ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Připravenost firem v České republice na GDPR

Readiness of companies in the Czech Republic for GDPR

Bc. Radek Sieber

Plzeň 2018

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Radek SIEBER**
Osobní číslo:	**K16N0108P**
Studijní program:	**N6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Název tématu:	**Připravenost firem v České republice na GDPR**
Zadávající katedra:	**Katedra podnikové ekonomiky a managementu**

Zásady pro vypracování:

1. Charakterizujte GDPR.
2. Představte způsob zavedení GDPR.
3. Realizujte výzkum pomocí dotazníkového šetření.
4. Popište způsob zpracovávání informací a jejich vyhodnocování.
5. Formulujte závěry práce.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma
„Připravenost firem v České republice na GDPR“
vypracoval samostatně pod odborným dohledem vedoucího diplomové práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni dne ……..... ……

podpis autora

Poděkování

Tímto bych chtěl poděkovat všem, které jsem potkal a kteří mě jakýmkoli způsobem obohatili o cenné rady či zkušenosti. Dále chci poděkovat své přítelkyni a své rodině za neutuchající podporu a přízeň. V neposlední řadě mé poděkování patří mé vedoucí diplomové práce paní Ing. Marii Černé, Ph.D. a panu Ing. Martinu Januškovi, Ph.D. za vstřícný přístup a připomínky při realizaci mé práce.

Obsah

Úvod

Téma *„Připravenost firem v České republice na GDPR“* bylo autorem zvoleno především proto, že se obecně zajímá o problematiku ochrany osobních údajů vzhledem k jeho podnikatelským aktivitám, při kterých se s touto problematikou setkává.

Hlavním cílem této diplomové práce je analyzovat na základě provedení a následného vyhodnocení vlastního výzkumu připravenost firem v České republice na 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) a definovat doporučení pro oblast ochrany osobních údajů. Pro realizaci tohoto výzkumu bylo provedeno dotazníkové šetření.

Metodicky práce vychází z teoretických poznatků, které byly použity k vypracování praktické části diplomové práce. V první části práce je zpracována důkladná literární rešerše z dostupných zdrojů pro problematiku ochrany osobních údajů. Jsou definovány historické milníky ochrany osobních údajů, a je zde uvedeno vysvětlení Obecného nařízení a klíčových pojmů, se kterými se lze v tomto nařízení setkat, včetně možných postupů při zavádění GDPR.

Následuje hlavní bod praktické části diplomové práce, a to vlastní výzkum připravenosti podnikatelských subjektů v České republice, který proběhl formou dotazování, které je jednou z metod marketingového výzkumu pro sběr primárních dat. Navazuje vyhodnocení tohoto šetření a z něj plynoucí závěry. Informace získané z vyhodnocení dotazníkového šetření jsou poté použity pro vytvoření doporučení pro oblast ochrany osobních údajů.

Metodika a cíle

Pro vypracování této práce byla využita česká odborná literatura, zákony a vyhlášky České republiky v platném znění, 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) a dále české a zahraniční internetové zdroje. Převážně se jedná o odborné portály ministerstev a evropských institucí, které se zaměřují na popisovanou problematiku.

Seznámení s tématem probíhalo formou důkladné rešerše odborných publikací a spolehlivých internetových zdrojů jak českých, tak zahraničních. Takto získané informace byly zpracovány, protříděny a následně interpretovány. Dotazníkové šetření proběhlo pomocí online dotazování a k vyhodnocení dat byly využity statistické postupy programu Microsoft Excel a online kalkulátoru pro Fisherův exaktní test.

Hlavní cíle diplomové práce sestávají z vymezení historických milníků problematiky ochrany osobních údajů, seznámení se s Obecným nařízením, provedením výzkumu připravenosti firem v České republice na GDPR, vyhodnocení dotazníkového šetření, následného zhodnocení závěrů vyplývajících z výzkumu a v neposlední řadě i nastínění možných řešení pro oblast ochrany osobních údajů.

1. Vývoj ochrany osobních údajů v Evropě a v České republice

Cílem této kapitoly je seznámení se s vývojem ochrany osobních údajů a s milníky, které ovlivnily vnímání citlivých osobních informací v Evropě a v České republice.

1.1. Vývoj ochrany osobních údajů v Evropě

První impuls k ochraně osobních údajů se objevil s příchodem náboženských válek, které pronásledovaly osoby s odlišným náboženským založením. Tato skutečnost vedla ke zvýšené opatrnosti a snaze ochraňovat své soukromí. Potřeba ochraňovat své soukromí vystoupila do popředí po skončení 2. světové války. Genocida a rasově motivované zákony v období nacismu jsou toho důkazem. Zrůdné chování bylo usnadněno tím, že v matrikách byla uváděna náboženská příslušnost. Zneužití výsledků statistického sčítání lidu z 30. let 20. století, které obsahovalo údaje o náboženském vyznání, přineslo důkaz, že osobní údaje mohou být snadno využity i státem a že výsledkem může být ohrožení lidských životů. (ČSÚ, 2010; Navrátil, 2018)

Navrátil (2018) se domnívá, že první psaný právní rámec týkající se ochrany soukromí se začal formovat v období Velké francouzské revoluce. Tímto dokumentem byla Deklarace práv člověka a občana, která byla sepsána v roce 1789. Naopak Weibull považuje za první snahy o ochranu soukromí regulace přístupu k veřejným záznamům ve Švédsku v roce 1766. (Britannica, 2018; Navrátil, 2018)

Dne 10. prosince 1948 Organizace spojených národů vydala Všeobecnou deklaraci lidských práv (dále jen „Deklarace“), která přímo navazuje na Deklaraci práv člověka a občana. Článek 12 této Deklarace uvádí, že nikdo nesmí být vystaven svévolnému zasahování do soukromého života ani útokům na svou čest a pověst. Tato Deklarace se stala důležitým dokumentem, což potvrzuje i fakt, že Mezinárodní pakt o občanských a politických právech doslovně převzal znění článku 12. (United Nations, 2018; OHCHR, 2018)

Navrátil (2018) označuje Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „Úmluva č. 108“) z roku 1981 za první dokument, který se hlouběji zabývá ochranou osobních údajů, protože až v tomto dokumentu dochází k definování zásad ochrany osobních údajů. Úmluvě č. 108 předcházela

Evropská úmluva o ochraně lidských práv a základních svobod, která byla Radou Evropy schválena v Římě 4. listopadu 1950, nicméně tato úmluva řešila ochranu osobních údajů jen částečně v článku 8. V Úmluvě č. 108 došlo k definování základních pojmů, které se dále rozšířily do právních předpisů členských států Rady Evropy a později i do mezinárodního práva. Úmluva vymezila pojem osobní údaj a zásady (například poctivý a právně zajištěný sběr a zpracování osobních údajů, časové omezení zpracování údajů po naplnění stanoveného účelu, shromažďování osobních údajů pouze pro vymezené legitimní účely, znemožnění zpracování údajů k jiným účelům, něž pro které byly údaje shromážděny atd.). (Kučerová, 2003; Mates, 2002; Navrátil, 2018)

Nový pohled na otázku ochrany osobních údajů přináší expanze a rozvoj odvětví s výpočetní technikou. Elektronické obchodování, elektronická forma komunikace podnikatelských subjektů, rozmach internetu a další skutečnosti otevřely prostor pro masový sběr a kumulovaní osobních údajů. Za další milník je možné považovat směrnici Evropského parlamentu a Rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice č. 95/46/ES“), jejíž platnost skončí v květnu 2018, kdy bude nahrazena **GDPR**. Cílem výše uvedené směrnice bylo sjednocení úpravy ochrany osobních údajů a umožnění jednoduššího pohybu osob po zemích tzv. Schengenského prostoru. (Navrátil, 2018)

1.2. Vývoj ochrany osobních údajů v České republice

Vývoj ochrany osobních údajů v České republice v období po 2. světové válce neprobíhal shodně se zbytkem západních zemí Evropy. Důvodem byl vládnoucí komunistický režim, který neakceptoval právo na ochranu soukromého života či osobních údajů. Kodifikace ochrany osobních údajů na našem území začala až v 90. letech 20. století přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Tento zákon však postrádal stanovení sankcí za porušování jím stanovených povinností a dalším nedostatkem byla absence ustanovení o zřízení nezávislého dozorového orgánu. (zákon č. 256/1992 Sb.)

Při žádosti o vstup do Evropské unie bylo zapotřebí přijmout odpovídající právní úpravu pro zajištění kompatibility s unijními předpisy. Z tohoto důvodu došlo parlamentem České republiky ke schválení zákona č. 101/2000 Sb., o ochraně osobních

údajů a o změně některých zákonů. Výše uvedený zákon vychází ze Směrnice č. 95/46/ES z 24. října 1995. Zákon o ochraně osobních údajů je v souladu s právy Evropských společenství a implementuje do právního řádu České republiky ustanovení Směrnice č. 95/46/ES a principy zakotvené v Úmluvě č. 108. (Maštalka, 2008; zákon č. 101/2000 Sb.)

Oproti původnímu zákonu č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, byl kladen větší důraz na pozici samotného subjektu údajů, ať už se jednalo o udělování souhlasu ke zpracování nebo o možnost vyžádání informací o zpracovávaných údajích nebo provádění oprav a výmazů nepravdivých údajů. (Šmíd, 2009)

2. Charakteristika GDPR

Níže je provedena stručná charakteristika GDPR. Cílem této kapitoly je definovat nejdůležitější pojmy, se kterými se v problematice setkáváme, uvést cíle GDPR, přiblížit nové principy, zásady a seznámit čtenáře s právy subjektu údajů.

2.1. GDPR – General Data Protection Regulation

General Data Protection Regulation, česky 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), se stává novým právním základem ochrany osobních údajů v Evropské unii. Forma nařízení zajišťuje, že ode dne své účinnosti, bude GDPR přímo určovat zásady pro zpracovávání osobních údajů ve všech zemích Evropské unie. V České republice dojde k nahrazení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. V závislosti na výše uvedeném nahrazení dojde k vydání nového zákona o zpracování osobních údajů, který bude mít za cíl úpravu bodů, které GDPR nechává otevřené. Příkladem je například nižší výše pokut za porušení předpisů. Dojde také k úpravě postavení a organizace českého Úřadu pro ochranu osobních údajů. (uoou.cz, 2017)

2.2. Nejdůležitější pojmy

2.2.1. Zpracovávání osobních údajů

Zpracování osobních údajů lze chápat jako činnost nebo soubor činností, které jsou vykonávány s osobními údaji nebo se soubory osobních údajů se zapojením nebo bez zapojení automatizovaných postupů. Automatizované postupy jsou například shromažďování, zaznamenávání, pozměnění, šíření, výmaz atd. Úřad pro ochranu osobních údajů zdůrazňuje, že jakékoli nakládání s osobními údaji nelze chápat jako zpracovávání. Zpracovávání je nutné považovat za promyšlenou a propracovanou činnost, která je správcem prováděna za jistým cílem měla by být vykonávána systematicky. (mvcr.cz, 2018)

2.2.2. Osobní údaj

Sousloví osobní údaj reprezentuje každá informace identifikující fyzickou osobu. Identifikovatelnost fyzické osoby probíhá přímo či nepřímo odkazem na určitý identifikátor, kterým může být chápat například jméno, číslo, atd. nebo odkaz na jeden či více zvláštních prvků fyzických, fyziologických, genetických, ekonomických nebo kulturních. Označení osobní údaj nedoznal změny oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Úřad pro ochranu osobních údajů poukazuje na skutečnost, že je nutné uvědomit si, že osobní údaj reprezentuje jakákoli informace týkající se identifikované či identifikovatelné fyzické osoby a fakt, že k identifikaci či identifikovatelnosti může dojít odlišnými způsoby, kterými může být například kód či IP adresa. (Maštalka, 2008; uoou.cz, 2018)

2.2.3. Subjekt údajů

Za subjekt údajů je označována fyzická osoba, které se osobní údaje týkají. Subjekt údajů jako takový není právnická osoba a osobní údaje se mohou vztahovat jen na žijící fyzické osoby. (mvcr.cz, 2018)

2.2.4. Správce osobních údajů

Primární odpovědnost za zpracování osobních údajů má správce, který určuje účely a prostředky díky kterým zpracování probíhá. Správce by měl být přítomen u každého zpracování. Zpracovávání probíhá pro účely vyplývající z činnosti správce, jako jsou například zákonem stanovené povinnosti nebo povinnosti vyplývající ze smluv. Dále je zpracovatel oprávněn zpracovávat údaje pro vlastní určené účely, kterými jsou například vlastní oprávněné zájmy, nicméně tyto zájmy nesmí převyšovat zájem na ochraně základních práv a svobod fyzických osob. Správcem osobních údajů se může stát jakýkoli subjekt včetně fyzické osoby. V případě právnické osoby je nutné zdůraznit fakt, že správcem je daná právnická osoba, nikoli její zaměstnanec, společník či jednatel. (uoou.cz, 2018)

2.2.5. Zpracovatel osobních údajů

Subjekt, který je správcem najímán za účelem provádění zpracovatelských operací se nazývá zpracovatel. Hlavní odlišnost mezi správcem a zpracovatelem je v tom, že zpracovatel může provádět jen takové zpracovatelské operace, ke kterým získal

pověření od správce. Zpracovatel se stává zpracovatelem jedině k údajům, které mu byly poskytnuty správcem, ne však k údajům, které se ho přímo týkají. Právní forma tohoto subjektu není určující stejně jako u správce osobních údajů. (Nulíček, 2017)

2.3. Cíle a hlavní principy GDPR

Navrátil (2018) definuje 4 základní cíle GDPR takto:

- *„přizpůsobení právní regulace a 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 souvisejícím předáváním osobních údajů mezi zeměmi.“*

Microsoft ve své publikaci sloužící k přípravě na GDPR uvádí hlavní principy obecného nařízení, které považuje za klíčové. Dle Microsoftu je GDPR založeno na šesti principech, které lze shrnout následovně:

- transparentnost manipulace s osobními daty,
- omezenost zpracovávání osobních údajů pouze na oprávněné účely,
- omezenost shromažďování a ukládání osobních údajů pouze na zamýšlené účely,
- dostupnost možnosti provádět změny svých dat pro jednotlivce nebo možnost jejich úplného odstranění,
- omezenost ukládání dat pouze na dobu nezbytně nutnou pro daný účel,
- zajištěnost adekvátní ochrany osobních údajů pomocí efektivních postupů.

Nicméně Úřad pro ochranu osobních údajů se primárně zmiňuje o dvou nových přístupech a principech. Jde o princip odpovědnosti správce a o přístup založený na riziku. (info.microsoft.com, 2018; Navrátil, 2018; uoou.cz, 2018)

2.3.1. Princip odpovědnosti správce

Ministerstvo vnitra České republiky vykládá princip odpovědnosti správce jako schopnost dodržet zásady zpracování, které jsou sepsány v článku č. 5 odstavec 1 Obecného nařízení a zároveň jako schopnost soulad s těmito zásadami doložit. Úřad pro ochranu osobních údajů dodává, že pro prokázání souladu mají správcům pomáhat záznamy o činnostech zpracování, pověřenec pro ochranu osobních údajů, kodexy, osvědčení a další instrumenty. (mvcr.cz, 2018; uoou.cz, 2018)

Základním nástrojem pro většinu správců by se měly stát výše zmíněné záznamy o činnostech zpracování. Tyto záznamy tvoří primárně obecné informace o prováděném zpracovávání, což by mělo správci ulehčit orientaci při zpracování, které vykonává. Ustanovení pověřence pro ochranu osobních údajů by mělo u některých správců a zpracovatelů působit jako kontrolní element, který zajistí správnost a soulad s obecným nařízením. Kodexy jsou prvkem, který má správcům posloužit jako návod správné praxe v průběhu zpracování osobních údajů s ohledem na specifičnost daného sektoru. Tvorba zmíněného kodexu není povinností a není nutné se k jeho dodržování hlásit. Oproti tomu osvědčení bude možné získat pouze akreditovaným subjektem. Osvědčení stejně jako kodex je možnost fakultativní. (mvcr.cz, 2018; uoou.cz, 2018)

2.3.2. Přístup založený na riziku

Přístup založený na riziku je možné chápat tak, že správce osobních údajů musí již při plánování zpracování osobních údajů brát ohled na povahu, rozsah, kontext a účel zpracování a zhodnotit možné rizikové faktory týkajících se práv a svobod fyzických osob a těmto faktorům přizpůsobit zabezpečení osobních údajů.

V rámci obecného nařízení tento přístup navíc zahrnuje implementaci dodatečných povinností pro některé správce osobních údajů. Jedná se o situace, kdy zpracování osobních údajů či porušení ochrany dat představuje riziko pro práva a svobody fyzických osob a je nutné implementovat tyto povinnosti. Níže uvedené povinnosti neplatí plošně a nevztahují se na všechny zpracovatele a správce. Jedná se o tyto povinnosti:

- vedení záznamů o činnostech zpracování,
- ustanovení pověřence pro ochranu osobních údajů,

- zhodnocení vlivu na ochranu osobních údajů,
- případná konzultace s úřadem, který dozoruje ochranu osobních údajů.

Další novou povinností je i povinnost ohlašování porušení ochrany či zabezpečení osobních údajů dozorovému úřadu. Výše uvedená povinnost se může dotknout každého zpracovatele nebo správce a to v případech kdy dojde k porušení zabezpečení závažnějšího rázu, ze kterého může vyplývat riziko pro práva a svobody fyzických osob. (mvcr.cz, 2018; uoou.cz, 2018)

2.4. Platnost a účinnost GDPR

Vzhledem k novým povinnostem, které zavedení GDPR přináší, byla pro nabytí účinnosti zvolena legisvakanční lhůta v době trvání více jak dvou let. Platnost GDPR začala 24. května roku 2016, nicméně začátek účinnosti byl odložen na 25. května 2018. V tento den dojde k vymahatelnosti GDPR a začne se podle něj řídit ochrana osobních údajů. Dnem 25. května 2018 dojde také k nabytí účinnosti nového českého zákona o zpracování osobních údajů. Důvodem pro dvouletou legisvakanční lhůtu byla skutečnost, že všichni, kdo pracují s osobními údaji, musí převést spravování a zpracování osobních údajů do formy kompatibilní s GDPR. (eugdpr.org, 2018; Navrátil, 2018)

2.5. GDPR a české zákony

GDPR pokrývá mnohé body, které v České republice dosud upravoval zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Z tohoto důvodu bude nový zákon o zpracování osobních údajů upravovat primárně postavení a organizační formu Úřadu pro ochranu osobních údajů, dále také dílčí body, které GDPR neobsahuje a v neposlední řadě také možné odchylky, které GDPR připouští. Příkladem takové odchylky je snížení sankcí. (Navrátil, 2018)

2.6. Zásady a právní důvody zpracování osobních údajů

Zásady zpracování osobních údajů jsou obsahem článku 5 odstavec 1 obecného nařízení. Řízení se těmito zásadami je pro správce velmi důležité, protože článek 5 odstavec 2 stanovuje povinnost pro správce, který musí být schopný dodržování níže

vypsaných zásad doložit. Pro zajištění souladu se zásadami zpracování budou sloužit správcům záznamy o činnostech zpracování, kodexy a osvědčení.

Zásady zpracování osobních údajů jsou tyto:

- *„zákonnost, korektnost, transparentnost,*
- *účelové omezení,*
- *minimalizace údajů,*
- *přesnost,*
- *omezení uložení,*
- *integrita a důvěrnost.“*

Zásada zákonnosti, korektnosti a transparentnosti znamená, že správce musí mít při zpracování osobních údajů minimálně jeden právní důvod k tomuto úkonu a musí údaje zpracovávat korektně a transparentně s ohledem na subjekt údajů.

Shromažďování osobních dat by mělo probíhat pouze pro účely určité a legitimní a nesmí docházet ke zpracovávání, které by bylo neslučitelné s výše uvedenými účely, to je zásada účelového omezení.

Minimalizací údajů se rozumí relevantnost množství dat ve vztahu k účelu, za jakým jsou data zpracovávána. Přesnost lze chápat jako zásadu přijetí rozumných opatření, které zajistí, aby osobní údaje, které jsou nepřesné, byly neprodleně smazány nebo opraveny.

Zásada omezení uložení říká, že by osobní údaje měly být ukládány v takové formě, která umožní identifikaci subjektu údajů po dobu nezbytnou pro stanovené účely, pro které jsou zpracovávány.

Technickým a organizačním zabezpečením osobních údajů se zabývá zásada integrity a důvěrnosti. Předně se jedná o zajištění adekvátního zabezpečení osobních údajů před neoprávněným zpracováním nebo před neočekávanou ztrátou či poškozením dat.

Právní důvody zpracování osobních údajů je možné chápat jako jistou formu oprávnění správce osobní údaje vůbec zpracovávat. Je to nezbytný předpoklad pro legální formu zpracování. Úřad pro ochranu osobních údajů zdůrazňuje, že osobní údaje mohou být zpracovávány pro různé účely, nicméně každý účel potřebuje právní důvod zpracování. Zpracování osobních údajů je vždy navázáno na účel, podle nějž se určí právní důvod

zpracování. Právní důvody, na jejichž základu lze osobní údaje zpracovávat, jsou následující:

- *„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.“*

První zmíněný právní důvod zahrnuje udělení souhlasu. Souhlasem rozumíme svobodný, konkrétní, informovaný a jednoznačný akt, kterým dochází k potvrzení souhlasu se zpracováním svých osobních údajů. Souhlas je zapotřebí tehdy, pokud zpracování nelze vykonat na základě důvodů, pro které souhlas není potřebný. Souhlas je odvolatelný a v případě odvolání má správce povinnost ukončit zpracovávání osobních údajů v souladu s účely definovanými v souhlasu. (mvcr.cz, 2018; Nulíček, 2017; uoou.cz, 2018)

2.7. Práva subjektu údajů

Důvodem přiznání práv subjektu údajů je tendence vyrovnat vztah mezi správcem a subjektem údajů. V komparaci se zákonem o ochraně osobních údajů lze konstatovat, že Obecné nařízení posiluje systém práv subjektů. Základním právem subjektu je právo na to být informován o zpracování svých osobních údajů. Cílem je primárně naplnění zásady transparentnosti zpracování formou podání informací o účelu zpracování, totožnosti správce, jeho odůvodněných zájmech atd. Tato skutečnost funguje jako pasivní právo, což znamená, že správce je povinen zpřístupnit a poskytnout náležité údaje subjektu údajů. Další práva stojící za zmínku jsou následující:

- právo na přístup k osobním údajům,
- právo na opravu, respektive doplnění,
- právo na výmaz,
- právo na omezení zpracování,
- právo na přenositelnost údajů.

Právem na přístup k osobním údajům rozumíme možnost subjektu údajů na jeho vlastní žádost získat od správce vyjádření, zda jsou či nejsou osobní údaje subjektu zpracovávány. V případě situace, kdy jsou údaje zpracovávány, má subjekt právo tyto osobní údaje získat a dále má právo na získání následujících informací:

- *„účely zpracování,*
- *kategorie dotčených osobních údajů,*
- *příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,*
- *plánovaná doba, po kterou budou osobní údaje uloženy,*
- *existence práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,*
- *právo podat stížnost u dozorového úřadu,*
- *veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,*
- *skutečnost, že dochází k automatizovanému rozhodování, včetně profilování.“*

Právo na výmaz neboli právo být zapomenut znamená povinnost pro správce vymazat osobní údaje, jestliže je splněna některá z následujících podmínek:

- *„osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,*
- *subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,*
- *subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,*
- *osobní údaje byly zpracovány protiprávně,*
- *osobní údaje musí být vymazány ke splnění právní povinnosti,*

- *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení.“*

Úřad pro ochranu osobních údajů upozorňuje na skutečnost, že právo na výmaz není absolutním právem, které by opravňovalo žádat kdykoli o smazání osobních údajů, vzhledem ke skutečnostem vyplývajícím z povinností o dalším uchovávání některých osobních údajů například při poskytování finančních služeb. (infosecurityeurope.com, 2017; Nulíček, 2017; uoou.cz, 2018)

2.8. Sankce a pokuty

Úřad pro ochranu osobních údajů, jakožto dozorčí orgán v České republice, uvádí, že ukládání pokut musí probíhat tak, aby byla zajištěna účinnost a přiměřenost pokut, nicméně by pokuty měly být odrazující od záměrného porušování Obecného nařízení. V případě porušení obecného nařízení může nejprve dojít k upozornění nebo napomenutí, sám Úřad pro ochranu osobních údajů vyvrací obavu, že každé porušení obecného nařízení bude pokutováno. (uoou.cz, 2018)

Výše pokut za porušení Obecného nařízení může být různá. Pokuty, které mohou být uděleny, lze rozdělit na dvě skupiny. V případě první skupiny může být pokuta udělena až do výše 10 000 000 EUR nebo do 2% celkového ročního celosvětového obratu povinného subjektu. Druhá skupina má maximální pokuty ve výši 20 000 000 EUR a 4% celkového ročního celosvětového obratu povinného subjektu. Důvodem rozdělení na dvě skupiny je zdůraznění důležitosti některých povinností, jejichž porušení by mohlo způsobit vyšší intenzitu zásahu do práva na ochranu osobních údajů, které zajišťuje obecné nařízení. Například porušení ustanovení ohledně záznamů o činnostech spadá do skupiny s nižší sazbou, naproti tomu podmínky souhlasu se zpracováním osobních údajů spadají do kategorie s vyšší sazbou. (mvcr.cz, 2018; uoou.cz, 2018)

Při posuzování deliktů bude brána v potaz zejména jeho závažnost, délka trvání, povaha a počet dotčených subjektů údajů. Velkou váhu má také skutečnost, zda se jednalo o úmyslné či nedbalostní porušení. V případě hmotné či nehmotné újmy, která by byla způsobena subjektu údajů v důsledku porušení obecného nařízení, má subjekt nárok na odškodnění. S žádostí o úhradu újmy je nutné obrátit se na správce či zpracovatele. V případě neplnění ze strany správce či zpracovatele, je nutné se obrátit na soud. (uoou.cz, 2018)

2.9. Zabezpečení osobních údajů

Zabezpečení osobních údajů je velmi diskutované téma a z obecného nařízení vyplývá, že každý správce je povinen přijmout adekvátní bezpečností opatření. Úřad pro ochranu osobních údajů dodává, že správce musí vzít v potaz povahu, rozsah a účely zpracování osobních údajů a musí být schopen doložit, že zpracování probíhá v souladu s výše zmíněným Obecným nařízením. Technická a organizační opatření, přijatá různými správci, se tak mohou lišit. (uoou.cz, 2018)

Náhodné nebo protiprávní zničení, změna, poskytnutí či ztráta osobních údajů jsou charakterizovány jako porušení zabezpečení osobních údajů. V případě, že porušení zabezpečení představuje vysoké riziko pro práva a svobody fyzických osob, je nutné skutečnost ohlásit dozorovému orgánu, případně subjektu údajů. Proces ohlášení incidentu Úřadu pro ochranu osobních údajů (dozorový orgán v České republice) by měl být uskutečněn do 72 hodin od okamžiku zjištění. Případné riziko může eliminovat použití pseudonymizace a šifrování dat. (mvcr.cz, 2018; uoou.cz, 2018)

Zhodnocení míry rizika vychází hlavně z povahy osobních údajů, které byly porušením zabezpečení dotčeny, způsobu porušení zabezpečení a z množství dotčených subjektů údajů. Údaje o zdravotním stavu a podobné údaje, které mohou způsobit subjektu údajů újmu či zásah do jeho práv jsou hodnocené vyšší rizikovostí. Je taktéž nutné přihlédnout k okolnostem porušení zabezpečení. V případě cíleného, úmyslného činu je riziko vyšší, protože je takový únik charakterizován jako útok na osobní údaje. (uoou.cz, 2018)

2.10. Pověřenec pro ochranu osobních údajů

Úkolem pověřence pro ochranu osobních údajů je primárně poskytování informací a poradenství pro správce, zpracovatele či zaměstnance, kteří se na zpracování podílejí. Dalším úkolem je monitoring souladu zpracování s Obecným nařízením a dalšími předpisy. Jmenování pověřence pro ochranu osobních údajů se netýká všech subjektů. Pověřenec musí být jmenován když:

- *„zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,*

- *hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,*
- *hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech.“*

Pověřenec pro ochranu osobních údajů by měl mít přímý přístup k vedení organizace, aby se předešlo prodlevám a komunikačním šumům. Mezi pověřencem a vedením organizace by neměl být další mezičlánek. Co se týká vzdělání pověřence, obecné nařízení nestanovuje konkrétní požadavky ve smyslu akademických titulů, nicméně pověřenec musí být osoba vybavená profesními kvalitami a odbornou znalostí práva a praxe v oblasti ochrany osobních údajů. Nedílnou součástí vzdělání pověřence je adekvátní znalost Obecného nařízení. Obecné nařízení nijak nepředpokládá certifikace pověřenců, takže správce může pověřencem jmenovat kteroukoli osobu, která disponuje adekvátními znalostmi. (uoou.cz, 2018)

3. Zavádění GDPR

V této kapitole je popsáno zavádění GDPR v podnikatelské sféře, protože velké množství podnikatelských subjektů před platností Obecného nařízení tuto problematiku přehlíželo. Níže bude uvedena stručná metodika, postupy a legislativa.

3.1. Fáze přípravy na GDPR

Subjekty, které se zaměřují na pomoc se zaváděním GDPR rozdělují přípravu do několika fází, které pojmenovávají různě, nicméně aktivity v jednotlivých fázích si jsou velmi podobné.

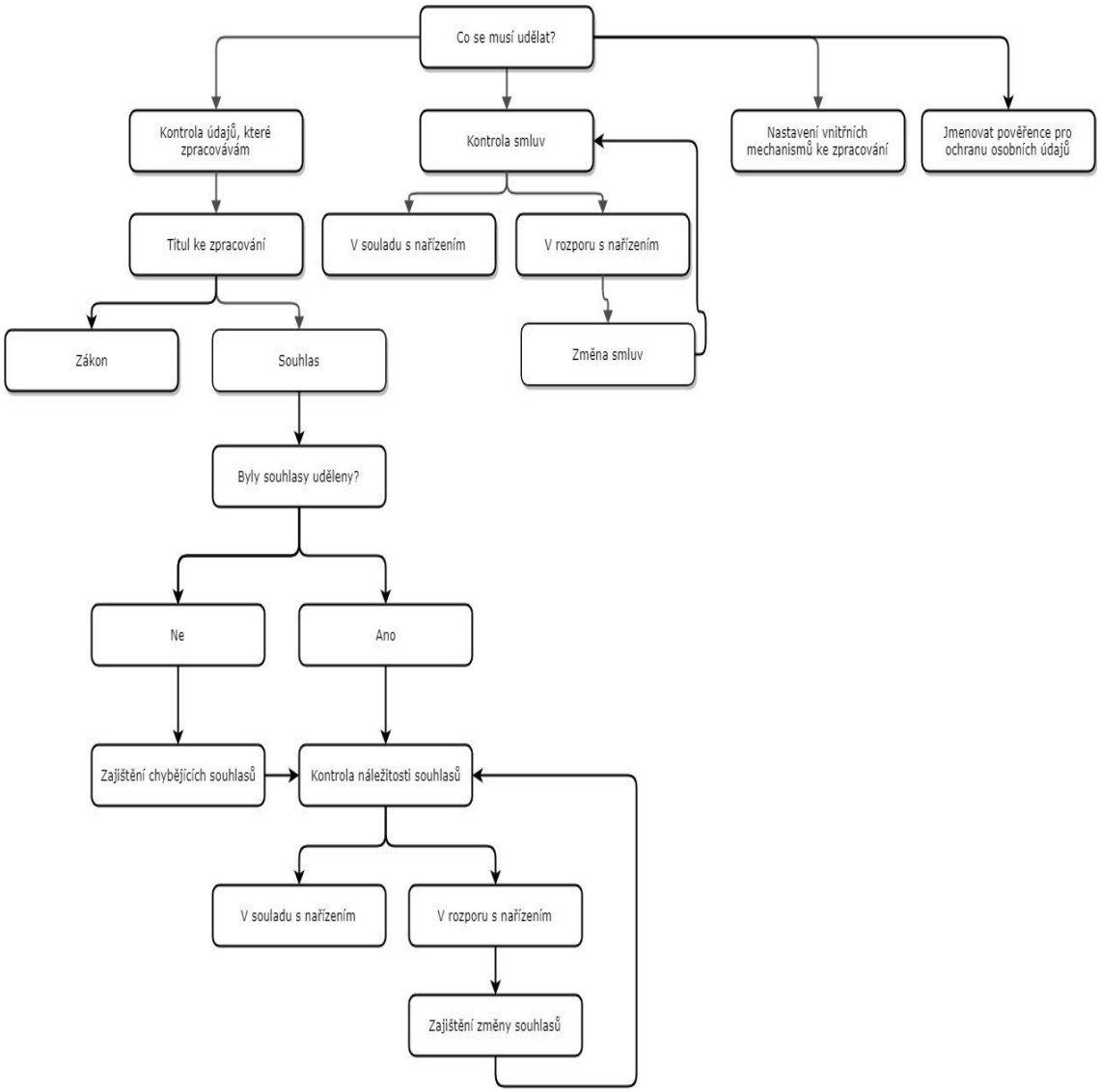
Obrázek 1: Fáze přípravy na GDPR

Zdroj: vlastní zpracování, 2018

Na přípravu na GDPR se lze podívat i z pohledu činností, které je nutné vykonat. Metodika vypracovaná Ministerstvem školství, mládeže a tělovýchovy tyto činnosti

shrnula do hierarchického grafu. V podnikatelské sféře nemusí každý subjekt jmenovat pověřence pro ochranu osobních údajů.

Obrázek 2: Činnosti, které je nutné vykonat před nabytím účinnosti GDPR



Zdroj: vlastní zpracování, 2018

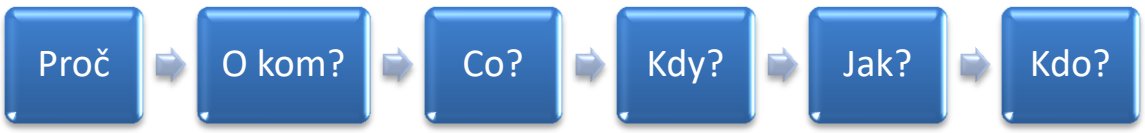
3.1.1. Systémová analýza

Prvním krokem, který se doporučuje, je systémová analýza, která odhalí jaká data má podnikatelský subjekt k dispozici a kde jsou uložená. Cílem mapování dat je rozpoznání dostupných osobních údajů a následně určení konkrétního místa jejich uložení. Například Microsoft doporučuje vytvořit soupis dat, která má podnikatelský subjekt k dispozici, s cílem rozpoznat umístění dat, jejich shromažďování a ukládání. Nedílnou

součástí soupisu by měl být závěr, proč jsou data shromažďována a jak dlouho jsou uchovávána. (info.microsoft.com, 2018)

Informační produkt zpracovaný pro implementaci GDPR do praxe úřadů v České republice v této fázi doporučuje zjistit všechny parametry související se zpracováním osobních údajů pomocí níže uvedených šesti otázek.

Obrázek 3: Otázky pro zjištění parametrů související se zpracováním osobních údajů



Zdroj: vlastní zpracování, 2018

Odpovědí na první otázku „***Proč?***“ je účel zpracování osobních údajů. Následující otázka „***O kom?***“ má za cíl identifikaci subjektu údajů. To slouží také k identifikaci osoby, která je oprávněna získávat informace o zpracování dat nebo žádat o jejich výmaz. Třetí otázka „***Co?***“ popisuje typ osobních údajů, jejich zdroj a právní důvod shromažďování. Výstupem otázky „***Kdy?***“ jsou informace časového rázu, které určují, kdy byly údaje získány, zda je nutné je aktualizovat a jak často a také jaká je doba jejich uchování. Předposlední otázka „***Jak?***“ si klade za cíl popsat způsob, jakým se údaje shromažďují, zpracovávají a ukládají. Součástí by měl být i popis postupu zpracování. Závěrečná otázka „***Kdo?***“ identifikuje osoby, které osobní údaje zpracovávají a kterým mohou být zpřístupněny. (spmo.cz, 2017)

3.1.2. Implementační plán

Implementační plán zahrnuje identifikaci a řízení rizik v současném systému. Tato fáze se zaměřuje na zkoumání současných opatřeních a na způsoby úpravy, které korespondují s požadavky obecného nařízení. Cílem je kontrolovat všechna rizika, která mohou nastat při zpracování osobních údajů, aby byla zajištěna maximální bezpečnost a ochrana údajů. (advisera.com, 2018)

3.1.3. Realizace úprav

Tato fáze přípravy se zaměřuje již na konkrétní úpravy a zajištění adekvátních řešení, která povedou k účinné a vyhovující ochraně osobních údajů v souladu s GDPR. V případě dodání řešení externí firmou je nutné zajistit soulad stávajících a nově

uzavíraných smluv s GDPR. Součástí této fáze je také aktualizace interních předpisů a směrnic, kterými se procesy řídí a díky nim také dochází ke kontrole. Osobní údaje, které nejsou zpracovávány dle zákona, vyžadují souhlas subjektu údajů. Tento souhlas musí být explicitní, bezpodmínečný a kvalifikovaný, což znamená oddělený od jiných právních dokumentů. Souhlasy dříve získané, které nesplňují podmínky GDPR, je nutné získat znovu. (spmo.cz, 2017)

3.1.4. Reporting

Vzhledem k povaze obecného nařízení, je nutné zajistit větší transparentnost v případě zpracovávání osobních údajů, ale také v případě udržování dokumentace, která definuje interní procesy a využívání osobních údajů. Subjekty, zpracovávající osobní údaje, jsou povinny uchovávat záznamy, které obsahují tyto informace:

- účel zpracování,
- kategorie zpracovávaného údaje,
- identita třetí strany, s níž jsou údaje sdíleny,
- přenesení údajů do jiných zemí a právní základ těchto přenosů,
- informace o bezpečnostních opatřeních,
- doba uchovávání.

Do reportingu spadá také vyřizování žádostí o data nebo oznamování narušení zabezpečení osobních údajů. (info.microsoft.com, 2018)

3.2. Správce a zpracovatel

Odpovědností správce je zavedení vhodného technického a organizačního opatření, s ohledem na zajištění zpracování osobních údajů v souladu s GDPR. Vhodným technickým a organizačním opatřením se rozumí například pseudonymizace nebo minimalizace údajů. Správce musí do zpracování začlenit potřebné záruky, které budou v souladu s obecným nařízením a zaručí tak ochranu práv subjektů údajů. Při zavádění opatření je nutné přihlédnout ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování a pochopitelně i k možným rizikům. (Nulíček, 2017)

V případě delegování zpracování osobních údajů na zpracovatele, smí správce využít pouze ty zpracovatele, kteří jsou schopni poskytnout adekvátní záruky zavedení

vhodných technických a organizačních opatření do té míry, aby dané řešení splňovalo podmínky obecného nařízení. Zodpovědnost za výběr zpracovatele nese správce.

3.2.1. Smlouva mezi správcem a zpracovatelem

Ve smlouvě o zpracování musí být uveden předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektu údajů. Součástí smlouvy jsou také práva a povinnosti správce. Mimo výše zmíněné musí tato smlouva stanovit, že zpracovatel:

- zpracovává údaje jen dle zdokumentovaných pokynů správce,
- zaručuje mlčenlivost osob, které jsou oprávněné zpracovávat osobní údaje,
- vykoná vše pro splnění opatření uvedených v článku 32 Obecného nařízení (například pseudonymizace a šifrování osobních údajů, zajištění důvěrnosti, integrity a dostupnosti systému, atd. Při zavádění těchto opatření je vždy nutno přihlédnout ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování.),
- v souladu s výrokem správce všechny osobní údaje vymaže nebo vrátí správci po ukončení zpracovávání, pokud právo Evropské unie nebo daného státu nevyžaduje uchovávání těchto údajů,
- poskytne správci informace, které dokládají splnění povinností, které stanovuje obecné nařízení a umožní kontroly prováděné správcem nebo osobou, kterou správce k tomuto úkonu pověřil.

Úspěšné dodržování povinností může být podpořeno například dodržováním schváleného kodexu chování nebo mechanizmu, který je nutný pro vydání osvědčení. (Navrátil, 2018; obecné nařízení, 2016)

3.2.2. Posouzení vlivu na ochranu osobních údajů

Posouzením vlivu na ochranu osobních údajů se zabývá článek 35 Obecného nařízení. V prvním bodě je definováno, kdy vůbec musí dojít k posouzení vlivu. Je to tehdy, pokud je pravděpodobné, že daný proces zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Nejčastější případy popsané v Obecném nařízení jsou tyto:

- systematické a rozsáhlé vyhodnocování osobních aspektů, které se týká různých fyzických osob a které probíhá díky automatizovanému zpracování, které zahrnuje profilování,
- zpracování zvláštních kategorií jako jsou údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení nebo například členství v odborech či zpracování genetických údajů,
- provádění rozsáhlého systematického monitorování veřejně přístupných prostor.

Posouzení vlivu na ochranu osobních údajů může být provedeno i v odlišných případech, než jsou ty, které jsou uvedeny výše. Například Navrátil (2018) doporučuje společnostem, které mají více než 250 zaměstnanců provedení tohoto posouzení dobrovolně z důvodu předcházení větším problémům.

Posouzení vlivu na ochranu osobních údajů musí obsahovat následující:

- *„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 uvedených v odstavci1; a*
- *plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.“* (Obecné nařízení, 2016)

3.2.3. Kodexy chování

Významným prvkem posouzení rizik mohou být interní kodexy chování pro oblast ochrany osobních údajů. Účelem těchto kodexů by měl být přínos k bezpečnému chování při správě a zpracování osobních údajů.

Tyto kodexy by se měly zaměřovat primárně na následující oblasti:

- legislativní správnost a transparentní zpracování osobních údajů,
- obecná pravidla pro bezpečné a legální shromažďování osobních údajů,
- pseudonymizace osobních údajů,
- míra informovanosti veřejnosti a subjektů údajů o ochraně osobních údajů v daném subjektu,

- zajištění výkonu práv subjektů údajů,
- zajištění dostatečného a hlavně srozumitelného poskytování informací mladistvým a dětem v souvislosti se sběrem a zpracováním jejich osobních údajů,
- vytváření opatření a postupů pro zajištění bezpečnosti při zpracování,
- správné nahlašování situací porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a fyzickým osobám, které jsou porušením zabezpečení dotčeny.

Schvalování kodexů je v kompetenci Úřadu pro ochranu osobních údajů. Kodexy podnikatelských subjektů by měly být předávány k registraci Úřadu pro ochranu osobních údajů a ten posoudí, zda tento návrh kodexu poskytuje dostatečné záruky pro ochranu osobních údajů. Kodexy se mohou vztahovat i na více členských zemí Evropské unie. (Navrátil, 2018; Obecné nařízení, 2016)

3.3. Hlavní zásady zpracování osobních údajů

Zpracování musí probíhat korektním, zákonným a transparentním způsobem, což znamená, že během zpracování osobních údajů musí být dodržovány všechny právní předpisy, které se zpracování týkají. Zároveň je nutné osobní údaje zpracovávat tak, aby bylo možné identifikovat, které osobní údaje byly zpracovány a jakým způsobem.

Shromažďování osobních údajů musí být pouze pro určité, výslovně vyjádřené a legální účely. Osobní údaje nesmí být dále zpracovány způsobem, který je neslučitelný s legitimností.

Sběr osobních údajů by měl být přiměřený, relevantní a omezený na nezbytný rozsah ve vztahu k účelu zpracování. Tak je možné chápat minimalizaci údajů, což znamená, že by měl probíhat pouze sběr potřebných dat.

Osobní údaje, které jsou nepřesné, neaktualizované nebo chybné musejí být bezodkladně vymazány nebo opraveny. Při sběru a správě osobních údajů je nutné přijmout taková opatření, která zajistí co nejvyšší bezchybnost.

Způsob ukládání osobních údajů by měl umožňovat identifikaci subjektů údajů po dobu nezbytnou pro účely, pro které jsou osobní údaje zpracovávány. Po uplynutí této doby by měla následovat kvalifikovaná skartace.

Zpracování osobních údajů by mělo probíhat za podmínek, které zajišťují náležité zabezpečení a ochranu pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před nenadálou ztrátou, poškozením či zničením. (Navrátil, 2018; Nulíček, 2017; Obecné nařízení, 2016)

Pro zákonné zpracování osobních údajů jsou dva důvody. Buď ke zpracování osobních údajů dochází u jiných zákonem stanovených důvodů, a proto není souhlas subjektu údajů nutný nebo byl subjektem údajů odpovídající souhlas udělen.

3.3.1. Zpracování osobních údajů bez souhlasu subjektu údajů

Zpracování osobních údajů je možné bez souhlasu subjektu jen tehdy, je-li splněna alespoň jedna z níže uvedených podmínek:

- zpracování je nutné pro naplnění smlouvy, jejíž smluvní stranou subjekt údajů je,
- zpracování je nutné pro splnění právní povinnosti, která je vztažena na správce
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiných fyzických osob
- zpracování je nutné pro splnění úkonu, který je prováděn ve veřejném zájmu nebo při výkonu veřejné moci
- zpracování je potřebné pro účely oprávněných zájmů příslušného správce či třetí strany (nad tímto zájmem stojí základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů)

Navrátil (2018) poukazuje na fakt, že poslední výše zmíněný bod z Obecného nařízení se dotýká například umístění kamerových systémů, kde je téměř neproveditelné získání souhlasů. V takový moment získání souhlasu nahrazují informační tabulky a umístění kamer musí být provedeno v souladu se zákonem, aby nedocházelo k narušení soukromí.

3.3.2. Zpracování osobních údajů se souhlasem subjektu údajů

V případě zpracování osobních údajů se souhlasem subjektu údajů, musí být správce schopen doložit souhlas, který mu byl subjektem údajů poskytnut. V případě písemných prohlášení, která se týkají zároveň i jiných skutečností, je nutná jasná odlišnost, přístupnost a rozlišitelnost souhlasu za pomoci jednoduchých jazykových prostředků.

V praxi to znamená, že souhlas musí být vyjádřen jednoznačně, správce musí být schopen jej doložit a nesmí být získán nátlakem, vynucením nebo lstí.

Příkladem výše uvedeného je například skutečnost, že v internetových vyhledávačích by již neměla být předem zaškrtnutá políčka souhlasu, která se týkají osobních údajů subjektu. Souhlas se zpracováním osobních údajů je dobrovolný a odvolatelný a toto odvolání by mělo být stejně jednoduché jako jeho poskytnutí. (dauc.cz, 2017)

4. Šetření připravenosti firem v České republice na GDPR

Šetření je zaměřeno na podnikatelské subjekty v České republice a na jejich připravenost na GDPR. Šetření zkoumá, jaké očekávání měly podnikatelské subjekty ohledně zavádění GDPR a dochází ke komparaci s výsledky subjektů, které již GDPR zavádějí.

4.1. Hlavní cíl dotazníkového šetření

Hlavním cílem dotazníkového šetření je analyzovat připravenost firem v České republice na 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). Dále je cílem šetření komparovat subjekty, které se na zavedení GDPR již připravují (jejich náklady) a subjekty, které příprava na zavedení GDPR teprve čeká.

4.2. Metodologie výzkumu

Otázky pro dotazníkové šetření byly navrženy takovým způsobem, aby splňovaly primárně deskriptivní funkci. Provedené šetření je kombinací kvantitativního a částečně kvalitativního výzkumu.

Dotazování probíhalo pomocí elektronického dotazníku vytvořeného na platformě www.vyplnto.cz. Otázky a jejich opodstatnění jsou podrobně rozepsány níže.

Analyzování výsledků šetření proběhlo pomocí metod statistické analýzy. Předmětem zkoumání byla četnost odpovědí a vztahy mezi nimi.

4.3. Respondenti

Vzorek respondentů je tvořen podnikatelskými subjekty z České republiky bez ohledu na umístění. Tento vzorek byl zvolen vzhledem k tomu, že obecné nařízení má plošnou působnost na celou Českou republiku.

4.4. Dotazník

V této kapitole jsou popsány jednotlivé otázky dotazníku, včetně odpovědí na ně. Je popsáno, co daná otázka zjišťuje, respektive jaké je využití otázek během výzkumu.

První část dotazníku obsahuje otázky, které zkoumají obecné informace o respondentech. Cílem prvních otázek je zjistit velikost podnikatelského subjektu, právní formu a obor podnikání. Jedná se o tyto otázky:

1. **Jaká je vaše právní forma podnikání?**
    a. Fyzická osoba - OSVČ
    b. S.R.O.
    c. A.S.
    d. V.O.S
    e. K.S
    f. Družstvo
    g. Evropská společnost
2. **Jaký je váš obor podnikání?**
    a. Auto-moto
    b. Bezpečnostní služby a agentury
    c. Cestovní agentury, kanceláře
    d. Doprava a logistika
    e. E-shopy
    f. Farmacie, léčiva
    g. Fotografie, video, grafika
    h. Finanční služby
    i. Hotely, ubytování, restaurace
    j. Kosmetika, kadeřnictví, wellness, masáže
    k. Marketingové služby, reklama
    l. Neziskové organizace
    m. Potravinářský průmysl
    n. Právnické služby
    o. Realitní kanceláře
    p. Řemesla
    q. Software a IT služby
    r. Stavebnictví, stavitelství, architekti
    s. Strojírenský průmysl
    t. Velkoobchod

u. Veřejná správa
v. Výroba
w. Vzdělávání, kurzy
x. Zdravotnictví
y. Zemědělství, chovatelství
z. ostatní

3. **Jaká je velikost vašeho podniku?**
    a. Mikro podnik (méně než 10 zaměstnanců, roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR)
    b. Malý podnik (méně než 50 zaměstnanců, roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR)
    c. Střední podnik (méně než 250 zaměstnanců, roční obrat nepřesahuje 50 milionů EUR nebo bilanční suma roční rozvahy nepřesahuje 43 milionů EUR)
    d. Velký podnik (není mikro, malý nebo střední dle výše uvedených parametrů)

Pomocí následující otázky byly podnikatelské subjekty rozděleny na dvě části za účelem následné komparace výsledků. První soubor tvoří podnikatelské subjekty, které se již na GDPR připravují a druhý soubor je tvořen subjekty, které zatím přípravu nezahájily.

4. **Připravujete se na GDPR?**
    a. Ano
    b. Ne

Pátá otázka dotazníkového šetření zjišťuje, v jaké fázi příprav se nacházejí respondenti, kteří se již začali na platnost GDPR připravovat. Na pátou otázku navazuje otázka číslo šest, která zjišťuje, zda měl pro přípravu podnikatelský subjekt nějakého partnera nebo zda se připravoval na Obecné nařízení sám.

5. **V jaké fázi příprav na GDPR se nacházíte?**
    a. Systémová analýza (jaké osobní údaje společnost shromažďuje, pro jaký účel, kdo k nim má přístup, jakým způsobem je prováděna kontrola oprávnění, jak se likvidují osobní údaje, apod.)
    b. Implementační plán (úprava vnitřních norem a procesů, určení, zda společnost potřebuje pověřence pro ochranu osobních údajů, zajištění bezpečnosti zpracování osobních údajů, apod.)
    c. Realizace úprav (revidování smluv mezi správcem a zpracovatelem, příprava záznamů o zpracování, kontrola bezpečnosti jednotlivých procesů, revize souhlasů se zpracováním osobních údajů)
    d. Jsme připraveni
6. **Probíhala vaše příprava na GDPR ve spolupráci s nějakým partnerem?**
    a. Ano
    b. Ne, GDPR si řešíme sami

Další dvě otázky zkoumají, jaké byly respondentovy předpoklady týkající se délky a ceny zavádění změn v rámci přípravy na GDPR. Získaná data tedy poskytla informace o tom, jaké byly představy respondentů o GDPR.

7. **Jaké byly vaše předpokládané náklady spojené se zavedením GDPR?**
    a. 1 - 50.000 Kč
    b. 50.000 – 150.000 Kč
    c. 150.000 – 400.000 Kč
    d. 400.000 a více Kč
8. **Jak dlouho jste předpokládali, že bude trvat vaše příprava na GDPR?**
    a. Do 1 měsíce
    b. 1 - 2 měsíce
    c. 2 - 4 měsíce
    d. 4 a více měsíců

Devátá a desátá otázka zkoumají, jaké byly skutečné časové a finanční náklady při zavádění změn v souvislosti s GDPR. Cílem těchto otázek je získat data pro komparaci s otázkami číslo sedm a osm, která poskytne představu o tom, jak se lišila očekávání podnikatelských subjektů oproti skutečnosti.

9. **Jaké byly vaše dosavadní/celkové náklady spojené se zavedením GDPR?**
    a. 1 - 50.000 Kč
    b. 50.000 – 150.000 Kč
    c. 150.000 – 400.000 Kč
    d. 400.000 a více Kč
10. **Jak dlouho celkem trvala/trvá vaše příprava na GDPR?**
    a. Do 1 měsíce
    b. 1 - 2 měsíce
    c. 2 - 4 měsíce
    d. 4 a více měsíců

Následují první dvě otevřené otázky, ve kterých respondent vypíše problémy, které předpokládal a se kterými se setkal během zavádění GDPR. Otázky jsou komparativního rázu. Tímto způsobem lze porovnat, jaká byla očekávání respondentů a jaké problémy respondenty skutečně potkaly.

11. **V čem jste předpokládali největší problém při zavádění GDPR?**

12. **Co byl pro vás největší problém při zavádění GDPR?**

Poslední čtyři otázky jsou určené pro respondenty, kteří odpověděli na otázku číslo čtyři, že se zatím na GDPR nepřipravují. Otázka číslo třináct zkoumá, zda se respondenti vůbec chystají na GDPR připravovat a pokud ano, kdy hodlají začít. Druhá otázka tohoto bloku se týká finanční stránky věci. Respondent upřesní svoji představu o předpokládaných nákladech na zavedení GDPR. Předposlední otázka se týká odhadu doby potřebné na přípravu na GDPR.

13. **Plánujete se připravovat na GDPR ?**
    a. Ano, chceme začít s přípravou než GDPR vejde v účinnost
    b. Ano, začneme až GDPR vejde v účinnost
    c. Ne, připravovat se nebudeme
14. **Jaké předpokládáte náklady spojené se zavedením GDPR?**
    a. 1 - 50.000 Kč
    b. 50.000 – 150.000 Kč
    c. 150.000 – 400.000 Kč
    d. 400.000 a více
15. **Jak dlouho předpokládáte, že bude trvat vaše příprava na GDPR?**
    a. Do 1 měsíce
    b. 1 - 2 měsíce
    c. 2 - 4 měsíce
    d. 4 a více měsíců

Posledním bodem dotazníku je otázka otevřená. Respondent uvede oblasti, které vyhodnotil jako potencionálně problematické při zavádění GDPR. Tímto způsobem lze zjistit představu respondentů, kteří ještě nezahájili přípravu na GDPR. Informace získané v rámci posledního bloku otázek jsou použity pro komparaci s výsledky získanými z odpovědí respondentů, kteří již přípravu na GDPR zahájili.

16. **V čem předpokládáte největší problém při zavádění GDPR?**

4.5. Stanovení předpokladů výzkumu

1. **Polovina ze všech respondentů se ještě nezačala připravovat na GDPR.**

Prvním předpokladem tohoto výzkumu je, že polovina respondentů se ještě nezačala připravovat na GDPR.

2. **Alespoň třetina z respondentů, kteří se již připravují, využila pomoc nějakého partnera.**

Druhým předpokladem je, že třetina respondentů, kteří již přípravu zahájili, využila pomoc nějakého partnera.

3. **Právní subjektivita ovlivňuje, zda se subjekt již připravuje na GDPR.**

Třetí předpoklad říká, že existuje vztah mezi právní subjektivitou a skutečností, zda se daný podnik na GDPR již připravuje nebo ne.

4. **Hlavním problémem pro podnikatelské subjekty bude nedostatek dostupných informací k problematice.**

Čtvrtý předpoklad se týká možných problémů, které respondenti považují za klíčové.

5. **Volba přípravy s partnerem na GDPR je závislá na právní subjektivitě.**

Pátý předpoklad je zaměřen na vztah mezi právní subjektivitou a volbou partnera pro přípravu na GDPR.

6. **Subjekty, které se na GDPR již připravují, očekávaly vyšší náklady než subjekty, které přípravu teprve zahájí.**

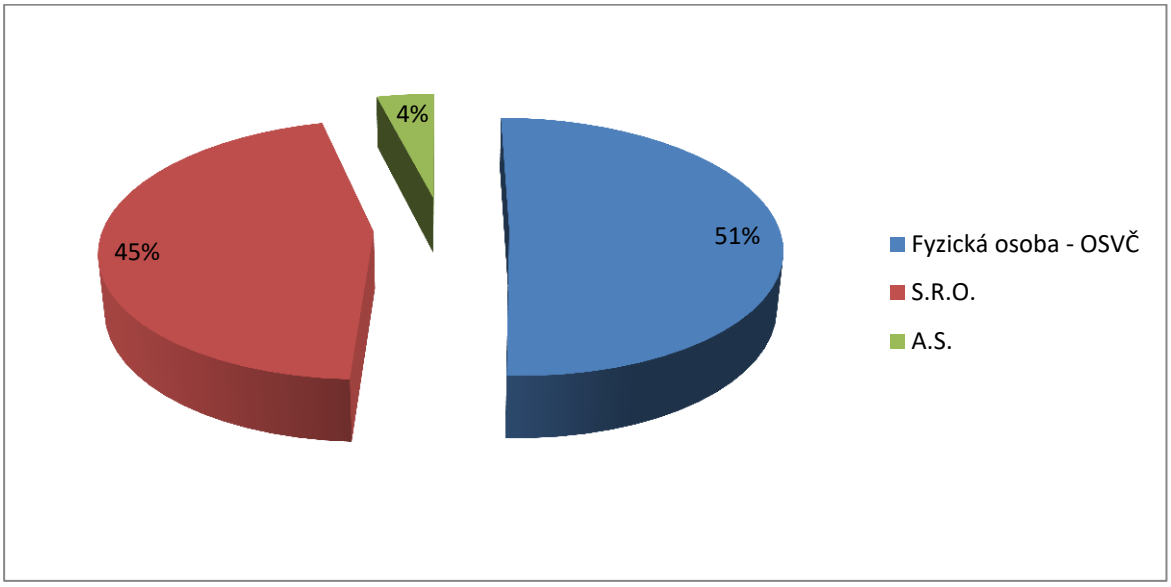
Šestý předpoklad říká, že subjekty, které již přípravu na GDPR zahájily, očekávaly vyšší náklady při přípravě než subjekty, které přípravu v době dotazníkového šetření ještě nezahájily.

5. Vyhodnocení výsledků dotazníkového šetření

V rámci této kapitoly jsou vyhodnoceny výsledky dotazníkového šetření, kterého se zúčastnilo 75 respondentů z celé České republiky. Primárně budou analyzovány odpovědi všech respondentů komplexně, ale vybrané otázky navíc zvlášť pro různé velikosti podniků či pro různé právní subjektivity. V případě kategorických otázek číslo 4 a 6 budou analyzovány vztahy mezi odpověďmi a právní subjektivitou pomocí Fisherova exaktního testu, který bude proveden pomocí online kalkulátoru, který je dostupný na http://astatsa.com/FisherTest/. Dále bude u předpokládaných nákladů všech subjektů provedena lineární regrese s cílem zjistit, zda je mezi získanými daty závislost a které proměnné jsou statisticky významné pro tvorbu závěrů.

1. **Jaká je vaše právní forma podnikání?**

Obrázek 4: Jaká je vaše právní forma podnikání?

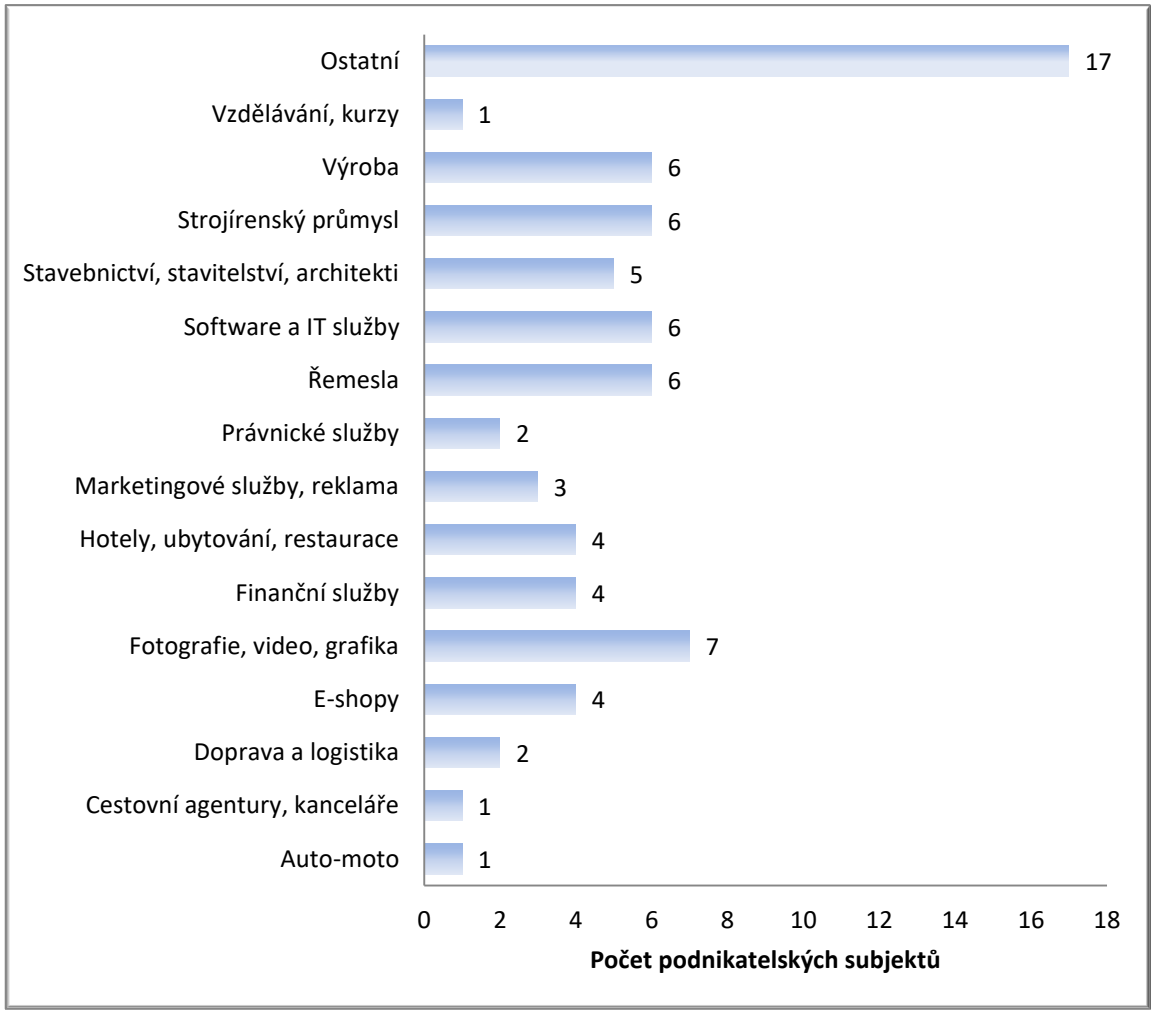


Zdroj: vlastní zpracování, 2018

Z výše uvedeného obrázku je patrné, že polovina respondentů jsou osoby samostatně výdělečně činné, konkrétně se jedná o 38 respondentů, v relativním vyjádření 50,67 % všech účastníků šetření. 34 respondentů označilo jakožto právní formu podnikání společnost s ručením omezeným a 3 respondenti reprezentovali akciové společnosti.

2. Jaký je váš obor podnikání?

Obrázek 5: Jaký je váš obor podnikání?

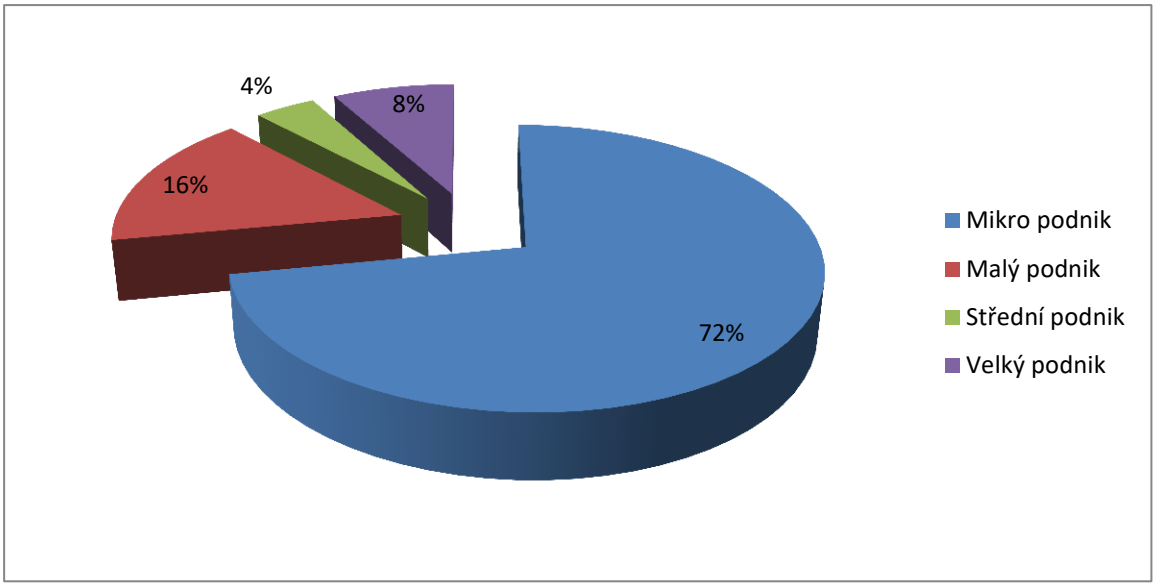


Zdroj: vlastní zpracování, 2018

Z výše uvedené tabulky je patrné, že nejvíce zastoupenou oblastí podnikaní v dotazníkovém šetření, je fotografie, video a grafika. Na druhém místě jsou s počtem šesti respondentů čtyři odvětví, a to výroba, strojírenský průmysl, software a IT služby a řemesla. Následuje stavebnictví, stavitelství, architekti, tuto možnost zvolilo 5 podnikatelských subjektů. Hotely, ubytování, restaurace, finanční služby a E-shopy zvolilo celkem 12 respondentů, každou kategorii shodně 4 dotazovaní. Celkem 17 respondentů zvolilo jako obor podnikání ostatní, tudíž nemůžeme přesně určit předmět podnikání.

3. Jaká je velikost vašeho podniku?

Obrázek 6: Jaká je velikost vašeho podniku?

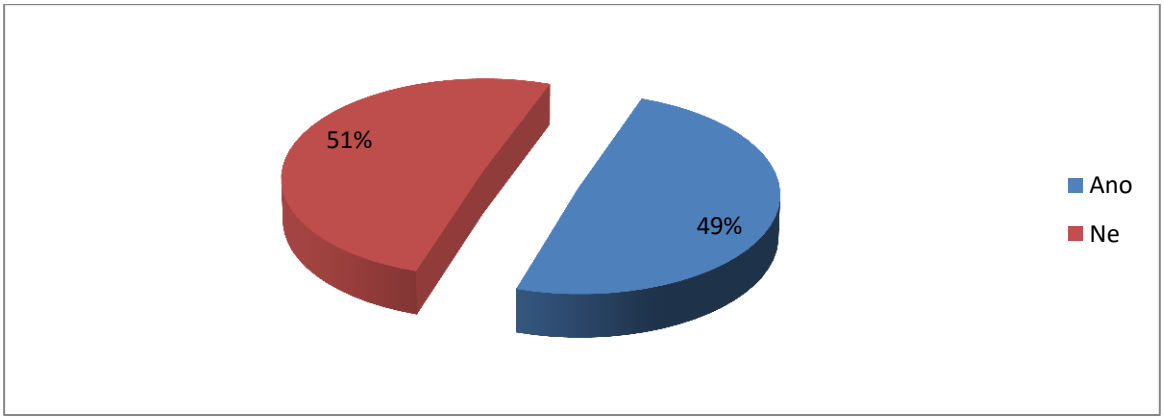


Zdroj: vlastní zpracování, 2018

Z odpovědí na třetí otázku byla nejčastěji volena možnost mikro podniku a to v 54 případech, což představuje 72 % dotázaných. Druhou nejčastější odpovědí byl malý podnik, který označilo 12 respondentů, tedy 16 % účastníků šetření. Velké podniky v našem dotazníkovém šetření reprezentovalo 6 respondentů a střední podniky 4 %, tedy 3 ze 75 dotázaných.

4. Připravujete se na GDPR?

Obrázek 7: Připravujete se na GDPR?



Zdroj: vlastní zpracování, 2018

Čtvrtá otázka dotazníkového šetření dávala respondentům vybrat ze dvou možností. 50,67 % subjektů respektive 38 dotázaných odpovědělo, že se na GDPR ještě nepřipravují. Dle výsledků šetření přípravu již zahájilo 49.33 % respondentů, což představuje 37 odpovědí.

Výsledky odpovědí získaných v rámci otázky číslo 4 potvrzují první předpoklad výzkum, že polovina respondentů ještě nezahájila přípravu na GDPR.

Tabulka 1: Vztah mezi velikostí podniku a přípravou na GDPR

	Mikro podnik	**Malý podnik**	**Střední podnik**	**Velký podnik**
Ano, připravujeme se	37 %	75 %	67 %	100 %
Ne, nepřipravujeme se	63 %	25 %	33 %	0 %
Celkem	100 %	100 %	100 %	100 %

Zdroj: vlastní zpracování, 2018

Výše uvedená tabulka uvádí vztah mezi velikostí podniku a skutečností, zda již byla zahájena příprava na GDPR. Z výsledků vyplývá, že u velkých podniků byla příprava zahájena ve 100 % případů, z mikro podniků, které jsou z velké části zastoupeny osobami samostatně výdělečně činnými, přípravu zahájilo pouze 37 % dotazovaných.

Tabulka 2: Vztah mezi právní subjektivitou a přípravou na GDPR

	Právní subjektivita		
Příprava	**OSVČ**	**S. R. O.**	**A. S.**
Ano (počet subjektů)	10	24	3
Ne (počet subjektů)	28	10	0

Zdroj: vlastní zpracování, 2018

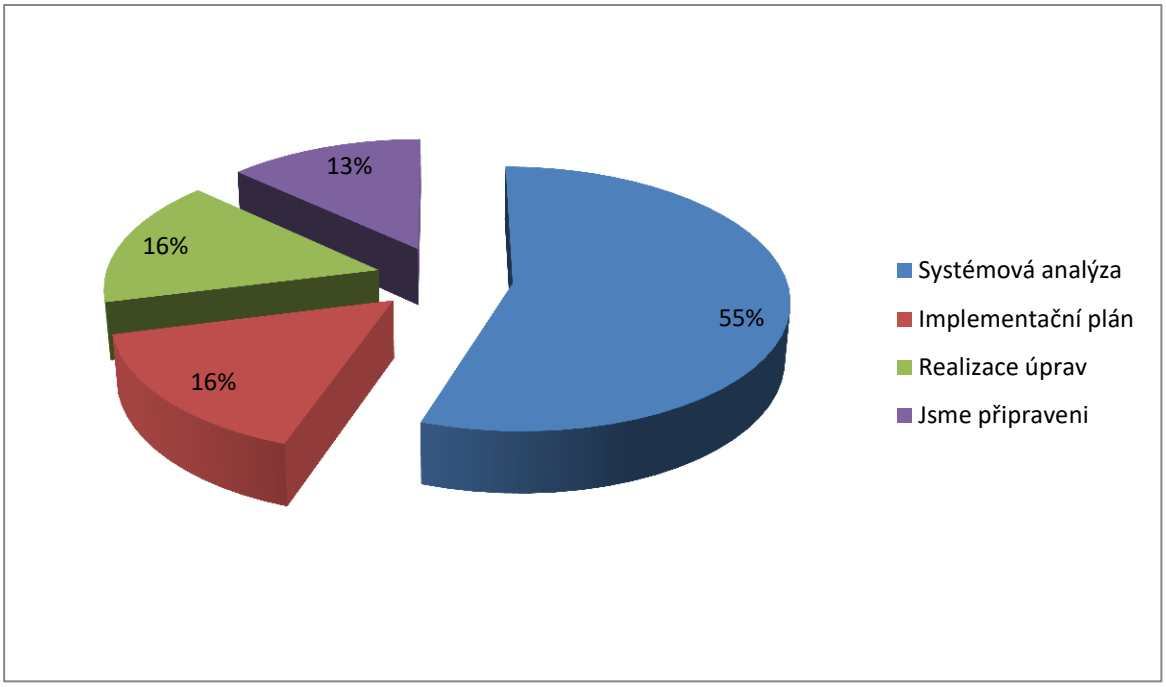
Tabulka číslo 2 slouží jako podklad pro Fisherův exaktní test, který zkoumá nezávislost kategorických proměnných. V tomto případě je zkoumán vztah mezi právní subjektivitou a skutečností, zda daná podnikatelská jednotka započala přípravu na GDPR či ne. Nulová hypotéza v případě tohoto testu zní takto: „Příprava na GDPR je

nezávislá na právní subjektivitě.“ P-hodnota vychází 0,0001, takže na základě tohoto výsledku zamítáme nulovou hypotézu.

Výše uvedený výsledek potvrzuje předpoklad číslo 3, který říká, že právní subjektivita ovlivňuje skutečnost, zda subjekt zahájil přípravu na GDPR nebo ne.

5. V jaké fázi příprav na GDPR se nacházíte?

Obrázek 8: V jaké fázi příprav na GDPR se nacházíte?



Zdroj: vlastní zpracování, 2018

Pátá otázka se již týká pouze respondentů, kteří zahájili svoji přípravu na GDPR. Nejvíce označovanou odpovědí byla systémová analýza, jakožto první fáze přípravy na GDPR, kterou vybralo 20 dotázaných. Druhou a třetí fázi, respektive implementační plán a realizaci úprav, zvolil stejný počet subjektů. Obě varianty byly zvoleny v šesti případech. Ze všech respondentů, kteří se již začali připravovat na GDPR bylo pouze 13 % již připraveno. Těchto 13 % představuje 5 podnikatelských subjektů z 37, kteří se již připravují na GDPR, ze 75 celkem dotázaných.

Tabulka 3: Vztah mezi velikostí podniku a fází přípravy na GDPR

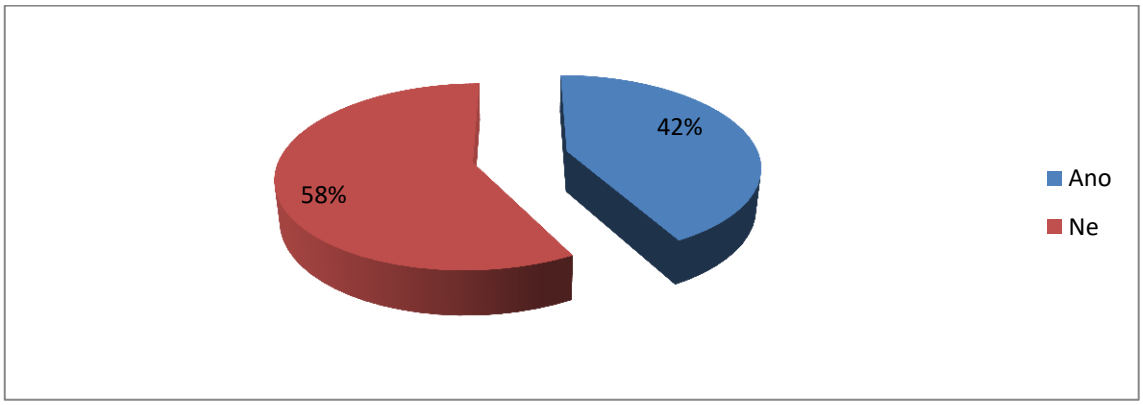
	Mikro podnik	Malý podnik	Střední podnik	Velký podnik
Systémová analýza	55 %	44,4 %	100 %	50,0 %
Implementační plán	20 %	11,1 %	0 %	16,7 %
Realizace úprav	10 %	33,3 %	0 %	16,7 %
Jsme připraveni	15 %	11,1 %	0 %	16,7 %
Celkem	100 %	100 %	100 %	100 %

Zdroj: vlastní zpracování, 2018

Tabulka číslo 3 uvádí vztah mezi velikostí podniku a fází přípravy na GDPR. Výsledky ukazují, že 50 % velkých podniků je zatím ve fázi systémové analýzy. V této fázi se nachází 100 % středních podniků, které se zúčastnily průzkumu a již se začaly připravovat a 44,4 % malých podniků. Z mikro podniků se ve fázi systémové analýzy nachází 55 % subjektů, což je v absolutním vyjádření 11 respondentů. Připravenost na GDPR vykazuje 16,7 % velkých podniků, což představuje jeden podnikatelský subjekt. Z mikro podniků hlásí připravenost 15 % dotazovaných, těchto 15 % procent představuje 3 respondenty. V závěrečné fázi realizace úprav se nachází 33,3 % malých podniků a 16,7% velkých podniků. Z mikro podniků se v této fázi nachází 10 % subjektů

6. Probíhala vaše příprava na GDPR ve spolupráci s nějakým partnerem?

Obrázek 9: Probíhala vaše příprava na GDPR ve spolupráci s nějakým partnerem?



Zdroj: vlastní zpracování, 2018

V rámci této otázky mohl respondent zvolit, zda si přípravu na GDPR řešil sám nebo zda využil spolupráci s nějakým partnerem. Čtyři desetiny respondentů, kteří se již připravovali, v absolutním vyjádření 16 dotazovaných, využilo pro přípravu partnera. Pro řešení bez partnera se rozhodlo 22 podnikatelských subjektů.

Druhý předpoklad výzkumu byl potvrzen, protože přípravu s partnerem realizovalo 42 % podnikatelských subjektů (předpoklad zněl alespoň třetina respondentů, kteří se již připravují).

Tabulka 4: Vztah mezi velikostí podniku a využitím partnera pro přípravu na GDPR

	Mikro podnik	**Malý podnik**	**Střední podnik**	**Velký podnik**
Ano, spolupracujeme s partnerem	35 %	33 %	50 %	83 %
Ne, GDPR si řešíme sami	65 %	67 %	50 %	17 %
Celkem	100 %	100 %	100 %	100 %

Zdroj: vlastní zpracování, 2018

Výsledky tabulky vztahu mezi velikostí podniku a využitím partnera pro přípravu na GDPR poukazují na fakt, že čím větší podnikatelský subjekt je, tím spíše využil pro přípravu partnera. Z velkých podniků využilo partnera celých 83 % subjektů, což je v absolutním vyjádření 5 podnikatelských jednotek z 6, které se dotazníkového šetření zúčastnily. Z mikro podniků, které se již začaly připravovat, využilo pomoc partnera 35 % dotazovaných. Situace u malých podniků je obdobná, zde využilo pomoc partnera 33 % podniků a v případě středních podniků dochází k využití partnera v 50 % případů.

Tabulka 5: Vztah mezi právní subjektivitou a volbou partnera pro přípravu na GDPR

	Právní subjektivita		
Partner	**OSVČ**	**S. R. O.**	**A. S.**
Ano (počet subjektů)	3	11	2
Ne (počet subjektů)	7	13	1

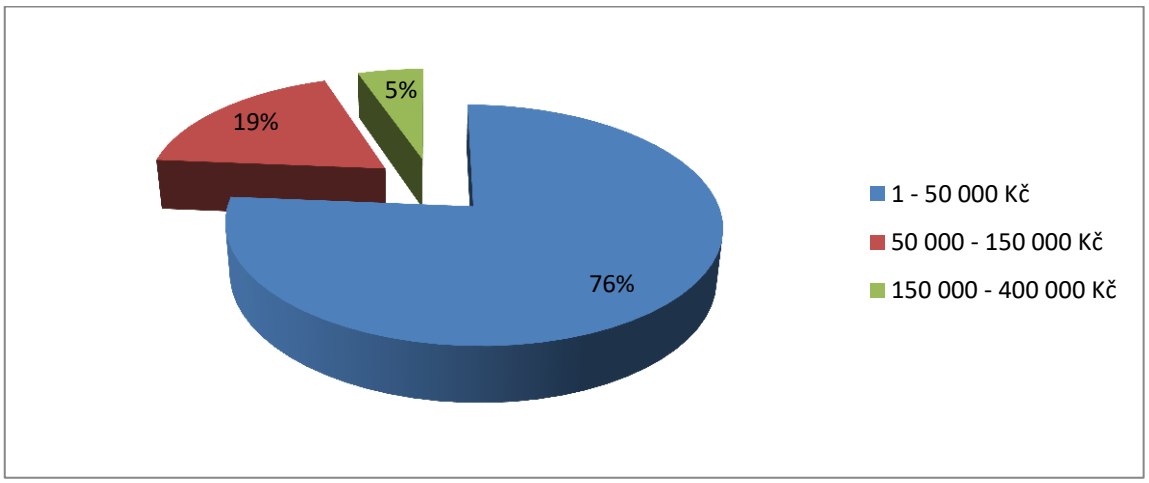
Zdroj: vlastní zpracování, 2018

Tabulka číslo 5 výše znázorňuje data, která slouží jako podklad pro Fisherův exaktní test. V tomto případě je zkoumán vztah mezi právní subjektivitou a volbou partnera pro přípravu na GDPR. Nulová hypotéza v tomto případě zní takto: „Volba přípravy s partnerem na GDPR je nezávislá na právní subjektivitě." P-hodnota Fisherova exaktního testu vychází 0,5144, tudíž na základě tohoto výsledku nelze zamítnout nulovou hypotézu.

Vzhledem k výsledkům Fisherova exaktního testu není možné potvrdit pátý předpoklad výzkumu, který říká, že volba přípravy na GDPR za pomoci partnera je závislá na právní subjektivitě.

7. Jaké byly vaše předpokládané náklady spojené se zavedením GDPR?

Obrázek 10: Jaké byly vaše předpokládané náklady spojené se zavedením GDPR?



Zdroj: vlastní zpracování, 2018

Otázka číslo sedm se zabývá předpokládanými náklady na zavedení GDPR u podnikatelského subjektu. Celkem 28 podnikatelských subjektů, v relativním vyjádření 76 %, označilo možnost 1 – 50 000 Kč. 19 % dotazovaných, kteří se již začali na GDPR připravovat, předpokládalo náklady ve výši 50 000 – 150 000 Kč. V absolutním vyjádření to představuje 7 respondentů. Pouze 2 z dotazovaných předpokládali náklady na zavedení GDPR ve výši 150 000 – 400 000 Kč, v rámci tohoto šetření se jedná 5 % podnikatelských subjektů, které se již začaly připravovat na zavedení GDPR.

Tabulka 6: Vztah mezi velikostí podniku a předpokládanými náklady na zavedení GDPR

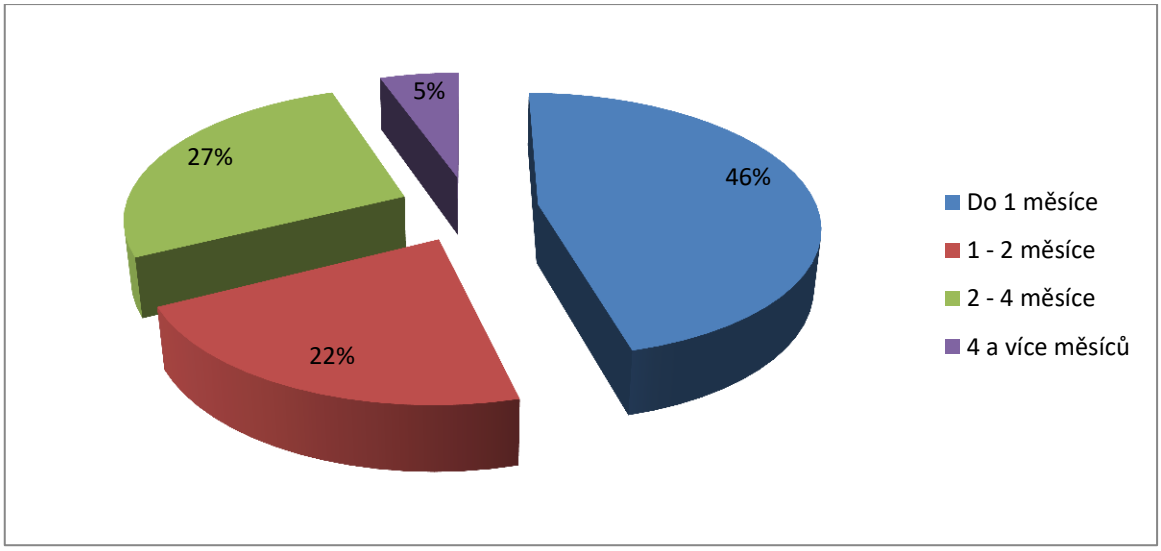
	Mikro podnik	**Malý podnik**	**Střední podnik**	**Velký podnik**
1 - 50 000 Kč	100,00 %	77,78 %	50,00 %	0,00 %
50 000 - 150 000 Kč	0,00 %	22,22 %	50,00 %	66,67 %
150 000 - 400 000 Kč	0,00 %	0,00 %	0,00 %	33,33 %
Celkem	100,00 %	100,00 %	100,00 %	100,00 %

Zdroj: vlastní zpracování, 2018

Vztah mezi velikostí podniku a předpokládanými náklady na zavedení GDPR mapuje tabulka číslo 5. Z tabulky jasně vyplývá úměrnost mezi velikostí podniku a předpokládanými náklady na zavedení GDPR. Zatímco 100 % mikro podniků předpokládá náklady v rozmezí 1 – 50 000 Kč, 22,22 % malých podniků už odhaduje náklady na 50 000 – 150 000 Kč. V tomto cenovém rozmezí odhaduje své náklady také 50 % středních podniků a 66,67 % velkých podniků.

8. Jak dlouho jste předpokládali, že bude trvat vaše příprava na GDPR?

Obrázek 11: Jak dlouho jste předpokládali, že bude trvat vaše příprava na GDPR?



Zdroj: vlastní zpracování, 2018

Z obrázku číslo 11 je patrné, že téměř polovina respondentů předpokládala, že doba přípravy na GDPR nebude delší než jeden měsíc. Tuto možnost zvolilo celkem 17 podnikatelských subjektů, tzn. 46 %. Druhou nejčastější odpovědí byla varianta 2 – 4 měsíce, která byla zvolena celkem 10 respondenty. 8 dotazovaných odhadovalo dobu přípravy na 1 – 2 měsíce a pouze 5 % subjektů, v absolutním vyjádření 2 dotazovaní, předpokládali dobu přípravy v délce 4 a více měsíců.

Tabulka 7: Vztah mezi velikostí podniku a předpokládanou dobou trvání přípravy na GDPR

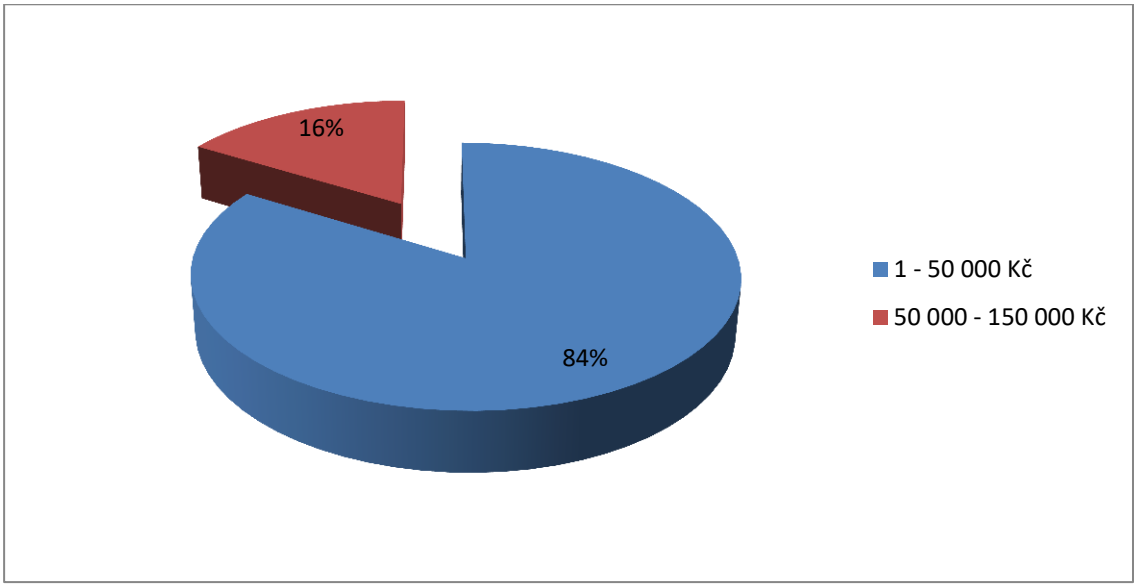
	Mikro podnik	**Malý podnik**	**Střední podnik**	**Velký podnik**
Do 1 měsíce	75,00 %	33,33 %	0,00 %	0,00 %
1 - 2 měsíce	25,00 %	11,11 %	0,00 %	33,33 %
2 - 4 měsíce	0,00 %	44,44 %	100,00 %	50,00 %
4 a více měsíců	0,00 %	11,11 %	0,00 %	16,67 %
Celkem	100,00 %	100,00 %	100,00 %	100,00 %

Zdroj: vlastní zpracování, 2018

Z tabulky číslo 6 je patrná úměra mezi velikostí podniku a předpokládanými výdaji na zavedení GDPR. V tabulce číslo 7 je situace podobná, tato tabulka popisuje vztah mezi velikostí podniku a předpokládanou dobou trvání přípravy na GDPR. Tři čtvrtiny dotazovaných z kategorie mikro podniků předpokládají dobu trvání přípravy do 1 měsíce, naproti tomu 100 % středních podniků a 50 % velkých podniků předpokládá dobu přípravy v rozmezí 2 – 4 měsíců. Dobu trvání přípravy 4 a více měsíců pak očekává 16,67 % velkých podniků a 11,11 % malých podniků.

9. Jaké byly vaše dosavadní/celkové náklady spojené se zavedením GDPR?

Obrázek 12: Jaké byly vaše dosavadní/celkové náklady spojené se zavedením GDPR?



Zdroj: vlastní zpracování, 2018

Otázka číslo 9 navazuje na otázku číslo 7 a zkoumá skutečné dosavadní nebo celkové náklady vynaložené při zavádění GDPR. Z obrázku číslo 8 vyplývá, že pouze 13 % z dotazovaných, kteří se již začali připravovat, již ukončilo přípravu na GDPR. Proto mohou být závěry vycházející z obrázku číslo 12 neúplné. Podnikatelské subjekty náklady ještě očekávají v dalších fázích přípravy na GDPR a nedokázaly je vyčíslit. Dle průzkumu 84 % podnikatelských subjektů, které se již začaly připravovat, měly dosavadní nebo celkové náklady v rozmezí 1 – 50 000 Kč. Náklady v intervalu 50 000 – 150 000 Kč zaznamenalo celkem 16 % respondentů.

Tabulka 8: Vztah mezi velikostí podniku a skutečnými náklady na zavedení GDPR

	Mikro podnik	Malý podnik	Střední podnik	Velký podnik
1 - 50 000 Kč	95,00 %	88,89 %	100,00 %	33,33 %
50 000 - 150 000 Kč	5,00 %	11,11 %	0,00 %	66,67 %
150 000 - 400 000 Kč	0,00 %	0,00 %	0,00 %	0,00 %
Celkem	100,00 %	100,00 %	100,00 %	100,00 %

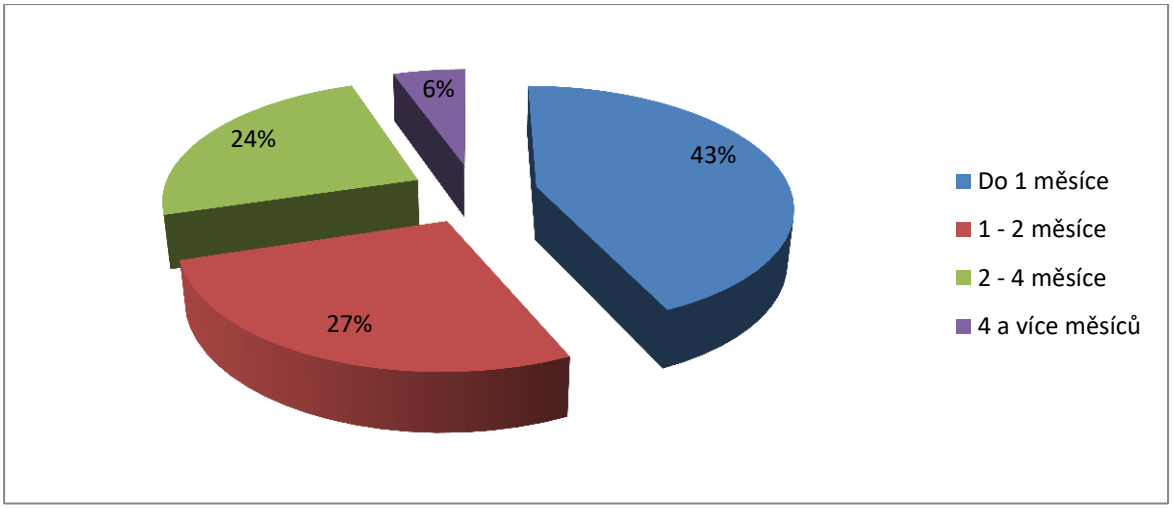
Zdroj: vlastní zpracování, 2018

V tabulce výše je shrnuta závislost mezi velikostí podniku a skutečnými náklady, které subjekty zatím vynaložily na zavedení GDPR. Tabulka číslo 8 navazuje na tabulku číslo 6, která dokumentovala očekávané náklady při zavádění GDPR. Při komparaci těchto dvou tabulek je možné zjistit, že v případě velkých podniků se dosavadní náklady 66,67 % respondentů shodovaly s očekáváním z tabulky 6.

V případě středních podniků mělo 100 % dotazovaných dosavadní náklady do 50 000 Kč, 50 % však odhadovalo náklady v rozmezí 50 000 – 150 000 Kč. Všechny střední podniky se nacházely v době výzkumu v první fázi systémové analýzy, takže celková částka, která bude skutečně vynaložena na zavedení GDPR může být odlišná.

10. Jak dlouho celkem trvala/trvá vaše příprava na GDPR?

Obrázek 13: Jak dlouho celkem trvala/trvá vaše příprava na GDPR?

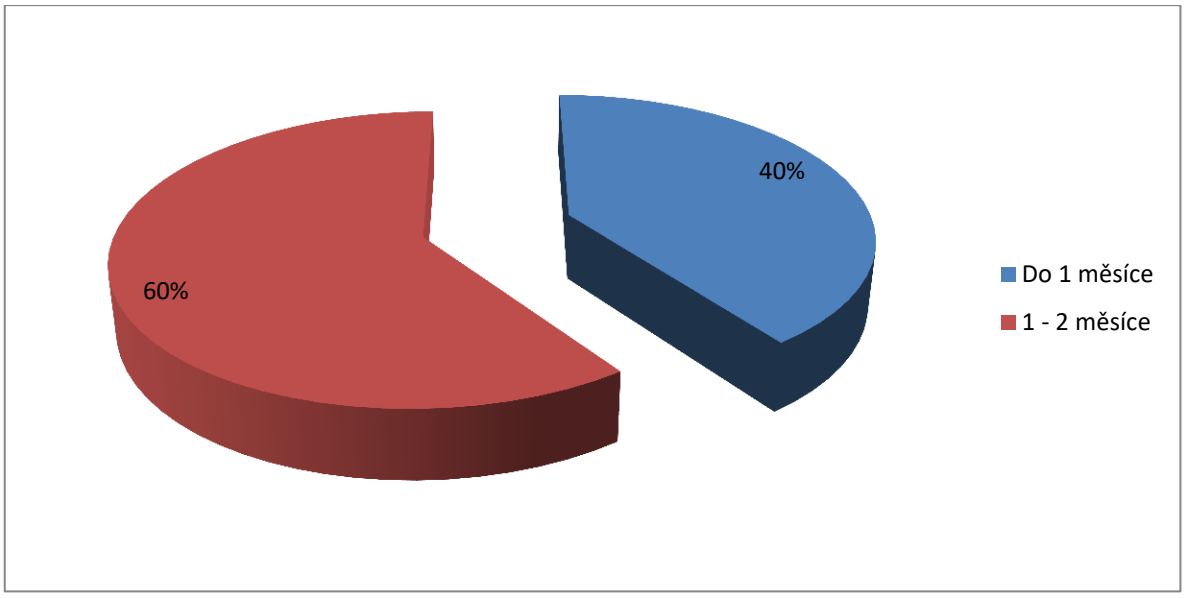


Zdroj: vlastní zpracování, 2018

Otázka číslo 10 navazuje na otázku číslo 8, která zkoumala očekávání respondentů týkající se časové náročnosti zavádění GDPR. Z výše uvedeného obrázku číslo 13 vyplývá, že 16 z dotazovaných podnikatelských subjektů zaznamenalo přípravu v horizontu do 1 měsíce. Celkem 27 % respondentů, v absolutním vyjádření 10 subjektů, označilo odpověď 1 – 2 měsíce jakožto dobu, po kterou se již připravují. 9 podnikatelských subjektů odpovědělo na otázku číslo 10, tak že jejich příprava trvala nebo trvá 2 – 4 měsíce a 2 respondenti uvedli, že jejich příprava trvá či trvala 4 a více měsíců.

Výše popsaná data nemají adekvátní vypovídací hodnotu, protože ne všechny subjekty již svou přípravu dokončily a tudíž se doby přípravy ještě mohou měnit. Vzhledem k těmto skutečnostem je níže vytvořen obrázek číslo 14, který mapuje pouze subjekty, které již svou přípravu na zavedení GDPR zdárně dokončily.

Obrázek 14: Jak dlouho celkem trvala příprava subjektů, které jsou již připraveny na GDPR.



Zdroj: vlastní zpracování, 2018

Dle dotazníkového šetření přípravu ukončilo celkem 5 subjektů ze 75 dotázaných. Z těchto 5 podnikatelských subjektů je jeden velký podnik, jeden malý podnik a 3 mikro podniky. Z grafu výše je patrné, že 40 % respondentů dokončilo přípravu do 1 měsíce a 60 % respondentů potřebovalo 1 – 2 měsíce na zavedení GDPR. V níže uvedené tabulce jsou uvedeny počty jednotlivých podnikatelských subjektů rozdělených dle velikosti podniku a časová rozmezí, které subjekty potřebovaly pro dokončení přípravy na GDPR.

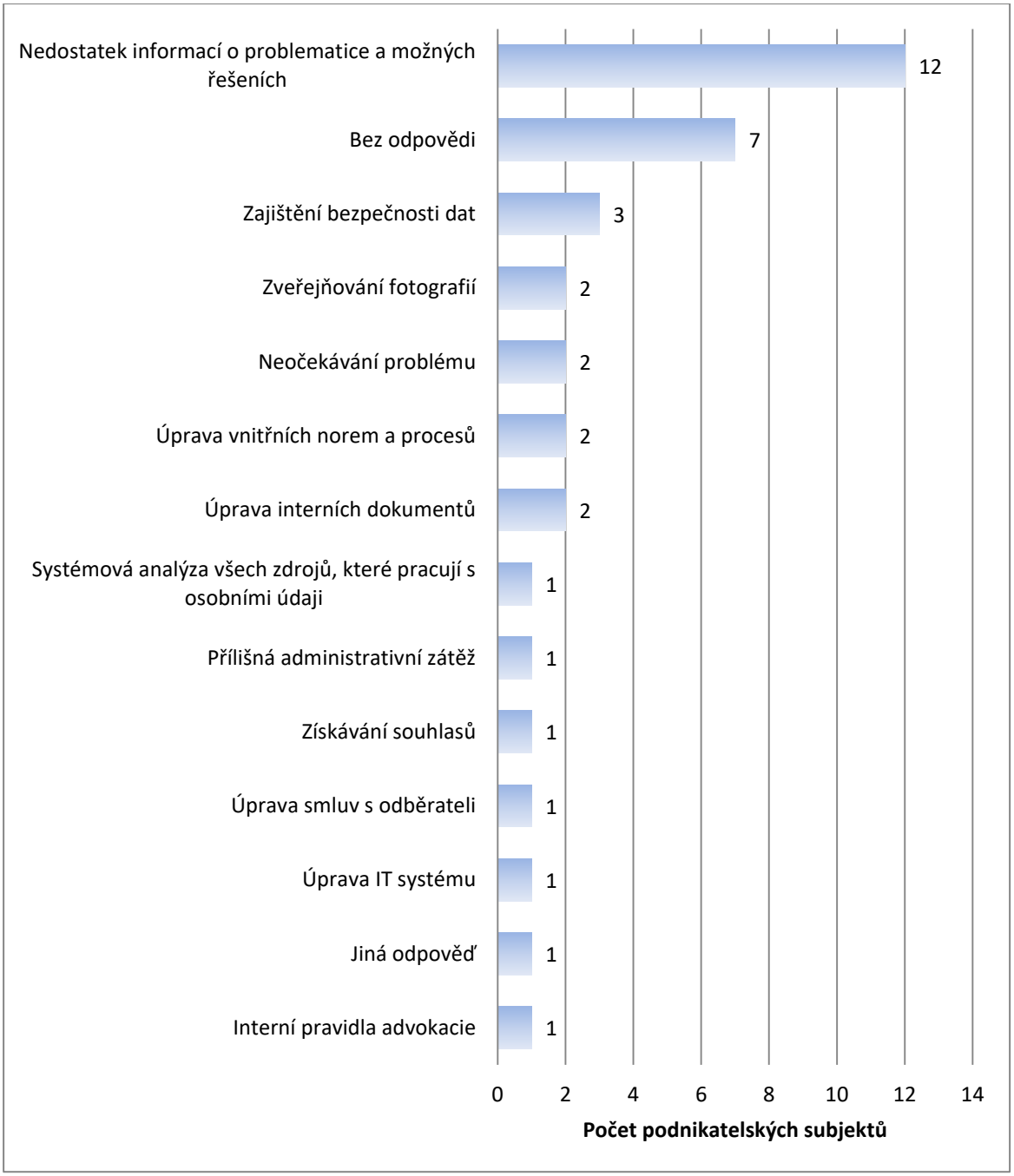
Tabulka 9: Vztah mezi velikostí podniku a dobou dokončení přípravy na GDPR

	Mikro podnik	**Malý podnik**	**Velký podnik**
Do 1 měsíce (počet subjektů)	2	0	0
1 - 2 měsíce (počet subjektů)	1	1	1

Zdroj: vlastní zpracování, 2018

11. V čem jste předpokládali největší problém při zavádění GDPR?

Obrázek 15: V čem jste předpokládali největší problém při zavádění GDPR?



Zdroj: vlastní zpracování, 2018

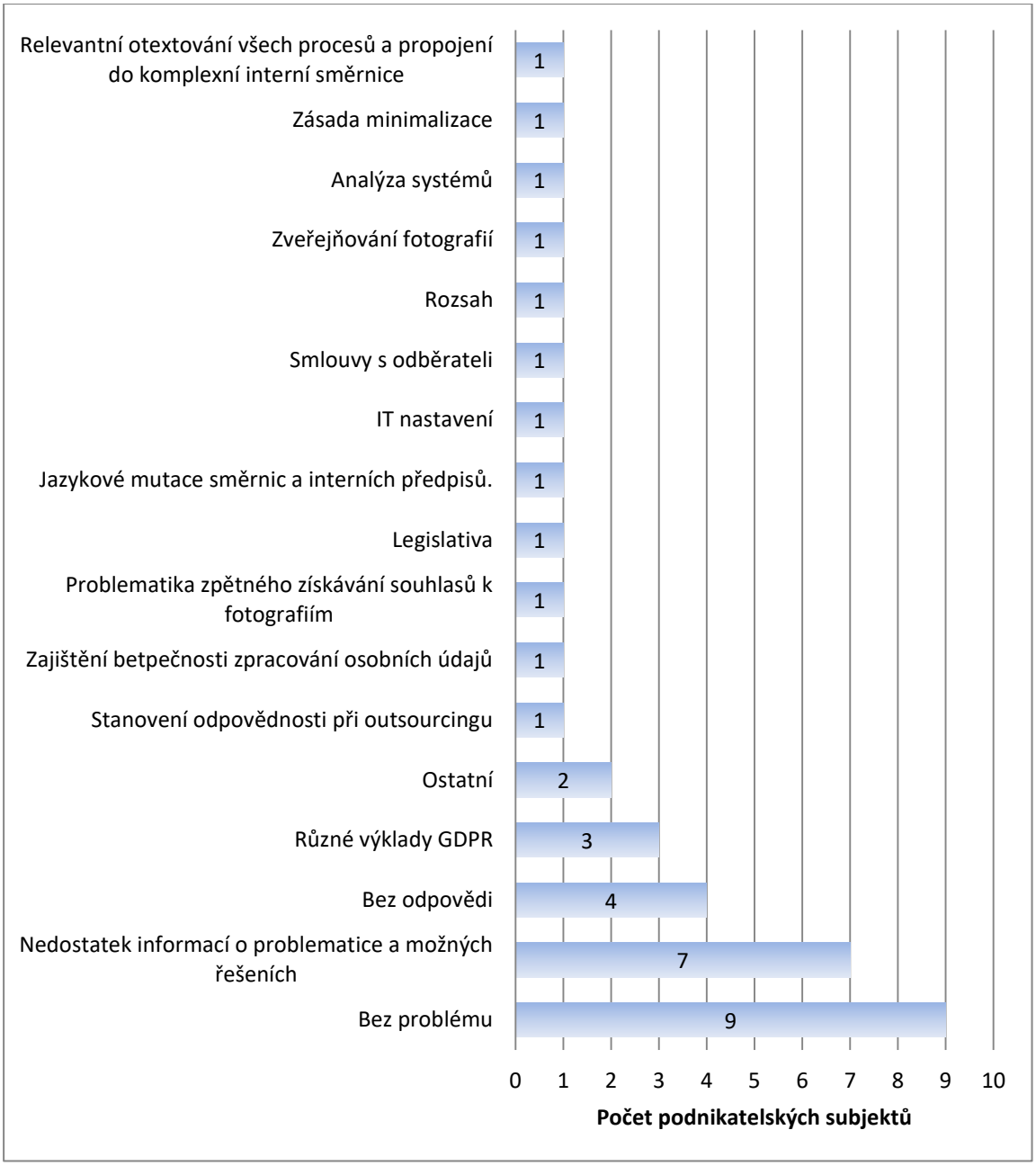
Otázky číslo 11, 12 a 16 byly otázky otevřené. Respondenti měli možnost napsat, co považovali za největší problém a v případě dotazovaných, kteří již zahájili přípravu,

bylo možné uvést i největší problém se kterým se doposud při implementaci GDPR setkali.

Z průzkumu vyplývá, že téměř třetina respondentů, kteří již přípravu zahájili, považuje za nejproblematičtější faktor skutečnost, že chybí informace o problematice GDPR a konkrétní řešení, která by byla dostačující pro případnou kontrolu. Další relevantní odpovědí byla obava o zajištění bezpečnosti dat nebo problematika zveřejňování fotografií. Subjekty více zainteresované do GDPR problémy neočekávaly a další nejčastěji uváděnou odpovědí byla problematika úpravy vnitřních norem a procesů. Zbylé odpovědi se týkaly hlavně IT řešení, administrativní zátěže, problematiky získávání souhlasů atd.

12. Co byl pro vás největší problém při zavádění GDPR?

Obrázek 16: Co byl pro vás největší problém při zavádění GDPR?



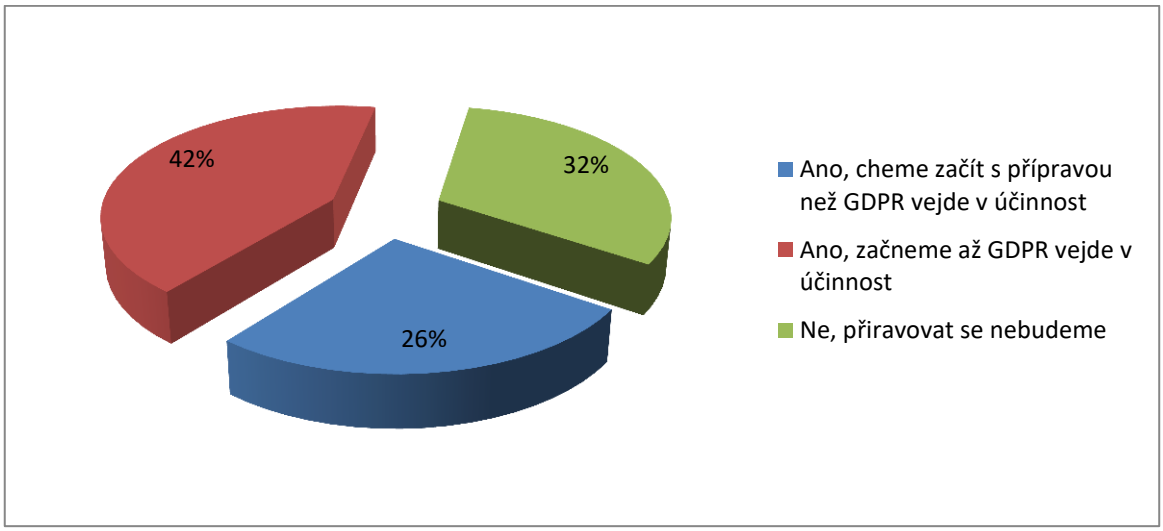
Zdroj: vlastní zpracování, 2018

Otázka číslo dvanáct se dotazovala již připravujících se respondentů na největší problémy, se kterými se v průběhu zavádění GDPR setkali. Celkem 24 % dotazovaných uvedlo, že se v průběhu implementace GDPR zatím nesetkalo s problémem. Naopak 19 % respondentů uvedlo, že informací k možným řešením není dostatek. Stejná

odpověď byla nejčastěji uváděnou volbou v předpokládaných problémech. Celkem 3 respondenti označili za problém, se kterým se setkali, různé výklady GDPR. Volbu této odpovědi lze přisuzovat faktu, že dotazníkové šetření probíhalo před nabytím účinnosti GDPR. Zbylé odpovědi byly individuálního charakteru s četností jednoho respondenta na odpověď.

13. Plánujete se připravovat na GDPR ?

Obrázek 17: Plánujete se připravovat na GDPR ?



Zdroj: vlastní zpracování, 2018

Z obrázku číslo 17 je patrné, že přípravu má v plánu zahájit 68 % podnikatelských subjektů, které prozatím přípravu nezahájili. 42 % dotazovaných, v absolutním vyjádření 16 respondentů, uvedlo, že svoji přípravu zahájí až GDPR vejde v účinnost. Celkem 12 ze 75 dotázaných odpovědělo, že se na GDPR připravovat nebudou.

Tabulka 10: Vztah mezi právní subjektivitou a plánováním přípravy na GDPR

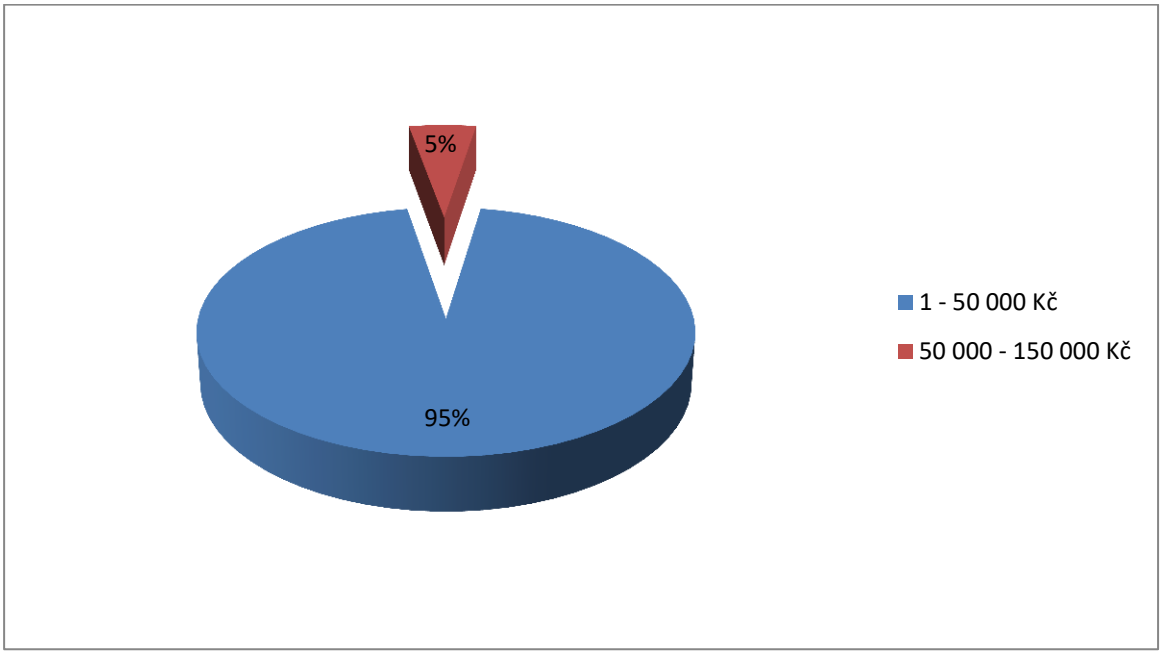
	Právní subjektivita		
Příprava	**OSVČ**	**S. R. O.**	**A. S.**
Ano, než GDPR vejde v účinnost (počet subjektů)	5	5	0
Ano, až GDPR vejde v účinnost (počet subjektů)	13	3	0
Ne (počet subjektů)	10	2	0

Zdroj: vlastní zpracování, 2018

Z výše uvedené tabulky je možné vyvodit závěry, které říkají, že přípravu na GDPR zanedbají hlavně osoby samostatně výdělečně činné, protože ze 75 respondentů dotazníkového šetření 16 % subjektů neplánuje přípravu, v absolutním vyjádření 12 podnikatelských subjektů, z čehož je 10 subjektů OSVČ.

14. Jaké předpokládáte náklady spojené se zavedením GDPR?

Obrázek 18: Jaké předpokládáte náklady spojené se zavedením GDPR?



Zdroj: vlastní zpracování, 2018

Obrázek 18 popisuje předpokládané náklady subjektů, které přípravu na GDPR ještě nezahájily. Z grafu je možné usuzovat, že většina respondentů této kategorie předpokládá, že náklady nepřevýší 50 000 Kč.

Pro předpokládané náklady spojené se zavedením GDPR všech podnikatelských subjektů byla provedena lineární regresní analýza, do které byly zahrnuty právní formy podnikání a také skutečnost, zda daný subjekt již zahájil přípravu na GDPR či ne. Došlo také k upravení intervalů odhadovaných nákladů na střední hodnoty těchto intervalů, což může způsobit jisté odchylky. Odhady regresních koeficientů a směrodatné odchylky jsou znázorněny v tabulce níže.

Tabulka 11: Odhady regresních koeficientů a směrodatné odchylky lineární regresní analýzy (v Kč)

	Připravenost na GDPR	A. S.	OSVČ	Absolutní člen
Regresní koeficient	10 268	117 078	-2 768	30 987
Směrodatná odchylka	8 177	18 859	8 177	7 854

Zdroj: vlastní zpracování, 2018

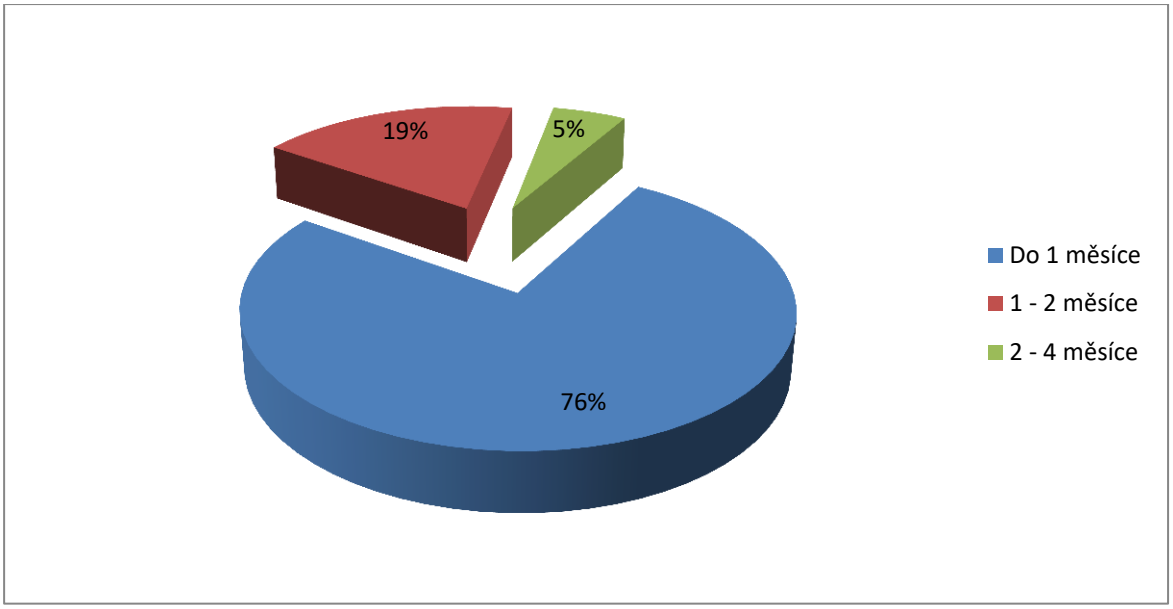
Poslední sloupec tabulky je absolutní člen, který značí průměrné odhadované náklady firmy, která odpovídá základním kategoriím. Při výpočtu byla využita firma s právní subjektivitou S. R. O., která se nepřipravuje na GDPR. Zbylé hodnoty v prvním řádku tabulky představují rozdíly v průměrných odhadovaných nákladech jiných právních subjektivit oproti absolutnímu členu. První sloupec tabulky značí rozdíl mezi subjekty, které se již připravují a těmi, které přípravu zatím nezahájily.

Výsledky lze interpretovat tak, že subjekty, které se připravují, odhadují své náklady o cca 10 000 Kč vyšší než subjekty, které se nepřipravují. V případě těchto závěrů je nutné zohlednit, že vzhledem k malému počtu dat nelze činit obecné závěry, neboť daný regresní koeficient není statisticky významný. Subjekty, které se nepřipravují, například A.S. odhadují své náklady na cca 148 000 Kč a OSVČ na 28 000 Kč. Na základě statistické významnosti regresního koeficientu příslušejícího A.S. lze zobecněně tvrdit, že existuje rozdíl mezi odhadovanými náklady akciových společností a společností s ručením omezeným.

Šestý předpoklad výzkumu nelze na základě výše uvedených výsledků potvrdit vzhledem k malému počtu dat. Výsledky ukazují, že subjekty, které se již připravují, očekávaly vyšší náklady než subjekty, které přípravu teprve zahájí, nicméně daný regresní koeficient není statisticky významný, tudíž nelze závěry zobecňovat.

15. Jak dlouho předpokládáte, že bude trvat vaše příprava na GDPR?

Obrázek 19: Jak dlouho předpokládáte, že bude trvat vaše příprava na GDPR?



Zdroj: vlastní zpracování, 2018

Z výše zobrazených výsledků vyplývá, že 76 % dotázaných subjektů, které přípravu ještě nezahájily, předpokládá, že příprava na GDPR nepřekročí dobu jednoho měsíce. Vztah mezi právní subjektivitou a předpokládanou dobou přípravy je možné vidět v tabulce číslo 12 níže.

Tabulka 12: Vztah mezi právní subjektivitou a předpokládanou dobou přípravy na GDPR

	OSVČ	S. R. O.
Do 1 měsíce	78,57 %	70,00 %
1 - 2 měsíce	17,86 %	20,00 %
2 - 4 měsíce	3,57 %	10,00 %
Celkem	100,00 %	100,00 %

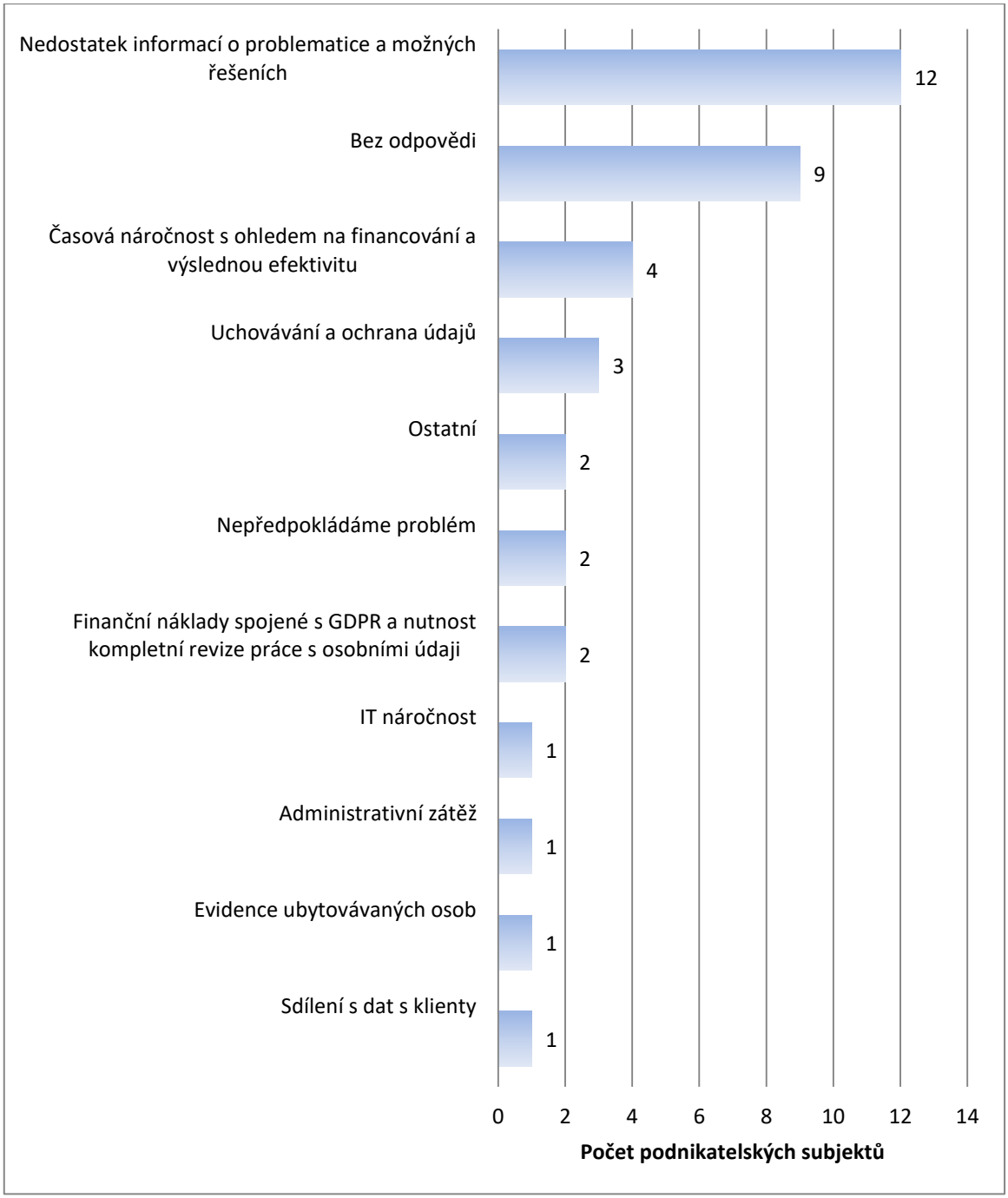
Zdroj: vlastní zpracování, 2018

Výsledky osob samostatně výdělečně činných a společností s ručením omezeným nejsou moc odlišné. 78 % OSVČ a 70 % S.R.O. předpokládá přípravu do 1 měsíce. V absolutním vyjádření to je 22 osob samostatně výdělečně činných a 7 společností

s ručením omezeným. Pouze jedna OSVČ a jedna společnost s ručením omezeným předpokládají přípravu v rozmezí 2 - 4 měsíců.

16. V čem předpokládáte největší problém při zavádění GDPR?

Obrázek 20: V čem předpokládáte největší problém při zavádění GDPR?



Zdroj: vlastní zpracování, 2018

Podnikatelské subjekty, které v průběhu dotazníkového šetření ještě nezahájily přípravu, uvedly, že největší problém předpokládají v nedostatku informací o dané problematice a o možných řešeních. Tato odpověď byla nejčastější i v případě respondentů, kteří již přípravu zahájili. Celkem 12 z 38 dotazovaných, kteří přípravu v době šetření nezahájili, zvolilo tuto možnost. Další frekventovanou odpovědí byla problematika časové náročnosti a zatížení, které dle respondentů není v jejich případě zcela efektivní. Problém časové náročnosti shledává přibližně 10 % dotazovaných. 3 respondenti uvedli, že se obávají problémů v případě uchovávání a ochrany osobních údajů.

Na základě výsledků získaných v rámci otázek číslo 11 a 16 lze konstatovat ověření předpokladu číslo 4. Nejčastěji uvedeným očekávaným problémem se stal nedostatek informací o dané problematice a o možných řešeních.

6. Závěry a doporučení pro oblast ochrany osobních údajů

V závěrečné části této diplomové práce jsou shrnuty závěry z provedeného výzkumu, který se věnoval připravenosti českých podnikatelských subjektů na GDPR. Tyto závěry budou dále využity pro tvorbu doporučení pro oblast ochrany osobních údajů, která budou primárně zaměřena na GDPR.

6.1. Závěry analýzy dotazníkového šetření

Výzkumu se zúčastnilo celkem 75 respondentů, z toho 38 osob samostatně výdělečně činných, 34 společností s ručením omezeným a 3 akciové společnosti. V první části šetření byly analyzovány obecné skutečnosti o podnikatelských subjektech a došlo k rozdělení na respondenty, kteří již zahájili přípravu na GDPR a na respondenty, kteří dosud s přípravou nezačali. Výsledek tohoto rozdělení vytvořil dvě skupiny podnikatelských subjektů, které byly téměř stejně velké. Přípravu na GDPR zahájilo 37 ze 75 podnikatelských subjektů, 38 dotazovaných přípravu dosud nezahájilo.

Velikost skupin však byla jedinou podobností, protože rozložení podnikatelských subjektivit bylo značně odlišné. Skupina připravující se na GDPR obsahovala 10 osob samostatně výdělečně činných, 24 společností s ručením omezením a 3 akciové společnosti. Naopak skupina subjektů, které přípravu nezahájily, se skládala z 28 osob samostatně výdělečně činných a 10 společností s ručením omezeným, akciová společnost zde nebyla žádná. V rámci vyhodnocení dotazníkového šetření byl zkoumán vztah mezi právní subjektivitou a skutečností, zda daná podnikatelská jednotka započala přípravu na GDPR či ne. Stanovená nulová hypotéza, která zněla takto: „Příprava na GDPR je nezávislá na právní subjektivitě.“, byla na základě výsledku Fisherova exaktního testu zamítnuta, tudíž je možné konstatovat, že existuje vztah mezi právní subjektivitou a skutečností, zda daný podnikatelský subjekt přípravu na GDPR zahájil.

Nejčastější fází přípravy respondentů, kteří již přípravu zahájili, byla systémová analýza, kterou označilo celkem 20 dotázaných. Druhou a třetí fázi přípravy, kterou představuje implementační plán a realizace úprav zvolilo 6 respondentů. Připravenost na GDPR potvrdilo pouze 5 z celkem 75 dotázaných podnikatelských subjektů.

Většina velkých podniků zvolila pro přípravu na GDPR možnost spolupráce s partnerem, konkrétně 83 % subjektů, které představují velké podniky. Dále se pro tuto

možnost rozhodlo 50 % středních podniků, 33 % malých podniků a 35 % mikro podniků. Kromě vztahu mezi velikostí podniků a volbou přípravy na GDPR s partnerem byl zkoumán i vztah mezi přípravou s partnerem a právní subjektivitou. Na základě výsledku Fisherova exaktního testu bylo konstatováno, že nelze zamítat nulovou hypotézu, která zněla takto: „Volba přípravy s partnerem na GDPR je nezávislá na právní subjektivitě.“ Tímto výsledkem se neprokázal vztah mezi právní subjektivitou a volbou přípravy na GDPR za pomoci partnera.

Nejčastěji označeným intervalem předpokládaných nákladů se zavedením GDPR se stalo rozmezí 1 – 50 000 Kč, které bylo zvoleno celkem 76 % již se připravujících subjektů a 95 % respondentů, kteří se ještě připravovat nezačali. Předpokládané náklady ve výši 50 000 – 150 000 Kč označilo celkem 19 % subjektů, které již přípravu zahájily a 5 % podnikatelských jednotek, které v době dotazníkového šetření přípravu ještě nezahájily. Náklady ve výši 150 000 – 400 000 Kč předpokládaly pouze dva dotázané subjekty. Pro výše zmíněná data v kombinaci s právními subjektivitami a skutečnostmi, zda dané subjekty již zahájily přípravu či ne, byla zpracována lineární regresní analýza, jejíž výsledky poukazují na trend dokumentující, že subjekty, které se připravují, odhadují své náklady o cca 10 000 Kč vyšší než subjekty, které se nepřipravují, tento trend však nelze obecně paušalizovat vzhledem k malému počtu dat, které neumožňují činit obecné závěry.

Nejčastěji zmiňovaná předpokládaná dobra přípravy na GDPR je horizont jednoho měsíce. Tuto variantu zvolilo 46 % připravujících se subjektů a 76 % nepřipravujících se respondentů. V případě subjektů, které se již připravují, byl položen dotaz směřující na délku dosavadní přípravy. Celkem 43% subjektů označilo horizont jednoho měsíce. Pouze 5 subjektů již přípravu dokončilo, proto nelze na základě těchto výsledků vyvozovat závěry, protože celkové doby přípravy se ještě mohou měnit.

Nejčetnější předpokládaný problém spojený se zaváděním GDPR je nedostatek informací o dané problematice a možných řešeních, která budou akceptována v případě kontroly z úřadu pro ochranu osobních údajů. Tuto odpověď uvedlo celkem 24 dotázaných z celkového počtu 75 účastníků výzkumu. Další nejčastěji uváděné předpokládané problémy se týkají zajištění bezpečnosti dat, sbírání souhlasů nebo zveřejňování fotografií.

6.2. Doporučení pro oblast ochrany osobních údajů

V této podkapitole jsou navržena doporučení pro oblast ochrany osobních údajů, respektive pro Úřad pro ochranu osobních údajů, který je v České republice dozorovým orgánem. Vzhledem ke změnám, které Obecné nařízení vnáší do této problematiky, lze předpokládat zvýšenou potřebu kvalitních a ověřených informací a také ověřených řešení, která mohou menší subjekty využívat. Zvýší-li se povědomí o ochraně osobních údajů, lze předpokládat, že bude docházet k menším únikům a neoprávněnému využívaní citlivých dat.

Doporučení byla tvořena především na základě dat získaných prostřednictvím provedeného výzkumu. Prvním doporučením je návrh vytvoření internetového portálu, pomocí kterého by mohly podnikatelské subjekty čerpat ověřené informace a řešení, sdílet své zkušenosti s danou problematikou a díku tomu zajistit lepší ochranu osobních údajů. Celkem 32% dotázaných během dotazníkového šetření uvedlo, že právě v této oblasti shledává největší problém spojený se zaváděním GDPR.

Druhým doporučením je přiblížení způsobů ochrany osobních údajů pomocí školení pro mikro podniky, které s přípravou nejvíce otálejí, což bylo potvrzeno výsledky výzkumu.

6.2.1. Internetový portál

Prvním návrhem je vytvoření internetového informačního portálu pod záštitou Úřadu pro ochranu osobních údajů. Dle výsledků výzkumu respondenti považují za největší problém nedostatek informací o dané problematice a možných řešeních, která budou akceptována v případě kontroly Úřadem pro ochranu osobních údajů. Hlavním cílem portálu by bylo informovat o možných řešeních a poskytovat ucelené a přehledné výklady Obecného nařízení. Každý podnikatel, který by portál navštívil, by mohl díky jednoduché analýze zjistit, jak moc se ho GDPR týká a které kroky by měl provést. Díky této analýze by podnikatel získal seznam doporučených oblastí, které by měl analyzovat a s pomocí vytvořených checklistů, by mohl analýzy provést. Na základě vyhodnocení checklistů by získal seznam GDPR úkolů, které je nutné provést pro splnění požadavků Obecného nařízení. Součástí vyhodnocení by bylo i doporučení produktů či poskytovatelů služeb, kteří nabízí řešení kompatibilní s GDPR. V neposlední řadě by podnikatelské subjekty získaly k dispozici vzorové dokumenty jako například souhlasy se zpracováním osobních údajů či dodatky ke smlouvám. Dále

by portál sloužil jako místo pro výměnu informací, zkušeností a poskytování poradenství.

6.2.2. Školení

Dle výzkumu s přípravou na GDPR nejvíce otálejí mikro podniky zastoupené hlavně osobami samostatně výdělečně činnými. Vzhledem k těmto výsledkům je druhé doporučení realizovat regionální školení či workshopy pro tyto skupiny podnikatelů, které by poskytlo ucelený a přehledný obraz o možných způsobech ochrany osobních údajů a odkazovalo by na výše zmíněný portál. Tato školení by měla za cíl primárně utřídit informace, které jsou podnikatelům poskytovány prostřednictvím médií, která GDPR označují například jako *„Největší strašák dnešní doby.“*(lupa.cz, 2017)

Závěr

Cílem této diplomové práce bylo analyzovat připravenost firem v České republice na zavedení 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) a následně na základě provedeného výzkumu vyvodit závěry a definovat doporučení pro oblast ochrany osobních údajů.

V první kapitole byly definovány historické milníky ochrany osobních údajů. Druhá kapitola měla za cíl charakterizovat Obecné nařízení, konkrétně důležité pojmy této problematiky, cíle a principy, platnost a účinnost GDPR. Dále bylo cílem kapitoly definovat právní souvislosti, ohraničit zásady a právní důvody pro zpracování osobních údajů a představit pověřence pro ochranu osobních údajů. Třetí kapitola diplomové práce byla zaměřena na důležité body spojené se zaváděním GDPR, například fáze implementace nebo náležitosti smlouvy mezi správcem a zpracovatelem osobních údajů. Druhá polovina diplomové práce se týkala vlastního dotazníkového šetření připravenosti firem. Byly popsány jednotlivé otázky dotazníku, definována metodika a respondenti. Bylo také vyhodnoceno dotazníkové šetření.

V poslední kapitole byly shrnuty závěry šetření a došlo k navrhnutí doporučení pro oblast ochrany osobních údajů, která byla vytvořena na základě informací získaných prostřednictvím výzkumu. Jednalo se především o návrh spuštění internetového informačního portálu, který by pomáhal s analýzou problematických záležitostí spojených s nutnou implementací GDPR podnikatelským subjektům a doporučoval by jim možná řešení. Stal by se tak pomocnou rukou při hledání řešení problémů spojených se zaváděním GDPR.

Seznam použitých tabulek

Seznam použitých obrázků

Seznam použitých zkratek

A.S. – akciová společnost

EU – Evropská unie

GDPR – General Data Protection Regulation

Kč – Korun českých

OSVČ – osoba samostatně výdělečně činná

S.R.O. – společnost s ručením omezeným

V.O.S. – veřejně obchodovatelná společnost

Seznam použité literatury

Knižní zdroje:

KUČEROVÁ, A. a kol. Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: Nakladatelství C.H.Beck, 2003. ISBN 978-80-7179-226-0

MAŠTALKA, Jiří. Osobní údaje, právo a my. V Praze: C.H. Beck, 2008. Beckova edice ABC. ISBN 978-80-7400-033-1.

MATES, P. Ochrana osobních údajů. Praha: Nakladatelství Karolinum, 2002. ISBN 80-246-0469-8.

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

NULÍČEK, Michal. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

Právní předpisy:

Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - Obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů : redakční uzávěrka 28.8.2017. Ostrava: Sagit, 2017. ÚZ. ISBN 978-80-7488-241-8.

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Internetové zdroje:

Co nového GDPR přináší - Ochrana osobních údajů. [online]. Copyright © 2018 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2018-03-26]. Dostupné z: http://www.mvcr.cz/gdpr/clanek/co-noveho-gdpr-prinasi.aspx

Československé sčítání lidu 1930. Český statistický úřad [online] 26.2.2010 [cit. 2018-03-26]. Dostupné z: https://www.czso.cz/csu/sldb/ceskoslovenske_scitani_lidu_1930

Freedom of the Press Act of 1766. Britannica.com [online]. Copyright ©2018 [cit. 2018-03-21]. Dostupné z: https://www.britannica.com/topic/Freedom-of-the-Press-Act-of-1766

Frequently Asked Questions about the GDPR. Home Page of EU GDPR [online]. Copyright © 2018 [cit. 2018-03-26] Dostupné z: https://www.eugdpr.org/gdpr-faqs.html

GDPR Best Practices Implementation Guide [online]. Copyright © 2017 [cit. 2018-03-28] Dostupné z: https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000

GDPR Data Protection Impact Assessment: 5-step methodology. ISO 9001, 13485, 14001, 18001, 20000, 27001, AS9100, IATF 16949 and ITIL implementation [online]. Copyright © 2018 Advisera Expert Solutions Ltd [cit. 2018-03-31]. Dostupné z: https://advisera.com/eugdpracademy/knowledgebase/5-phases-of-the-eu-gdpr-data-protection-impact-assessment/

How to accelerate your GDPR journey . [online]. Copyright © Microsoft 2018 [cit. 2018-03-26]. Dostupné z: https://info.microsoft.com/CE-SCRTY-CNTNT-FY18-08Aug-30-HowtoaccelerateyourGDPRjourney351101_004_01Registration-ForminBody.html

Implementace GDPR do praxe úřadu [online]. 17.7.2017 [cit. 2018-03-30]Dostupné z: https://spmo.cz/wp-content/uploads/2017/07/Implementace-GDPR-e-kniha.pdf

Nejdůležitější pojmy: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-25]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293

Největší strašák dnešní doby se skrývá pod zkratkou GDPR - Lupa.cz. Lupa.cz - server o českém Internetu [online]. 7.9.2017 [cit. 2018-04-01]. Dostupné z: https://www.lupa.cz/clanky/nejvetsi-strasak-dnesni-doby-se-skryva-pod-zkratkou-gdpr/

Nové přístupy a povinnosti: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-27]. Dostupné z: https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268

Obecné nařízení: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-25]. Dostupné z: https://www.uoou.cz/1-obecne-na-izeni/d-27266

Obsah sčítání lidu - 1930. Český statistický úřad [online] 22.1.2010 [cit. 2018-03-20]. Dostupné z: https://www.czso.cz/csu/sldb/obsah_scitani_lidu_1930

OHCHR | International Covenant on Civil and Political Rights. [online]. Copyright © OHCHR 1996 [cit. 2018-03-23]. Dostupné z: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Pověřenec pro ochranu osobních údajů: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-31]. Dostupné z: https://www.uoou.cz/9-pov-enec-pro-ochranu-osobnich-udaj/d-27280

Práva subjektu údajů: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-28]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaj/d-27276

Sankce - Ochrana osobních údajů. Ministerstvo vnitra České republiky [online]. Copyright © 2018 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2018-03-30]. Dostupné z: http://www.mvcr.cz/gdpr/clanek/sankce.aspx

Sankce, pokuty: Úřad pro ochranu osobních údajů [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-30]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287

Souhlas se zpracováním osobních údajů podle nové právní úpravy (GDPR) [online] 5.10.2017 [cit. 2018-04-01] Dostupné z: https://www.dauc.cz/dokument/?modul=li&cislo=238303

Šmíd, V. Informační právo. Ochrana osobních údajů [online] 26.2.2009 [cit. 2018-03-22] Dostupný z: http://www.fi.muni.cz/~smid/inf_pravo_ochd1.html

Universal Declaration of Human Rights. Welcome to the United Nations [online]. Copyright ©2018 [cit. 2018-03-22]. Dostupné z: http://www.un.org/en/universal-declaration-human-rights/

Zabezpečení osobních údajů - Ochrana osobních údajů. Ministerstvo vnitra České republiky [online]. Copyright © 2018 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2018-03-30]. Dostupné z: http://www.mvcr.cz/gdpr/clanek/zabezpeceni-osobnich-udaju.aspx

Zabezpečení osobních údajů: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-31]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

Základní pojmy v GDPR - Ochrana osobních údajů. Ministerstvo vnitra České republiky [online]. Copyright © 2018 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

Zásady a právní důvody zpracování: Úřad pro ochranu osobních údajů. [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 2018-03-27]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

Zásady zpracování osobních údajů - Ochrana osobních údajů. Ministerstvo vnitra České republiky [online]. Copyright © 2018 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2018-03-28]. Dostupné z: http://www.mvcr.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx

Seznam příloh

Přílohy

Příloha A/1: Dotazník

povinná otázka

1. Jaká je vaše právní forma podnikání?

- Fyzická osoba – OSVČ
- S.R.O.
- A.S.
- V.O.S.
- K.S.
- Družstvo
- Evropská společnost

povinná otázka

2. Jaký je váš obor podnikání?

- Auto-moto
- Bezpečnostní služby a agentury
- Cestovní agentury, kanceláře
- Doprava a logistika
- E-shopy
- Farmacie, léčiva
- Fotografie, video, grafika
- Finanční služby
- Hotely, ubytování, restaurace
- Kosmetika, kadeřnictví, wellness, masáže
- Marketingové služby, reklama
- Neziskové organizace
- Potravinářský průmysl
- Právnické služby
- Realitní kanceláře
- Řemesla
- Software a IT služby
- Stavebnictví, stavitelství, architekti
- Strojírenský průmysl
- Velkoobchod
- Veřejná správa
- Výroba
- Vzdělávání, kurzy
- Zdravotnictví
- Zemědělství, chovatelství
- ostatní

povinná otázka

3. Jaká je velikost vaší firmy?

- Mikro podnik (méně než 10 zaměstnanců, roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR)
- Malý podnik (méně než 50 zaměstnanců, roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR)
- Střední podnik (méně než 250 zaměstnanců, roční obrat nepřesahuje 50 milionů EUR nebo bilanční suma roční rozvahy nepřesahuje 43 milionů EUR)
- Velký podnik (není mikro, malý nebo střední dle výše uvedených parametrů)

povinná otázka

4. Připravujete se na GDPR?

- Ano
- Ne

Příloha A/2: Dotazník

povinná otázka

5. V jaké fázi příprav na GDPR se nacházíte?

- Systémová analýza (jaké osobní údaje společnost shromažďuje, pro jaký účel, kdo k nim má přístup, jakým způsobem je prováděna kontrola oprávnění, jak se likvidují osobní údaje, apod.)
- Implementační plán (úprava vnitřních norem a procesů, určení, zda společnost potřebuje pověřence pro ochranu osobních údajů, zajištění bezpečnosti zpracování osobních údajů, apod.)
- Realizace úprav (revidování smluv mezi správcem a zpracovatelem, příprava záznamů o zpracování, kontrola bezpečnosti jednotlivých procesů, revize souhlasů se zpracováním osobních údajů)
- Jsme připraveni

povinná otázka

6. Probíhala vaše příprava na GDPR ve spolupráci s nějakým partnerem?

- Ano
- Ne, GDPR si řešíme sami

povinná otázka

7. Jaké byly vaše předpokládané náklady se zavedením GDPR?

- 1 – 50.000 Kč
- 50.000 – 150.000 Kč
- 150.000 – 400.000 Kč
- 400.000 a více

povinná otázka

8. Jak dlouho jste předpokládali, že bude trvat vaše příprava na GDPR?

- Do 1 měsíce
- 1 -2 měsíce
- 2-4 měsíce
- 4 a více měsíců

Příloha A/3: Dotazník

povinná otázka

9. Jaké byly vaše dosavadní/celkové náklady se zavedením GDPR?

- 1 – 50.000 Kč
- 50.000 – 150.000 Kč
- 150.000 – 400.000 Kč
- 400.000 a více

povinná otázka

10. Jak dlouho celkem trvala/trvá vaše příprava na GDPR?

- Do 1 měsíce
- 1 –2 měsíce
- 2–4 měsíce
- 4 a více měsíců

povinná otázka

11. V čem jste předpokládali největší problém při zavádění GDPR?

(text)

povinná otázka

12. Co byl pro vás největší problém při zavádění GDPR?

(text)

Příloha A/4: Dotazník

povinná otázka

13. Plánujete se připravovat na GDPR ?

- ○ Ano, chceme začít s přípravou než GDPR vejde v účinnost
- ○ Ano, začneme až GDPR vejde v účinnost
- ○ Ne, připravovat se nebudeme

povinná otázka

14. Jaké předpokládáte náklady se zavedením GDPR?

- ○ 1 – 50.000 Kč
- ○ 50.000 – 150.000 Kč
- ○ 150.000 – 400.000 Kč
- ○ 400.000 a více

povinná otázka

15. Jak dlouho předpokládáte, že bude trvat vaše příprava na GDPR?

- ○ Do 1 měsíce
- ○ 1 –2 měsíce
- ○ 2–4 měsíce
- ○ 4 a více měsíců

povinná otázka

16. V čem předpokládáte největší problém při zavádění GDPR?

(text)

Odeslat dotazník

Abstrakt

SIEBER, Radek. *Připravenost firem v České republice na GDPR*. Plzeň. 2018. 75 s. Diplomová práce. Západočeská univerzita v Plzni. Fakulta ekonomická.

Klíčová slova: ochrana osobních údajů, GDPR, Obecné nařízení

Předložená práce je zaměřena na ochranu osobních údajů v České republice. Po definování pojmu GDPR a uvedení legislativních požadavků na ochranu osobních údajů je proveden výzkum připravenosti firem v České republice na zavedení GDPR. Následující kapitola je tvořena vyhodnocením dotazníkového šetření. V závěru práce dochází k představení výsledků získaných prostřednictvím provedeného výzkumu a k navržení možných řešení definovaných problémů.

Abstract

SIEBER, Radek. *Readiness of companies in the Czech Republic for GDPR*. Pilsen. 2018. 75 p. Thesis. University of West Bohemia. Faculty of Economics.

Key words: personal data protection, GDPR, General regulation

This thesis is focused on personal data protection in the Czech Republic. The thesis is introduced by the definition of GDPR and legislative requirements for protection of personal data, then the research of readiness for GDPR implementation by companies in the Czech Republic is realized. Next chapter represents the evaluation of questionary research. At the end of thesis, are summarized the outcomes of conducted quantitative research and there are also specified the possible improvements of identified problematic issues.