

ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

**Dopady zavedení General Data Protection Regulation
na vybraný ekonomický subjekt**

**Impact of the General Data Protection Regulation
implementation on a selected economic entity.**

Bc. Lenka Harmáčková

Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta ekonomická

Akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Lenka HARMÁČKOVÁ**
Osobní číslo: **K17N0022P**
Studijní program: **N6208 Ekonomika a management**
Studijní obor: **Podniková ekonomika a management**
Název tématu: **Dopady zavedení General Data Protection Regulation na vybraný ekonomický subjekt**
Zadávající katedra: **Katedra financí a účetnictví**

Zásady pro vypracování:

1. Charakterizujte problematiku General Data Protection Regulation.
2. Proveďte srovnání předchozího a současného stavu.
3. Představte vybraný ekonomický subjekt.
4. Popište a vyhodnoťte proces zavedení General Data Protection Regulation ve vybraném ekonomickém subjektu.
5. Navrhněte doporučení ke zlepšení stávajícího stavu v oblasti ochrany dat.


Rozsah grafických prací: **neuveden**
Rozsah kvalifikační práce: **60 - 80**
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:


- BHATIA, Punit. *Intro to GDPR: A Plain English Guide to Compliance*. Zagreb: Advisera Expert Solutions Ltd, 2018. ISBN 978-953-8155-18-51.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. In: *Úřední věstník Evropské unie*. 2016.
- NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-689-7.
- NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.
- ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

Vedoucí diplomové práce: **Prof. Ing. Lilia Dvořáková, CSc.**
Katedra financí a účetnictví

Datum zadání diplomové práce: **23. října 2018**
Termín odevzdání diplomové práce: **23. dubna 2019**


Doc. Ing. Michaela Krechovská, Ph.D.
děkanka




Ing. Pavlína Hejduková, Ph.D.
vedoucí katedry

V Plzni dne 23. října 2018

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma
„Dopady zavedení General Data Protection Regulation na zvolený ekonomický subjekt“
vypracovala samostatně pod odborným dohledem vedoucí diplomové práce za použití
pramenů uvedených v příložené bibliografii.

Plzeň dne

.....

Lenka Harmáčková

Poděkování

Děkuji vedoucí diplomové práce paní prof. Ing. Lili Dvořákové, CSc. za cenné rady a připomínky. Současně děkuji i jednateli společnosti za poskytnutí součinnosti při sběru informací.

Obsah

Úvod	8
1 Cíl a metodika práce.....	9
2 Problematika General Data Protection Regulation.....	10
2.1 Důvody vzniku General Data Protection Regulation.....	11
2.2 Koho se General Data Protection Regulation týká	12
2.3 Definice pojmů důležitých pro General Data Protection Regulation.....	13
2.4 Zásady a odpovědnosti správce pro zpracování osobních údajů	15
2.4.1 Zákonnost, korektnost a transparentnost	15
2.4.2 Účelové omezení.....	17
2.4.3 Minimalizace údajů.....	17
2.4.4 Přesnost.....	17
2.4.5 Omezení uložení	18
2.4.6 Integrita a důvěrnost	18
2.4.7 Zásada zodpovědnosti správce.....	19
2.5 Práva subjektů osobních údajů.....	19
2.5.1 Právo na informace	19
2.5.2 Právo na přístup	21
2.5.3 Právo na opravu a doplnění	22
2.5.4 Právo na výmaz.....	22
2.5.5 Právo na omezení zpracování	22
2.5.6 Právo přenositelnosti.....	23
2.5.7 Právo vznést námitku.....	23
2.6 Sankce za nedodržování pro správce	23
3 Srovnání zákona o ochraně osobních údajů s General Data Protection Regulation.....	25

3.1	Zásady General Data Protection Regulation vs. Zákon o ochraně osobních údajů	25
3.2	Personalistika	26
3.2.1	Zpracování osobních údajů ve výběrovém řízení	26
3.2.2	Zpracování osobních údajů v době trvání pracovního poměru.....	27
3.2.3	Zpracování osobních údajů po skončení pracovního poměru	29
3.3	Kamerový systém se záznamem na pracovišti.....	30
3.4	Dílčí shrnutí.....	32
4	Charakteristika společnosti	33
5	Proces zavedení General Data Protection Regulation.....	37
5.1	Analýza stavu před zavedením General Data Protection Regulation	37
5.2	Postup přípravy na zavedení General Data Protection Regulation a zavedení General Data Protection Regulation	40
5.2.1	Zjišťování informací	40
5.2.2	Identifikace osobních údajů	41
5.2.3	Identifikace způsobu zpracování osobních údajů	42
5.2.4	Identifikace a implementace postupů	45
5.2.5	Identifikace a implementace nových povinností	45
5.3	Analýza stavu po zavedení General Data Protection Regulation.....	46
5.3.1	Stěhování a zabezpečení v novém objektu	46
5.3.2	Vyčíslení nákladů	47
5.3.3	Dotazníkové šetření	48
6	Vyhodnocení dotazníku	50
6.1	Vyhodnocení dotazníku – zaměstnanci.....	50
6.2	Vyhodnocení dotazníku – správce	58
7	Návrhy opatření na zlepšení v oblasti ochrany dat	66
	Závěr	68

Seznam zdrojů.....	69
Seznam tabulek	72
Seznam obrázků.....	73
Seznam příloh.....	74

Úvod

Téma „Dopady zavedení General Data Protection Regulation na zvolený ekonomický subjekt“ bylo autorem zvoleno, protože se o problematiku osobních údajů zajímá vzhledem k tomu, že se s touto problematikou ve svém pracovním životě často setkává.

Předkládaná diplomová práce se zabývá problematikou nové legislativy „Nařízení Evropského parlamentu a rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)“, která byla v roce 2016 přijata Evropskou unií a nabyla účinnosti dne 25. 5. 2018.

Další oblastí, kterou se práce zabývá, je srovnání dosavadní právní úpravy o ochraně osobních údajů „Zákona č. 101/2000 Sb., o ochraně osobních údajů“ a Obecného nařízení.

Poslední částí je analýza procesu příprav na zavedení opatření v souladu s novou legislativou a procesu zavedení nových postupů dle této legislativy. Závěrem tohoto procesu je následně provedené dotazníkové šetření a v návaznosti na něj navržené další opatření.

1 Cíl a metodika práce

Hlavními cíli diplomové práce jsou analýza a hodnocení procesu zavedení nové legislativy upravující ochranu osobních údajů ve vybraném ekonomickém subjektu, provedení dotazníkového šetření spočívajícího v ověření poskytnutých informací o zavedení opatření v souladu s Obecným nařízením a spočívající v ověření znalostí zaměstnanců v oblasti ochrany osobních údajů, v neposlední řadě navržení dalších možných opatření a vylepšení v oblasti ochrany dat.

Pro splnění stanovených cílů je diplomová práce rozdělena do několika částí. První část se zabývá problematikou GDPR a srovnáním Zákona č. 101/2000 Sb., o ochraně osobních údajů a Nařízením 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).

Druhá část je věnována charakteristice vybrané účetní jednotce, analýze a hodnocení procesu zavedení GDPR a vyhodnocení dotazníkového šetření. V poslední části jsou doporučené návrhy na další opatření a zlepšení současného stavu.

2 Problematika General Data Protection Regulation

Evropská unie vydává několik právních předpisů, přičemž některé mají působnost na území celé Evropské unie a jiné se týkají pouze některých zemí. Právními předpisy, které může vydávat, jsou:

- Nařízení – platí na území celé Evropské unie a je právně závazné.
- Směrnice – každá členská země musí splnit cíl, který směrnice stanovuje, přičemž je již na každé zemi, jak těchto cílů dosáhnou.
- Rozhodnutí – vztahuje se pouze na určité organizace, kterým je rozhodnutí určeno.
- Doporučení – doporučením mohou orgány Evropské unie projevit svůj názor a navrhnout určité kroky, které ale nedávají zákonnou povinnost.
- Stanovisko – nezakládá zákonnou povinnost, orgán Evropské unie se pouze prostřednictvím stanoviska může vyjádřit k určitému problému. (Evropská unie, 2018)

Anglické označení General Data Protection Regulation (dále jen GDPR) se do češtiny překládá jako obecné nařízení o ochraně osobních údajů. Jedná se o novou legislativu Evropské unie ve formě nařízení, jejímž cílem je především sjednotit pohled na ochranu osobních údajů napříč všemi členskými zeměmi. Celý název legislativy je: „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 jen Obecné nařízení). (Nezmar, 2017)

Evropská unie přijala toto nové Obecné nařízení o ochraně osobních údajů v roce 2016, jejíž účinnost vstoupila v platnost 25. května 2018. S tímto datem musí splnit požadavky tohoto nařízení každá organizace, instituce, obec či škola, která ukládá nebo zpracovává osobní údaje, které pocházejí z jakéhokoliv členského státu. (Nezmar, 2017)

GDPR lze také definovat jako soubor pravidel, které shrnují pokyny pro zpracování osobních údajů fyzických osob. Těmito fyzickými osobami lze chápat zákazníky, zaměstnance, případně zaměstnance dodavatelů určité obchodní společnosti. Tyto fyzické osoby jsou označovány jako subjekty údajů, a jsou jejich nositeli. (Bhatia, 2018)

2.1 Důvody vzniku General Data Protection Regulation

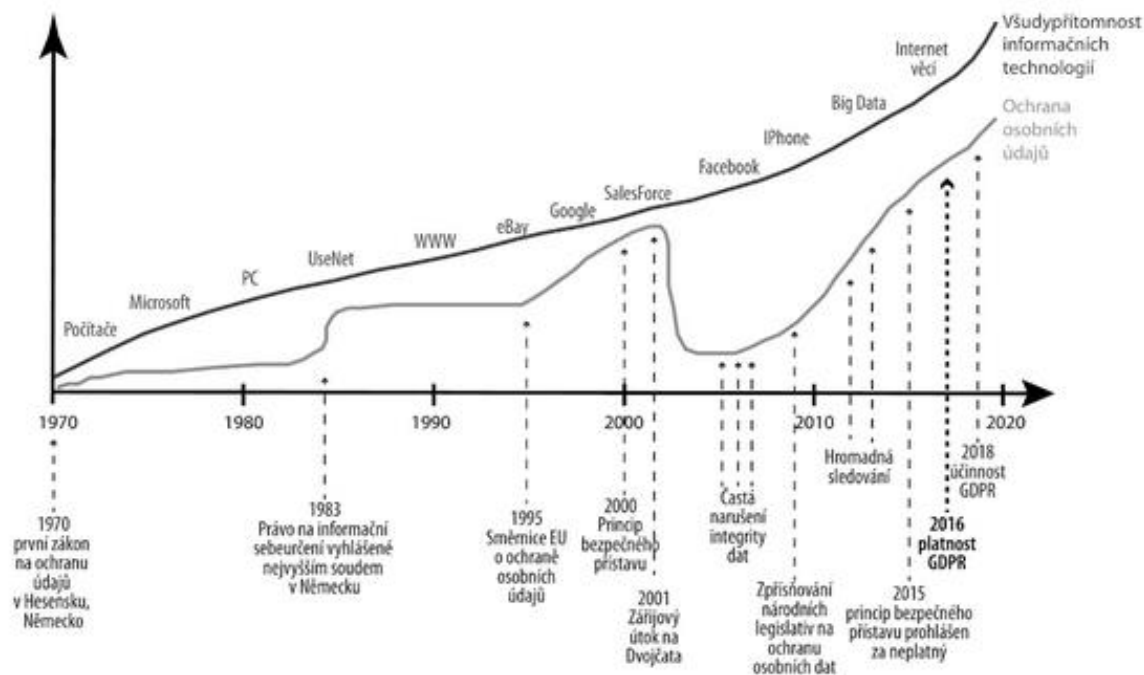
Důvodů pro vznik nové sjednocené legislativy je hned několik. Lidé si čím dál více uvědomují vysokou hodnotu informací, a tak i osobní údaje se staly velmi hodnotnou komoditou. Vlivem globalizace a vývojem technologií se stále častěji lze potkat s kybernetickými útoky. Opatření proti nim je stále diskutovaným tématem a jedná se o jeden z klíčových úkolů budoucnosti, jak se proti nim bránit. Pokud tedy lze hovořit o krádeži osobních údajů, jedná se o velmi významné riziko, spočívající v jejich zneužití. (Nezmar, 2017)

Dalším důvodem vzniku byla zastaralost právní legislativy, která již byla obtížně aplikovatelná na nové technologie. Původní legislativa totiž pocházela z 80. let minulého století. Také lze říci, že neexistovala, žádná sjednocená legislativa na úrovni Evropské unie. Každý členský stát původní směrnici 95/46 převedl s odchylkami do svých zákonů na úrovni národního práva. Toto Obecné nařízení má tedy tuto roztržičnost odstranit. (Nonneman, 2018)

GDPR má také posílit práva v oblasti ochrany osobních údajů a dosáhnout sjednoceného výkladu GDPR dozorovými úřady jednotlivých členských zemí Evropské unie. (Navrátil, 2018)

Obrázek č. 1 zachycuje vývoj technologií v porovnání s vývojem legislativy. Je zřejmé, že technologie již od počátku byla vždy o pár kroků oproti legislativě napřed. Kolem roku 2000 se tento propad trochu zmírnil, ale vývoj se nezastavil a pokračovat dál. Se vznikem sociální sítě Facebook začalo docházet k narušování celistvosti dat a na to již současná legislativa nebyla dostačující a problematika ochrany dat se tím dostávala do velkých potíží. Kolem roku 2010 se legislativa začala novelizovat, vznikala nová legislativa a propad se začal mírnit. Poslední velkou změnou v této oblasti je vznik GDPR v roce 2016 a následně jeho účinnost v roce 2018. Otázkou a problémem budoucnosti je, jaký bude další vývoj. Dá se předpokládat, že se technologie budou stále vyvíjet, budou vznikat další nové sociální sítě a bude tedy zapotřebí vymýšlet novou legislativu.

Obrázek č. 1: Porovnání vývoje technologií a legislativy



Zdroj: Nezmar, 2017

Dalším důvodem a i cílem zavedení GDPR je posílit důvěryhodnost Evropské unie a dalších zemí, které pod GDPR spadají, tedy i jiných zemích, které mají zájem obchodovat s členskými zeměmi Evropské unie a s tím související předávání osobních údajů. (Navrátil, 2018)

2.2 Koho se General Data Protection Regulation týká

Obecné nařízení říká, že se jím musí řídit každý subjekt, který provádí zpracování osobních údajů. Dále se jím musí řídit také zpracovatel nebo dozorové úřady. (Nezmar, 2017)

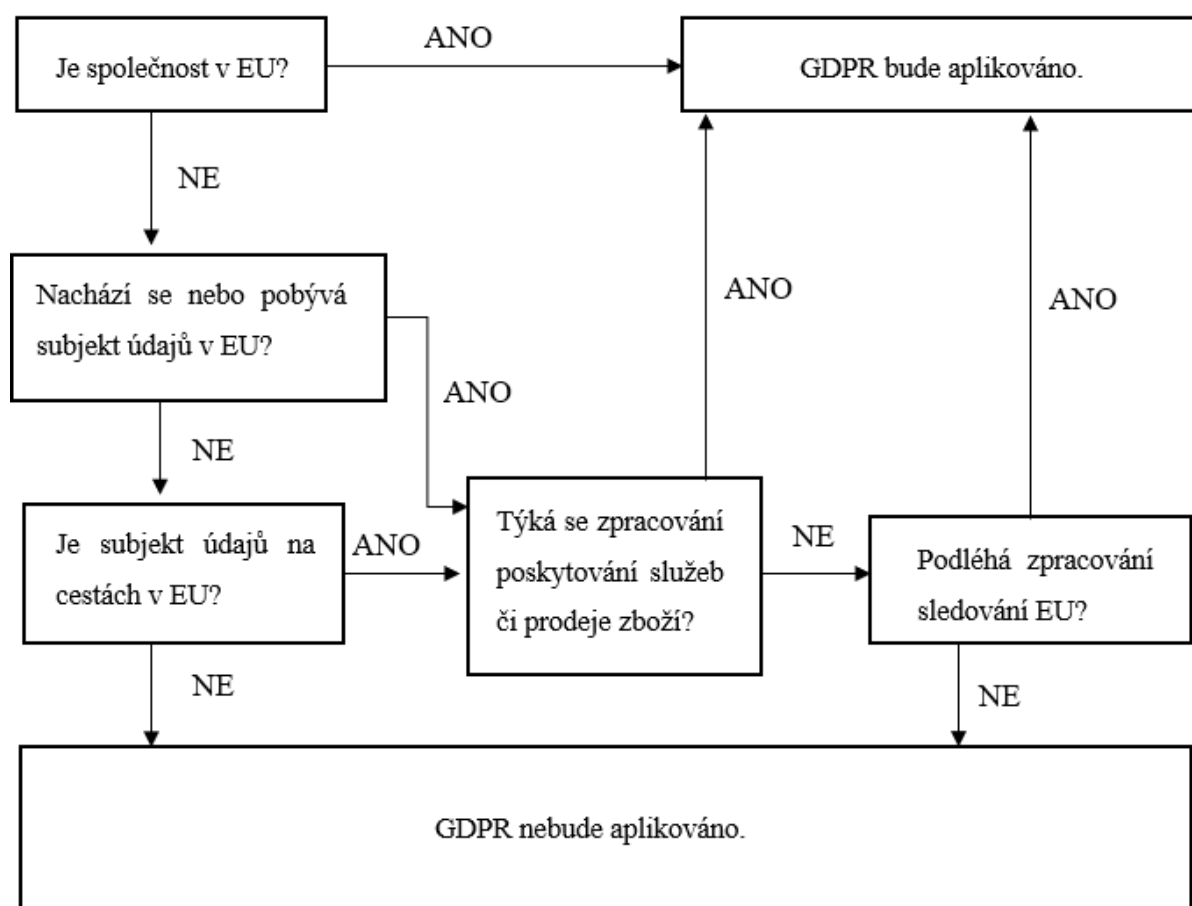
Obecným nařízením se nemusejí řídit pouze organizace zpracovávající osobní údaje občanů Evropské unie, ale také organizace, které s Evropskou unií obchodují. Týká se i případů, kdy občan Evropské unie podniká ve Spojených státech amerických. Dalším případem jsou lékařské záznamy obsahující osobní údaje občanů evropské unie, jakožto pacientů nemocnice ve Spojených státech amerických. (Miglicco, 2018)

Aby se organizace musela řídit Obecným nařízením, nemusí mít sídlo na území Evropské unie, ale stačí, aby si na tomto území zřídila pobočku. Poté související aktivity s touto pobočkou musejí být celé zpracovány v souladu s Obecným nařízením. Dalším případem je, pokud správce sídlí mimo území Evropské unie, ale poskytuje

zboží nebo služby občanům Evropské unie a přitom zpracovává jejich osobní údaje. Správce nemusí přímo poskytovat zboží nebo službu, ale může jen monitorovat chování občanů. Typickým příkladem je internet, kdy provozovatel e-shopu zjevně zaměřuje svoji činnost i na obyvatele Evropské unie, poté je povinen respektovat Obecné nařízení. (Nonnemann, 2018)

Pro lepší přehlednost, jakých organizací a za jakých situací se GDPR týká, je vytvořen následující schéma, které znázorňuje, za jakých podmínek bude GDPR aplikováno.

Obrázek č. 2: Schéma organizací, které aplikují GDPR



Zdroj: Miglicco, 2018, vlastní zpracování

2.3 Definice pojmů důležitých pro General Data Protection Regulation

Klíčovým pojmem, který se v této práci vyskytuje, je osobní údaj. Převážná většina lidí považuje za osobní údaj: jméno, příjmení, rodné číslo či trvalé bydliště. Obecné nařízení osobní údaj definuje takto, veškeré informace o identifikované nebo identifikovatelné osobě, tedy informace, které mohou být použity k identifikaci jakékoliv lidské bytosti.

Všechny tyto informace o identifikované osobě označuje pojmem identifikátor. Za identifikátor se tedy dle legislativy považují již výše uvedené informace, ale i mnoho dalších, mezi které například řadí:

- identifikační číslo,
- síťový identifikátor,
- zvláštní prvky fyzické, fyziologické, genetické, psychické a jiné.

Některé publikace rozlišují definici osobních dat na 2 kategorie. Jednou z kategorií jsou osobní data jako taková. V této oblasti se vyskytují informace, které mohou být použity přímo či nepřímo k identifikaci osob. Tyto prvky se shodují s Obecným nařízením. Druhou oblastí jsou speciální znaky osobních dat, které se také vyskytují v nařízení, ale jsou dále rozšířené. Sem se řadí osobní údaje, které odhalují například rasový nebo etnický původ, náboženské přesvědčení, pohlaví, zdraví, politické názory a dokonce i kriminální historii. (Bhatia, 2018)

Za zpracování se podle právního předpisu Obecné nařízení považuje jakýkoliv soubor operací, nebo jednotlivé operace s osobními údaji či jejich souborem, s kterými jsou prováděny určité postupy. Mezi tyto postupy se například řadí:

- shromáždění,
- zaznamenávání,
- uspořádání,
- strukturování,
- uložení,
- vyhledávání,
- šíření
- a jiné.

Správce osobních údajů je pro účely legislativy upravující problematiku GDPR fyzická nebo právnická osoba, orgán veřejné moci, agentura či jiný subjekt, který určuje účely a prostředky zpracování osobních údajů. (Advokátní kancelář CÍSAŘ, ČEŠKA, SMUTNÝ, 2018)

Z této definice lze usoudit, že tedy správcem je obvykle organizace, která udává důvody pro zpracování osobních údajů.

Zpracovatel je jakýkoliv subjekt, který je pověřen správcem, aby zpracovával osobní údaje. Správce může, ale nemusí zpracovatele tímto úkolem pověřit. Rozdíl mezi

správce a zpracovatelem je dán postavením vůči osobním údajům. Zpracovatel zpracovává osobní údaje, které mu správce svěří a mu i určí způsob zpracování. Typickým příkladem je shromažďování informací. Pokud by, ale zpracovatel zpracovával osobní údaje pro vlastní účel, už se jedná o správce. (Žůrek, 2017)

Za souhlas se zpracováním osobních údajů je jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává zjevným potvrzením svolení ke zpracování svých osobních údajů. (Žůrek, 2017)

2.4 Zásady a odpovědnosti správce pro zpracování osobních údajů

Je důležité, aby si každý, kdo zpracovává osobní údaje, uvědomil 6 základních zásad. Tyto zásady jsou podstatné pro pochopení GDPR, protože je lze chápat jako přehled nejdůležitějších povinností. Tyto zásady lze nalézt v článku 5 Obecného nařízení. (Nezmar, 2017)

Podle Obecného nařízení mezi tyto základní zásady patří:

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

Dále v článku 5 Obecného nařízení lze nalézt další povinnosti správce, proto aby dodržel výše uvedené základní zásady. Touto povinností se rozumí, že správce musí být schopen doložit, že dodržel stanovené zásady. Tuto povinnost lze pojmut jako doplňující zásadu a to zásadu odpovědnosti správce. (Regulation (EU) 2016/679)

2.4.1 Zákonnost, korektnost a transparentnost

Zásada zákonnosti se považuje za nejdůležitější ze všech zásad. Tato zásada se vyznačuje tím, že správce osobních údajů může zpracovávat osobní údaje pouze tehdy, pokud má k takovému zpracování právní důvod. Tyto důvody jsou vedeny v čl. 6 odst. 1 Obecného nařízení. (Žůrek, 2017)

Navrátil, 2017 uvádí, že zpracování je také zákonné, pokud je udělen souhlas dotčenou osobou. Dále uvádí důvody, které jsou považovány za právní důvod ke zpracování osobních údajů. Mezi tyto důvody patří:

- Je-li zpracování nezbytné pro splnění smlouvy, nebo pro provedení opatření přijatých bez uzavření smlouvy.
- Pokud zpracováním správce plní své právní povinnosti.
- Jestliže zpracování zajistí ochranu životně důležitých zájmů subjektu údajů.
- Je-li zpracování prováděno za účelem splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci.
- Pokud zpracování je pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy mají přednosti základní práva a svobody vyžadující ochranu osobních údajů, zejména pokud je subjektem dítě.

Zásada korektnosti je poctivé zpracování osobních údajů. Aby se dalo mluvit o korektním zpracování, je důležité, aby se případy posuzovaly jednotlivě, po zohlednění všech okolností. Každá odpovědná osoba za zpracování by měla zohledňovat zájmy a očekávání dotčených osob a nesmí je bezdůvodně přehlížet. Pokud mají dotčené osoby mylné představ, nesmí této situace využívat. (Navrátil, 2018)

Zásada transparentnosti by měla především zaručit, že dotčené osoby mají právo rozhodnout o tom, které údaje o sobě poskytnou, musí to být, ale v rámci zákonem stanovených hranic. Zásadu transparentnosti zajišťuje správně nastavené prostředí, ale může ji zajišťovat i technika. Za správně nastavené prostředí se považují technická a organizační opatření, jejichž účelem je provádět zásady ochrany údajů, účinným způsobem a začlenit do zpracování tak, aby splnily požadavky Obecného nařízení. Předpokladem pro tuto zásadu je, aby všechny informace byly přístupné srozumitelné a vyhotovené v jasné a jednoduché formě a řeči. Zároveň mají fyzické osoby právo požadovat informaci či potvrzení o tom, které údaje o nich byly zpracovány. Také musí být tyto osoby poučeny o rizicích, předpisech a právech, které mají v souvislosti s daným zpracováním osobních údajů, a jak je mohou využít. (Navrátil, 2018)

Zásada zákonnosti odpovídá § 5 zákona o ochraně osobních údajů, ve kterém lze najít, že je zakázáno shromažďovat údaje k jinému účelu. Zásadu transparentnosti lze v zákoně o ochraně osobních údajů najít pouze částečně. Správce nesmí shromažďovat údaje, které byly zjištěny k různým účelům. Tímto spojením by mohlo dojít ke vzniku nové kvality osobního údaje, který není běžně k dispozici. Subjekt údajů by mohl být poté krácen ve svých právech, protože by ztratil přehled o zpracovávaných údajích. Toto zpracování by již nebylo dostatečně korektní ani transparentní. (Janečková, 2018)

2.4.2 Účelové omezení

Tato zásada se také nazývá omezení účelu. Lze ji chápat tak, že osobní údaje smí být shromažďovány pro určité legitimní účely, a nesmějí být zpracovány takovým způsobem, který by byl s těmito účely neslučitelný. Na základě této zásady je správce povinen zavést vhodná technická a organizační opatření, aby zajistil, že se budou zpracovávat pouze osobní údaje, které jsou nezbytné pro každý konkrétní účel daného zpracování. (Žůrek, 2017)

Existují tři výjimky, které nemusejí být v souladu s touto zásadou. Patří mezi ně:

- souhlas dotčené osoby,
- právní předpis unijního nebo národního práva to dovoluje,
- další zpracování je v souladu s veřejným archivačním zájmem. (Navrátil, 2018)

Příkladem pro výjimku může být právní norma, která by umožňovala výměnu osobních údajů mezi bezpečnostními orgány státu. (Navrátil, 2018)

Tuto zásadu lze najít také v zákoně o ochraně osobních údajů, který udává povinnost správci zpracovávat osobní údaje pouze v souladu s účelem. (Janečková, 2018)

2.4.3 Minimalizace údajů

Zásada minimalizace údajů spočívá v tom, že zpracování musí být přiměřené, relevantní a omezené na takový rozsah, který je nezbytný ve vztahu k účelu. To znamená, že by správce měl určit minimální množství dat, které musí mít k dispozici proto, aby mohl správně naplnit svůj cíl podnikání. Neměl by mít více informací, než které potřebuje. (Nezmar, 2017)

Tuto zásadu lze najít i v podobném znění v zákoně o ochraně osobních údajů, který říká, že správce má povinnost shromažďovat osobní údaje pouze k stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu. (Janečková, 2018)

2.4.4 Přesnost

Zásadu přesnosti znají občané i podnikatelé již ze zákona o ochraně osobních údajů, který říká, že správce osobních údajů je povinen aktualizovat údaje, které zpracovává. Ovšem obecné nařízení do této problematiky přináší novinku. Osobní údaje musí být v případě potřeby aktualizované a musí být přijatá veškerá rozumná opatření, aby údaje, které jsou nepřesné či nepotřebné k danému účelu, byly okamžitě opraveny či vymazány. (Janečková, 2018)

2.4.5 Omezení uložení

Tato zásada říká, že osobní údaje se uchovávají pouze po dobu nezbytně nutnou k účelu jejich zpracování, přičemž jedna kategorie osobních údajů může být zpracovávána pro více účelů a na základě více právních titulů. Pokud některé osobní údaje již nejsou nezbytné pro zpracování žádného ze zbývajících účelů, musí být tyto údaje vymazány nebo alespoň anonymizovány. Anonymizací subjekt docílí velmi podobného efektu, jako kdyby údaje vymazal. Anonymizací se pro účely Obecného nařízení rozumí proces, ve kterém jsou osobní údaje upraveny tak, že z nich nelze identifikovat fyzickou osobu. (Nulíček, 2018)

Zásadu omezení uložení podnikatelé znají z dosavadní právní úpravy. Obecné nařízení ale tuto zásadu rozšiřuje právě o pojem anonymizace. Obecné nařízení přímo stanovuje, že správce nesmí uchovávat osobní údaje ve formě umožňující identifikaci po dobu nezbytně nutnou pro účely zpracování. (Nulíček, 2018)

2.4.6 Integrita a důvěrnost

GDPR správci ani zpracovateli neukládá žádná konkrétní opatření pro dodržení této zásady, která klade důraz na bezpečnost zpracovávaných údajů. Je tedy na dané organizaci, aby pro zpracování údajů zvolila vhodná organizační a technická opatření. Pro každou kategorii osobních údajů může správce zvolit odlišné bezpečnostní prvky, ale musí být schopen doložit a zdůvodnit proč nastavil bezpečnost určitým způsobem. GDPR uvádí několik vhodných bezpečnostních opatření:

- šifrování osobních údajů,
- schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů zpracovávajících osobních údajů,
- schopnost obnovit dostupnost dat včas v případě fyzických či technických incidentů,
- proces pravidelného testování, posuzování a hodnocení účinnosti zavedených opatření. (Nonnemann, 2018)

Tato zásada se v zákoně o ochraně osobních údajů objevuje jako základní povinnost při zpracování osobních údajů. (Janečková, 2018)

2.4.7 Zásada zodpovědnosti správce

Správce musí být vždy schopen doložit, že dodržuje všechna pravidla obsahující nové Obecné nařízení nebo-li GDPR. Tato zásada je úplnou novinkou, kterou zatím podnikatelé neznali. Tato zásada správci ukládá povinnost zajistit vhodná technická a organizační opatření, právě proto, aby byl schopen doložit, že zpracování osobních údajů bylo a je prováděno v souladu s Obecným nařízením. (Janečková, 2018)

2.5 Práva subjektů osobních údajů

Nedílnou součástí každodenního života jsou práva. Každý má svoje práva, ať už o nich ví či neví. Není tomu ani jinak v Obecném nařízení. Práva v něm obsažená vyjadřují vztah mezi správcem a subjektem údajů. Obecné nařízení obsahuje práva, která jsou již obsažena v původní směrnici či v zákoně o ochraně osobních údajů, ale v propracovanějším a aktualizovaném znění. Mezi tyto práva patří například právo na informace či na přístup k osobním údajům. Zahrnuje také i zcela nová práva, mezi ně patří kupříkladu právo na přenositelnost. (Žůrek, 2017)

2.5.1 Právo na informace

Právo na informace je jedním z nejzákladnějších práv, které v Obecném nařízení lze najít. Naplňuje zásadu transparentnosti subjektu a má zaručovat řádnou informovanost o zpracování jeho osobních údajů. Na jedné straně lze tedy hovořit o právu, které má subjekt, na druhé straně lze říci, že správce má povinnost subjekt informovat o aspektech zpracování osobních údajů. (Žůrek, 2017)

Většina informací, které musí správce poskytnout, jsou v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, ale Obecné nařízení doplňuje i další informace, které musí správce poskytnout. Poskytnuté informace v rámci zpracování osobních údajů, musí splňovat určité podmínky. Musí být stručné, jasné srozumitelné snadno dostupné, psané jasným a srozumitelným jazykem, zdarma čili bez poplatků. (Nezmar, 2017)

Obsah informací je rozdělen do 2 kategorií podle toho, zda byly poskytnuty správci přímo od subjektu, či je od něho přímo nezískal. Dle těchto kategorií Obecné nařízení stanovuje základní poskytované minimum, které je správce povinen subjektu poskytnout. Pro přehlednost následující tabulka uvádí, kterých informací se povinnost týká. (Žůrek, 2017)

Tabulka č. 1: Povinnost správce poskytnout základní poskytované minimum

Základní poskytované minimum	Získáno od subjektu	Nezískáno od subjektu
Totožnost a kontaktní údaje správce, případně jeho zástupce	✓	✓
Kontaktní údaje na pověřence, pokud byl ustaven	✓	✓
Účely a právní důvody zpracování	✓	✓
Oprávněné zájmy správce či třetí strany, je-li zpracování prováděno na základě právního důvodu	✓	✗
Případný příjemce osobních údajů	✓	✓
Případný úmysl správce předat osobní údaje do třetí země	✓	✓
Kategorie dotčených osobních údajů	✗	✓

Zdroj: Žůrek, 2017, Zpracování vlastní

Správce by měl v návaznosti na způsobu získání osobních údajů, informovat o všech vyjmenovaných bodech v tabulce číslo 1, aby splnil informační povinnost. (Žůrek, 2018)

Také se subjektu údajů poskytují další informace, pokud je to nezbytné pro splnění a zajištění spravedlivého a transparentního zpracování. (Žůrek, 2017)

Tabulka č. 2: Další poskytované informace

Další informace	Získáno od subjektu	Nezískáno od subjektu
Doba uložení osobních údajů, případně kritéria pro stanovení této doby	✓	✓
Oprávněné zájmy správce či třetí strany, je-li zpracování prováděno na základě právního důvodu	Poskytuje se již jako základní minimum	✓
Existence práva požadovat přístup k osobním údajům, jejich opravu nebo výmaz	✓	✓

Možnost odvolat souhlas	✓	✓
Existence práva podat stížnost u dozorového orgánu	✓	✓
Zdroj osobního údaje	✗	✓
Informace o tom, zda poskytnutí osobních údajů je zákonným či smluvním požadavkem	✓	✗
Informace, zda dochází k automatizovanému rozhodování, včetně profilování a informace o použitém postupu	✓	✓

Zdroj: Žůrek, 2018, Zpracování vlastní

Další poskytované informace uvedené v tabulce číslo 2, nemusí být využity úplně, ale pouze z části, s ohledem na charakter zpracování. Příkladem je, že odvolat souhlas se využije v případě, kdy je zpracování osobních údajů založeno na souhlasu subjektu. (Žůrek, 2018)

2.5.2 Právo na přístup

Právo na přístup umožňuje subjektům ověřit si zákonnost zpracování jejich údajů. Má právo vědět a být informován o:

- účelech zpracování,
 - kategorii dotčených osobních údajů,
 - příjemcích nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
 - plánované době, po kterou budou osobní údaje uloženy,
 - existenci práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku,
 - právu podat stížnost u dozorového úřadu,
 - veškerých dostupných informací o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,
 - skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.
- (Škorníčková, 2018 a)

2.5.3 Právo na opravu a doplnění

Právo na opravu a doplnění souvisí se zásadou přesnosti. Správce je povinen bez zbytečného odkladu opravit nepřesné údaje, případně doplnit neúplné osobní údaje subjektu. (Žůrek, 2018)

V případě, že správce zpřístupnil osobní údaje třetím stranám, má povinnost, pokud je to možné, třetí strany informovat o úpravě, a zároveň informovat subjekt o třetích stranách, kterým byly údaje poskytnuty. (Nezmar, 2017)

2.5.4 Právo na výmaz

Právo na výmaz ukládá správci bez zbytečného odkladu vymazat osobní údaje subjektu, pokud nastane jeden z následujících důvodů:

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
- Subjekt odvolá souhlas se zpracováním údajů a neexistuje žádný další právní důvod pro zpracování.
- Subjekt vznesl námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
- Osobní údaje byly zpracovány protiprávně.
- Jestliže není dán rodičovský souhlas se zpracováním osobních údajů dětí.
- Právní povinnost stanovená právem Unie nebo členským státem. (Škorníčková, 2018 b)

2.5.5 Právo na omezení zpracování

K omezení zpracování osobních údajů dochází za určitých okolností:

- Jestliže dojde k zpochybnění osobních údajů, omezí se zpracování, dokud se neověří přesnost.
- Pakliže subjekt vznesl námitky proti zpracování.
- Pokud zpracování je protiprávní a subjekt odmítá výmaz.
- Správce již osobní údaje nepotřebuje, ale subjekt je požaduje pro výkon nebo obhajobu právních nároků. (Nezmar, 2017)

2.5.6 Právo přenositelnosti

Subjekty mohou požádat o kopie svých osobních údajů v běžném elektronickém formátu. Smyslem je jejich snadný přenos a opětovné využití pro vlastní účely. Právo na přenositelnost platí pouze, pokud:

- osobní údaje poskytl správci sám subjekt,
- je zpracování založeno na souhlasu nebo na plnění smlouvy,
- je-li zpracování prováděno automatizovanými prostředky. (Nezmar, 2017)

2.5.7 Právo vznést námitku

Námítka se mohou vznášet proti zpracování:

- založenému na oprávněných důvodech nebo výkonu veřejné moci,
- pro direct marketing,
- za účelem vědeckého výzkumu. (Nezmar, 2017)

Správce dále nezpracovává osobní údaje, pokud neprokáže závažné oprávněné důvody pro jejich zpracování, které převažují nad právy a svobodami subjektů. (Žůrek, 2018)

2.6 Sankce za nedodržování pro správce

Obecné nařízení dělí výše pokut do 2 kategorií. Kategorie se liší maximální výší pokuty v návaznosti na možném dopadu porušení ochrany práv a svobod subjektu definovaných Obecným nařízením. (Žůrek, 2018)

V první kategorii prohřešení se jedná o porušení ustanovení o povinnostech správce a zpracovatele. Výše pokuty je až do 10 000 000 EUR nebo 2 % celkového ročního obrátu. Nejčastěji se v praxi správce setká s těmito prohřešky v povinnostech:

- při zabezpečení ochrany osobních údajů,
- spolupráce s dozorovým úřadem,
- týkajících se činnosti při získávání osvědčení,
- při ohlašování
- týkajících se jmenování a podmínek pověřence,
- posoudit vliv na ochranu osobních údajů. (Žůrek, 2018)

V druhé kategorii lze udělit pokutu do výše 20 000 000 EUR nebo do 4 % celkového ročního obrátu. Jedná se především o prohřešky nesplnění základních zásad pro zpracování včetně podmínek týkajících se souhlasu. Nejčastěji se v praxi správce setká s těmito porušeními:

- zásad a zákonnosti zpracování,
- podmínek vyjádření souhlasu,
- práv subjektu,
- podmínek pro předávání osobních údajů do třetích zemí,
- nesplnění příkazu dozorového úřadu nebo neposkytnutí přístupu při uplatnění dozorové pravomoci,
- povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování. (Žůrek, 2018)

Správci či zpracovatelé osobních údajů nehrozí jen takto vysoké pokuty, ale čelí i hrozbě žalob podaných fyzickými osobami s nárokem na náhradu škody. Společnosti jsou také vystaveny ztrátě důvěry a reputačním rizikům nesprávným zacházením s osobními údaji. (Škorníčková, 2018 c)

3 Srovnání zákona o ochraně osobních údajů s General Data Protection Regulation

Tato kapitola se především věnuje největším změnám, které nastaly zavedením nové legislativy. Porovnává 2 právní předpisy z různých pohledů, těmito předpisy jsou: Zákon č. 101/2000 Sb., o ochraně osobních údajů s působností na území České republiky a Obecné nařízení s působností na území celé Evropské unie.

Zákon o ochraně osobních údajů vstoupil v platnost v dubnu roku 2000 s účinností od 1. 6. téhož roku. (Úřad pro ochranu osobních údajů, 2013) Dnem účinnosti Obecného nařízení, tj. 25. 5. 2018 byl zákon o ochraně osobních údajů částečně nahrazen Obecným nařízením. Po novele tento zákon již bude upravovat pouze vybrané aspekty týkající se Úřadu pro ochranu osobních údajů a záležitosti, které Obecné nařízení neupravuje, nebo je možné je upravit na vnitrostátní úrovni. (Ministerstvo vnitra České republiky, 2019)

3.1 Zásady General Data Protection Regulation vs. Zákon o ochraně osobních údajů

Jak již bylo uvedeno v předchozí kapitole u jednotlivých zásad, některé podnikatelé znali, jiné jsou úplnou novinkou. Následující tabulka znázorňuje v přehledné formě, které zásady jsou nové a které již podnikatelé znají z dosavadní právní úpravy.

Tabulka č. 3: Známost zásad ze zákona o ochraně osobních údajů

Zásada	Známá/nová
Zásada zákonnosti	Známá
Zásada transparentnosti	Částečně známá
Účelové omezení	Známá
Minimalizace údajů	Známá
Přesnost	Známá
Integrita a důvěrnost	Známá
Zodpovědnosti	Nová

Zdroj: Vlastní zpracování, 2019

3.2 Personalistika

V této části práce je rozebírána problematika uchovávání a zpracování osobních údajů v oblasti personalistiky. Problém nezačíná u podpisu smlouvy, ale již u výběrového řízení, protože již u výběrového řízení personalisté pracují se životopisy, které obsahují osobní údaje. Další problematickou částí je období trvání pracovního poměru a poslední je období po skončení pracovního poměru, kdy často dochází k likvidaci nepotřebných údajů.

3.2.1 Zpracování osobních údajů ve výběrovém řízení

Zákon o ochraně osobních údajů

Problém shromažďování a zpracování osobních údajů nastává již před uzavřením pracovního poměru. Hlavní úpravou vztahů mezi fyzickou osobou a potenciálním zaměstnavatelem je zákon o zaměstnanosti a zákoník práce. Vznikaly především výkladové a aplikační problémy z hlediska ochrany osobních údajů a jejich zpracování, protože tzv. prepracovní vztahy nebyly v zákoně o zaměstnanosti vůbec upraveny. Největší problémy vznikaly především v rozsahu osobních údajů vyžadovaných potenciálními zaměstnavateli, případně požadovaných od personálních agentur. Velmi složitá situace byla v tom, že zákon o ochraně osobních údajů stanovuje povinnost správci shromažďovat osobní údaje pouze ke stanovenému účelu a v rozsahu nezbytném k naplnění účelu, ale tento účel byl v zákoně pouze obecně. Často se stávalo, že byly shromažďovány informace klientů personálních agentur, které neměly vztah k potenciálnímu zaměstnání. Na druhé straně je nutné zmínit, že zákon o zaměstnanosti stanovuje rozsahy údajů, které nejsou ve fázi výběru zaměstnanců přípustné. (Bartík & Janečková, 2016)

GDPR

Obecné nařízení problematiku fáze výběru zaměstnanců také upravuje a říká, že je důležité nalézt rovnováhu mezi potřebou informací potenciálního zaměstnavatele a právem žadatele na respektování soukromého života. Zaměstnavatel by měl být v tomto případě otevřený a žadatel by si měl být vědom, jaké informace o něm organizace shromažďuje a jaké budou použity. Typickým příkladem zpracování dat v této fázi pracovního vztahu je životopis nebo žádost o vyplnění formuláře. (Nezmar, 2017)

Každá organizace by tedy měla při výběru svých uchazečů dodržovat určitá pravidla a postupy:

- Při zadávání inzerátu by měla organizace zajistit správnou identifikaci, a to z důvodu, aby uchazeči věděli, na koho se obracejí.
- Informace, které jsou během této fáze shromážděny, mají být využity pouze pro tento konkrétní účel. Jestliže jsou využity i pro jiný účel, musí to organizace řádně odůvodnit, jasně vysvětlit a zdokumentovat.
- Důležité je, aby organizace zajistila, že osoby podílející se na výběrovém řízení jednali dle Obecného nařízení a dodržovaly v něm stanovená pravidla.
- Organizace nesmí ve výběrovém řízení shromažďovat více informací, než k této fázi pracovního poměru skutečně potřebuje.
- Organizace by neměla od všech uchazečů žádat stejné informace, které nakonec bude potřebovat pouze od uchazeče, kterého se rozhodne zaměstnat. Typickým příkladem je rodné číslo, bankovní spojení či číslo občanského průkazu.
- Získané informace se musejí uchovávat bezpečně a zamezit tak přístup k těmto informacím jiné organizaci.
- Pokud organizace požaduje ověření poskytnutých dat, uchazeč by měl být informován o této skutečnosti a také o způsobu ověření a jakých dat se ověření týká.
- Informace získané náborovými činnostmi se smějí uchovávat pouze tak dlouho, dokud je to potřeba. Následně organizace musí zajistit jejich skartaci a likvidaci. (Nezmar, 2017)

3.2.2 Zpracování osobních údajů v době trvání pracovního poměru

Zákon o ochraně osobních údajů

První otázkou, kterou by si měly organizace klást, je zda mají povinnost se registrovat u Úřadu pro ochranu osobních údajů. Zákon o ochraně osobních údajů říká, že ten, kdo hodlá zpracovávat osobní údaje jako správce, je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů ještě před zahájením zpracování. Oznamovací povinnost se, ale nevztahuje na zpracování osobních údajů, které ukládá zvláštní zákon, nebo toto zpracování slouží k plnění práv a povinností vyplývajících ze zvláštní právní úpravy. Pokud tedy zaměstnavatel zpracovává osobní údaje pouze za účelem vedení personální a mzdové agendy proto, aby splnit svou povinnost

uloženou zvláštními právními předpisy, nemusí svou oznamovací povinnost plnit. (Bartík & Janečková, 2013)

Zákoník práce umožňuje zaměstnavateli vést u zaměstnance osobní spis, který musí obsahovat pouze nezbytné dokumenty k výkonu práce. Jedná tedy o jisté omezení, které splňuje podmínku, že osobní údaje se smí zpracovávat pouze v určitém rozsahu za účelem splnění účelu zpracování. (Bartík & Janečková, 2016)

V osobním spisu lze nalézt osobní dotazník, který často zaměstnanec vyplňuje ještě před uzavřením a podepsáním pracovní smlouvy. Dotazník obsahuje základní identifikační údaje o zaměstnanci (jméno a příjmení, rodné číslo, bydliště, číslo občanského průkazu, minulá zaměstnání, řidičská oprávnění a mnoho dalších). Dále v osobním spisu nalezneme dokumenty související k dokumentaci zaměstnaneckého poměru. Typicky se jedná o platební výměr, pracovní smlouvu, kopie dokladů o dosaženém vzdělání a případných dalších kvalifikacích. (Bartík & Janečková, 2013)

Přestože v osobním dotazníku zaměstnanec uvádí číslo svého občanského průkazu, zaměstnavatel nemá žádné zákonné právo pořizovat jakýmkoliv způsobem kopie občanského průkazu. Jestliže by přesto zaměstnavatel chtěl pořizovat a uchovávat kopii takového dokladu, musí mít prokazatelný souhlas občana, kterému občanský průkaz byl vydán. (Janečková & Bartík, 2016)

GDPR

Obecné nařízení se snaží nalézt rovnováhu mezi potřebou zaměstnavatele uchovávat záznamy a právy pracovníka s respektem na jeho soukromý život. Zaměstnavatel nepotřebuje k zaznamenávání o průběhu zaměstnání souhlas zaměstnance, ale je třeba se ujistit, že je zaměstnancům známo, jak budou tyto záznamy používány. Případně zda budou zpřístupněny i třetím osobám. (Nezmar, 2017)

Organizace nese odpovědnost za pracovníky, kteří mají přístup k personální dokumentaci, zda mají povědomí o pravidlech na ochranu osobních údajů, zda je dodržují a že s osobními údaji zacházejí s respektem. Dále organizace by měla provádět kontrolu, jaké záznamy uchovává. Při této kontrole se zaměří především na takové informace, které jsou irelevantní, zastaralé či příliš velkého rozsahu. Následně nepotřebné informace musí vymazat, jestliže nemají skutečný význam a neexistuje žádná zákonná povinnost tyto informace držet. (Nezmar, 2017)

Obecné nařízení není v rozporu se zákonnou povinností zveřejňovat informace, ale organizace si musí dávat pozor, jaké informace zveřejňuje, aby nezveřejnila více, než je požadováno či nezbytně nutné. V případě trestního stíhání, při vyšetřování daňových povinností či soudního řízení lze poskytnout informace i bez souhlasu zaměstnance. Jedná se totiž o výjimky stanovené v Obecném nařízení. (Nezmar, 2017)

Záznamy by měly být uchovávány na bezpečném místě, v případě listinné podoby pod zámekem s omezeným přístupem pracovníků, v případě digitálních informací musí být zabezpečeny kvalitním heslem. Jestliže organizace již nemá důvod či zákonnou povinnost uchovávat údaje o pracovním poměru, musí být tyto informace bezpečně zlikvidovány. (Navrátil, 2018)

3.2.3 Zpracování osobních údajů po skončení pracovního poměru

Zákon o ochraně osobních údajů

Ačkoliv po skončení pracovního poměru pominul účel zpracování dat, zaměstnavatel ale musí ještě určitou dobu uchovávat a archivovat vybrané osobní údaje bývalého zaměstnance. Vybranými údaji se rozumí takové, které podléhají zákonné archivační době. Typickým příkladem jsou evidenční a mzdové listy, nebo se může jednat o uchování nezbytných informací po dobu trvání promlčecí lhůty, která je stanovená na 3 roky. Doporučuje se ale dokumenty uchovávat po dobu čtyř let s ohledem, že žaloba může být žalovanému zaměstnavateli doručena i několik měsíců po uplynutí tříleté promlčecí lhůty. (Kučerová, 2018)

GDPR

Obecné nařízení říká, jestliže organizace již nemá důvod či zákonnou povinnost uchovávat údaje o pracovním poměru, musí být tyto informace bezpečně zlikvidovány. (Nezmar, 2017) V personalistice se objevují různé typy dokumentů, které se týkají mezd, pracovního poměru či osobních údajů zaměstnance, a každý typ dokumentu se dle různých zákonů archivuje různou dobu. V následující tabulce je přehled vybraných dokumentů a doba archivace stanovená právními předpisy. (Kučerová, 2018)

Tabulka č. 4: Vybrané dokumenty v oblasti personalistika a jejich archivace (v letech)

Dokument	Doba archivace
Evidenční list důchodového pojištění	3
Mzdové listy	30
Doklady z oblasti nemocenského pojištění a daňové doklady	10
Doklady o pracovně právních náležitostech	30
Doklady o vzniku, trvání a ukončení pracovně právního vztahu	30
Vnitřní předpis	10
Docházka do zaměstnání	3
Doklady o pracovním volnu bez náhrady příjmu	30
Dovolenky	10
Důtky, výtky, pozitivní hodnocení zaměstnance	3
Pracovní výkazy	3
Mzdové a účetní rekapitulace	30
Výplatní pásky	30

Zdroj: Kučerová, 2018, zpracování vlastní

3.3 Kamerový systém se záznamem na pracovišti

Zákon o ochraně osobních údajů

Pomocí nových technologií mohou zaměstnavatelé neustále sledovat své zaměstnance na pracovištích. Často dochází i ke sledování a kontrole elektronické pošty či monitorování počítačů. Tato oblast je velmi problematická, protože se zde střetávají zájmy zaměstnanců, kteří mají zaručená osobnostní práva (na soukromí, ochranu cti či projevů osobní povahy), se zájmy zaměstnavatelů, jejichž cílem je usilovat, aby zaměstnanci prováděli práci efektivně a aby byl chráněn majetek společnosti. (Janečková & Bartík, 2011)

Zákoník práce stanovuje, že zaměstnavatel nesmí narušovat soukromí zaměstnanců na pracovištích a ve společných prostorách tím, že je podrobuje kamerovým sledováním, pokud k tomu nemá závažný důvod. Dle Zákoníku práce zaměstnavatel

nesmí instalovat kamery na pracovištích ani se souhlasem všech zaměstnanců, jelikož by porušil jejich základní právo na ochranu soukromí na pracovišti. V Zákoníku práce lze ale nalézt i výjimku spočívající ve zvláštní povaze činnosti zaměstnavatele. Na základě této výjimky smí zaměstnavatel instalovat kamerový systém se záznamem. (Bartík & Janečková, 2016)

Je-li instalován v organizaci kamerový systém, může se dle zákona o ochraně osobních údajů jednat i o zpracování osobních údajů, za předpokladu, že z těchto záznamů lze přímo či nepřímo identifikovat fyzickou osobu. Fyzickou osobu lze identifikovat, pokud je možné ze záznamu rozpoznat charakteristické rysy, například obličej. (Janečková & Bartík, 2016)

V případě instalace kamerového systému musí být zaměstnanci seznámeni s účelem a rozsahem zpracování jejich osobních údajů prostřednictvím kamerového systému. Zaměstnavatelé tuto podmínku splní tím, že vydají vnitřní předpis, ve kterém budou všechny tyto informace obsaženy a víc v něm budou informováni o tom, jak budou jejich údaje zpracovávány a kdo k nim bude mít přístup. Zaměstnanci musí být zároveň s tímto předpisem seznámeni a to prokazatelným způsobem, čili podpisem. (Kubičková & Patáková, 2017)

GDPR

Dle obecného nařízení připadají pouze 2 právní důvody, na základě kterých lze pomocí kamerového systému zpracovávat osobní údaje. Jedná se o zpracování nezbytné pro splnění právní povinnosti správce a o zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany. Oprávněným zájmem je ochrana majetku správce. Aby se jednalo o tento případ, musí objektivně převážít zájem správce na sledování určitého prostoru právo na ochranu soukromí zaměstnanců. (Žůrek, 2018)

Rozhodne-li se zaměstnavatel instalovat kamerové systémy, musí tento kamerový systém řádně zabezpečit a řešit otázku, koho či co chce chránit. Zabezpečení musí odpovídat podmínkám Obecného nařízení týkající se ochrany osobních údajů. Správce se musí zamyslet nad vhodným umístěním zařízení, které bude obsahovat záznamy, a musí vyřešit přístupová práva. Obecné nařízení přitom říká, že není přímo nutné, aby byly záznamy šifrovány, ale doporučuje zajistit záznamy logováním, aby bylo zjistitelné, kdo se na daný záznam díval. (Žůrek, 2018)

3.4 Dílčí shrnutí

Z porovnání lze učinit závěr, že GDPR nepřináší žádné velké změny, přesto lze najít několik odlišností. Následující tabulka zobrazuje nejdůležitější změny, které s sebou Obecné nařízení přináší oproti původnímu zákonu o ochraně osobních údajů.

Tabulka č. 5: Nejdůležitější změny, které přináší GDPR

Položka	Změna
Zásady	Pouze 1 nová zásada (Zásada zodpovědnosti). GDPR přináší nový pojem <u>anonymizace</u> .
Zpracování osobních údajů při výběrovém řízení	Zpřesnění a vymezení účelu, ke kterému jsou osobní údaje zpracovány GDPR stanovuje pravidla a postupy v této oblasti.
Zpracování osobních údajů v době trvání pracovního poměru	Důraz kladen na zabezpečení osobních údajů, kontrolu rozsahu a účelu zpracovávaných dat.
Zpracování osobních údajů po skončení pracovního poměru	Dodržování zákonem stanovených lhůt pro archivaci dokumentů obsahující osobní údaje.
Kamerový systém	Pouze 2 právní důvody pro zavedení kamerového systému.

Zdroj: Vlastní zpracování, 2019

Ačkoliv bylo GDPR velmi diskutované téma, dle mého názoru se podnikatelé zavádění GDPR bát nemuseli. GDPR pouze doplňuje nebo zpřesňuje již uvedené povinnosti v zákoně o ochraně osobních údajů. Takže ti, co tento zákon dodržovali, museli provést pouze pár drobností, aby splňovali podmínky uvedené v Obecném nařízení.

4 Charakteristika společnosti

Společnost DISCOMP s.r.o. byla založena v roce 1999 se sídlem v Plzni. V současné době má sídlo a centrálu stále v Plzni, ale lze ji najít i v Praze a Ostravě, kde má společnost pobočky. Hlavní činností, na kterou se společnost zaměřuje je koupě a prodej zboží, další oblastí, kterou se zabývá je poskytování služeb v oblasti IT. na obrázku č. 3 je zobrazeno logo společnosti. (výroční zpráva dostupná na Justici.cz)

Obrázek č. 3: Logo společnosti



Zdroj: Discomp, 2018

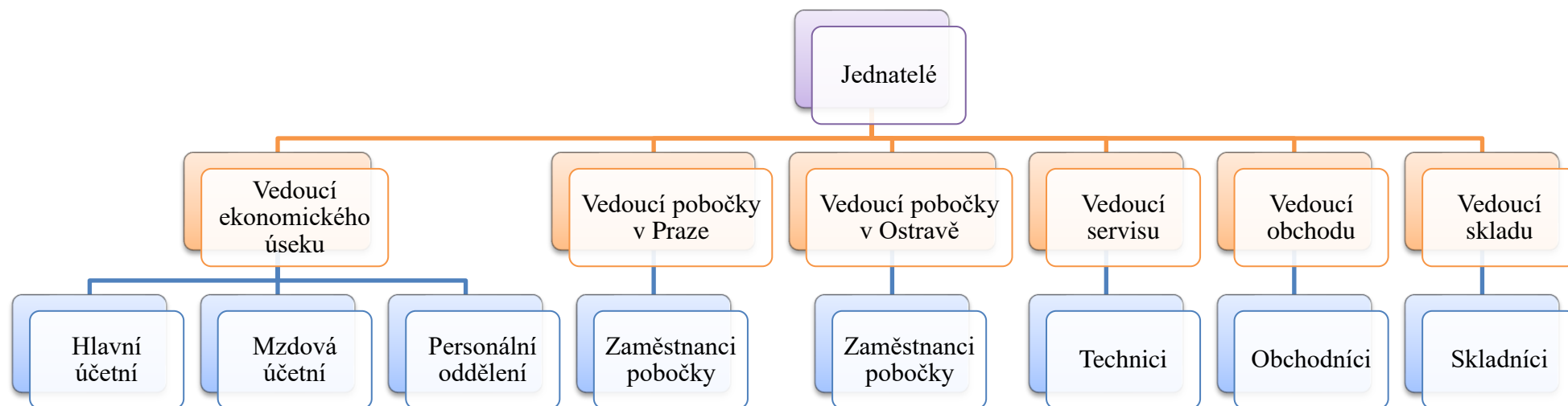
Společnost vyvíjí i vlastní značky MaxLink a EuroLan, se kterými poprvé vstoupila na trh v roce 2006. Také se společnost snaží o získání různých distribucí, kterých má již plnou řadu. Například se stala distributorem většiny světových výrobců Wi-Fi (MikroTik a UbiuqityNetworks) a také RF Elements. Od roku 2012 společnost rozšířila svou působnost na trhu a začala se také specializovat na oblast IP Security. (Discomp, 2018)

V roce 2016 společnost koupila rozestavený objekt, který koncem roku 2018 byl dokončen. Zároveň v roce 2018 své sídlo a centrálu přestěhovala do nového objektu. Podnik se přestěhoval z okraje Plzně, přesněji z Nové hospody blíže k centru města, a sice kousek od bauMaxu. V lednu roku 2019 bylo zažádáno o změnu sídla na novou adresu, zápis do obchodního rejstříku proběhl v únoru téhož roku. (Interní zdroje)

Společnost nepůsobí pouze na českém trhu, ale zapojuje se i do obchodu v rámci Evropské unie, dokonce dodává zboží do zemí mimo území Evropské unie, čili do třetích zemí. Celkem organizace dodává zboží do 50 zemí. V rámci Evropské unie lze jmenovat Německo, Slovensko, Belgie, Polsko či Španělsko. Mimo Evropskou unii jsou zajímavé státy: Irsko, Albánie, Alžírsko, Ekvádor, Filipíny nebo Cookovy ostrovy. Nejčastějšími zeměmi, ze kterých organizace zboží dováží, jsou: Čína, Rusko a Japonsko. (Interní zdroje)

Společnost k 31. 12. 2018 zaměstnávala celkem 32 osob na hlavní pracovní poměr a 5 osob na dohodu o provedení práce. V pobočce v Ostravě pracují celkem 4 zaměstnanci, v Praze 2 zaměstnanci a nejvíce zaměstnanců (26) je v centrále společnosti. Všichni pracovníci na dohodu o provedení práce jsou zaměstnaní v centrále. Zaměstnanci v pobočkách zastávají funkci obchodníků i skladníků. A v každé pobočce je jeden vedoucí. V centrále v ekonomickém úseku se nachází 4 zaměstnanci včetně 2 pracovníků na dohodu. V oddělení obchodu pracuje 5 obchodníků, v oddělení servisu pracuje 6 techniků a ve skladu pracuje 11 skladníků, Přičemž v každém z oddělení je jeden vedoucí, který zodpovídá za hladký průběh oddělení. Zbývající 2 zaměstnanci jsou zároveň jednatele společnosti, kteří dohlíží na hladký proces fungování společnosti. Následující obrázek znázorňuje organizační strukturu společnosti.

Obrázek č. 4: Organizační struktura



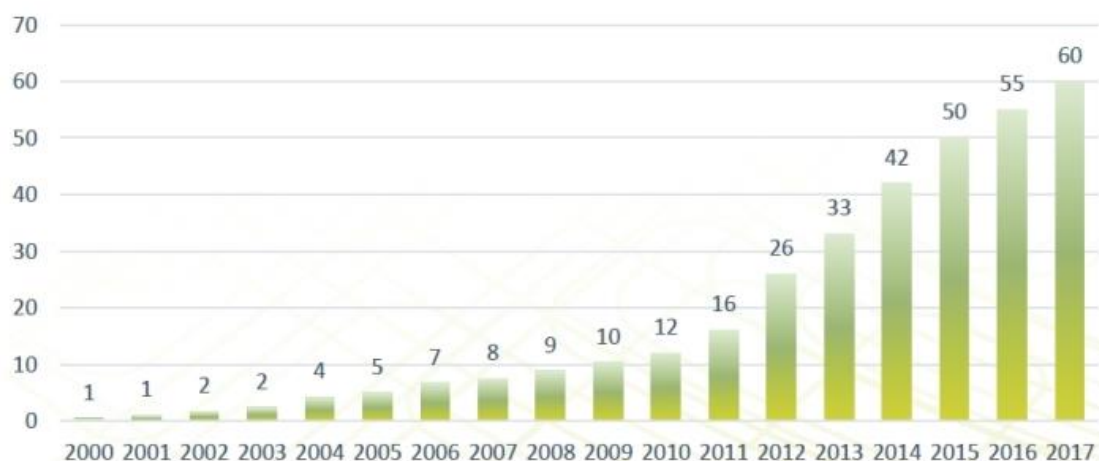
Zdroj: Vlastní zpracování, 2018

Dle zákona č. 563/1991 Sb., o účetnictví, který byl v roce 2016 novelizován, společnost patří do středních účetních jednotek. V zákoně jsou uvedeny příslušné hranice pro střední účetní jednotky. Střední účetní jednotkou jsou ty, které nejsou mikro ani malou účetní jednotkou a zároveň nepřekračuje alespoň 2 z hraničních kritérií. Hraničními kritérii jsou:

- aktiva celkem 500.000.000 Kč,
- úhrn ročního čistého obrátu 1.000.000.000 Kč
- průměrný počet zaměstnanců 250.

Brutto aktiva byly v roce 2017 ve výši 469.810.000 Kč a čistý obrat činil 1.238.597.000 Kč. Společnost tedy překračuje pouze jedno kritérium, a to obrat (účetní závěrka umístěná na Justice.cz). Na obrázku č. 5 je zaznamenán vývoj obrátu od roku 2000 do roku 2017.

Obrázek č. 5: Vývoj obrátu v mil. USD



Zdroj: Discomp, 2019

Dle zákona č. 563/1991 Sb., o účetnictví společnost Discomp podléhá auditu, protože tento zákon říká, že velké a střední účetní jednotky mají povinnost mít účetní závěrku ověřenou auditorem vždy. Společnost je také měsíčním plátcem DPH a účtuje dle českých účetních standardů.

5 Proces zavedení General Data Protection Regulation

Kapitola týkající se procesu zavedení nejprve zkoumá stav před zavedením GDPR, čili plnění požadavků dle zákona o ochraně osobních údajů. Poté se zabývá přípravou společnosti na zavedení nové legislativy a samotným zavedením. V poslední části této kapitoly se nachází analýza stavu po zavedení GDPR, která obsahuje i dotazníkové šetření, sloužící pro ověření získaných dat.

5.1 Analýza stavu před zavedením General Data Protection Regulation

Jak již bylo uvedeno v předchozí kapitole, společnost DISCOMP vznikla v roce 1999 a byla založena jediným společníkem, který byl zároveň zaměstnancem společnosti. Dále společnost v roce 1999 zaměstnávala ještě jednoho zaměstnance. Již od vzniku společnost musela brát v úvahu ochranu osobních údajů svých zaměstnanců, a to v souladu se zákonem o svobodném přístupu k informacím. V roce 2000 vstoupil v platnost nový zákon přímo upravující ochranu osobních údajů.

Aby společnost jednala v souladu se zákonem o ochraně osobních údajů, musela zavést několik opatření a změn. Například si společnost určila správce, kontrolovala účel, k němuž měly být osobní údaje zpracovány, a provedla některá opatření, aby nemohlo dojít k zneužití osobních údajů zaměstnanců.

Tím, jak se společnost rozrůstala, byla nucena přijmout nové pracovníky. Společnost si stanovila pravidlo, že při výběru pracovníků bude shromažďovat pouze informace, které jsou uvedeny v životopisech. Je to z toho důvodu, aby dodržela základní povinnost uvedenou v zákoně o ochraně osobních údajů, že správce smí zpracovávat a uchovávat informace pouze ke stanovenému účelu. Společnost tedy vedla ve své evidenci pouze základní informace o uchazečích. Těmito údaji byly: jméno, příjmení, adresa trvalého bydliště, dosažené vzdělání, předchozí zaměstnání spolu s pozicí a časovým obdobím, jazykové schopnosti a dovednosti a případně další certifikaci a oprávnění. Jen těchto málo informací stačilo pro výběr těch nejlepších adeptů, kteří pokračovali dál ve výběrovém řízení.

V další fázi výběrového řízení vhodného adepta na pracovní pozici společnost vždy provedla osobní pohovor, kde uchazeče seznámila s jejich náplní práce, povinnostmi a benefity, které společnost nabízí. Při přijímání tyto nové zaměstnance vždy při

podpisu pracovní smlouvy seznámila s jejich právy v oblasti zpracování osobních údajů. Noví zaměstnanci však nebyli seznámeni s tím, kdo jejich osobní údaje bude zpracovávat a jak se budou archivovat, či jak budou zabezpečeny.

Při podepisování smlouvy zároveň zaměstnanci podepisovali i souhlas se zpracováním a shromažďováním osobních údajů a souhlas s uváděním jejich rodného čísla. Oba tyto dokumenty jsou uvedeny v příloze (příloha A). Dále zaměstnanci vyplňovaly osobní dotazník, ve kterém vyplňují nejen své osobní údaje (jméno, příjmení, bydliště, číslo občanského průkazu,...), ale také své přechodí zaměstnání spolu s pracovní pozicí, na které působili, dosažené vzdělání, a jazykové znalosti. Jedná se v podstatě o ověření a doplnění informací uvedených v životopise, který společnost měla již k dispozici. Tento dokument lze nalézt v příloze B.

V době trvání pracovního poměru společnost zpracovávala osobní údaje, které při přijetí zaměstnanců získala. Společnost však nekontrolovala jednotlivé složky svých zaměstnanců, zda neobsahují nepotřebné informace, nebo jestli nepominul účel, ke kterému dané osobní údaje potřebovala. Jestliže by se v jednotlivých složkách objevili některé nepotřebné informace k naplnění danému účelu, správce by tak nemohl zajistit jejich řádnou likvidaci, a tím tedy porušoval zásadu minimalizace údajů.

V roce 2009 se vedení společnosti rozhodlo otevřít novou pobočku v Ostravě. Problémem bylo, jak přeposílat osobní údaje zaměstnanců z nové pobočky do centrály a obráceně. Potřebné dokumenty se zasílaly nejprve prostřednictvím e-mailu, ale to se později vedení společnosti nezdálo jako vhodný způsob, a tak se dokumenty začaly posílat poštou. Později se přišlo na to, že posílání poštou je poměrně nákladné. Proto se zamysleli nad levnějším způsobem a dospěli k závěru, že posílají různé balíky se zbožím prostřednictvím přepravní společnosti. Proto se rozhodli využít tento způsob přepravy, a tak se tyto dokumenty daly do obálky a poslaly v zabaleném balíku se zbožím.

Když v roce 2013 vedení společnosti otevřelo novou pobočku v Praze, měla již jasno, jak bude přepravovat osobní údaje zaměstnanců. Společnost využila stejný způsob jako při posílání dat do či z pobočky v Ostravě.

Společnost se také potýkala s problematikou zabezpečení osobních údajů. Bylo totiž potřeba, aby společnost jakožto správce zajistila, že se k osobním údajům nedostanou neoprávněné osoby a že nedojde k jejich zneužití. Osoba, která zpracovávala osobní

údaje na základě pověření správce, podepsala prohlášení, ve kterém bylo, že si je vědoma, jaké údaje zpracovává, že je smí zpracovávat pouze ke stanovenému účelu a že je nesmí nikde šířit či dokonce zneužívat. Tato osoba byla také seznámena s postihy, pokud tato pravidla poruší. Postihem bylo především zaplacení pokuty, v případě úmyslného zneužití osobních údajů se jednalo o okamžité rozvázání pracovního poměru a následné soudní stíhání.

Společnost uchovává a zpracovává údaje v listinné podobě, ale také v elektronické podobě. Zabezpečení těchto dat v listinné podobě probíhalo tak, že osobní složky všech zaměstnanců byly uloženy v samostatné místnosti, která se zamykala a přístup do ní měl pouze omezený počet lidí, přesněji pouze společník, personalista a mzdová účetní. V případě elektronické podoby, bylo opatření zabezpečení dat podobné. Údaje se ukládaly na disk, který měly na svých počítačích zpřístupněny pouze pověřené osoby, a k tomu jednotlivé soubory byly opatřeny heslem, které znaly pouze oprávněné osoby.

Společnost v roce 2010 změnila své sídlo, proto musela zajistit bezpečný převoz i osobních údajů svých zaměstnanců. Jednotlivé složky zaměstnanců daly oprávněné osoby do jedné krabice, která se zalepila, sami si ji převezli do nového sídla a zde ji sami rozlepili a složky vyndali. Opět byly uloženy do místnosti s omezeným přístupem.

Rozvázal-li se pracovní poměr s některým ze zaměstnanců, či sám zaměstnanec ukončil pracovní poměr, došlo po 3 letech od konce roku, ve kterém tato událost nastala, ke kontrole, jaké informace složka obsahuje. V souladu se zákonem o ochraně osobních údajů se nepotřebné informace již mohly zlikvidovat skartací, jiné se musely ještě uchovat po dobu nezbytně nutnou, protože tak ukládá jiný právní předpis.

V novém sídle od roku 2010 byly na pracovištích namontovány kamery z důvodu ochrany majetku společnosti. V oddělení sklad tyto kamery zároveň sloužily jako důkazní prostředek. Ne jednou se totiž stalo, že přepravní společnost zamítla reklamaci na rozbitý balík, z důvodu chybného zabalení. Prý chyběly správné výplně a tím došlo k následnému poškození. Na základě kamerového záznamu poté reklamaci přepravní společnost uznala. Zaměstnanec, který byl na záznamu z kamery, jak zboží dává do krabice a řádně vyplňuje prázdný prostor, byl informován o použití tohoto záznamu jako důkazního prostředku.

Jako velké pochybení vedení společnosti v oblasti ochrany osobních údajů je to, že společnost předem neinformovala a ani neměla podepsaný souhlas se zavedením kamerového systému. Dle mého názoru se jednalo o veliký problém a společnost měla nějakým způsobem své zaměstnance informovat, nejlépe písemně, že na pracovištích jsou umístěny kamery se záznamem. V takovémto dokumentu by bylo uvedeno, že slouží pouze pro ochranu majetku společnosti případně jako důkazní prostředek při vedení sporů. Dále, že pokud by byl záznam použit jako důkazní prostředek společnost je povinna své zaměstnance o této skutečnosti informovat, umožnit jim náhled záznamu a vědět komu byl záznam zaslán či ukázán.

5.2 Postup přípravy na zavedení General Data Protection Regulation a zavedení General Data Protection Regulation

Postup přípravy je rozdělen do několika oblastí. Nejprve se společnost seznámila s Obecným nařízením a zjišťovala informace, povinnosti správce a práva subjektů osobních údajů. Poté, co se společnost informovala tak si stanovila konkrétní postup, který je zároveň v souladu s Obecným nařízením. Tento postup společnost musela podstoupit k úspěšné implementaci GDPR a skládá se z těchto kroků:

- identifikace osobních údajů,
- identifikace způsobu zpracování osobních údajů,
- identifikace a implementace postupů,
- identifikace a implementace nových povinností.

5.2.1 Zjišťování informací

Společnost chtěla být předem připravena na novinky uvedené v Obecném nařízení, a tak se začala předem informovat a na zavedení připravovat. Vedení společnost se poprvé o Obecném nařízení dozvědělo z médií v roce 2017, kdy bylo již jasné, že v roce 2018 vstoupí v platnost nová legislativa upravující ochranu osobních údajů.

Další zmínkou a ujištěním pro vedení byla účast na každoročním školení, které pořádá auditorská společnost. Tato auditorská společnost zajišťuje ve společnosti už léta audit, který má společnost ze zákona povinný a je zároveň i daňovým poradcem. Na tomto školení společnost zjistila ve větší míře, co novinka v podobě GDPR obnáší. Na základě tohoto školení se zamyslela, jak nejlépe toto Obecné nařízení aplikovat a dodržet.

Protože společnost nemá žádného svého firemního právníka, tak se obrátila na právníka, se kterým dlouhodobě spolupracuje. Důvodem konzultace s tímto právníkem bylo zajištění, zda bylo Obecné nařízení správně pochopeno a vyloženo.

5.2.2 Identifikace osobních údajů

Prvním krokem k implementaci GDPR je identifikace osobních údajů, které společnost zpracovává a také koho se tyto informace týkají. Společnost si musela uvědomit, jaké informace v osobních složkách zaměstnanců uchovává. Protože správce ani zpracovatel osobních údajů u každého zaměstnance od začátku pracovního poměru nekontroloval, jaké informace ve složkách jsou, bylo zapotřebí jednotlivé složky zkontrolovat. Případně nepotřebné informace řádně zlikvidovat nebo alespoň anonymizovat.

Protože se jedná o společnost, která prodává zboží, bylo nutné si také uvědomit, jaké informace zpracovává o svých zákaznících a dodavatelích. Společnost také využívá e-shop, ve kterém je možné zboží objednat, a tak bylo nutné zabezpečit, aby zákazníci potvrdili svým souhlasem zpracování osobních údajů. Proto společnost přidala zaškrtačací políčko do internetového obchodu, ve kterém zákazníci při objednávce souhlasí se zpracováním. Také zde přibyla možnost, aby noví zákazníci vyjádřili svůj souhlas se zasíláním newsletterů. Stávajícím zákazníkům byl rozeslán e-mail, ve kterém byli informováni, že pokud nesouhlasí se zasíláním newsletterů, aby na tento e-mail reagovali s tím, že si nepřejí zasílat novinky. Pokud tak neučiní, bude to bráno jako souhlas, a newslettery jim budou zasílány i nadále.

V následující tabulce jsou uvedeny osobní údaje, které společnost zpracovává a uchovává v jednotlivých odděleních, a kdo je nositelem osobních údajů.

Tabulka č. 6: Osobní údaje, které společnost zpracovává

Oddělení	Nositel osobních údajů	Osobní údaje
Personální	Uchazeči o zaměstnání	Jméno, příjmení, bydliště, vzdělání, předchozí zaměstnání, dovednosti a schopnosti, telefon
	Zaměstnanci	Jméno, příjmení, bydliště, rodné číslo, číslo občanského průkazu, jména a rodná čísla dětí, vzdělání, předchozí zaměstnání, dovednosti a schopnosti, bankovní spojení, telefon, zdravotní pojišťovna, vstupní a dále preventivní lékařská prohlídka
Mzdová účtárna	Zaměstnanci	Jméno, příjmení, bydliště, rodné číslo, číslo občanského průkazu, jména a rodná čísla dětí, vzdělání, předchozí zaměstnání, dovednosti a schopnosti, bankovní spojení, telefon, zdravotní pojišťovna
Obchodní	Zákazníci	Jméno, příjmení, bydliště, bankovní spojení, telefon
	Dodavatelé	Sídlo, bankovní spojení, telefon, kontaktní osoba

Zdroj: Vlastní zpracování, 2019

5.2.3 Identifikace způsobu zpracování osobních údajů

Druhým krokem byla identifikace způsobu zpracování osobních údajů, ve kterém si společnost musela stanovit konkrétní účel zpracování osobních údajů, a jakým způsobem osobní údaje bude chtít zpracovávat a uchovávat. Zároveň si společnost musela určit dobu, po kterou budou údaje zpracovávány a archivovány, a to v návaznosti na dodržení zásady omezení uložení. Společnost ale také musela dbát na požadavky různých zákonů, týkajících se doby archivace dokladů.

Společnost zpracovává osobní údaje v elektronické podobě za pomoci 2 systémů, jedním je účetní software POHODA a druhým je obchodní a účetní software I6. Systém POHODA společnost využívá pouze na zpracování mezd a vedení personalistiky,

system I6 společnost využívá na účtování běžných obchodní transakcí a vedení celého účetnictví v rámci vykonávané ekonomické činnosti. V tomto softwaru společnost zpracovává osobní údaje o zákaznících a dodavatelích. Společnost nevyužívá pouze elektronickou podobu, ale také listinnou podobu, ve které osobní údaje zpracovává a uchovává.

Personální oddělení zpracovává osobní údaje zaměstnanců pro podnikatelské účely. Potřebné dokumenty získává na základě souhlasu a právního základu. Uchovává je v elektronické podobě v heslem zabezpečených serverech a v listinné podobě v místnostech s omezeným přístupem. Doba archivace podléhá zákonné lhůtě.

Oddělení mzdová účtárna osobní údaje zpracovává také pro podnikatelské účely a v rámci právního základu. Pro toto oddělení platí stejná pravidla jako pro oddělení personální. Zpracování probíhá v listinné i elektronické podobě, doba archivace podléhá zákonem stanovené lhůtě.

Obchodní oddělení zpracovává osobní údaje zákazníků a dodavatelů. Tyto údaje zpracovává pro svou podnikatelskou činnost, aby bylo možné kontaktovat a komunikovat se svými obchodními partnery. Tyto údaje jsou pouze pro interní záležitosti. Společnost si vede zvláštní dokumentaci o problémových zákaznících, aby předešla případným komplikacím při placení zboží. Údaje jsou vedeny pouze v elektronické podobě na heslem zabezpečených serverech.

Tabulka č. 7 ukazuje přehledně, jaké oddělení údaje zpracovává, za jakým účelem jsou osobní údaje zpracovávány, jejich doba archivace, kdo k nim má přístup a jak jsou zabezpečeny.

Tabulka č. 7: Způsoby zpracování osobních údajů

Oddělení	Osobní údaje	Účel zpracování	Přístup	Doba archivace	Zabezpečení
Personální	Jméno, příjmení, bydliště, rodné číslo, číslo občanského průkazu, jména a rodná čísla dětí, vzdělání, předchozí zaměstnání, dovednosti a schopnosti, bankovní spojení, telefon, zdravotní pojišťovna, vstupní a dále preventivní lékařská prohlídka	Podnikatelská činnost	Vedení, personalista, mzdová účetní	Dokud nepomine účel	Zamykatelné místnosti, server společnosti
Mzdová účtárna	Jméno, příjmení, bydliště, rodné číslo, číslo občanského průkazu, jména a rodná čísla dětí, vzdělání, předchozí zaměstnání, dovednosti a schopnosti, bankovní spojení, telefon, zdravotní pojišťovna	Podnikatelská činnost	Vedení, mzdová účetní	Dokud nepomine účel	Zamykatelné místnosti, server společnosti
Obchodní	Jméno, příjmení, bydliště, bankovní spojení, telefon	Podnikatelská činnost	Vedení, obchodníci	Není stanovena	Server společnosti

Zdroj: Vlastní zpracování, 2019

5.2.4 Identifikace a implementace postupů

Třetím krokem společnosti byla identifikace a implementace postupů pro poskytování práv subjektů údajů. V rámci tohoto kroku také zajišťovala jednotlivé zásady, které Obecné nařízení uvádí.

Společnost si také určila, jak bude postupovat v případě, že subjekty osobních údajů budou uplatňovat svá práva. Například, jak zajistí právo na výmaz v případě zpracování osobních údajů pomocí softwarů, tedy jaké možnosti jim tyto softwary nabízí.

V případě práva na přístup společnost rozhodla, že zákazníci, kteří mají na e-shopu udělanou registraci, mají možnost kdykoliv se podívat na svém účtu jaké osobní údaje o nich společnost zpracovává a případně tyto údaje aktualizovat, nebo případně některé údaje vymazat.

Dodavatelé mohou požádat o výpis údajů z obchodního a účetního softwaru I6, které o nich společnost zpracovává, většinou se jedná o právnické osoby, které ale zastupuje nějaký zaměstnanec. Takže společnost, jak již bylo uvedeno výše, zpracovává pouze v souvislosti s GDPR osobní údaje o kontaktní osobě. Uvádí tedy jen jméno, příjmení a telefon.

Zaměstnanci mohou kdykoliv personální či mzdové oddělení požádat o nahlédnutí do svého osobního spisu v listinné podobě, nebo do osobní složky vedenou v účetním softwaru POHODA. Zaměstnanci těchto oddělení, reagují okamžitě a tyto informace se snaží zaměstnancům zpřístupnit ještě v den podání žádosti. Žádost nemusí být písemná, stačí ústní. Předpokladem je, že zaměstnanec požádá o nahlédnutí v pracovní době, pokud si vzpomene například 10 minut před koncem pracovní doby, většinou mu není vyhověno ten den, ale až následující pracovní den.

5.2.5 Identifikace a implementace nových povinností

Posledním krokem byla identifikace a implementace nových povinností, kdy společnost prozkoumávala jednotlivé povinnosti, které jí Obecné nařízení ukládá. Bylo potřeba, aby došlo k aktualizaci dosavadních smluv. Musely se určit nedostatky dokumentu, ve kterém zaměstnanci vyjadřovali souhlas se zpracováním osobních údajů. Chyběly především náležitosti:

- účel zpracování,
- práva subjektu osobních údajů,

- rozsah zpracování,
- informace o tom, kdo bude jejich osobní údaje zpracovávat.

Společnost proto musela vytvořit nové dokumenty, které byly v souladu s Obecným nařízením a které chybějící informace již v sobě obsahovaly. Jednalo se o dokumenty: Informování zaměstnanců o kamerovém systému (Příloha C) a Souhlas se zpracováním osobních údajů (Příloha D). Oba dokumenty zároveň konzultovala s právníkem.

Součástí této fáze bylo i zamyšlení se nad zabezpečením osobních údajů. Společnost měla osobní údaje dobře zabezpečeny již před dnem platnosti Obecného nařízení, a proto nemusela přijímat žádná další opatření. Nicméně se zamýšlela nad zabezpečením osobních údajů v novém objektu, do kterého se, jak již bylo uvedeno v kapitole představení společnosti, přestěhovala. Vedení společnosti chtělo, aby nová budova byla již moderní, proto se rozhodla zavést oprávnění vstupu do jednotlivých místností na čipy.

5.3 Analýza stavu po zavedení General Data Protection Regulation

Tato část práce se věnuje rozborem stavu po zavedení GDPR. V této části jsou i vyčísleny náklady, které společnost musela vynaložit na činnosti a opatření související se zavedením GDPR. Je zde provedeno dotazníkové šetření, které má za cíl zjistit, zda jsou si zaměstnanci vědomi svých práv a zda je vše nastaveno tak, jak má být.

Společnost má zaměstnance i mimo své sídlo společnosti, těmto zaměstnancům posílá výplatní pásky a případné dokumenty obsahující jejich osobní údaje v zalepených obálcích, nadepsané křestním jménem zaměstnance. Některé dokumenty jsou jim zasílány prostřednictvím e-mailu. Tento způsob se používá zřídka, protože je e-mail méně bezpečný než posláni obálky.

5.3.1 Stěhování a zabezpečení v novém objektu

Stěhování do nového objektu probíhalo již po zavedení pravidel splňující Obecné nařízení. Vedení společnosti postupovalo stejným způsobem, jako při stěhování společnosti před zavedením GDPR v roce 2010. Pouze oprávněné osoby mohly manipulovat se šanony obsahující osobní údaje zaměstnanců. Tyto šanony se dávaly do krabic, které se popsaly a bezpečně zalepily. Poté mzdová účetní a personalista sami převezli krabice a vybalili v nových místnostech.

Při stěhování bylo nutné zabezpečit i osobní údaje v elektronické podobě, to měl na starosti hlavní technik, který musel odpojit servery a bezpečně přepravit do nového sídla. V novém sídle došlo k zapojení a vyzkoušení, zda jsou servery správně zapojeny, zda mají oprávněné osoby nastavený přístup na svých počítačích a zkontrolovat že neoprávněné osoby tento přístup naopak nemají. Případně neoprávněným osobám tento přístup odebrat a zase oprávněným osobám tento přístup udělit.

V novém sídle společnosti má každý zaměstnanec svůj vlastní čip, se kterým jsou spojená práva na vstup do jednotlivých místností. Je tedy jasné, že k osobním údajům mají přístup pouze oprávněné osoby.

První týdny po přestěhování docházelo k drobným nedostatkům nastaveného systému, ty byly ale okamžitě odstraněny úpravou práv, které prováděl hlavní technik. Docházelo k tomu, že mzdová účetní se například nemohla dostat do místnosti s uloženými osobními spisy nebo do archivu, ve kterém byly uloženy dokumenty o bývalých zaměstnancích. Tento problém se vyřešil během pár minut, kdy hlavní technik opravil práva k příslušnému čipu.

5.3.2 Vyčíslení nákladů

Společnost byla nucena vynaložit finanční prostředky k zavedení GDPR. Prvními výdaji bylo zaplacené školení od auditorské společnosti. Školení se účastnily 2 osoby a cena byla stanovena na 2.000 Kč. Není možné počítat do nákladů celou částku, protože celé školení se nevěnovalo problematice Obecného nařízení, ale převážná část byla věnována problematice účetnictví a daní. Školení trvalo přibližně 6 hodin, z toho byla problematice GDPR věnována pouze 1 hodina. Takže do nákladu je započítána pouze částka 333 Kč na osobu, za obě osoby necelých 700 Kč.

Další položkou v nákladech byly služby poskytnuté právníkem. S právníkem byla vedena čtyřhodinová konzultace a příprava nových dokumentů. Právník si účtuje za své služby hodinovou taxu 2.000 Kč. Celkové náklady za právní služby byly vyčísleny ve výši 12.000 Kč.

Nejdražší položkou bylo zabezpečení na čipy. Součástí toho zabezpečení bylo nutné zakoupit zvláštní software, který není zrovna levný, stál 80.000 Kč. Společnost si musela také zakoupit jednotlivé čipy, každý stál 200 Kč a společnost jich zakoupila 30. Potřebovala sice jen 25, ale počítala s tím, že bude přijímat nové zaměstnance, a tak je lepší mít nějaké do zásoby. V souvislosti s čipy se hlavní technik musel účastnit

i školení, aby věděl, jak správně software nastavit a obsluhovat. Školení stálo 10.000 Kč. Instalace tohoto zabezpečovacího systému stála 20.000 Kč. V následující tabulce jsou vyčísleny celkové náklady na zavedení GDPR.

Tabulka č. 8: Vyčíslení nákladů v Kč

Položka	Výše nákladů
Školení za 2 osoby	666
Právní služby	12.000
Zabezpečení na čipy	116.000
Celkem	128.666

Zdroj: Vlastní zpracování

Celkové náklady byly společností vyčísleny na necelých 130.000 Kč. Lze posoudit, že se nejedná zrovna o nejlevnější záležitost, nicméně v celkových nákladech společnosti není tato záležitost největší položkou.

5.3.3 Dotazníkové šetření

V rámci dotazníkového šetření byly vytvořeny 2 dotazníky. Každý dotazník se zaměřuje na jinou skupinu respondentů. První dotazník je určen pro správce a druhý pro zaměstnance. Oba dotazníky se zaměřují na znalost problematiky GDPR.

Účel

Účelem dotazníkového šetření je zjistit znalost nové legislativy upravující ochranu osobních údajů z pohledu správce a z pohledu zaměstnanců. Cílem dotazníku určeného pro zaměstnance je zjistit, zda mají povědomí o svých právech a o tom, jaké informace o nich smí správce shromažďovat a zpracovávat. Hlavním cílem dotazníkového šetření u správce je ověřit, zda se zavedená opatření v souladu s GDPR stále využívají.

Metodologie výzkumu

Provedené šetření je založeno na kombinaci kvantitativního a kvalitativního výzkumu, kdy otázky byly vytvořeny tak, že plní převážně deskriptivní funkci.

Dotazování probíhalo formou elektronického dotazníku vytvořeného na Googlu. Tento dotazník byl rozeslán prostřednictvím e-mailu zaměstnancům vybrané společnosti.

Analýza a vyhodnocení dotazníků probíhalo za pomoci excelu, grafů a statistických metod. Předmětem zkoumání byla především četnost odpovědí a analýza vztahu mezi pozicí a znalostmi GDPR.

Respondenti

Respondenti byli zaměstnanci a správci společnosti DISCOMP, protože v této společnosti zároveň probíhala analýza procesu zavedení GDPR.

6 Vyhodnocení dotazníku

V této kapitole je zobrazeno vyhodnocení obou dotazníků. V první části je vyhodnocení dotazníku určeného zaměstnancům, v druhé části je vyhodnocení dotazníku zaměřeného na správce.

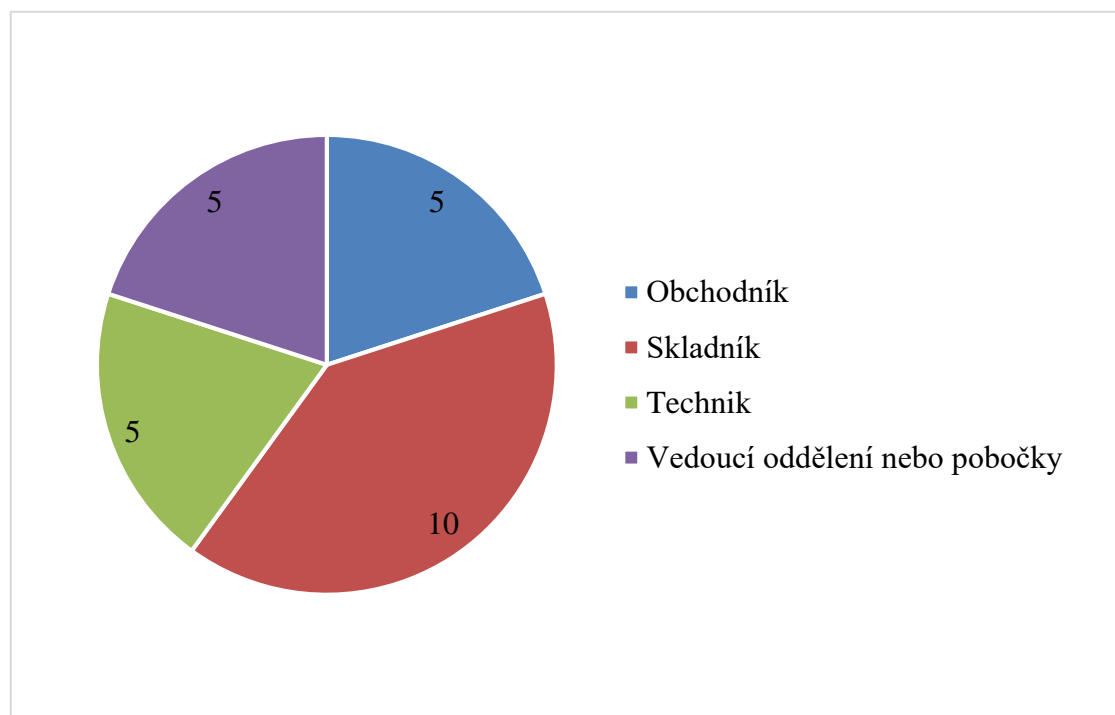
6.1 Vyhodnocení dotazníku – zaměstnanci

Návratnost dotazníkového šetření byla vysoká. Téměř všichni zaměstnanci byli ochotni odpovídat na otázky v dotazníku. Dotazník byl rozeslán celkem 28 zaměstnancům a 25 z nich se dotazníkového šetření účastnilo. Návratnost dotazníkového šetření byla vysoká, činila 89,29 %.

1. Na jaké pozici pracujete?

Tato otázka byla zvolena proto, aby bylo možné dále analyzovat povědomí jednotlivých pracovníků na určité pozici. Dotazníkového šetření se účastnili zaměstnanci na pozicích: skladník, obchodník, technik a vedoucí oddělení či pobočky. Následující obrázek znázorňuje počet zaměstnanců na pozicích.

Obrázek č. 6: Počet pracovních pozic



Zdroj: Vlastní zpracování, 2019

V následující tabulce je zobrazeno, kolik procent dotazovaných na určité pozici bylo ochotných se zúčastnit dotazníkového šetření.

Tabulka č. 9: Procento zúčastněných zaměstnanců dotazníkového šetření

Pracovní pozice	Procento zúčastnění (v %)
Skladník	100
Technik	100
Obchodník	71,43
Vedoucí oddělení nebo pobočky	83,33

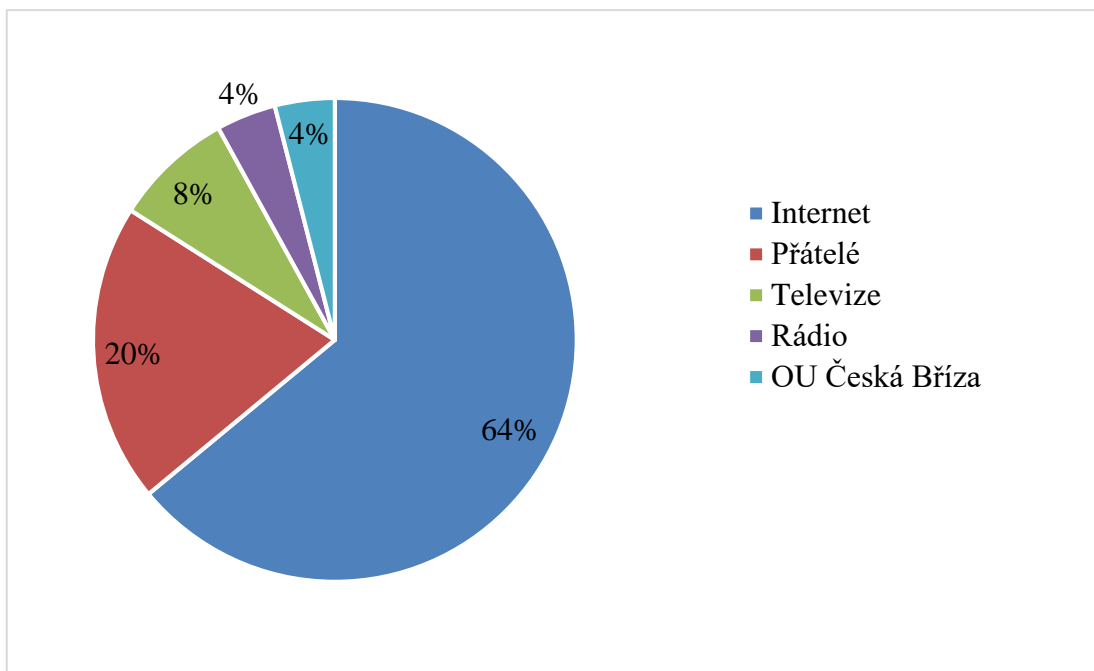
Zdroj: Vlastní zpracování, 2019

Nejvíce ochotni odpovídat byli skladníci a technici. Pracovníci na těchto pozicích odpověděli všichni. Na pozici vedoucích oddělení nebo pobočky neodpověděl pouze jeden zaměstnanec a procento návratnosti je tedy 83,33 %. Ze 7 obchodníků odpovědělo pouze 5 a tedy návratnost je 71,43 %.

2. Odkud jste se o GDPR dozvěděli poprvé?

Zaměstnanci měli na výběr z několika možností: internet, přátelé, rádio, televize, případně mohli napsat i jinou možnost. Nejpočetnější vybranou variantou byl internet se 16 odpověďmi. Na druhém místě se vyskytují přátelé s 5 odpověďmi. Pouze 2 vybrali televizi a po jedné vybrané variantě zaměstnanci vybrali rádio a jinou možnost. V jiné odpovědi se vyskytla možnost Obecní úřad Česká Bříza. V následujícím obrázku je zobrazeno procentní zastoupení odpovědí.

Obrázek č. 7: Odkud jste se o GDPR dozvěděli poprvé?



Zdroj: Vlastní zpracování, 2019

Lze usoudit, že zaměstnanci nejvíce sledují novinky na internetu, poté zprávy rozebírají se svými kamarády a sledují dění kolem sebe prostřednictvím televize. Jako poslední zdroje informací jsou rádio a jiné možnosti, v tomto případě Obecní úřad.

3. Od kdy je GDPR účinné

Jak již bylo uvedeno v kapitole 2, GDPR vstoupilo v platnost 25. 5. 2018. Bohužel ne všichni dotazovaní na tuto otázku odpověděli správně. Na výběr měli:

- 25. 4. 2018,
- 25. 5. 2018,
- 25. 6. 2018.

Velkým překvapením bylo, že 9 zaměstnanců odpovědělo jinou variantu než tu, která je správná. Přičemž 3 si mysleli, že GDPR je účinné o měsíc později a 6 o měsíc dříve. V následující tabulce je ukázáno, kolik procent vědělo správné datum v závislosti na pracovní pozici.

Tabulka č. 10: Vztah mezi pracovní pozicí a datem

	Skladník	Obchodník	Technik	Vedoucí oddělení nebo pobočky
25. 4. 2018	40 %	40 %	0 %	0 %
25. 5. 2018	30 %	60 %	100 %	100 %
25. 6. 2018	30 %	0 %	0 %	0 %
Celkem	100 %	100 %	100 %	100 %

Zdroj: Vlastní zpracování, 2019

Datum účinnosti GDPR správně označily všichni technici a vedoucí oddělení nebo pobočky. Z 5 obchodníků vybrali 3 správný datum, což je 60 % správných odpovědí a z 10 skladníků pouze 3, což je 30 % správných odpovědí. Je možné že při vyplňování se mohli zaměstnanci splést, nic méně dle mého názoru by o datu účinnosti nové legislativy upravující ochranu osobních údajů měl každý zaměstnanec vědět.

4. Víte, jaké informace o Vás správce smí shromažďovat?

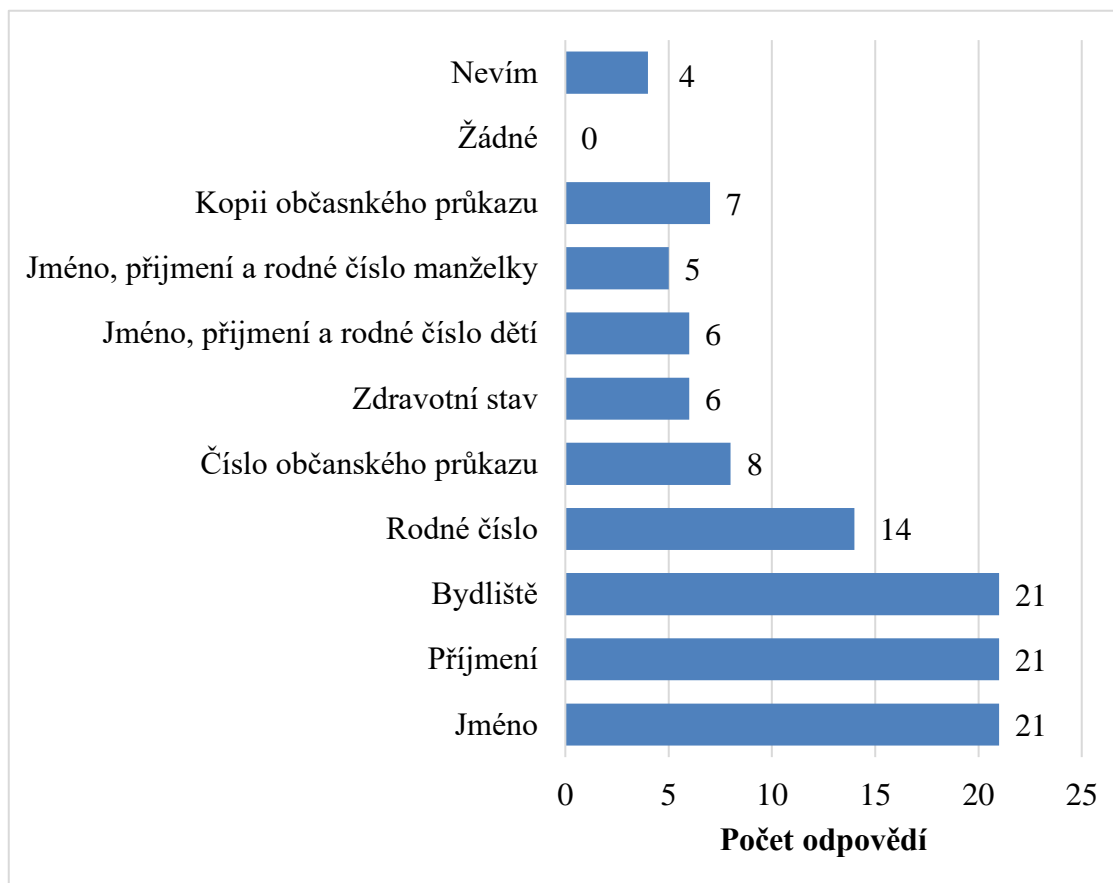
Otázka měla za úkol zjistit, jestli mají zaměstnanci povědomí o tom, jaké typy osobních údajů o nich smí zaměstnavatel shromažďovat a zpracovávat. Dle mého názoru by měla každá fyzická osoba vědět, co o nich smí zaměstnavatel či jiné instituce zpracovávat.

Zaměstnanci vybírali více odpovědí z následujících možností:

- jméno,
- příjmení,
- bydliště,
- rodné číslo,
- číslo občanského průkazu,
- zdravotní stav,
- jméno, příjmení a rodné číslo dětí,
- jméno, příjmení a rodné číslo manželky,
- kopii občanského průkazu,
- žádné,
- nevím.

Četnost odpovědí byla různorodá. Velkým překvapením bylo, že ani jeden zaměstnanec nezaškrtl všechny správné odpovědi. Většinou byly vybrány ty nejzákladnější. Počet odpovědí je zobrazen v následujícím obrázku.

Obrázek č. 8: Víte, jaké informace o Vás správce smí shromažďovat?



Zdroj: Vlastní zpracování, 2019

Správným výběrem jsou všechny možnosti, kromě kopie občanského průkazu, pokud k tomu nemá zaměstnavatel jakožto správce právní důvod. Právní důvody byly již uvedeny v kapitole 2.4.1. V kapitole 3.2.2 bylo uvedeno, že zaměstnavatel nemá žádné zákonné právo pořizovat kopii občanského průkazu, pokud občan nevydá písemný souhlas s pořízením kopie.

Nejpočetnějšími odpověďmi byly: bydliště, příjmení a jméno. Jedná se o základní osobní údaje a měly shodně po 21. Pouze 4 nemají žádné tušení, jaké osobní údaje smí správce zpracovávat. To znamená, že kromě těchto 4 všichni vybrali ty 3 výše uvedené osobní údaje.

Pouze 14 vybralo rodné číslo, které patří také mezi základní osobní údaj z důvodu správné identifikace zaměstnance pro potřeby státních institucí, například Okresní

správy sociálního zabezpečení. Okresní správa sociálního zabezpečení potřebuje znát i rodné číslo například pro evidenci odpracované doby, zakládající účast na sociálním pojištění z důvodu pobírání starobního důchodu. Jedná se o právní důvod plnění správní povinnosti správce.

V případě zdravotního stavu a jména, příjmení a rodného čísla manželky a dětí se jedná také o právní důvod plnění správní povinnosti správce, protože pokud zaměstnanec uplatňuje dle Zákona o dani z příjmu daňové zvýhodnění na dítě nebo slevu na manželku, je nutné uvádět jména a rodná čísla těchto osob.

I v případě zdravotního stavu se jedná o plnění právní povinnosti správce. Zaměstnavatel je totiž povinen evidovat například potvrzení o trvání dočasné pracovní neschopnosti (karantény), které je zaměstnanci vystaven v případě nemoci či hospitalizaci v nemocnici.

Pozitivní bylo, že žádný zaměstnanec nevybral možnost žádné. To znamená, že předpokládají a vědí, že alespoň nějaké osobní údaje smí správce zpracovávat, i když netuší jaké.

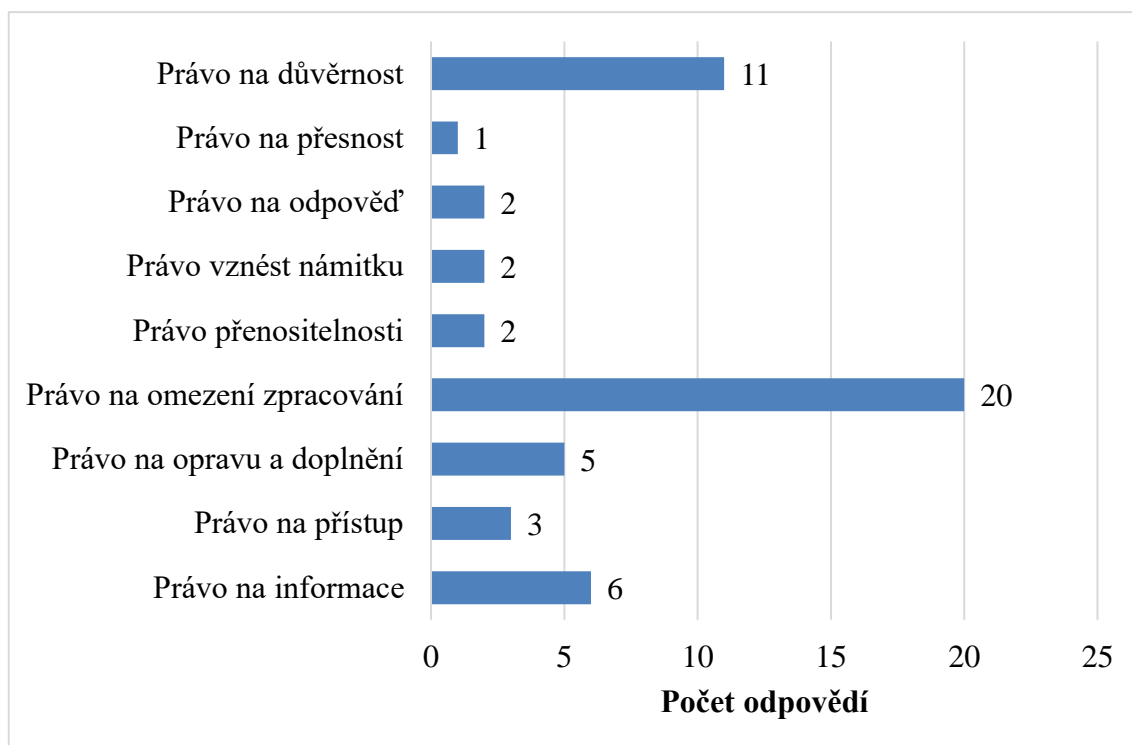
5. Jaká práva Vám GDPR přináší?

Cílem této otázky bylo zjistit, zda zaměstnanci vědí, jaká práva jim nová legislativa GDPR přináší. Na výběr měli celkem z 9 možností, z toho 6 práv jim opravdu GDPR přináší a 3 práva byla vymyšlená. Možnostmi byly:

- právo na informace,
- právo na přístup,
- právo na opravu a doplnění,
- právo na omezení zpracování,
- právo přenositelnosti,
- právo vznést námitku,
- právo na odpověď,
- právo na přesnost,
- právo na důvěrnost,

Na následujícím obrázku je znázorněn počet odpovědí.

Obrázek č. 9: Jaká práva Vám GDPR přináší



Zdroj: Vlastní zpracování, 2019

Jednotlivá práva jsou vysvětlena v kapitole 2.5. Správnou odpovědí mělo být: Právo na informace, právo na přístup, právo na odpověď, právo přenositelnosti, právo na omezení zpracování.

Zaměstnanci nejčastěji vybírali právo na omezení zpracování, tuto možnost vybralo 20 zaměstnanců. 11 zaměstnanců vybralo i právo na důvěrnost, které bohužel GDPR neuvádí a toto právo bylo vymyšleno. Dále vybírali právo na informace (6 odpovědí), právo na opravu a doplnění (5 odpovědí) a právo na přístup (3 odpovědi). Po dvou odpovědích mělo: právo přenositelnosti, právo vznést námitku a vymyšlené právo, právo na odpověď. Jeden zaměstnanec vybral možnost právo na přesnost, jedná se také o vymyšlené právo.

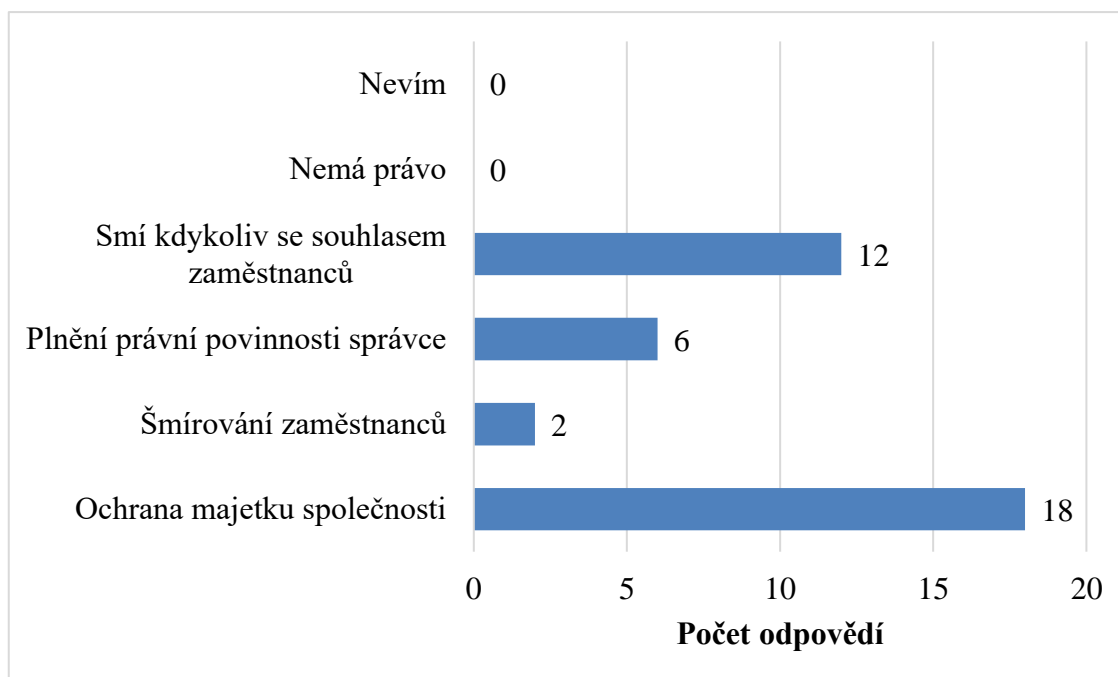
Lze usoudit, že zaměstnanci netuší, jaká práva mají, studiem legislativy se zřejmě nezabývali a informace si nikde nezjišťovali. Podle mě je to velká škoda, protože se jedná především o jejich ochranu a každý by měl znát jaká práva má, čeho se smí domáhat a aby věděl, o co smí žádat správce osobních údajů. Mělo by se jednat především o jejich vlastní zájem.

6. Za jakým účelem dle GDPR smí zaměstnavatel využívat na pracovišti kamery?

Tato otázka měla za cíl prověřit, zda zaměstnanci vědí, kdy smí zaměstnavatel mít na pracovišti umístěný kamerový systém. Na výběr měli:

- ochrana majetku společnosti,
- šmírování zaměstnanců,
- plnění právní povinnosti správce,
- smí kdykoliv se souhlasem zaměstnanců,
- nemá právo,
- nevím.

Obrázek č. 10: Za jakým účelem dle GDPR smí zaměstnavatel využívat na pracovišti kamery?



Zdroj: Vlastní zpracování, 2019

V kapitole 3.3 bylo uvedeno, že zaměstnavatel smí dle GDPR využívat kamerové systémy jen ze 2 právních důvodů, a to pro plnění právní povinnosti správce a pro ochranu majetku společnosti. Přitom GDPR neuvádí povinnost správce získat od svých zaměstnanců písemný souhlas. Je nutné, aby správce dokázal prokázat, že ochrana majetku společnosti převyšuje nad právy ochrany soukromí zaměstnanců.

Tyto 2 právní důvody zaměstnanci vybrali v případě ochrany majetku společnosti osmnáctkrát a plnění správní povinnosti pouze šestkrát. Možnost, že smí zaměstnavatel

umístit kamerové systémy kdykoliv se souhlasem zaměstnanců, byla druhou nejpočetnější vybranou možností, byla vybrána dvanáctkrát. Nejméně početnou možností, pouze 2 odpovědi, bylo za účelem šmírování zaměstnanců.

Shrnutí dotazníkové šetření – zaměstnanci

Celkové povědomí zaměstnanců o GDPR je velmi nízké. Celkem 9 zaměstnanců neví, od kdy je GDPR účinné. Většina zaměstnanců:

- netuší jaké všechny osobní údaje o nich a jejich rodině smí zaměstnavatel jakožto správce zpracovávat a uchovávat,
- neznají všechna svá práva, která jim GDPR přináší,
- neví, za jakým účelem smí kamerový systém správce využívat.

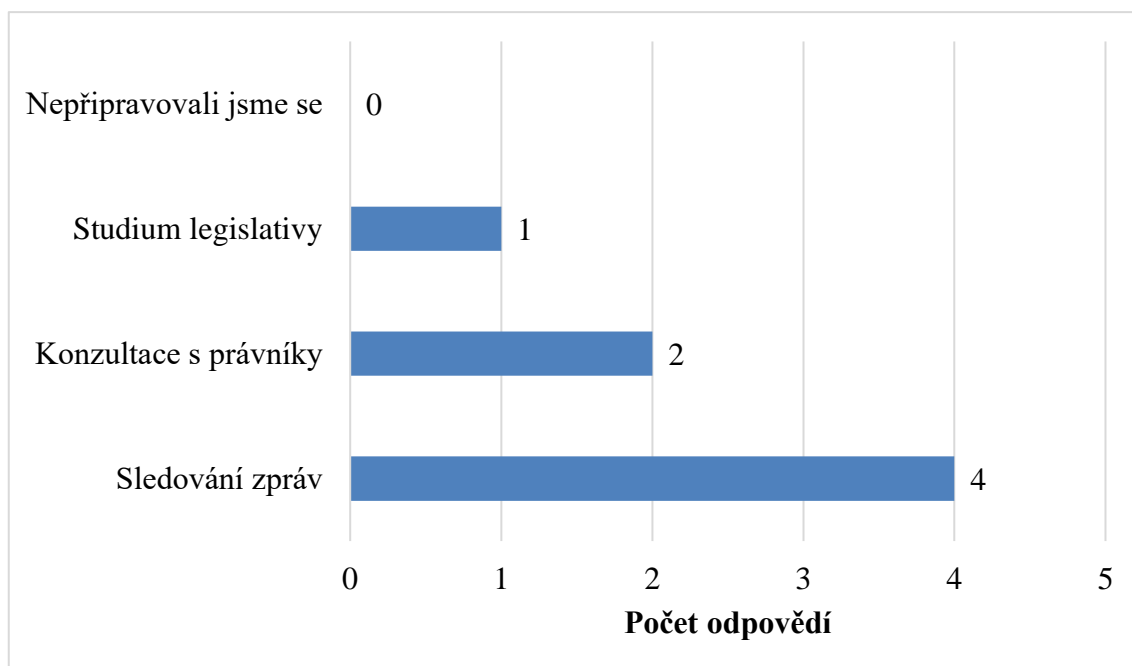
6.2 Vyhodnocení dotazníku – správce

Dotazník určený pro správce vyplňovaly celkem 4 osoby, oba jednatelé a dále mzdová účetní a personalista. Tyto osoby odpovídali na 8 otázek, které měly za úkol prověřit již získané informace a jestli, to, co uvedli je pravdivé.

1. Jak jste se připravovali na zavedení GDPR?

U této otázky měli správci na výběr ze 3 možností, jak se na GDPR připravovali a jednu možnost, která uváděla, že se nepřipravovali. Na následujícím obrázku je uveden počet odpovědí u jednotlivých možnostech.

Obrázek č. 11: Jak jste se připravovali na zavedení GDPR?



Zdroj: Vlastní zpracování, 2019

Všichni správci se připravovali na zavedení nové legislativy tak, že sledovali aktuální dění prostřednictvím zpráv. Zprávy sledovali nejen v televizi, ale i v rádiu, nebo na internetu. Jednatelé konzultovali novou legislativu s právníky a personalista zjišťoval informace prostřednictvím studia legislativy. Byli tedy využity všechny možnosti, které mohli správci využít. To znamená, že nechtěli být zaskočení a přípravu nepodcenili.

2. Jak dlouho jste se připravovali na zavedení GDPR?

U této otázky se všichni dotazovaní správci shodli a odpověděli, že jeden měsíc. Dle mého názoru se nejedná o velmi dlouhou dobu, nic méně na zjištění bližších informací a přípravu na zavedení GDPR je to dostačující. Vzhledem k tomu, že GDPR nepřináší žádné velké změny, je příprava v časovém horizontu jeden měsíc postačující.

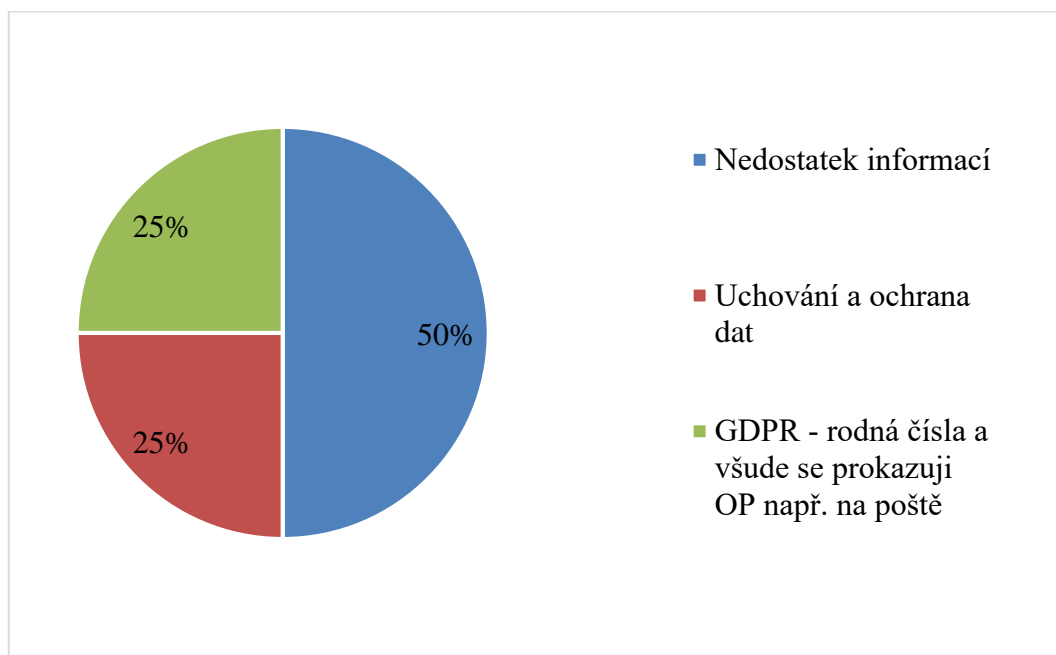
3. V čem jste viděli největší problém při zavádění GDPR?

Tato otázka byla položena za účelem zjištění, co se správcům zdálo jako největší problém při zavádění GDPR. Správci vybírali z možností:

- nedostatek možností,
- uchování a ochrana dat,
- sdílení osobních údajů s úřady nebo
- jiné.

Na následujícím obrázku je znázorněno procento vybraných odpovědí.

Obrázek č. 12: V čem jste viděli největší problém při zavádění GDPR?



Zdroj: Vlastní zpracování, 2019

Dva správci viděli jako největší problém při zavádění GDPR nedostatek informací. Jeden správce viděl největší problém v uchování a ochraně dat a zbývající správce viděl problém prokazování totožnosti prostřednictvím Občanského průkazu, na kterém jsou uvedeny osobní údaje, například rodné číslo.

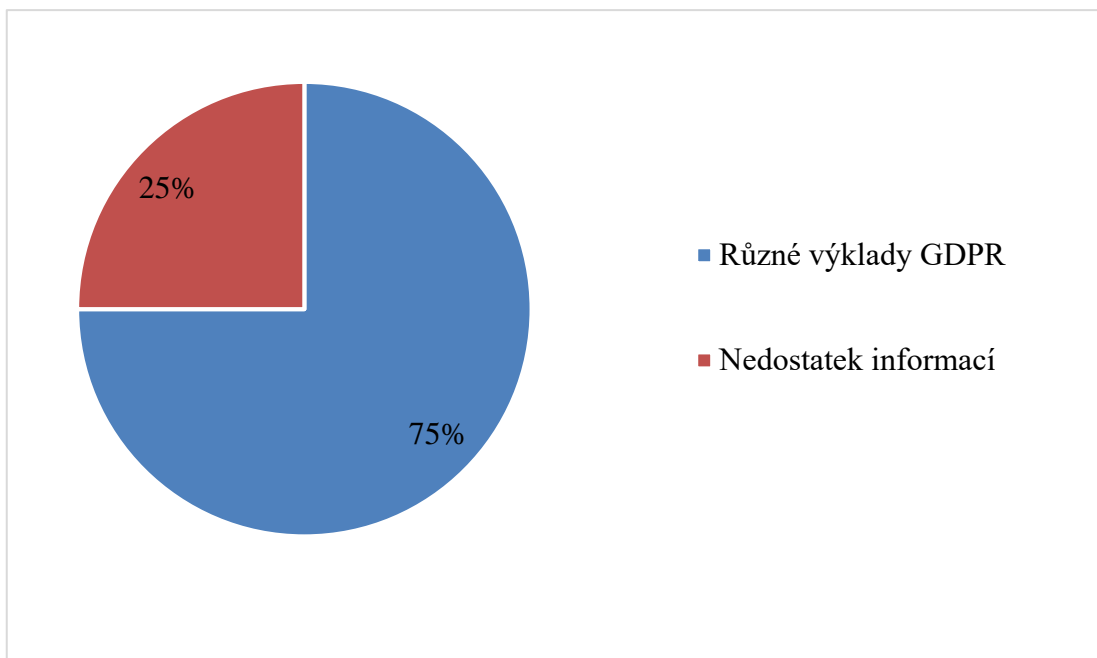
4. Jaký byl pro Vás největší problém při zavádění GDPR?

Tato otázka byla do dotazníkového šetření zvolena, kvůli zjištění, co pro správce bylo největším problémem při zavádění GDPR. Správci vybírali z několika možností:

- různé výklady GDPR,
- nedostatek informací,
- zveřejňování fotografií,
- kamerové systémy,
- zajištění bezpečnosti zpracování osobních údajů.

Na následujícím obrázku je zobrazeno procento odpovědí.

Obrázek č. 13: Jaký byl pro Vás největší problém při zavádění GDPR?



Zdroj: Vlastní zpracování, 2019

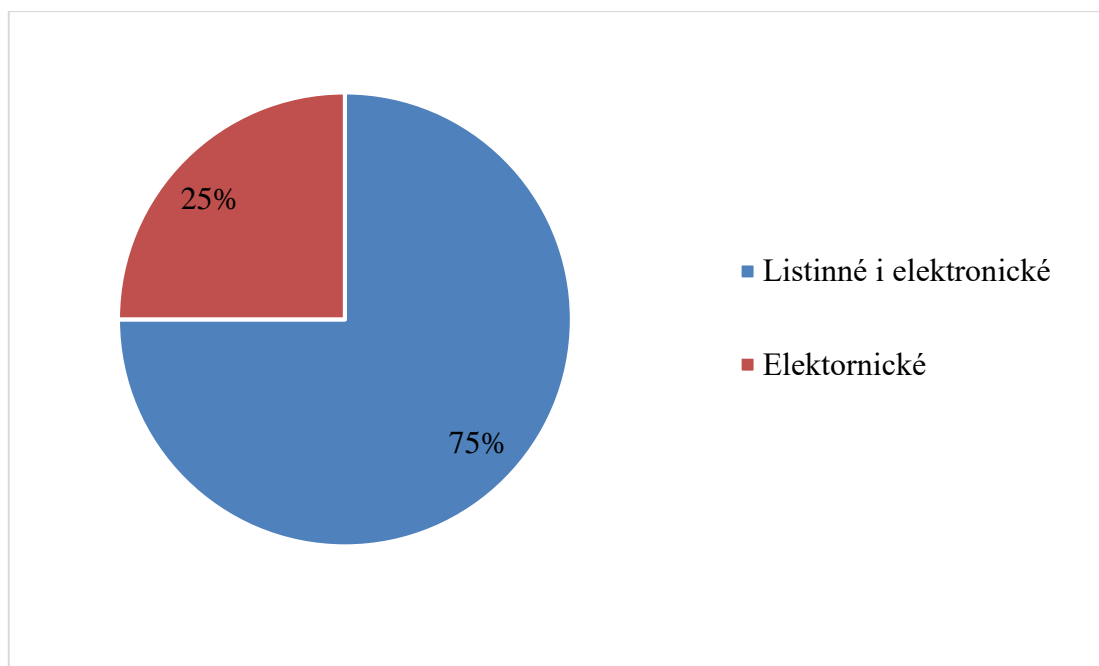
Pouze jeden z dotazovaných správců zvolil možnost nedostatek informací. Byl to ten, který v první otázce, která se zabývala přípravou na zavedení GDPR, zvolil sice všechny možnosti, ale přesto se mu zdálo, že je informací nedostatek. Bohužel není další způsob, který by umožňoval zjišťování informací, snad už jen internet.

Zbylí správci zvolili možnost různých výkladů vztahujících se k GDPR. S tímto problémem se lze setkat nejen u nové legislativy, ale i u té stávající. Každý právník má na zákony a právní předpisy jiný pohled a každá osoba může napsané definice či zákony chápat jinak.

5. V jaké podobě zpracováváte osobní údaje zaměstnanců?

Úkolem této otázky bylo prověřit, v jaké podobě správce zpracovává osobní údaje zaměstnanců. Osobní údaje mohou totiž zpracovávat pouze v listinné podobě, pouze v elektronické podobě, případně využít obě varianty. Na následujícím obrázku je znázorněno procento odpovědí.

Obrázek č. 14: V jaké podobě zpracováváte osobní údaje zaměstnanců?



Zdroj: Vlastní zpracování, 2019

Pouze jeden ze 4 správců odpověděl, že se ve společnosti zpracovávají osobní údaje zaměstnanců pouze v elektronické podobě. Byl to jeden z jednatelů, a to ten, který se nezabývá oblastí personalistiky ani zpracováním mezd. Je tedy jasné, že nemá moc velké ponětí o tom, jaké a jak se osobní údaje zaměstnanců zpracovávají.

Zbylí 3 správci odpověděli, že v listinné a zároveň i v elektronické podobě. Především personalista a mzdová účetní by tuto skutečnost měli vědět. Druhý ze správců vybral také tuto možnost, protože dříve pomáhal v této oblasti. To je taky důvod, proč dohlíží právě nad těmito zaměstnanci.

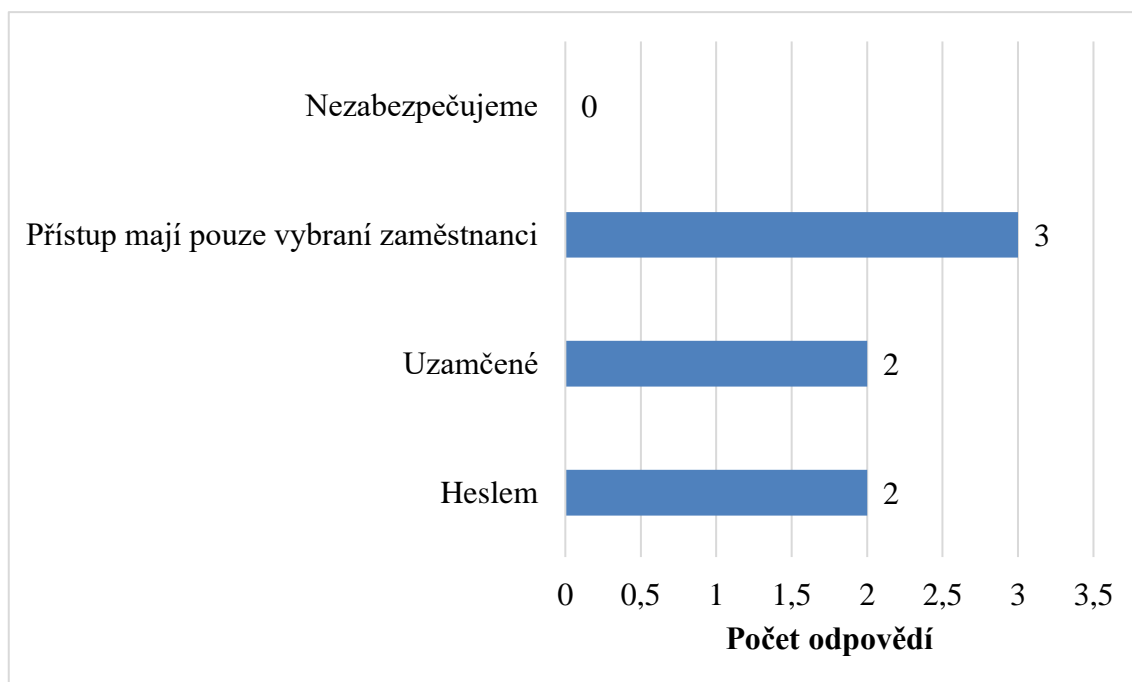
6. Jak zabezpečujete osobní údaje zaměstnanců?

Cílem této otázky bylo ověřit tvrzení ohledně zabezpečení osobních údajů. Osobní údaje mohou být zabezpečeny:

- heslem,
- uzamčením,
- oprávněným přístupem pouze vybraných zaměstnanců.

Další možností, kterou mohli správci vybrat bylo, že osobní údaje nijak nezabezpečují případně mohli doplnit další způsob zabezpečení, který ve společnosti využívají. Na následujícím obrázku je znázorněn počet jednotlivých odpovědí.

Obrázek č. 15: Jak zabezpečujete osobní údaje?



Zdroj: Vlastní zpracování, 2019

Jen 3 správci zvolili možnost, že přístup mají pouze vybraní zaměstnanci. Jeden si zřejmě neuvědomil, že v novém objektu je zabezpečení na čipy, a ne každý má přístup všude, nebo o této skutečnosti neví.

Dva správci zvolili možnost, že údaje jsou zabezpečené heslem a že jsou zamčené. Uzamčené jsou ale pouze v místnostech, nikoliv ve skříních a týká se to pouze osobních údajů v listinné podobě. V případě zabezpečení pomocí hesla se jedná o osobní údaje v elektronické podobě.

7. Jak často aktualizujete osobní údaj, které zpracováváte?

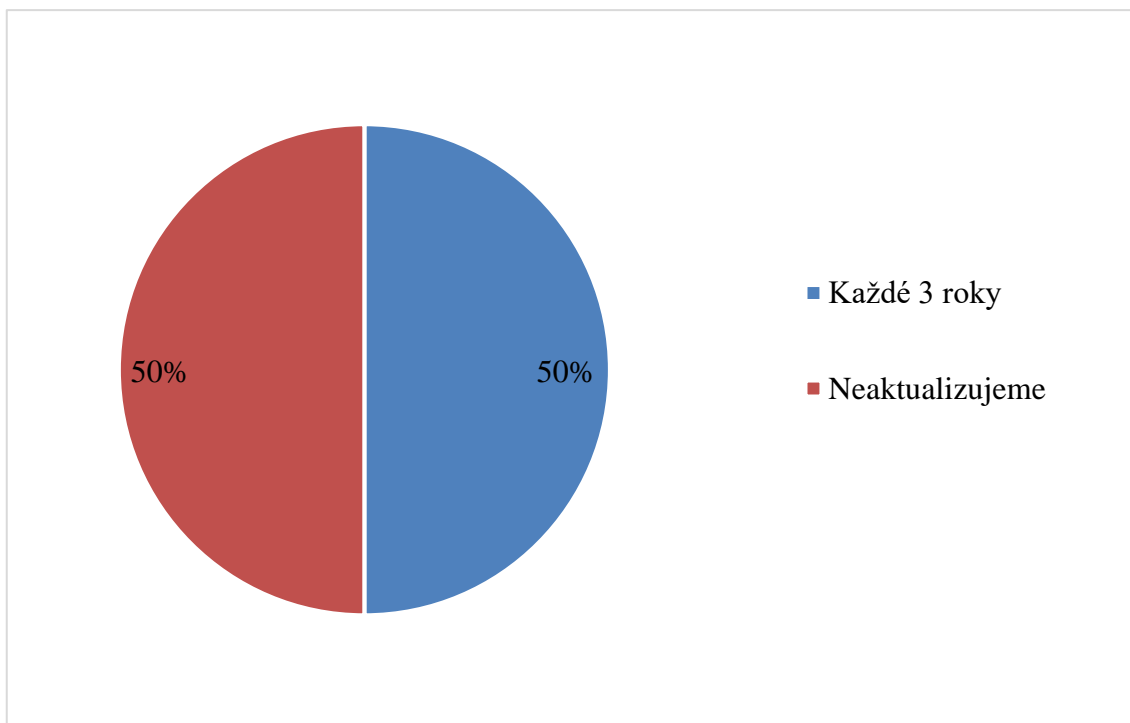
Tato otázka měla za cíl ověřit, jak často se ve společnosti aktualizují osobní údaje.

Na výběr z možností byly:

- každé 3 roky,
- každých 5 let,
- neaktualizujeme.

Následující obrázek znázorňuje procento odpovědí.

Obrázek č. 16: Jak často aktualizujete osobní údaje, které zpracováváte?



Zdroj: Vlastní zpracování, 2019

V této otázce jsou výsledky 50 % každé 3 roky a 50 %, že osobní údaje neaktualizují. Skutečnost, že osobní data nejsou aktualizována odpověděli personalista a mzdová účetní.

Jednatelé odpověděli, že se osobní údaje aktualizují každé 3 roky. To může znamenat pouze 2 skutečnosti. Buď je ve vnitřní směrnici stanoveno, že se mají osobní údaje pravidelně aktualizovat, ale správci toto neplní, nebo s tímto postupem uvedeným vnitropodnikové směrnici nejsou zpracovatelé (personalista a mzdová účetní) seznámeni.

8. Jak dlouho zpracováváte osobní údaje?

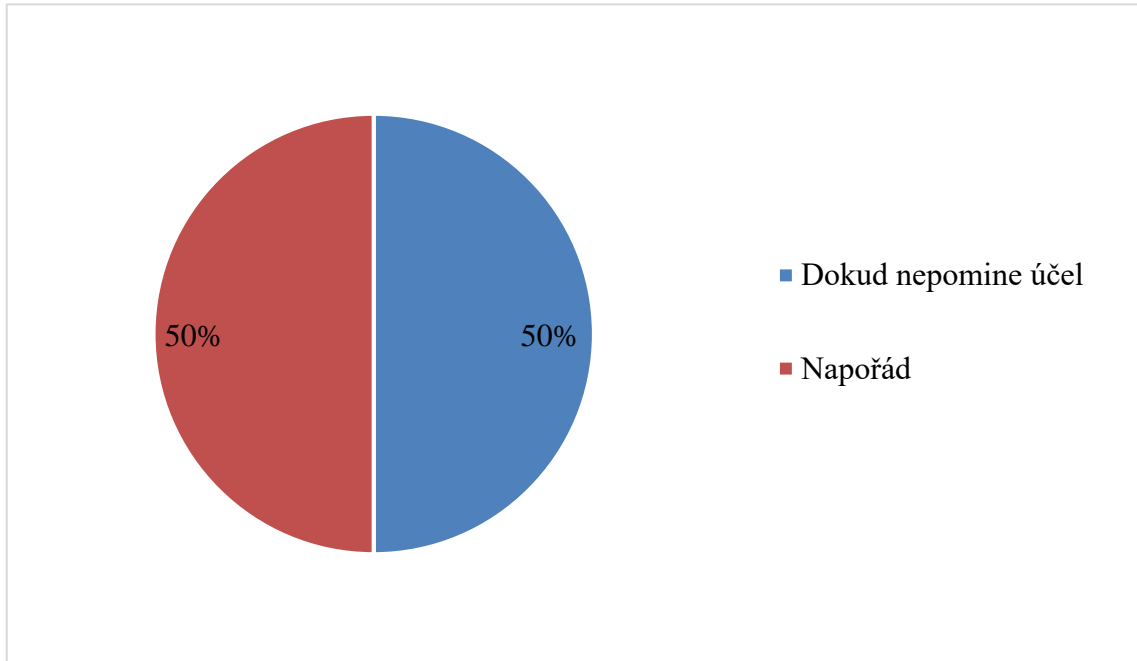
Cílem této otázky bylo zjistit, jak dlouho jsou ve společnosti zpracovávány osobní údaje. Na výběr měli z možností:

- 3 roky,
- 5 let,
- 10 let,
- napořád,

- nearchivujeme,
- dokud nepomine účel.

Na následujícím, obrázku je zobrazeno procento odpovědí.

Obrázek č. 17: Jak dlouho zpracováváte osobní údaje?



Zdroj: Vlastní zpracování, 2019

Stejně jako v předchozí otázce se i zde rozcházejí odpovědi jednatelů a zpracovatelů. Jednatelé odpověděli, že se osobní údaje zpracovávají, dokud nepomine účel, zatímco zpracovatelé uvedli, že se osobní údaje zpracovávají napořád.

Výsledky jsou v návaznosti na předchozí otázku. Jak by mohli zjistit, jestli již účel uplynul nebo ne, když údaje nejsou aktualizovány? Je logické, že pokud zpracovatelé uvádějí, že se osobní údaje neaktualizují, nemohou se tedy ani zpracovávat, dokud nepomine jejich účel, a jsou tedy všechny údaje zpracovávány napořád.

Shrnutí dotazníkového šetření – správce

Výsledkem dotazníkového šetření je, že se jednatelé i zpracovatelé ve většině otázek shodli. Ovšem v posledních 2 otázkách se jejich názory rozcházejí. Jednatelé nemají pod kontrolou veškeré postupy související s ochranou osobních údajů. Zpracovatelé neplní všechna pravidla, která jsou ve společnosti stanovena vnitropodnikovou směrnicí.

7 Návrhy opatření na zlepšení v oblasti ochrany dat

V této kapitole jsou navržena některá opatření pro zlepšení stávajícího stavu v oblasti ochrany osobních údajů ve společnosti DISCOMP. Doporučení se netýká jen správců a zpracovatelů, ale týkají se i zaměstnanců společnosti.

Prvním opatřením, které se jeví jako velmi důležité v návaznosti na výsledky dotazníku pro zaměstnance je, aby se pro zaměstnance udělalo školení v oblasti ochrany dat. Zájem zaměstnavatele je ten, aby byli zaměstnanci s novou legislativou plně seznámeni, protože i někteří z nich zpracovávají osobní údaje zákazníků. Tito zaměstnanci nemají podepsaný žádný dokument o plné odpovědnosti, a tak v případě případného soudního sporu ze strany stížnosti zákazníků by veškeré náklady musela uhradit společnost.

S problematikou podepsané odpovědnosti za zpracování osobních údajů souvisí druhé opatření. Dle mého názoru mají mít všichni zaměstnanci, kteří nějakým způsobem zpracovávají osobní údaje, podepsanou odpovědnost za zpracování. Vedení společnosti se tímto krokem bude moci domáhat alespoň částečné náhrady v případě udělené pokuty při porušení pravidel stanovených GDPR. Takovýto dokument mají sice podepsaní zpracovatelé osobních údajů zaměstnanců, ale obchodníci, kteří zpracovávají osobní údaje odběratelů, již tento dokument podepsaný nemají.

Co se týče doporučení pro správce jako vhodné opatření je uložení osobních spisů zaměstnanců do uzamykatelných skříní. Je sice pravda, že jsou již v uzamčených místnostech s omezeným přístupem prostřednictvím čipů, ale čipy také nejsou všemocné. Klidně se může stát, že jsou chybně nastavena práva a tím pádem i neoprávněná osoba by mohla mít přístup k osobním údajům zaměstnanců. Když budou spisy uloženy ještě v zamykatelných skříních bude pro zaměstnance obtížnější se k nim dostat.

Dalším návrhem je, aby jednatele seznámili řádně všechny osoby zpracovávající osobní údaje ať zaměstnanců či odběratelů s vnitropodnikovou směrnicí, ve které jsou uvedeny postupy pro zpracovávání osobních údajů. Následně mají jednatele dbát na dodržování těchto pravidel a pravidelně zpracovatele kontrolovat.

Dle mého názoru je na místě, aby se zpracovatelé osobních údajů zaměstnanců zúčastnili školení zaměřeného na problematiku GDPR. Na tomto školení, se mohou dozvědět mnoho užitečných informací, které jim mohou usnadnit práci při zpracovávání

osobních údajů. Dalšími informacemi, které prostřednictvím školení získají jsou, jak často údaje aktualizovat a následně jak dlouho, které informace archivovat. Částečný výčet písemností a dob archivačních lhůt je uveden v kapitole 3.2.3, ale na školení zjistí více informací.

Návrhy opatření na zlepšení v oblasti ochrany dat jsou demonstrovány v tabulce č. 11.

Tabulka č. 11: Návrhy opatření na zlepšení v oblasti ochrany dat

Návrh opatření	Přínos pro organizaci
Školení pro zaměstnance	Vzdělání zaměstnanci
Podepsaná odpovědnost zpracování pro všechny zaměstnance, kteří zpracovávají osobní údaje	Spoluúčast zaměstnanců při náhradě škody v případě soudního sporu
Uložení osobních spisů do zamykatelných skříní	Lepší zabezpečení
Řádně seznámit všechny zaměstnance s vnitropodnikovou směrnicí	Informování zaměstnanci o postupech stanovené organizací, snazší kontrola
Školení pro zpracovatele	Větší informovanost zpracovatelů v oblasti ochrany dat, zjednodušení postupů při zpracovávání osobních údajů

Zdroj: Vlastní zpracování, 2019

Závěr

Cílem této práce bylo analyzovat proces zavedení GDPR, celým názvem: 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), ve zvoleném podnikatelském subjektu.

V první kapitole byl uveden cíl a metodika řešení. Ve druhé kapitole bylo vysvětleno, čím se Obecné nařízení zabývá, byly definovány důležité pojmy pro GDPR, uvedeny a vysvětleny zásady, představeny práva nositelů osobních údajů a na závěr této kapitoly byly uvedeny sankce pro správce za nedodržování GDPR. Třetí kapitola se zabývá srovnáním zákona o ochraně osobních údajů s GDPR. Srovnání bylo provedeno z několika pohledů a výsledkem bylo, že GDPR nepřináší žádné velké změny.

Ve čtvrté kapitole byl představen zvolený ekonomický subjekt, ve kterém probíhala analýza a hodnocení procesu zavedení GDPR. Pátá kapitola je zaměřena již na samotnou analýzu zavedení. Nejprve je popsán stav před zavedením GDPR, poté příprava na jeho zavedení a následná analýza stavu po jeho zavedení. Součástí analýzy stavu po zavedení GDPR je dotazníkové šetření, které je rozděleno na 2 části. První částí je ověření znalosti GDPR u zaměstnanců. Druhou částí je ověření zjištěných informací u správců.

Poslední 2 kapitoly se zabývají vyhodnocením dotazníků a návrhům k vylepšení stávajícího stavu vycházející z dotazníkového šetření. Mezi návrhy bylo zařazeno školení a podepsání prohlášení o odpovědnosti zpracovatele za zpracovávání osobních údajů.

Seznam zdrojů

Advokátní kancelář CÍSAŘ, ČEŠKA, SMUTNÝ (2018). *E-government a GDPR: (soubor zákonů)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk.

Bartík, V. & Janečková, E (2013). *Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací*. Olomouc: ANAG.

Bartík, V. & Janečková, E (2016). *Ochrana osobních údajů v aplikační praxi: (vybrané problémy)*. Praha: Wolters Kluwer.

Bhatia, P. (2018). *Intro to GDPR: a Plain English Guide to Compliance*. Zagreb: Advisera Expert Solutions Ltd.

Discomp (2018). *O nás*, cit. 3.9.2018, dostupné z:

<https://www.discomp.cz/default.asp?show=wm&wmpart=article&wmaid=46>

Discomp (2019). *O nás*, cit. 1.2.2019, dostupné z:

<https://www.discomp.cz/default.asp?show=wm&wmpart=article&wmaid=46>

Evropská unie (2018). *Nářízení, směrnice a další právní akty*, cit. 11. 11. 2018, dostupné z: https://europa.eu/european-union/eu-law/legal-acts_cs

Interní zdroje

Janečková, E. (2018). *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer.

Janečková, E & Bartík, V. (2011). *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde.

Janečková, E. & Bartík, V. (2016). *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer.

Kubíčková, A. & Pátáková V. (2017). *Ochrana osobních údajů zaměstnanců od a (přes GDPR) do Z*. Wolters Kluwer ČR, a. s., cit. 21. 1. 2019, dostupné z: <http://www.mzdovapraxe.cz/archiv/dokument/doc-d58022v70817-ochrana-osobnich-udaju-zamestnancu-od-a-pres-gdpr-do-z/>

Kučerová, D. (2018). *GDPR a výmaz osobních údajů po skončení pracovního poměru*, cit. 21. 1. 2019, dostupné z: <https://www.podnikatel.cz/clanky/gdpr-a-vymaz-osobnich-udaju-po-skonceni-pracovniho-pomeru/>

- Miglicco, G. (2018). GDPR is here and it's time to get serious, *Computer Fraud & Security*. 18(9), 9-12. Dostupné z:
<https://reader.elsevier.com/reader/sd/pii/S136137231830085X?token=0EF216098CBD05086F9A041C7371E8338BD2DB88E86C5CA0FF6C3B5AE1ECEF87E12BC47124A43BF1536ACCE1DDC70191>
- Ministerstvo vnitra České republiky (2019). *Co je GDPR*, cit. dne 19. 2. 2019. Dostupné z: <https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx>
- Nařízení evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. In: *Úřední věstník Evropské unie*. 2016
- Navrátil, J. (2018). *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk
- Nezmar, L. (2017). *GDPR: praktický průvodce implementací*. Praha: Grada Publishing.
- Nonnemann, F. (2018). *Progres Guru. 3 důvody vzniku nového nařízení GDPR*, cit. 31. 8. 2018, dostupné z: <https://www.progresguru.cz/blog/107-3-duvody-vzniku-noveho-narizeni-gdpr>
- Nonnemann, F (2018). *Příručka pověřence pro ochranu osobních údajů*. Praha: Klika
- Nulíček, M (2018). *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. In: *Official Journal of the European Union*. 2016
- Škorníčková, E. a. (2018). GDPR. *Právo na přístup*, Cit. 2. 1. 2019, dostupné z: <https://www.gdpr.cz/gdpr/heslo/pravo-na-pristup/>
- Škorníčková, E. b. (2018). GDPR. *Právo na výmaz*, Cit. 2. 1. 2019, dostupné z: <https://www.gdpr.cz/gdpr/heslo/pravo-na-vymaz/>
- Škorníčková, E. c. (2018). GDPR. *Jaké sankce hrozí firmám, které budou GDPR ignorovat*, cit. 2. 1. 2019, dostupné z: <https://www.gdpr.cz/gdpr/sankce/>

Účetní závěrka umístěná na Justice.cz. Dostupné z: <https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=55192067&subjektId=164502&spis=483545>

Úřad pro ochranu osobních údajů (2018). *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. července 2017*, cit. dne 19. 2. 2019. Dostupné z: <https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-cervence-2017/ds-3109/archiv=0&p1=1257>

Výroční zpráva umístěná na Justice.cz. Dostupné z: <https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=55192067&subjektId=164502&spis=483545>

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Zákon č. 563/1991 Sb., o účetnictví

Zákon č. 586/1992 Sb., o daních z příjmů

Žůrek, J. (2017). *Praktický průvodce GDPR*. Olomouc: ANAG.

Žůrek, J. (2018). *Praktický průvodce GDPR*. Olomouc: ANAG.

Seznam tabulek

Tabulka č. 1: Povinnost správce poskytnout základní poskytované minimum	20
Tabulka č. 2: Další poskytované informace.....	20
Tabulka č. 3: Známost zásad ze zákona o ochraně osobních údajů.....	25
Tabulka č. 4: Vybrané dokumenty v oblasti personalistika a jejich archivace (v letech)	30
Tabulka č. 5: Nejdůležitější změny, které přináší GDPR.....	32
Tabulka č. 6: Osobní údaje, které společnost zpracovává	42
Tabulka č. 7: Způsoby zpracování osobních údajů.....	44
Tabulka č. 8: Vyčíslení nákladů v Kč.....	48
Tabulka č. 9: Procento zúčastněných zaměstnanců dotazníkového šetření.....	51
Tabulka č. 10: Vztah mezi pracovní pozicí a datem.....	53
Tabulka č. 11: Návrhy opatření na zlepšení v oblasti ochrany dat	67

Seznam obrázků

Obrázek č. 1: Porovnání vývoje technologií a legislativy	12
Obrázek č. 2: Schéma organizací, které aplikují GDPR.....	13
Obrázek č. 3: Logo společnosti.....	33
Obrázek č. 4: Organizační struktura	35
Obrázek č. 5: Vývoj obratu v mil. USD	36
Obrázek č. 6: Počet pracovních pozic.....	50
Obrázek č. 7: Odkud jste se o GDPR dozvěděli poprvé?	52
Obrázek č. 8: Víte, jaké informace o Vás správce smí shromažďovat?	54
Obrázek č. 9: Jaká práva Vám GDPR přináší.....	56
Obrázek č. 10: Za jakým účelem dle GDPR smí zaměstnavatel využívat na pracovišti kamery?.....	57
Obrázek č. 11: Jak jste se připravovali na zavedení GDPR?	59
Obrázek č. 12: V čem jste viděli největší problém při zavádění GDPR?	60
Obrázek č. 13: Jaký byl pro Vás největší problém při zavádění GDPR?	61
Obrázek č. 14: V jaké podobě zpracováváte osobní údaje zaměstnanců?	62
Obrázek č. 15: Jak zabezpečujete osobní údaje?	63
Obrázek č. 16: Jak často aktualizujete osobní údaje, které zpracováváte?.....	64
Obrázek č. 17: Jak dlouho zpracováváte osobní údaje?	65

Seznam příloh

Příloha A: Souhlas se zpracováním a shromažďováním osobních údajů	75
Příloha B: Osobní dotazník.....	76
Příloha C: Informování zaměstnanců o kamerovém systému	78
Příloha D: Souhlas se zpracováním osobních údajů	79
Příloha E: Dotazník – zaměstnanci	83
Příloha F: Dotazník – správce.....	85

Příloha A: Souhlas se zpracováním a shromažďováním osobních údajů

Souhlas se zpracováním a shromažďováním osobních údajů

Já níže podepsaný/á/, v souladu s § 5 odst.5 zákona č. 101/2000 Sb., o ochraně osobních údajů, uděluji tímto souhlas k tomu aby můj zaměstnavatel – firma Discomp s.r.o.zastoupená ing. ~~Harmáčkem~~, mohl používat mé osobní údaje včetně rodného čísla k účelům souvisejícím s pracovním poměrem /pracovní smlouva, osobní dotazník, tiskopisy pro zdravotní pojišťovnu, OSSZ atd./ a aby tyto údaje byly založeny v mém osobním spisu.

Příjmení jméno : RČ:

Datum Podpis

Příloha B: Osobní dotazník

OSOBNÍ DOTAZNÍK

Fotografie

Příjmení, jméno, titul		Den, měsíc, rok narození	
rodné číslo dřívější		Místo, okres (stát)	Rodné číslo
Trvalé bydliště – část I PSČ	číslo popisné/orientační	Přechodné bydliště - PSČ	číslo
ulice	telefon	ulice	telefon
Občanský průkaz číslo		Zdravotní pojišťovna	Státní příslušnost
Rodinný stav	Datum sňatku, rozvodu, ovdovění	Cestovní pas pro služební účely číslo platnost do roku	
RODINNÍ PŘÍSLUŠNÍCI			
Jméno, příjmení (i rodné)	Datum narození	Invalidní	Bydliště
Zaměstnan(a), studuje - kde			
Manžel(ka), druh, družka			
Děti			
Rodiče			
Ostatní vyživované osoby			
DOKONČENÉ VZDĚLÁNÍ			
vzdělání	druh školy, výchovy, obor	počet tříd (semestrů)	rok ukončení
Druh zkoušky			
základní			
střední odborné			
úplně střední (učební obor s mat.)			
úplně střední všeobecné			
úplně střední odborné			
vyšší odborné			
vysokoškolské			
vědecká výchova			
postgraduální studium			
nahrazující předepsané			
Nedokončené - včetně současného studia při zaměstnání			
Dlouhodobé kurzy odborná školení apod.			
znalost cizích řečí			
jazyk	stupeň znalosti	zkoušky	

Příloha C: Informování zaměstnanců o kamerovém systému

INTERNÍ SMĚRNICE SPOLEČNOSTI DISCOMP s.r.o.

**Informování zaměstnanců společnosti DISCOMP s.r.o. , IČO:
252 36 792, se sídlem Plzeň, Dopravní 1218/2a, PSČ 318 00, o
kamerovém systému**

Zpracování osobních údajů

Jméno:

datum narození:

bytem:

(dále také jako „**Zaměstnanec**“)

svým podpisem stvrzuje, že jej **DISCOMP s.r.o.** , IČO: 252 36 792, se sídlem Plzeň, Dopravní 1218/2a, PSČ 318 00 (dále také jako „**Zaměstnavatel**“), jakožto správce osobních údajů, řádně informoval o zpracování osobních údajů Zaměstnance prostřednictvím obrazového záznamu kamerového systému provozovaného za účelem ochrany majetku a dalších oprávněných zájmů Zaměstnavatele, přičemž svým podpisem Zaměstnanec dále stvrzuje, že byl seznámen s počtem a rozmístěním kamerových zařízení, s dobou uchovávání záznamů a režimem kamerového sledovacího systému.

V Plzni dne

.....

Zaměstnanec

Příloha D: Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů

Zaměstnanec :

Zaměstnavatel: **DISCOMP s.r.o.**, IČO: 252 36 792, se sídlem Plzeň,
Dopravní 1218/2a, PSČ 318 00

Svým podpisem **vyjadřuji souhlas se** zpracováním mých osobních údajů společností DISCOMP s.r.o., IČO: 252 36 792, se sídlem Plzeň, Dopravní 1218/2a, PSČ 318 00, zapsané v obchodním rejstříku vedeném Krajským soudem v Plzni oddíl C vložka 11558, **v rozsahu a pro účely, které jsou uvedeny níže.**

- Souhlas uděluji pro mnou předané anebo společností DISCOMP s.r.o. pořízené **adresní a identifikační údaje**, a to jméno, příjmení, datum narození, rodné číslo, adresu trvalého bydliště, zdravotní pojišťovna zaměstnance, příslušné pracoviště ČSSZ
 - rodinný stav a údaje o rodinných příslušnících zaměstnance (děti, manžel), včetně jejich jména, příjmení, data narození a státní příslušnosti
 - číslo bankovního účtu zaměstnance
- fotografie, videa a články určené k publikaci, za účelem jejich použití **pro potřeby firemního marketingu:**
- zasilání blahopřání k životnímu nebo pracovnímu jubileu
 - zasilání pozvánek na interní akce pořádané společností DISCOMP s.r.o. zveřejnění fotografie v aplikaci Outlook (interní komunikace)
 - zveřejnění fotografie na firemních webových stránkách (veřejná prezentace)
 - zveřejnění fotografie nebo videa pořízených v rámci pořádání firemních akcí

Můj souhlas uděluji na **dobu trvání zaměstnaneckého poměru s přesahem tří let po ukončení zaměstnaneckého poměru** se společností DISCOMP s.r.o.

Současně potvrzuji, že jsem byl společností DISCOMP s.r.o., informován:

- **správce osobních údajů** je společnost DISCOMP s.r.o., IČO: 252 36 792, se sídlem Plzeň, Dopravní 1218/2a, PSČ 318 00,
- udělený souhlas mohu u společnosti DISCOMP s.r.o. **kdykoliv odvolat** na výše uvedené adrese

- mé údaje **bude zpracovávat** za účelem plnění zákonných povinností a dále pro marketingové oddělení a jednatel společnosti DISCOMP s.r.o.
- **zpracovatelem osobních údajů** je společnost, se kterou má správce osobních údajů uzavřenou **Smlouvu o zpracování osobních údajů**
- **Způsob zpracování:** Osobní údaje zaměstnanců budou zaměstnavatelem zpracovávány manuálně i automatizovaně. K osobním údajům budou mít přístup pověřeni pracovníci zaměstnavatele na pozici personalista, správce IT, dále statutární orgán zaměstnavatele, účetní zaměstnavatele, externí advokátní kancelář, daňový poradce.
- Osobní údaje budou v souladu se zákonem poskytovány následujícím subjektům:
 - Úřadu práce ČR
 - zdravotní pojišťovně zaměstnance
 - příslušné správě sociálního zabezpečení
 - příslušnému Finančnímu úřadu
- Zaměstnavatel vede v souladu s čl. 30 nařízení záznamy o činnostech zpracování. Podrobnosti o vedení těchto záznamů stanoví vnitřní předpis zaměstnavatele.
- o mých právech dle článků 13, 15, 16, 17, 18, 20 a 21 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), a to zejména že:

1. Právo na informace

Práve na informace se rozumí veškerá práva subjektu obsažená v čl. 13 nařízení. Zejména se jedná o právo na znalost totožnosti a kontaktních údajů správce a o znalost účelu, pro který jsou osobní údaje subjektu společností shromažďovány a zpracovávány.

2. Právo na přístup k osobním údajům

Práve na přístup k osobním údajům se rozumí veškerá práva subjektu obsažená v čl. 15

nařízení. Zejména se jedná o právo subjektu na získání potvrzení od společnosti, zda a

případně za jakým účelem jsou osobní údaje subjektu zpracovávány.

3. Právo na opravu

Právem na opravu se rozumí veškerá práva subjektu obsažená v čl. 16 nařízení, zejména

pak právo na to, aby společnost opravila bez zbytečného odkladu nepřesné nebo nesprávné osobní údaje, které se subjektu týkají.

4.Právo na výmaz (být zapomenut)

Právem na výmaz se rozumí veškerá práva subjektu obsažená v čl. 17 nařízení, zejména

se jedná o právo subjektu, aby společnost bez zbytečného odkladu na požádání subjektu

vymazala osobní údaje subjektu za předpokladu, že pro to budou naplněny podmínky

dané nařízením.

5.Právo na omezení zpracování

Právem na omezení zpracování se rozumí veškerá práva subjektu obsažená v čl. 18

nařízení.

6.Právo na přenositelnost údajů

Právem na přenositelnost údajů se rozumí veškerá práva subjektu obsažená v čl. 20

nařízení, zejména pak právo subjektu získat své osobní údaje, které poskytl společnosti,

ve strukturovaném, běžně používaném a strojově čitelném formátu.

7.Právo vznést námitku

Právem vznést námitku se rozumí veškerá práva subjektu obsažená v čl. 21 nařízení.

Zjistí-li nebo domnívá-li se subjekt, že společnost zpracovává jeho osobní údaje v rozporu

s ochrannou subjektu soukromého života, v rozporu s nařízením nebo v rozporu se

zákonem může požadovat po společnosti vysvětlení či požadovat, aby byl takovýto stav

odstraněn.

Subjekt má dále právo obrátit se se stížností na Úřad pro ochranu osobních údajů, který plní

úlohu dozorového úřadu ve věcech ochrany osobních údajů.

Právo subjektu na jiné prostředky soudní a správní ochrany tím není dotčeno.

Závěrem stvrzuji, že jsem byl poučen, že poskytnutí osobních údajů je dobrovolné.

V Plzni dne

.....,

zaměstnanec

Znalost GDPR - Zaměstnanci

V následujícím dotazníku je uveno několik málo otázek zabývajících se problematikou GDPR. Prosím o vyplnění toho krátkého dotazníku, který slouží jako podklad k diplomové práci. Vyplnění je anonymní a zabere Vám pár minut.

***Povinné pole**

1. Na jaké pozici pracujete? *

Označte jen jednu elipsu.

- Skladník
- Technik
- Obchodník
- Vedoucí oddělení nebo pobočky

2. Odkud jste se o GDPR dozvěděli poprvé? *

Označte jen jednu elipsu.

- Internet
- Televize
- Rádio
- Přátelé
- Jiné: _____

3. Od kdy je GDPR účinné? *

Označte jen jednu elipsu.

- 24.4.2018
- 24.5.2018
- 24.6.2018

4. Víte, jaké informace o Vás správce smí shromažďovat? **Zaškrtněte všechny platné možnosti.*

- Jméno
- Přímení
- Bydliště
- Rodné číslo
- Číslo občanského průkazu
- Zdravotní stav
- Jméno, příjmení a rodné číslo dětí
- Jméno, příjmení a rodné číslo manželky
- Kopii občanského průkazu
- Žádné
- Nevím

5. Jaká práva Vám GDPR přináší? **Zaškrtněte všechny platné možnosti.*

- Právo na informace
- Právo na přístup
- Právo na opravu a doplnění
- Právo na omezení zpracování
- Právo přenositelnosti
- Právo vznést námitku
- Právo na odpověď
- Právo na přesnost
- Právo na důvěrnost

6. Za jakým účelem dle GDPR smí zaměstnavatel využívat na pracovišti kamery? **Zaškrtněte všechny platné možnosti.*

- Ochrana majetku společnosti
- Šmírování zaměstnanců
- Plnění právní povinnosti správce
- Smí kdykoliv se souhlasem zaměstnanců
- Nemá právo
- Nevím

Znalost GDPR - Správce

V následujícím dotazníku je uvedeno několik málo otázek zabývajících se problematikou GDPR. Prosim o vyplnění toho krátkého dotazníku, který slouží jako podklad k diplomové práci. Vyplnění je anonymní a zabere Vám pár minut.

***Povinné pole**

1. Jak jste se připravovali na zavedení GDPR? *

Zaškrtněte všechny platné možnosti.

- Sledování zpráv
- Konzultace s právníky
- Studium legislativy
- Nepřipravovali jsme se

2. Jak dlouho jste se připravovali na zavedení GDPR? *

Označte jen jednu elipsu.

- 1 měsíc
- 2-4 měsíce
- 5 a více měsíců

3. V čem jste viděli největší problém při zavádění GDPR? *

Označte jen jednu elipsu.

- Nedostatek informací
- Uchování a ochrana dat
- Sdílení osobních údajů s úřady
- Jiné: _____

4. Jaký byl pro Vás největší problém při zavádění GDPR? *

Označte jen jednu elipsu.

- Různé výkaldy GDPR
- Nedostatek informací
- Zveřejňování fotografií
- Kamerové systémy
- Zajištění bezpečnosti zpracování osobních údajů
- Jiné: _____

5. V jaké podobě zpracováváte osobní údaje zaměstnanců? **Označte jen jednu elipsu.*

- Listinné
- Elektornické
- Listinné i elektronické
- Žádné nezpracováváme

6. Jak zabezpečujete osobní údaje zaměstnanců? **Zaškrtněte všechny platné možnosti.*

- Helsem
- Uzamčené
- Přístup mají pouze vybraní zaměstnanci
- Nezabezpečujeme
- Jiné: _____

7. Jak často aktualizujete osobní údaje, které zpracováváte? **Označte jen jednu elipsu.*

- Každé 3 roky
- Každých 5 let
- Neaktualizujeme

8. Jak dlouho zpracováváte osobní údaje? **Označte jen jednu elipsu.*

- 3 roky
- 5 let
- 10 let
- Napořád
- Nearchivujeme
- Dokud nepomine účel

Abstrakt

HARMÁČKOVÁ, Lenka. *Dopady zavedení General Data Protection Regulation na zvolený ekonomický subjekt*. Plzeň. 2019. 74 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 ve vybraném ekonomickém subjektu. Po seznámení se s GDPR a definování důležitých pojmů je provedeno srovnání GDPR se zákonem o ochraně osobních údajů. Následně je popsán proces zavedení GDPR ve společnosti DISCOMP a provedeno dotazníkové šetření. V závěru práce dochází k vyhodnocení dotazníkového šetření na jsou navržena možná opatření na zlepšení stávajícího stavu na základě dat získaných z analýzy a hodnocení procesu zavedení GDPR a z dotazníkového šetření.

Abstract

HARMÁČKOVÁ, Lenka. *Impact of the General Data Protection Regulation implementation on a selected economic entity*. Plzeň. 2019. 74 pages Diploma thesis University of West Bohemia in Pilsen. Faculty of Economics.

Key words: Personal data protection, GDPR, general regulation

This thesis focuses on personal data protection in a selected economic entity. At first, the thesis thoroughly describes GDPR and defines the most significant terms. Subsequently, GDPR is compared with Act on the Protection of Personal Data. In the main part of the thesis, GDPR implementation in the organization DISCOMP is elaborated with further research utilizing questionnaire survey. Eventually, results of the questionnaire survey are evaluated with subsequent proposal of measures leading to improvement of current situation on the basis of data analysis and assessment of the GDPR implementation process and survey.