte hesla.

Dotazníkové šetření - informace o organizaci I.

1. Jaká je právní forma Vaší organizace? *

Vyberte

ZPĚT DALŠÍ

Strana 2 z 13

Nikdy přes Formuláře Google neposílejte hesla.

Dotazníkové šetření - specifikování obchodní společnosti

1a. O jakou obchodní společnost se jedná?

Vyberte

ZPĚT DALŠÍ

Strana 3 z 13

Nikdy přes Formuláře Google neposílejte hesla.

Dotazníkové šetření - specifikování veřejnoprávní právnické osoby

1a. O jakou veřejnoprávní právnickou osobu se jedná?

- ○ Kraj
- ○ Obec
- ○ Svazek obcí
- ○ Příspěvková organizace
- ○ Vysoká škola

ZPĚT DALŠÍ Strana 4 z 13

Dotazníkové šetření - specifikování příspěvkové organizace

1b. O jakou příspěvkovou organizaci se jedná?

- ○ Mateřská škola
- ○ Základní škola
- ○ VOŠ

ZPĚT DALŠÍ Strana 5 z 13

Dotazníkové šetření - informace o organizaci II.

2. Jaký je typ Vaší organizace? *

- ○ Výrobní podnik
- ○ Společnost poskytující služby
- ○ Společnost zabývající se obchodem nebo zprostředkováním obchodu
- ○ Mateřská či základní škola
- ○ Střední škola (SOŠ, SOU, Gymnázium)
- ○ Vysoká škola, VOŠ
- ○ Nemocnice
- ○ Jiné zdravotnické zařízení
- ○ Úřad v rámci samosprávy, samosprávní celek
- ○ Organizační složka státu
- ○ Jiné:

2a. Mohli byste specifikovat, čím se Vaše organizace zabývá?

Vaše odpověď

3. Jaká je velikost Vaší organizace? *

- ○ MIKROPODNIK - méně než 10 zaměstnanců
- ○ MALÝ PODNIK - méně než 50 zaměstnanců
- ○ STŘEDNÍ PODNIK - méně než 250 zaměstnanců
- ○ VELKÝ PODNIK - více než 250 zaměstnanců

4. Jaký typ osobních údajů Vaše organizace zpracovává? *

- ☐ adresní a identifikační údaje (např. jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, telefonní spojení domů, do zaměstnání, ...)
- ☐ citlivé údaje (údaje vypovídající o národnostním, rasovém nebo etnickém původu, členství v odborových organizacích, odsouzení za trestný čin, sexuálním životě, genetickém údaji, politických postojích, náboženství a filosofickém přesvědčení, zdravotním stavu nebo biometrickém údaji)
- ☐ popisné údaje (např. vzdělání, znalost cizích jazyků, odborné znalosti a dovednosti, počet dětí, obrazový záznam z kamerového systému, vojenská služba, předchozí zaměstnání, zdravotní pojišťovna, mzda, číslo cestovního dokladu, bankovní spojení, ...)
- ☐ údaje o jiné osobě (např. adresní a identifikační údaje člena rodiny, manžel/manželka, dítě, ...)

Dotazníkové šetření - implementace GDPR

5. Jak dlouhou přípravu na GDPR jste očekávali? *

- ○ na GDPR jsme se nepřipravovali
- ○ do 1 měsíce
- ○ 2 - 3 měsíce
- ○ 4 - 5 měsíců
- ○ 6 a více měsíců

6. Jak dlouho reálně trvala Vaše příprava na GDPR? *

- ○ na GDPR jsme se nepřipravovali
- ○ do 1 měsíce
- ○ 2 - 3 měsíce
- ○ 4 - 5 měsíců
- ○ 6 a více měsíců

7. Jakým způsobem jste prováděli přípravu na GDPR? *

- ○ interně
- ○ ve spolupráci s poradcem/společností zabývající se implementací GDPR
- ○ Jiné:

8. Jaké změny jste uskutečnili pro splnění povinností GDPR? *

- ☐ Revize obchodních podmínek
- ☐ Jmenování pověřence pro ochranu osobních
- ☐ Zavedení šifrování a pseudonymizace osobních údajů
- ☐ Zavedení záznamů o činnostech zpracovani
- ☐ Konzultace zpracování osobních údajů s dohodovým orgánem
- ☐ Zpracování posouzení vlivu na ochranu osobních údajů (DPIA)
- ☐ Jiné: _____

9. Jaké byly Vaše očekávané náklady na zavedení GDPR? *

Vyberte

10. Jaké byly Vaše skutečné náklady na zavedení GDPR? *

Vyberte

ZPĚT DALŠÍ Strana 7 z 13

Dotazníkové šetření - nabídky konzultačních společností

11. Obdrželi jste nabídky od konzultačních společností na zavádění GDPR do Vaší organizace? *

- ANO
- NE

12. Pokud ANO, o kolik nabídek se jednalo?

- 1 nabídka
- 2 - 4 nabídky
- 5 a více nabídek

13. Pokud jste při zavádění GDPR spolupracovali s konzultační společností, co Vás ovlivnilo při její volbě?

- [ ] Cena
- [ ] Reference
- [ ] Rychlost
- [ ] Znalost konzultační společnosti
- [ ] Jiné:

ZPĚT DALŠÍ Strana 8 z 13

Dotazníkové šetření - komplikace při implementaci GDPR

14. Vyskytly se při implementaci změn ve Vaší organizaci nějaké komplikace? *

- ANO
- NE

15. Pokud ANO, mohli byste zmínit o jaké komplikace se jednalo?

Vaše odpověď

16. Pokud byste měli zavádět změny ohledně GDPR znovu a už víte co všechno to obnáší, udělali byste něco jinak?

Vaše odpověď

ZPĚT DALŠÍ Strana 9 z 13

Dotazníkové šetření - pověřenec

17. V případě, že vaše společnosti jmenovala Pověřence pro ochranu osobních údajů, kolik je na jeho činnost měsíčně vynakládáno?

- 0 - 10 000 Kč
- 10 000 - 20 000 Kč
- 20 000 - 30 000 Kč
- 30 000 - 40 000 Kč
- 40 000 Kč a více
- Jiné: _____

ZPĚT DALŠÍ Strana 10 z 13

Dotazníkové šetření - ohlašovací povinnost při porušení zabezpečení

18. Došlo od nabytí účinnosti ve Vaší společnosti k porušení zabezpečení osobních údajů? *

- ○ Ne
- ○ Ano, ale bez rizika pro práva a svobody dotčených fyzických osob
- ○ Ano, došlo k porušení práv s rizikem pro práva a svobody dotčených fyzických osob

19. V případě, že došlo k porušení zabezpečení, ohlásili jste tuto skutečnost příslušnému orgánu?

- ○ Ano, do 72 hodin od zjištění
- ○ Ano, déle než do 72 hodin
- ○ Porušení jsme neohlásili

ZPĚT DALŠÍ Strana 11 z 13

Nikdy přes Formuláře Google neposílejte hesla.

Dotazníkové šetření

Jaká je Vaše pracovní pozice v organizaci? *

Vaše odpověď

ZPĚT DALŠÍ Strana 12 z 13

Nikdy přes Formuláře Google neposílejte hesla.

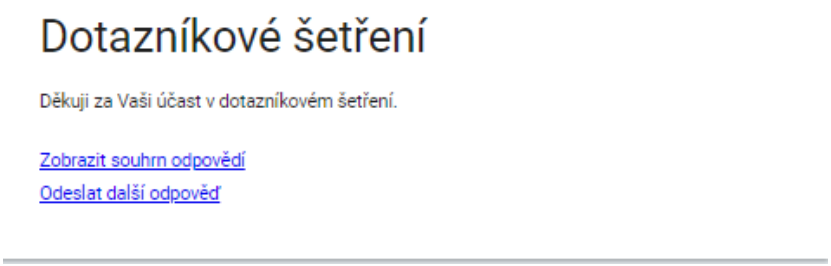
Dotazníkové šetření - připomínky a doplňující informace

Prostor pro Vaše připomínky, případně doplňující informace týkající se GDPR ve Vaší organizaci (nepovinné):

Vaše odpověď

ZPĚT ODESLAT Strana 13 z 13

Nikdy přes Formuláře Google neposílejte hesla.



Zdroj: Vlastní zpracování, 2019

Abstrakt

MAŇOUROVÁ, Markéta. *GDPR – Vyhodnocení dopadů GDPR na podniky v České republice.* Plzeň. 2019. 76 s. Diplomová práce. Západočeská univerzita v Plzni. Fakulta ekonomická.

Klíčová slova: GDPR, ochrana osobních údajů, Nařízení, vyhodnocení dopadů, analýza, dotazníkové šetření

Předložená diplomová práce se zabývá tématem ochrany osobních údajů a dopady GDPR na podniky a organizace v České republice. Práce začíná představením pojmu GDPR a poté se věnuje definováním pojmů, které jsou s touto problematikou spojené. Následující kapitoly jsou zaměřené na provedené dotazníkové šetření, které se zabývá šetřením dopadů GDPR na podniky a organizacemi v České republice. V závěru práce jsou uvedena doporučení pro zajištění stále aktuálních opatření pro zabezpečení ochrany osobních údajů.

Abstract

MAŇOUROVÁ, Markéta. *GDPR – Evaluation of the Impacts of GDPR on Businesses in the Czech Republic*. Pilsen. 2019. 76 p. Thesis. University of West Bohemie. Fakulty of Economics.

Key words: GDPR, personal data protection, Regulation, Evaluation of the Impacts, Analysis, Survey

This thesis deals with the protection of personal data and the impact of GDPR on businesses and organization in the Czech Republic. The thesis begins with the introduction of the term GDPR and then it is devoted to defining terms that are related to this issue. The following chapters focus on the questionnaire survey, which deals with the impact of od GDPR in businesses and organizations in the Czech Republic. At the end of this thesis, there are recommendations for ensuring the current measures to protect personal data.