ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Diplomová práce

Problematika General Data Protection Regulation ve vybraném ekonomickém subjektu

The issue of General Data Protection Regulation in selected economic entity

Bc. Zuzana Stará

Plzeň 2020

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Zuzana STARÁ**
Osobní číslo:	**K19N0044K**
Studijní program:	**N6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika a management**
Téma práce:	**Problematika General Data Protection Regulation ve vybraném ekonomickém subjektu**
Zadávající katedra:	**Katedra financí a účetnictví**

Zásady pro vypracování

1. Definujte problematiku General Data Protection Regulation.
2. Analyzujte úkoly a kritéria General Data Protection Regulation.
3. Charakterizujte vybraný podnik.
4. Ve zvoleném podniku proveďte analýzu současné situace v oblasti General Data Protection Regulation.
5. Vyhodnoťte současnou situaci a navrhněte možná zlepšení.

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

Seznam doporučené literatury:

- JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018. ISBN 978-80-7552-248-1.
- FOULSHAM, Mark a Brian HITCHEN. *GDPR: Guiding Your Business To Compliance: A practical guide to meeting GDPR regulations*. Second edition. England: Independently published, 2018. ISBN -13: 978-1521309698.
- NAVRÁTIL, Jiří. *GDPR pro praxi*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Pro praxi. ISBN 978-80-7380-689-7.
- ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

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

Datum zadání diplomové práce: **22. října 2019**
Termín odevzdání diplomové práce: **22. dubna 2020**

L.S.

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

Ing. Pavlína Hejduková, Ph.D.
vedoucí katedry

V Plzni dne 22. října 2019

Čestné prohlášení

Prohlašuji, že jsem bakalářskou/diplomovou práci na téma

„Problematika General Data Protection Regulation ve vybraném ekonomickém subjektu“

vypracovala samostatně pod odborným dohledem vedoucí diplomové práce za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne..... .....

podpis autora

Na tomto místě bych ráda poděkovala vedoucí mé diplomové práce Prof. Ing. Lilie Dvořákové, CSc. za odborné vedení mé práce, za její čas, cenné poznámky a za ochotu a možnost konzultací i v těchto současných nelehkých podmínkách. Dále bych ráda poděkovala jednateli společnosti XY, že mi umožnil využít interní data potřebná pro zpracování diplomové práce a za poskytnutý rozhovor. V neposlední řadě bych také ráda poděkovala všem respondentům, za jejich přínos pro výzkumnou část této diplomové práce.

OBSAH

ÚVOD

Problematika General Data Protection Regulation (dále jen GDPR) se týká v určitých situacích každého z nás. V současné době, kdy stále větší část našeho života přebírají moderní technologie, počítače, sociální sítě a softwary na zpracování dat, je více než důležité, mít povědomí o tom, co je to osobní údaj a jak takový údaj chránit před zneužitím. Je nezbytné si uvědomit, že osobním údajem není pouze rodné číslo a adresa, že se jedná i o takové údaje, které poskytujeme každý den. Že za osobní údaj může být považována i fotografie, kterou například vložíme na sociální sítě.

Samozřejmě je třeba si osobní údaje hlídat v našem osobním životě. Neměli bychom ale zapomínat ani na náš pracovní život. Osobní údaje totiž poskytujeme například zaměstnavateli při podpisu pracovní smlouvy. Nemůžeme se spoléhat pouze na to, že zaměstnavatel udělá vše pro to, aby naše údaje byly ochráněny. Proto je důležité mít v této problematice alespoň základní znalosti, abychom byli schopni se zaměstnavatele sami zeptat, jak je s našimi osobními údaji pracováno a jak budou chráněny.

Níže zpracovaná diplomová práce zaměřuje na problematiku GDPR v kontextu vybraného ekonomického subjektu. Autorka práce se dlouhodobě pohybuje v prostředí gastronomie a konkrétně gastronomických provozů. I proto právě vybraným subjektem bude společnost vlastnící několik takovýchto provozoven. Zkušenost autorky ukazuje, že zaměstnavatelé v této oblasti problematice GDPR nevěnují dostatečnou pozornost. V mnoha případech si ani neuvědomují, že pracují s osobními údaji, které GDPR podléhají a je nutno k nim i takto přistupovat.

Dle autorky práce tento problém není pouze na straně zaměstnavatele. Často se můžeme setkat s tím, že zaměstnanci v této problematice nemají dostatečné znalosti. Nejsou si vědomi toho, že by jejich osobní údaje měly být chráněny. Zaměstnanci nemají potřebu ptát se zaměstnavatele, jak jejich údaje chrání, jak jsou uloženy, jak se s nimi pracuje a kdo k nim má přístup.

Autorka práce se také domnívá, že v těchto společnostech je často opomíjena dokumentace, která by mapovala, jak je s daty nakládáno. Stejně tak chybí manuál pro zaměstnance, jak s daty pracovat a jak je chránit.

Informace, obsažené v teoretické části práce, pomáhají k definování rizik, která se ve vybraném ekonomickém subjektu v souvislosti s GDPR objevují. Tato rizika jsou v praktické části práce zhodnocena a poté jsou navržena možná zlepšení a způsoby, jak těmto rizikům v budoucnu předejít.

Vzhledem k již zmiňovanému dlouhodobému pracovnímu poměru ve vybraném subjektu je cílem práce formulovat sdělení tak, aby v případě zájmu jednatele společnosti mohla být reálně implementována. Autorka práce by ráda tuto diplomovou práci jednateli společnosti poskytla, aby tyto návrhy a informace mohl využít v praxi.

1. CÍLE A METODIKA PRÁCE

1.1 CÍLE PRÁCE

Cíle této diplomové práce můžeme rozdělit na tři větší celky. Prvním z těchto celků je teoretická analýza provedená na základě dostupných zdrojů k problematice General Data Protection Regulation. Ze zpracování této části práce by měla být patrna teoretická problematika tématu. Mělo by dojít k vysvětlení důležitých oblastí a pojmů, které poté budou využity v následujících částech práce. Dílčím cílem této první části je také definovat úkoly a kritéria problematiky GDPR. Druhým cílem práce je prakticky analyzovat současnou situaci v oblasti GDPR ve vybraném ekonomickém subjektu. Aby k této analýze mohlo dojít, dílčím cílem je teoretické vysvětlení problematiky GDPR v souvislosti s podnikatelskými subjekty, neboť vybraný ekonomický subjekt je podnikatelský. Dále by mělo v této části práce dojít k představení podniku a analýze současné situace v kontextu problematiky GDPR. Posledním, třetím cílem, je zhodnocení současné situace v kontextu vypracované teorie a na základě tohoto zhodnocení navrhnout možná zlepšení, která by mohl podnikatelský subjekt v oblasti GDPR zrealizovat. Je dobré také zmínit, že se jedná o poměrně malou společnost, a proto je nutné při navrhování možných zlepšení brát v úvahu finanční situaci společnosti. Z toho důvodu bude vypracován finanční plán, který názorně ukáže, jak finančně náročné tyto změny mohou být a jak by bylo možné je rozložit tak, aby nepředstavovaly velký zásah do měsíčního rozpočtu společnosti.

1.2 METODIKA PRÁCE

K získání potřebných výsledků, díky kterým bude moci být provedena následná analýza a návrh možných zlepšení současné situace, bude použit výzkum, který proběhne v případě jednatele společnosti formou rozhovoru a v případě zaměstnanců společnosti formou dotazníkového šetření. Dotazníkového šetření se zúčastní anonymně všichni zaměstnanci společnosti. Vhodnou kombinací otázek bude identifikován potřebný výstup, který bude dál využit, pro výše zmiňovaná doporučení. Jelikož autorka práce ve vybrané společnosti dlouhodobě pracuje, rozhovor i dotazníkové šetření zrealizuje sama, tak aby byly minimalizovány náklady. Dalším zdrojem analýzy budou zkušenosti autorky práce, které získala během několikaletého pracovního poměru u vybrané společnosti.

Z výstupu poté vyplyne, kde se nacházejí slabá místa v oblasti problematiky GDPR. Na základě těchto poznatků bude vypracován návrh doporučení, díky kterým by mělo dojít ke zlepšení situace. Součástí návrhu bude i postup možné realizace těchto zlepšení včetně nastínění finanční náročnosti jednotlivých úkonů. Jednatel společnosti bude mít k těmto závěrům přístup, aby je mohl sám zhodnotit a za předpokladu, že je posoudí jako přínosná a realizovatelná, je bude moci implementovat.

2. HISTORIE OCHRANY OSOBNÍCH ÚDAJŮ A PROBLEMATIKA GENERAL DATA PROTECTION REGULATION

Podíváme-li se do dávné historie, dle publikace Sharma (2020) jedním z prvních případů ochrany osobních údajů byl koncept *„A home is one´s castle“*, volně přeloženo do českého *„Můj dům, můj hrad“*, tento koncept stanovil Sir Edward Coke v Anglii v roce 1604. Obsahoval zejména přístup, že pokud se osoba nacházela ve svém domě, tedy v soukromí, nikdo ji do něj nemohl zasahovat. V té době byla tato ochrana dostačující. V současné době, kdy se technologie vyvíjí téměř každý den, v době internetu, sociálních sítí a mobilních telefonů je ochrana osobních údajů výrazně komplikovanější.

Klosek (2020) zmiňuje, že obavy o dostatečnou ochranu osobních údajů nejsou ve světě ničím novým. Strach ze zneužití nebo krádeže dat existuje stejně dlouho, jako dochází k přenosu a distribuci osobních dat.

Sharma (2020) se domnívá, že kořeny ochrany osobních údajů můžeme najít v základních lidských právech. Jedná se zejména o právo na soukromý život, které říká, že žádná osoba by neměla být subjektem svévolného rušení jeho soukromí, rodiny, domu nebo korespondence a také by neměla čelit útokům na svou čest nebo reputaci. Dále se jedná o právo na svobodu slova a vyjadřování. Toto právo říká, že osoba by měla mít možnost vyjádřit své názory bez vyrušování a měla by mít možnost vyhledat, udělit a získat informace a nápady skrze všechna media navzdory hranicím.

Brandeis a Warren ve svém článku, který vyšel v roce 1980 *„The Rigth to Privacy“ již* tehdy upozorňují na hrozbu, kterou představují invence a metody využívány v obchodu a zdůrazňují, že je nutné se na ochranu osobních údajů zaměřit. Autoři článku tehdy varovali zejména před používáním fotografií a mechanismů, které data zpracovávají. Nicméně hlavní myšlenka článku, tedy potřeba chránit osobní data, stále přetrvává.

2.1 HISTORIE VZNIKU GENERAL DATA PROTECTION REGULATION

General Data Protection Regulation historicky vychází z původní směrnice o ochraně osobních údajů, kterou vydala Evropská Unie. Tato směrnice existuje již dvacet let. Jak dále uvádí Nezmar (2017) ve své publikaci, směrnice o ochraně osobních údajů

stanovuje minimální standard zákona o ochraně údajů v členských státech Evropské unie. Česká republika zákon, který se týká ochrany osobních údajů, přijala v roce 2000.

Nezmar (2017) mapuje vývoj ochrany osobních údajů. Ten začíná již v roce 1981, kdy dochází k podpisu smlouvy o ochraně osob s ohledem na automatické zpracování osobních údajů. Tato smlouva byla podepsána jako Úmluva Rady Evropy č. 108. Dalším důležitým datem je 4. říjen 1995. V tento den byla podepsána již výše zmiňována Evropská směrnice o ochraně osobních údajů. Tato směrnice byla vytvořena jako základní prvek ochrany soukromí v rámci Evropské Unie.

Foulsham & Hitcham (2018) uvádějí, že i přesto, že výše zmíněná Evropská směrnice obsahovala 8 principů ochrany osobních údajů, které obsahovaly mnoho nových způsobů ochrany, společnosti i tak objevily slabiny dokumentu, které poté využívaly ve svůj prospěch. Jednou z těchto slabých stránek byla například skutečnost, že společnosti mohly pro subjekt dopředu zaškrtnou pole, ve kterém se zpracováním osobních údajů souhlasí. Pokud by subjekt nesouhlasil, musel toto zaškrtnutí zrušit.

Jelikož dochází během následujících let nejen k vývoji technologií, ale jsou také analyzovány výše zmíněné slabé stránky, v roce 2012 Evropská komise navrhuje komplexní reformu pravidel Evropské unie ochrany osobních údajů z roku 1995. Tento návrh je založen právě na důležitosti následování technologického pokroku a globalizace. Byl výrazně změněn způsob, jakým jsou osobní data shromažďována, zpřístupňována a využívána. Nedlouho po tomto návrhu zveřejňuje Evropský parlament studii nazvanou *„Reforming the Data Protection Package“*. Tato studie upozorňuje právě na nutnost zlepšení ochrany subjektů a závažné nedostatky, které se týkají právě nových technologií a služeb. V roce 2014 dává Evropský parlament silnou podporu GDPR. Na základě tohoto hlasování dochází k významnému pokroku v reformě ochrany osobních údajů. (Nezmar, 2017)

Nejprve dosahuje obecné shody ohledně GDPR Rada Evropské Unie, a to v roce 2015, díky tomu může zahájit jednání s Evropským parlamentem, za cílem dosažení celkové dohody o problematice. Dne 27. dubna 2016 je v Úředním věstníku Evropské Unie uveřejněno Nařízení Evropského parlamentu a Rady 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. Zrušená směrnice je výše zmiňovaná směrnice o ochraně osobních údajů. Tímto momentem vstupuje GDPR v platnost.

Účinnost nařízení GDPR nastává 25. května 2018. (Základní příručka k ochraně osobních údajů, 2020)

Autoři Voigt a Bussche (2017) uvádějí, že GDPR bylo přijato jako nutné opatření vzhledem k velkému nárůstu digitálně zpracovávaných dat, kdy schopnost jejich efektivní a rychlé analýzy může ovlivňovat zásadní rozhodování a chování strategických podniků a společností. Zároveň také mělo dojít k podpoře digitální ekonomie napříč Evropou a získání důvěry lidí v souvislosti s tím, jak je s jejich osobními údaji pracováno a jak jsou chráněny. Můžeme tvrdit, že osobní údaje se staly velmi cennou komoditou a jejich krádež vystavuje poškozeného velkému riziku.

Lze říci, že řada společností, firem a organizací tuto problematiku opomenula a nevěnovala jí pozornost. GDPR stanovuje firmám a organizacím mnohem větší zodpovědnost za zabezpečení osobních dat a kontrolu procesů. Platí zvýšené sankce za porušení tohoto nařízení. To dává mnohem větší práva subjektům, tedy lidem – občanům a stanovuje mnohem přísnější požadavky jak správcům, tak zpracovatelům informací. Nařízení je dále výjimečné v tom, že platí nejen pro všechny země Evropské unie, ale také pro kohokoliv, kdo by chtěl zpracovávat data jejích občanů. Klíčovým aspektem je i to, v jaké zemi se data fyzicky nacházejí, tedy kde se nachází umístění serverů. (Nezmar, 2017)

Dle publikace, kterou vydal ITGP Privacy Team (2019) ve Velké Británii, byl jedním z důvodů vzniku obecného nařízení o ochraně osobních údajů fakt, že řada zemí svými zákony a zákonnými opatřeními šla více do hloubky v oblasti ochrany osobních údajů. Pro občany Evropské unie se tak stalo velice obtížným vyznat se v tom, jak jsou jejich osobní údaje chráněny napříč Evropskou Unií. Stejně tak bylo obtížné pro organizace rozhodnout, kterým souborem práv a povinností se řídit. Proto Evropská Unie rozhodla, že jeden zákon bude více efektivní v dosažení dvou stanovených cílů. Tyto cíle jsou chránit práva, soukromí a svobodu fyzických osob v Evropské unii, zmírnit bariéry podnikání a usnadnit volný pohyb údajů po celé Evropské Unii.

Článek publikovaný autory Burri & Shär (2016) upozorňuje na skutečnost, že přijetí nařízení není pouze komplexní řešení ochrany osobních dat, ale že se jedná i o politickou hru, která se za přijetím tohoto nařízení ukrývá. Z článku je patrné, že na přijetí nařízení se podílely ekonomické subjekty stejně tak jako instituce Evropské Unie. Například Evropská komise kladla mnohem větší důraz na ekonomické a bezpečnostní

důvody, zatímco Evropský Parlament se stavil zejména za ochranu individuálních práv. Dle autora článku je právě jiný pohled různých důvodem, proč je GDPR v mnohých ohledech kompromisem mezi ekonomickou sférou a subjekty osobních údajů.

2.2 Tři pilíře GDPR

Gawronski (2019) ve své publikaci uvádí, že cíle GDPR stojí na třech pilířích, mezi které patří:

- zákonnost – pravidlo, že organizace jsou povinny zákonnost neustále dodržovat a pracovat v souladu s ní,
- práva – práva subjektů, kterých se týká zpracování osobních údajů a zároveň také z pohledu organizace specifické procesy, které mají být provedeny
- ochrana – proces neustálého zajištění ochrany, jedná se o podmínky, které musí organizace následovat, aby byla zajištěna důvěrnost, integrita a také ochrana proti nebezpečí, které se může vyskytnout.

2.3 Působnost GDPR

2.3.1 Místní působnost

V samotném nařízení se můžeme dočíst, že se vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny zpracovatele nebo správce v Evropské Unii, a to bez ohledu na to, zda toto zpracování probíhá na území Unie nebo mimo. Zároveň se také vztahuje na jakéhokoliv správce nebo zpracovatele, který nemá sídlo na území Evropské unie, ale spravuje data subjektů, kteří v Evropské Unii sídlo nebo trvalé bydliště mají.

2.3.2 Osobní působnost

Osobní působnost zejména určuje, na které subjekty se nařízení vztahuje. Jedná se zejména o správce, zpracovatele, dozorové úřady a subjekty údajů. Pro všechny subjekty, kterých se nařízení týká, jsou stanovena práva a vymezeny povinnosti, resp. úkoly a pravomoci. (Žůrek, 2017)

2.3.3 Věcná působnost

Věcná působnost vymezuje zejména to, na co se obecné nařízení vztahuje, ale také to, čeho se netýká. Můžeme tedy říci, že obecné nařízení upravuje zpracování osobních údajů, a to jak neautomatizované, tak automatizované. (Žůrek, 2017)

Dle samotného nařízení dále také můžeme říci, že obecné nařízení se nevztahuje na zpracování údajů pro osobní potřebu. Jedná se o případy, kdy údaje zpracovává fyzická osoba v průběhu výlučně osobních či domácích činností. Na zpracování prováděné příslušnými orgány týkající se trestných činů a dále se nevztahuje na osobní údaje zesnulých osob.

2.3.4 Časová působnost

Časová působnost je velice důležitý faktor. Uvádí totiž, v jaké době je právní předpis součástí právního řádu. Existuje určitý rozdíl mezi platností a účinností. Jak je již zmiňováno v práci výše, obecné nařízení je platné od 24. 5. 2016 a účinné od 25. 5. 2018. Dvouletá lhůta, která byla stanovena mezi platností a účinností, sloužila zejména k uvedení zpracování osobních údajů do souladu s Obecným nařízením. (Žůrek, 2017)

2.4GDPR v porovnání se Zákonem o ochraně osobních údajů

Nová právní úprava v podobě Nařízení o ochraně osobních údajů základní parametry zásadně nemění, rozšiřuje ale požadavky. Rozdílem oproti zákonu o ochraně osobních údajů je, že zákon zvažuje souhlas jako prvotní základ pro zpracování osobních údajů a až posléze stanovuje výjimky, kdy mohly být údaje zpracovány bez souhlasu. Nařízení výlučné postavení souhlasu nezná. Staví jej na stejnou úroveň jako jiné důvody pro zpracování osobních údajů. Naopak doporučuje, aby byl souhlas zvolen až jako jedna z posledních možností, pokud neexistuje zákonný důvod. Nařízení neklade požadavek písemnosti souhlasu se zpracováním osobních údajů. Jednoznačně je však uvedeno, že takový souhlas musí být konkrétní, zároveň také nařízení uvádí, že mlčení neznamená souhlas, když uvádí, že předem zaškrtnutá pole daného dokumentu nebo nečinnost by za souhlas považovány být neměli. (Janečková, 2018)

V případě informační povinnosti uvádí Nařízení o ochraně osobních údajů (2018) v článku 12 základní povinnost správce, který má přijmout vhodná opatření, aby poskytl subjektu stručným, srozumitelným, transparentním a snadno přístupným způsobem za použití jednoduchých a jasných jazykových prostředků veškeré informace. Informace by měli být poskytnuty písemně nebo jinými prostředky. Ve vhodných situacích může být použita i elektronická forma. Janečková (2018) k této skutečnosti doplňuje, že původní úprava, tedy zákon o ochraně osobních údajů nestanoví, jak má poskytnutá informace vypadat.

V tabulce 1 jsou přehledně zobrazeny práva a povinnosti tak, jak je buď upravují, nebo neupravují oba dokumenty. Tabulka je zpracována na základě získaných informací při studiu Zákona o ochraně osobních údajů a Nařízení o ochraně osobních údajů a literatury, která se touto problematikou zabývá.

Tabulka 1: Porovnání původního zákona o ochraně osobních údajů se současnou úpravou GDPR

Upravovaná problematika	**Zákon o ochraně osobních údajů (1995)**	**GDPR**
Právo na přístup	✓	✓
Právo na nápravu	✓	✓
Právo na výmaz	✓	✓
Právo zastavit přímý marketing	✓	✓
Právo být informován	×	✓
Právo na omezení zpracování dat	×	✓
Právo na přenositelnost dat	×	✓
Právo na námitku	×	✓
Povinnost oznámení o porušení	×	✓
Povinnost jmenovat úředníka pro ochranu údajů	×	✓
Právo na udělení pokuty od 0,5% až do 4% z celkového ročního obratu	×	✓

Zdroj: Vlastní zpracování, 2020

2.5 SHRNUTÍ KAPITOLY

V této kapitole práce došlo zejména k teoretickému vysvětlení problematiky GDPR. Nejprve byl vysvětlen historický kontext problematiky a důvody, které vedly k tomu, že bylo nutné provést v roce 2016 aktualizaci tehdy platných zákonů a nařízení, které tuto problematiku upravovaly. Dále jsou v této kapitole popsány základy, tedy tři pilíře, na kterých je postaven cíl GDPR a také působnost tohoto nařízení. V poslední části kapitoly dochází k porovnání současné úpravy s původním zněním, aby bylo patrné, kde se nacházejí změny a k čemu vedlo přijetí nařízení o ochraně osobních údajů.

3. ÚKOLY A KRITÉRIA GDPR

3.1 HLAVNÍ ÚKOLY GDPR

Krysztofek (2019) ve své publikaci uvádí dva klíčové úkoly GDPR:

- ochrana základních práv a svobod fyzických osob, zejména pak ochrana jejich osobních dat,
- volný pohyb osobních dat fyzických osob v rámci Evropské Unie, pokud tento pohyb není zakázán nebo omezen z důvodů, které souvisejí s ochranou fyzických osob v souvislosti se zpracováním osobních údajů, v souvislosti s pohybem osobních dat musí být také zajištěno dodržování práv občanů členských států na ochranu jejich osobních údajů.

Dalším úkolem GDPR je také přizpůsobení se moderní době, ve které jsou mnohem více využívány moderní technologie v oblasti poskytování informací. Dále také přizpůsobení se všudypřítomnému online zpracovávání dat a stále se zvyšující popularitě sociálních sítí a internetovému nakupování.

3.2 NA KOHO SE GDPR VZTAHUJE?

Nebývá výjimkou, že s novým zákonem, či opatřením přichází řada otázek. Jednou z takovýchto otázek, která byla poměrně častá v souvislosti se zavedením GDPR byla otázka, na koho se vlastně tento zákon vztahuje. Obecně lze říci, že se GDPR vztahuje na kohokoliv, kdo sbírá, uchovává nebo zpracovává osobní údaje patřící osobě s místem pobytu v některé ze zemí Evropské Unie. Naopak GDPR se nevztahuje na případy, kdy se jedná o jedince, který má data jiné osoby s jeho svolením uchované například v počítači. Zároveň je třeba zmínit, že GDPR se nevztahuje pouze na organizace, které se nacházejí na území některého státu Evropské Unie. Vztahuje se na každou organizaci, která zpracovává data občanů zemí Evropské Unie. (Denley & kol., 2019)

3.3 SOUHLAS SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

Souhlas se zpracováním osobních údajů v souvislosti s GDPR musí být dán svobodně. Osoba, která tento souhlas poskytuje, musí být informována o všech skutečnostech, které by mohly udělení tohoto souhlasu ovlivnit. Souhlas se zpracováním osobních údajů musí být udělen v právně uznatelné formě. Za souhlas není možné považovat mlčení nebo předvyplněné boxy se souhlasem. Dále je nutné, aby byl tento

souhlas ověřitelný stejně tak jako skutečnost, že osoba, která souhlas poskytla, tak neučinila pod nátlakem. Souhlas se zpracováním osobních údajů může osoba, které se osobní údaje týkají, kdykoli zrušit. (Denley & kol., 2019)

3.4 Práva subjektů údajů

Srovnáme-li Obecné nařízení a původní zákon o ochraně osobních údajů můžeme říci, že obecné nařízení posiluje systém práv subjektů údajů a jejich aktualizací. Dále se také zabývá podrobnějším zpracováním i zavedením zcela nových práv. Jedním takovým je například právo o přenositelnosti. Účelem práv subjektu údajů je zejména vyvažovat vztah mezi subjektem údajů a správcem údajů. (Základní příručka k ochraně osobních údajů, 2020)

Žůrek (2017) k tomuto tématu dodává, že výkon práv subjektů nesmí být podceněn zejména správcem, pokud by došlo k porušení těchto práv, správce se bude potýkat s vyššími pokutami, než jaké by byly uděleny například za porušená méně závažných povinností.

Článek 12 Obecného nařízení stanovuje, že správce musí provádět výkon práv nebo o něm informovat stručným, srozumitelným, snadno přístupným a transparentním způsobem. Dále také musí používat jednoduché a jasné jazykové prostředky. Tento článek dále také upravuje lhůty. Správce je povinen poskytnout na žádost subjektu údajů informace o přijatých opatřeních, a to maximálně do jednoho měsíce od obdržené této žádosti. Tuto lhůtu je možné prodloužit, pouze pokud se jedná o odůvodněný odklad a nejvýše na dobu dvou měsíců. Subjekt údajů musí být o tomto prodloužení informován.

3.4.1 Právo na informace

Právo na informace má každý subjekt, jehož osobní údaje jsou zpracovávány. Správce je povinen subjekt údajů automaticky informovat i tehdy, aniž by si subjekt o tyto informace požádal. Informování subjektů musí být srozumitelné a jednoduché. Pokud správce získal údaje z jiného zdroje, musí o tom subjekt údajů informovat neodkladně. Nejpozději však ve lhůtě jednoho měsíce nebo při první komunikaci se subjektem údajů. (Janotová, 2018)

3.4.2 Právo na přístup k osobním údajům

Pokud jsou informace subjektu zpracovávány, subjekt má právo, na základě žádosti, být informován o tom, jak toto zpracovávání probíhá. Pokud tyto údaje zpracovávány jsou, subjekt má právo mít k těmto osobním údajům přístup a zároveň získat informace o účelu zpracování, kategoriích údajů, době uložení, právu na opravu nebo výnos, má také právo podat stížnost. (Obecné nařízení, článek 15)

3.4.3 Právo na opravu a doplnění

Žůrek (2017) uvádí, že toto právo vychází ze zásady přesnosti. Správce nemá povinnost aktivně vyhledávat nepřesné nebo neplatné údaje. Bez zbytečného odkladu je ale povinen údaje opravit nebo doplnit, pokud je na to upozorněn subjektem údajů. V případě podezření na nesprávnost údajů má správce možnost subjekt požádat o kontrolu aktuálnosti těchto údajů.

3.4.4 Právo vznést námitku

Dle článku 20 obecného nařízení má subjekt údajů oprávnění protestovat proti zpracování svých osobních údajů, pokud se jedná o zpracování osobních údajů, které nesouvisí s výkonem veřejné moci, není nevyhnutelné z důvodů oprávněných zájmů jiných osob nebo nesouvisí s veřejným zájmem.

3.4.5 Právo nebýt předmětem automatizovaného individuálního rozhodování

O právních účincích se, kromě některých stanovených výjimek, nesmí rozhodovat jen pomocí automatizovaných postupů. Tedy postupů zcela bez lidského posouzení. I subjekt údajů má tedy právo, aby o něm nebylo rozhodováno pouze automatizovaným způsobem, jedná se zejména o případy, kdy toto rozhodování má pro subjekt právní účinky nebo se jej týká jiným podstatným způsobem. (Základní příručka k ochraně osobních údajů, 2020)

3.4.6 Právo na přenositelnost údajů

Žůrek (2017) právo na nepřenositelnost údajů představuje jako zcela nové právo subjektů údajů. Oproti právu na přístup k údajům je rozdíl zejména ve stanovení formátu, ve kterém osobní údaje musí být poskytnuty a také v možnosti předání údajů jinému správci. Článek 20 obecného nařízení, který toto právo upravuje, udává, že subjekt údajů může u správce vyžadovat poskytnutí svých údajů, které jsou zpracovávány a také jejich předání dalšímu správci, kterého si subjekt určí.

3.4.7 PRÁVO NA VÝMAZ

Právo na výmaz neboli právo být zapomenut udává, že správce má povinnost vymazat osobní údaje subjektu, který na tento výmaz má právo, podle podmínek uvedených v článku 17 Obecného nařízení.

3.5 ZÁKLADNÍ KRITÉRIA GDPR

Nařízení neobsahuje pouze změny zmíněné v druhé kapitole, které jsou nejvíce viditelné, obsahuje také velké množství drobných změn, které dopomohly k tomu, že se kolem dokumentu začala šířit celá řada mýtů. Často se můžeme setkat i s názorem, že se jedná o naprosto novou právní úpravu, o zcela nový dokument v oblasti ochrany osobních údajů. Skutečnost je ale opačná. Nejedná se o nový dokument, celá řada povinností je shodná s dosavadními zákony a předpisy. Většina povinností, které nařízení ukládá, vyplývá z kritérií – zásad zpracování osobních údajů. Tyto zásady si přiblížíme.

Dle Gobea a kol. (2018) jsou tato kritéria v podstatě etickými úmysly, o které se celá legislativa opírá a na kterých je založena. V obrázku 1 jsou tato kritéria, která jsou dále podrobněji vysvětlena, grafiky znázorněna.

Obrázek 1: Základní zásady GDPR

Zdroj: Six privacy principles,2020

3.5.1 ZÁSADA ZÁKONNOSTI, KOREKTNOSTI A TRANSPARENTNOSTI

Zpracovávání osobních údajů je možné pouze na základě zákonných titulů, které musí být dostatečně specifické, transparentní a korektní. Jedná se tedy o to, že ke každému zpracování osobních údajů musí být vždy minimálně jeden z důvodů, které nařízení udává. V případě, že zákonný důvod nebyl nalezen anebo pomine, je nutné a nezbytné osobní údaj zlikvidovat. Pokud od začátku neexistoval důvod pro zpracování osobních údajů, jedná se o nelegální zpracování. Zásada zákonnosti, tedy přítomnost právního důvodu, je základním předpokladem k tomu, aby bylo možné o zpracování osobních údajů hovořit jako o zákonném. Součástí transparentnosti je také to, že správce nebude zastírat pravý účel, pro který byly osobní údaje shromážděny a jsou zpracovávány, ale také, že nebude zastírat svou pravou identitu, způsob zpracování a také, že bude plnit svou informační povinnost. (Janečková, 2018)

Dle Žůrka (2019) zásada transparentnosti vyžaduje, aby informace, které subjekt údajů od správce dostává, či na něž má právo, byly snadno přístupné a srozumitelné za použití jasných jazykových prostředků.

3.5.1.1 ZÁKONNÉ DŮVODY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Účelem zpracování osobních údajů bývá většinou konkrétní agenda. Může se jednat například o evidenci řidičů, vydávání služebních průkazů nebo třeba o agendu střetu zájmů. Správce může tento účel zpracování stanovit přímo nebo účel může představovat činnost správce, pro kterou osobní údaje potřebuje zpracovávat. Velmi často se jedná o zákonem stanovený důvod ke zpracování osobních údajů. (Janečková, 2018)

Pro zpracování osobních údajů je vždy nutné najít některý ze zákonných důvodů. Dle Janečkové (2018) článek 6 nařízení uvádí tyto zákonné důvody pro zpracování osobních údajů:

- subjekt, kterého se údaje týkají, udělil souhlas se zpracováním těchto údajů pro jeden nebo více účelů,
- zpracování údajů je nezbytné pro plnění smlouvy, ve které je subjekt údajů smluvní stranou, nebo pro provedení opatření před uzavřením smlouvy,
- na správce se vztahuje právní povinnost, kvůli které je zpracování údajů nezbytné,
- zpracováním údajů jsou chráněny životně důležité zájmy subjektu údajů nebo jiné fyzické osoby,

- zpracování osobních údajů je nezbytné pro splnění úkolu, který je prováděný ve veřejném zájmu nebo pří výkonu veřejné moci, kterým je správce údajů pověřen,
- zpracování je nutné pro účely oprávněných zájmů příslušného správce nebo třetí strany, výjimku tvoří případy, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektů údajů vyžadující ochranu osobních údajů, jedná se zejména o případy, kdy je subjektem údajů dítě.

Není možné, aby byly osobní údaje zpracovávány, pokud se jejich zpracování neopírá o některý z výše zmíněných důvodů.

3.5.2 Zásada účelového omezení

Zásada účelového omezení nám říká, že osobní údaje je možné zpracovávat pouze pro určité, výslovně vyjádřené a legitimní účely. Je nepřípustné, aby správce údaje shromáždil k určitému účelu a následně je on nebo zpracovatel použil k jiným účelům, za předpokladu, že subjekt informace by o tomto novém účelu nebyl informován. V tomto případě je výrazně zohledněno pravidlo, že subjekt údajů by měl být ten, kdo má plnou informaci o zpracovávání svých osobních údajů a v mezích by měl mít také možnost rozhodovat, jak s jeho údaji bude naloženo. (Janečková, 2018)

Denley a kol. (2019) k této zásadě doplňují, že osobní údaje by neměly být použity pro další procesy, než pro které byly primárně získány, zároveň ale jako výjimku uvádějí případy, kdy jsou údaje použity pro archivační účely ve veřejném zájmu, vědecké či historické výzkumy nebo statistické údaje. To tedy znamená, že pro tyto účely lze osobní údaje zpracovávat i nad rámec původně stanoveného účelu.

3.5.3 Zásada minimalizace údajů

Dle této zásady zpracování údajů musí být relevantní, přiměřené a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou údaje zpracovávány. Splnění této povinnosti vyžaduje přesné vymezení minimálního rozsahu konkrétních osobních údajů, které budou v daném případě skutečně potřebné. (Základní příručka k ochraně osobních údajů, 2020)

Je tedy třeba o každém osobním údaji rozhodnout, zda je či není pro daný účel potřebný. Cílem této zásady je dosažení stavu, kdy účelu zpracování bude dosaženo

s použitím co nejužší skupiny osobních údajů. Údaje, o kterých správce rozhodne, že nespadají do potřebného minima, by měli být okamžitě zlikvidovány. (Janečková, 2018)

3.5.4 Zásada přesnosti

Správce údajů je povinen aktualizovat údaje, které zpracovává. V praxi se ukázalo, že mít údaje neustále aktualizované a kompletně aktuální je téměř nemožné. Proto bylo stanoveno, že by správce měl přijmout veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné, byly bezodkladně vymazány nebo opraveny. Přesnost a aktuálnost by měla být zjišťována v celém průběhu zpracovávání osobních údajů. Z výše uvedeného je tedy patrné, že kdo zpracovává osobní údaje, musí v závislosti na rozsahu a okolnostech předmětného zpracování přijmout takový systém opatření, díky kterému zajistí, že nebudou zpracovávány nepřesné nebo chybné osobní údaje. Dobré je také zdůraznit, že zpracování nepřesných osobních údajů není jen zpracování údajů například s gramatickou chybou, ale také údajů, které jsou sice formálně správně, ale uvádějí nesprávnou informaci. (Janečková, 2018)

3.5.5 Zásada omezení uložení

Osobní údaje by měly být uloženy v takové formě, která umožňuje identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou tyto údaje zpracovávány. I tato zásada byla promítnuta v dosavadní právní úpravě, tedy v Zákoně o ochraně osobních údajů. Správce je ve většině případů povinen uschovací dobu určit sám a za dobu, kterou určí, nese odpovědnost. Pokud správce zpracovává osobní údaje na základě zvláštního zákona a tento zákon neupravuje dobu uchování údajů, je správce osobních údajů oprávněn uchovávat tyto údaje pouze po dobu, po kterou trvá daná povinnost nebo právní vztah. (Janečková, 2018)

3.5.6 Zásada integrity a důvěrnosti

Osobní údaje mají být zabezpečeny před hrozbami nejen uvnitř organizace, ale také vně. A to ve všech podobách zpracování, ať už se jedná o zpracování automatizované nebo papírové. (Janečková, 2018)

Žůrek (2019) také uvádí, že zabezpečení osobních údajů musí vždy odpovídat povaze, rozsahu, kontextu a účelům zpracování. Údaje by měli být zabezpečeny pomocí vhodných technických nebo organizačních opatření, které by je měli chránit nejen před neoprávněným, či protiprávním zpracováním, ale také například před náhodnou ztrátou, zničením nebo poškozením.

3.5.7 Zásada odpovědnosti

Veškerou odpovědnost za dodržování všech pravidel stanovených GDPR nese správce, který také musí být schopen doložit fakta, která potvrzují, že tato pravidla dodržuje. Zásada odpovědnosti je jedním z nových prvků v oblasti zpracování osobních údajů. (Gawronski, 2019)

Článek 24 obecného nařízení říká, že s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, zavede správce technická a organizační opatření. Tato opatření slouží k tomu, aby správce zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Taková opatření musí být podle potřeby aktualizována a revidována. Díky této zásadě má tedy správce mnohem větší odpovědnost. (Janečková, 2018)

3.6 Shrnutí kapitoly

Tuto kapitolu lze rozdělit na dvě části. První část obsahuje popis hlavních úkolů GDPR a také toho, na koho se GDPR vztahuje a kdo se jím musí řídit a jakým způsobem je dáván souhlas ke zpracování osobních údajů. V další části kapitoly jsou popsána kritéria GDPR. Nejprve se jedná o práva subjektů, která jsou velice důležitá a správcem osobních údajů nesmí být podceněna. Jedná se o práva, která má subjekt údajů garantována proto, aby nemohlo dojít zejména ke zneužití jeho osobních údajů. Ve zkratce lze tedy říci, že jde o ochranu subjektu údajů. Dále jsou v této kapitole práce popsány zásady, kterými se GDPR řídí. Tyto zásady přehledně a jednoznačně definují povinnosti, které nařízení ukládá.

4. POŽADAVKY NA OSOBNÍ ÚDAJE V OBLASTI GDPR

Definice osobního údaje je podle Žůrka (2018) stěžejní pro aplikaci nařízení o Ochraně osobních údajů. Osobním údajem je podle definice obsažené v článku 4 obecného nařízení veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

Identifikovatelnou osobou je fyzická osoba, kterou lze přímo nebo nepřímo identifikovat. Identifikace probíhá zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje nebo na jeden či více prvků fyzické, fyziologické, genetické, psychické, ekonomické, společenské nebo kulturní identity této osoby. Nová definice osobního údaje se příliš neodlišuje od definice, které byla v původním zrušeném nařízení 95/46/ES, pouze rozšiřuje výčet identifikátorů, podle kterých může být fyzická osoba identifikována nebo identifikovatelná. Z přidaných identifikátorů stojí za zmínku například přidání síťového identifikátoru, tedy IP adresy. (Žůrek, 2018)

Clader (2018) ve své publikaci uvádí, že mezi data, která je nutno považovat za osobní údaj patří jakákoli informace, která může být použita k identifikování subjektu údajů. Zdůrazňuje, že mezi tyto patří například i fotografie a korespondence subjektu.

Dle Janečkové (2018) není důležité, zda je údaj zcela pravdivý nebo objektivně měřitelný, stejně tak jako jestli je údaj pouhým odhadem charakteristiky člověka. Zároveň také nehraje roli, jak jsou údaje uchovávány. Tedy jestli jsou uchovávány v písemné formě nebo ve formě audio či video záznamu. Rozhodující je vztah informace k identifikovatelné či identifikované osobě.

Fyzická osoba, které se osobní údaje týkají, je nazývána jako subjekt údajů. Často se lze setkat s milným názorem, že mezi identifikátory patří jen obecně známé identifikační údaje, jako je jméno, příjmení, rodné číslo nebo datum narození. Je tedy dobré zmínit, že za osobní údaje se považují jak údaje identifikační, které ve své podstatě zajišťují, že jde o osobní údaje, protože vytváří vazbu mezi fyzickou osobou a údaji, tak také další údaje, které jsou o identifikované či identifikovatelné osobě shromažďovány a zpracovány. Je tedy nutné za osobní údaj považovat například i údaj o platu nebo odměnách konkrétního zaměstnance. Tento zaměstnanec nemusí být označen jen jménem a příjmením, ale třeba také jedinečným označením pozice, kterou zastává. Samozřejmě můžeme v praxi narazit na příklady, kdy je možné polemizovat nad tím, zda jsou údaje

osobní či nikoliv. Pokud tyto pochybnosti máme, je lepší považovat takové údaje za osobní. (Janečková, 2018)

Údaje o právnických osobách nejsou podle Žurka (2018) osobními údaji. Mluvíme-li ale o údajích členů statutárních orgánů či společníků, již se v případě fyzických osob o osobní údaje jedná.

Dle Janečkové (2018) v minulosti vznikaly problémy v souvislosti s fyzickými osobami podnikajícími. Pohled byl takový, že subjektem údajů může být i fyzická osoba podnikající a jako taková může být zasažena ve svém soukromí, avšak pouze v závislosti na skupině osobních údajů, které jsou zpracovávány. Pokud byly zpracovávány pouze osobní údaje, které se týkaly osoby jako podnikatelského subjektu a údaje, které se týkaly pouze podnikatelské aktivity této osoby, nemohlo dojít k neoprávněnému zásahu do soukromí. Podnikatelská činnost totiž nemůže zasáhnout do soukromí tak, jak jej chápe občanské právo. Těmto údajům proto nebyla ochrana podle zákona přiznána. Časem se ale ukázalo, že většina údajů, které se týkají fyzických osob podnikajících, se překrývá s osobními údaji, které se vztahují k soukromí těchto osob. V současné době jsou proto i tyto údaje považovány za údaje, které používají ochrany Nařízení.

4.1 Anonymní údaje

Anonymní údaje se zcela odlišují od osobních údajů. Anonymní údaje nelze vztáhnout k identifikované či identifikovatelné osobě. Anonymní údaj je tedy takový údaj, u kterého neexistuje pouto se subjektem údajů nebo dříve existující pouto nemůže již být správcem ani nikým jiným obnoveno. V důsledku výše zmíněného, zpracování anonymních informací nespouští použití GDPR. (Drożdż, 2020)

Původní obecné nařízení definice anonymního údaje neobsahuje, pouze je vylučuje z působnosti. Zákon o ochraně osobních údajů (č. 101/2000 Sb.), který byl k 24. dubnu 2019 zrušen, anonymní údaj definuje v §4 písmena c) jako údaje, které buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určitelnému nebo určenému subjektu údajů.

4.2 Rodné číslo jako osobní údaj

Rodné číslo si mezi osobními údaji zaslouží zvláštní pozornost. Laickou veřejností je rodné číslo často považováno za citlivý údaj, který ale nepatří mezi osobní údaje, jelikož se nenachází v taxativním výčtu těchto údajů. I přesto, že není rodné číslo

v žádné zvláštní kategorii osobních údajů, má zvláštní postavení. Toto postavení spočívá v určení zákonných podmínek, za kterých je lze využívat.

Podmínky pro využívání rodných čísel jsou stanoveny v zákoně č. 133/2000 Sb, o evidenci obyvatel a rodných číslech a o změně některých zákonů. Tento zákon stanovuje, že rodné číslo je oprávněna užívat, či rozhodovat o jeho využívání v mezích zákona pouze jen osoba, které bylo rodné číslo přiděleno. Tedy pouze jeho nositel. Výjimkou je zákonný zástupce. Jinak lze rodné číslo využívat jen v případech stanovených §13c tohoto zákona. Mezi tyto případy patří i ty, kdy se jedná o činnost ministerstev, jiných správních úřadů, soudů, orgánu pověřených výkonem státní správy nebo pro notáře k vedení Centrální evidence závětí, dále pokud tak stanovuje zvláštní zákon nebo pokud nositel nebo zákonný zástupce s využitím souhlasí.

Pokud správce zpracovává rodné číslo, jeho zpracování pro něj bude stanovovat zvláštní právní předpis, který na činnost správce dopadá. Tento předpis stanoví, zda správce může rodné číslo použít jako součást smlouvy uzavírané s fyzickou osobou. Typickým subjektem, který musí rodné číslo zpracovávat je zaměstnavatel. (Žůrek, 2018)

Dále platí, že rodné číslo bylo vytvořeno jako identifikátor ke specifickým účelům. A to zejména pro státní instituce. Proto není vhodným identifikátorem fyzických osob v zákaznických systémech, jako například číslo zákazníka, a to ani v případě, je-li správce rodné číslo oprávněn zpracovávat. Doporučuje se jej nahradit vlastním identifikátorem. (Žůrek, 2018)

4.3 OBČANSKÝ PRŮKAZ

Existuje mnoho situací, kdy je osoba požádána o poskytnutí kopie občanského průkazu, proto je dobré si tuto problematiku alespoň okrajově přiblížit. Společně s kopií je vhodné také zmínit číslo občanského průkazu. Někteří správci toto číslo využívají jako doplňkový údaj společně s dalšími základními identifikačními údaji. Tento postup není v rozporu se zákonem č.328/1999 Sb., o občanských průkazech, jelikož neexistuje zvláštní zákon, jako existuje například pro rodná čísla zmiňovaná výše, který by stanovoval pro čísla občanských průkazů pravidla pro jejich zvláštní využití.

Číslo občanského průkazu je často využíváno jako doplňkový identifikační údaj pro evidenci návštěvníků při vstupu do budov. Touto problematikou se zabývá Úřad pro ochranu osobních údajů ve svém stanovisku č. 3/2016 Evidence návštěvníků při vstupech

do budov a kopírování dokladů. Číslo občanského průkazu lze při vstupu do budovy či areálu zapsat společně se jménem a příjmením, pokud se nejedná o pracovní návštěvu, při které by se měl primárně vypisovat název vysílající organizace a číslo služebního průkazu. Někteří správci přistupují při ověření totožnosti osoby také k tomu, že si vytvoří kopii občanského průkazu. V případě, že se nejedná o zákonnou výjimku nebo o pořízení pouze částečné kopie s údaji, které lze pro účely ověření totožnosti evidovat, není tato praxe příkladná.

Zákon č. 328/1999 Sb., o občanských průkazech upravuje problematiku pořizování kopií občanských průkazů tak, že je zakázáno bez prokazatelného souhlasu občana, kterému byl průkaz vydán, pořizovat jakýmikoli prostředky kopie občanského průkazu. Výjimku tvoří zvláštní případy, které mohou být stanoveny ve zvláštním zákoně nebo v mezinárodní smlouvě, kterou je Česká republika vázána. V tomto zákoně je také stanoven zákaz shromažďování, ukládání, upravování, podávání, šíření, zveřejňování nebo uchovávání strojově čitelných údajů v občanském průkazu, pokud zákon o občanských průkazech nebo jiný předpis nestanoví jinak.

Je důležité se touto problematikou zabývat zejména proto, že občanský průkaz je veřejná listina, kterou občan prokazuje své jméno, příjmení, podobu a státní občanství, jakož i údaje v něm zapsané. Tyto údaje jsou způsobilé ke zfalšování a zneužití identity. Proto je velmi nebezpečné, pokud se tento soubor informací dostane do rukou komukoliv dalšímu. Navíc s každou další kopií roste riziko jejího zneužití.

4.4 Zabezpečení osobních údajů

Janečková (2018) ve své publikaci uvádí, že osobní údaje by měly být zpracovány způsobem, který zaručuje náležitou důvěrnost a bezpečnost těchto údajů. Zejména za účelem zabránění neoprávněnému přístupu k osobním údajům a také k zařízením, které se používají k jejich zpracování. K zabezpečení údajů se vyjadřuje také recitál 83. Dle tohoto recitálu v zájmu zachování bezpečnosti a zabránění zpracování, které by mohlo být v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika, které mohou vzniknout v souvislosti se zpracováním údajů a následně přijmout opatření ke zmírnění těchto rizik. V souvislosti s povahou a riziky, které se k různým kategoriím osobních údajů vztahují, by měla být zajištěna náležitá úroveň zabezpečení včetně důvěrnosti s ohledem na stav techniky, náklady a způsob provedení.

Zabezpečení osobních údajů je upraveno v článku 32. Tento článek uvádí, že s přihlédnutím ke stavu techniky, nákladům na provedení, rozsahu, kontextu, povaze a účelům zpracování i k různě pravděpodobným a závažným rizikům pro práva a svobody fyzických osob provedou správce a zpracovatel vhodná organizační a technická opatření tak, aby zajistili odpovídající úroveň zabezpečení daného rizika. (Nulíček a kol., 2018)

Janečková (2018) ve své publikaci uvádí, že zabezpečení může být mimo jiné provedeno například pomocí:

- pseudonymizace a šifrování osobních údajů,
- schopnosti zajistit neustálou integritu, důvěrnost, dostupnost a odolnost systému a služeb zpracování,
- v případě technických incidentů zajistit schopnost zavčasu obnovit dostupnost osobních údajů a přístup k nim,
- procesu pravidelného posuzování, testování a hodnocení účinnosti zavedených organizačních a technických opatření pro zajištění bezpečnosti zpracování.

Nařízení tedy jednoznačně stanoví to, co zákon o ochraně osobních údajů pouze dozoroval. A to skutečnost, že při výběru zabezpečení osobních údajů je nutné zohlednit způsob jejich zpracování, prostředků zpracování i objem a charakter zpracování údajů. Zároveň ale nařízení neukládá povinnost využít specifická opatření. Jak je již zmiňováno výše, správce či zpracovatel mají použít technická opatření korespondující se stavem techniky a organizačních opatření.

Při posuzování vhodné úrovně zabezpečení je dobré zohlednit zejména rizika, která představuje zpracování. Jedná se zejména o náhodné nebo protiprávní zničení, ztrátu, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů nebo také neoprávněný přístup k nim. Jedním z prvků, díky kterému lze doložit, že správce pracuje v souladu s požadavky, které Nařízení stanovuje, je dodržování schváleného kodexu chování nebo uplatňování chváleného mechanismu pro vydávání osvědčení. Správce a zpracovatel dále také musí přijmout opatření, které zajišťuje, aby jakákoli fyzická osoba, která je z jejich pověření oprávněna osobní údaje zpracovávat, zpracovávala tyto údaje pouze na jejich pokyn. Výjimku tvoří případy, kdy zpracování daných údajů ukládá právo Unie nebo členského státu. (Janečková, 2018)

Jako porušení zabezpečení osobních údajů chápe Nařízení o ochraně osobních údajů (2018) takové porušení zabezpečení, které vede k protiprávnímu nebo náhodnému zničení, změně, ztrátě nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. Pokud taková situace nastane, správce je povinen bez zbytečného odkladu tuto skutečnost ohlásit dozorovému úřadu. Pokud by bylo nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob, není nutné takové porušení bezprostředně hlásit.

4.5 SPRÁVCE A ZPRACOVATEL OSOBNÍCH ÚDAJŮ

Janečková (2018) ve své publikaci uvádí, že je důležité rozklíčovat postavení subjektů v každém účelu zpracování, tedy zda se nachází v postavení správce či zpracovatele.

Žůrek (2018) uvádí, že správce osobních údajů je hlavní subjekt, bez kterého se neobejde žádné zpracování osobních údajů. A za zpracovatele označuje subjekt, který byl zpracováním osobních údajů pověřen správcem. Důležité je také zmínit, že správcem či zpracovatelem je v případě právnických osob vždy organizace jako taková, nikdy se nejedná pouze o statutární orgán, personalistu nebo například účetní.

4.5.1 SPRÁVCE OSOBNÍCH ÚDAJŮ

Správce odpovídá za dodržování povinností, které jsou Nařízením stanoveny. Zcela zásadní je pak dodržování zásad zpracování. Dodržení těchto zásad musí být správce schopen také doložit. Jak je již zmiňováno v předchozích kapitolách, je nutné, aby byl schopen doložit řádný právní důvod, proč jsou osobní údaje zpracovávány. Zároveň se mimo jiné stará také o to, aby byly osobní údaje řádně zabezpečeny (Nezmar, 2018)

Dle Žůrka (2019) není ani tolik důležitá právní forma či status subjektu, ale to, že určí účely a prostředky zpracování těchto údajů. Zároveň si správce musí být vědom skutečnosti, že za zpracování údajů odpovídá i v případě, že jmenoval ke zpracování pověřence. Odpovědnosti se nezbaví ani tehdy, pokud pověří zpracováním zpracovatele.

Calder (2017) uvádí, že správce dat může data zpracovávat pouze jménem tzv. kontrolora osobních údajů. Dále dodává, že je velmi běžné, že správce a ten, kdo data kontroluje je stejný subjekt.

4.5.1.1 SPOLEČNÍ SPRÁVCI

Pokud prostředky a účely zpracovávají dva nebo více správců, mluvíme o společných správcích. Zákon o ochraně osobních údajů neobsahoval bližší ustanovení, která by se této problematiky týkala. To ale nevylučuje jejich existenci. Charakteristickým znakem společných správců je, že účely a prostředky stanovují dva a více správců mezi sebou. V praxi se jedná o různé projekty, které zahrnují zpracování osobních údajů a které jsou provozovány dvěma a více od sebe odlišnými subjekty. Může se jednat i o konkurenční subjekty. (Žůrek, 2018)

Nezmar (2017) upozorňuje, že je důležité, pokud se jedná o společné zpracování dvou a více správců, před zahájením zpracování jasně stanovit, vzájemné odpovědnosti a povinnosti mezi správci. Důležitá je také dokumentace těchto rozhodnutí.

Dle Žůrka (2018) je subjektu údajů takto poskytnuta zvýšená míra ochrany, jelikož může bez ohledu na podmínky a ujednání mezi správci vykonávat svá práva u každého z nich a vůči každému z nich. Aby byla zajištěna účinná náhrada újmy subjektů údajů, je stanoveno, že pokud odpovídá více než jeden správce za způsobenou újmu, nese každý správce vinu za celou újmu.

4.5.2 ZPRACOVATEL

Zpracovatel je takový subjekt, kterého správce může a nemusí využít ke zpracování osobních údajů. Opět, stejně jako v případě správce, není rozhodnuto, jakou má právní formu. Zpracovatel zpracovává osobní údaje, které mu byly svěřeny správcem. Správce také určuje způsob, jakým mají být tyto údaje zpracovávány. Zpracovatel musí mít dostatečně proškolené zaměstnance. Zejména v oblasti zabezpečení osobních údajů. Pokud dojde k porušení zabezpečení údajů je povinen tuto skutečnost neprodleně ohlásit správci, který ho zpracováním pověřil. Pokud má správce zájem využít služby zpracovatele, může takto učinit kdykoli. Nepotřebuje souhlas subjektu údajů, či jiný právní důvod pro zpracování. Je tomu tak, protože, jak je již zmíněno výše, zpracovatel zpracování provádí pouze pro účely definované správcem, nikoliv pro své účely. K využití správce nejčastěji dochází, pokud správce nemá dostatečný personál, či technické prostředky pro zpracování údajů. Dalším důvodem může být to, že je to pro správce výhodné. (Žůrek, 2019)

Každý zpracovatel musí splňovat požadavky, které jsou správcem určeny dle GDPR. Smluvní vztahy, které vznikají mezi zpracovateli a správci musí naplňovat řadu specifických požadavků. Tyto požadavky jsou dány v rámci nařízení. (Nezmar, 2017)

4.5.2.1 ŘETĚZENÍ ZPRACOVATELŮ

Řetězení zpracovatelů znamená zapojení dalšího zpracovatele do zpracování. Toto zapojení přichází ze strany zpracovatele. Takto vznikne řetěz, kde jsou jednotlivými články správce -> 1. zpracovatel -> 2. zpracovatel a tak dále. Takovéto řetězení je bez předchozího schválení správce údajů zakázáno. Správce si tedy řetězení musí být vědom, a to zejména z toho důvodu, že je správce za zpracování osobních údajů odpovědný, a tudíž i za to, kdo bude údaje zpracovávat. Kdyby správce nad tímto zapojením neměl kontrolu, mohlo by dojít k zapojení zpracovatele, který by neposkytoval dostatečné záruky ohledně zpracování. Další zpracovatel může být stanoven již ve smlouvě, kterou mezi sebou první zpracovatel a správce uzavírají. Pokud je stanoven až po uzavření této prvotní smlouvy, je nutné, aby měl další zpracovatel na základě smlouvy stejné povinnosti v ochraně osobních údajů, které jsou uvedeny mezi správcem a zpracovatelem. Je nepřípustné, aby se zapojením dalšího zpracovatele snížil standard ochrany osobních údajů. (Žůrek, 2019)

4.5.3 VZTAH SPRÁVCE A ZPRACOVATELE

Dle Žůrka (2018) má správce možnost využít pouze takové zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných organizačních a technických opatření tak, aby zpracování osobních údajů splňovalo požadavky Obecného nařízení a také, aby byla zajištěna ochrana práv subjektů údajů, které jsou zpracovávány. Každé zpracování tak může klást rozdílné požadavky na kvalitu zpracovatele v závislosti na kategorii osobních údajů nebo například rozsahu zpracování.

Správce je tím, kdo má primárně odpovědnost za uzavření smlouvy, nebo jiného právního aktu, který vymezuje vztah mezi správcem a zpracovatelem. Odpovědnost správce nikdy zcela nezaniká a ani se nepřenáší na zpracovatele, se kterým se rozhodne spolupracovat. Výjimku tvoří případ, kdy došlo k porušení zcela na straně zpracovatele. V tomto případě by byla odpovědnost správce vyloučena. I tak by ale mohl být správce konfrontován s tím, že nevybral dostatečně kvalifikovaného zpracovatele nebo že ho dostatečně neprověřil.

Podstatným instrumentem, který upravuje vztah správce a zpracovatele je smlouva o zpracování osobních údajů nebo podobný právní akt. Účelem je zejména zajistit bezpečnost osobních údajů při využití zpracovatele a zároveň nastolit bezpečný vztah mezi oběma stranami. Obecné nařízení stanovuje náležitosti, které by smlouva nebo obdobný právní akt měl obsahovat. Jedná se zejména o předmět a dobu zpracování, dále povahu a účel zpracování, kategorii subjektů údajů a typ osobních údajů, dále také povinnosti a práva správce. Jakýkoliv právní akt, který tento vztah upravuje, musí být vyhotoven v písemné podobě. Není ale nutné, aby se jednalo o samostatný právní akt, smlouva může být součástí jiné smlouvy. U smluv, které byly uzavřeny ještě v době, kdy byl účinný zákon o ochraně osobních údajů, je nutné provést revize a nevyhovující smlouvy upravit tak, aby splňovaly aktuálně požadované náležitosti. (Žůrek, 2018)

Zákon č. 110/2019 Sb. o zpracování osobních údajů uvádí, že smlouva mezi správcem a zpracovatelem především určuje:

- předmět a také dobu trvání zpracování,
- povahu a účel zpracování,
- typ osobních údajů, které budou zpracovávány,
- kategorie subjektů údajů a
- práva a povinnosti zpravujícího orgánu.

4.6 SHRNUTÍ KAPITOLY

K tomu, aby byla problematika GDPR pochopena jako celek, bylo důležité vysvětlit základní pojmy, které se v souvislosti s GDPR nejvíce používají. A právě tím se zabývá tato kapitola práce. Nejprve vysvětluje pojem osobní údaj, který je stěžejní pro aplikaci nařízení. Osobní údaj je v této kapitole vysvětlen jako veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Dále je v kapitole popsán rozdíl v implementaci nařízení v případě fyzické a právnické osoby. Podrobněji se kapitola práce soustředí na osobní údaje, které se mohou zdát matoucí. Mezi ty autorka zařazuje rodné číslo, které i přesto, že se nenachází v taxativním výčtu citlivých údajů, má zákonem určené zvláštní podmínky, za kterých se může využívat. Dále je v této kapitole zmíněn občanský průkaz, který je zdrojem mnoha osobních údajů, jako je například jméno, příjmení, adresa a státní příslušnost. Tyto údaje je možné využít pro zfalšování nebo zneužití identity, proto je velmi nebezpečné, pokud by se tento soubor informací dostal do rukou cizí osobě, která by měla v plánu tyto informace zneužít. I proto je další

částí této kapitoly zabezpečení osobních údajů na což navazuje rozbor toho, kdo a jak údaje zpracovává.

5. ZAVÁDĚNÍ GDPR DO ČINNOSTI PODNIKATELSKÝCH SUBJEKTŮ A CHARAKTERISTIKA VYBRANÉHO PODNIKU

5.1 ZAVÁDĚNÍ GDPR DO ČINNOSTI PODNIKATELSKÝCH SUBJEKTŮ

GDPR celkově nepřináší žádné převratné povinnosti ani pro podnikatelskou sféru, ani pro samosprávu, státní úřady nebo zdravotnická zařízení. U podnikatelské sféry je situace poněkud odlišná, jelikož mnoho těchto subjektů tuto problematiku přehlíželo nebo ji řešilo jen jako součást celkové ochrany důvěrných informací. Správce je povinen zavést vhodná organizační a technická opatření tak, aby zajistil, že zpracování údajů je v souladu s GDPR.

5.1.1 TECHNICKÁ OPATŘENÍ K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

Písemnosti a jiné hmotné nosiče dat je možné uchovávat pouze v uzamykatelných místnostech, ideálně i v uzamykatelných skříních. Pokud by byly písemnosti uloženy v uzamčené skříni v jiné místnosti, musí být zajištěno, že přístup do této místnosti nemá nikdo jiný než zaměstnanci podniku.

Dle Navrátila a kol. (2018) je možné elektronické datové soubory uchovávat v paměti počítače pouze:

- pokud je přístup k těmto údajům chráněn doménovým jménem a díky tomu je možné zpětně zjistit, kdo do dokumentů nahlížel a komu byly poskytnuty, přístup musí být také chráněn heslem,
- pokud je přístup do počítače, ve kterém jsou údaje uloženy, chráněn heslem nebo vhodným zámkem,
- pokud jsou veškerá data pravidelně zálohována a zálohovaná media musí být v přiměřených intervalech měněna, tyto datové nosiče musí být umístěny na místě, kde jim nehrozí negativní ovlivnění vnějšími vlivy,
- pokud příslušné osoby mají přístup pouze k osobním údajům a datům, které odpovídají oprávnění těchto osob na základě zvláštních uživatelských práv, které byly zřízeny, taková oprávnění uděluje vedoucí pracovník nebo členové nejvyššího vedení společnosti.

Všechna hesla a pokyny k používání elektronických datových souborů by měly být uvedeny v neveřejném manuálu, ke kterému by měli mít přístup pouze pověřené osoby. Veškeré listiny a elektronické materiály, které byly použity jednorázově anebo již nejsou potřeba, by měly být zlikvidovány pod dohledem pověřené osoby.

Citlivé osobní údaje, tedy údaje o národnostním, rasovém nebo etnickém původu, politických postojích a náboženství atd. jsou uchovány jen, pokud je to nezbytně nutné k plnění zákonných povinností a musí být zvláště pečlivě chráněny. Dle Caldera (2017) mezi další data, která tuto speciální ochranu vyžadují, musí zařadit také data o zdraví subjektu.

Vybraný ekonomický subjekt, který je popsán níže, disponuje kamerovým systémem. Dle Bártíka (2013) je kamerový systém považován za zpracování osobních údajů, pokud je prováděn současně s kamerovým záznamem také záznam pořizovaných obrazových, popřípadě zvukových záběrů.

Kamerové a audio záznamy mohou být pořizovány jen v souladu s příslušnými právními předpisy. Záznamy z těchto kamer musí být chráněny heslem nebo kódem. Pokud není žádný důvod pro to, aby byly záznamy uchovávány déle, musí být uchovány pouze po dobu určenou podnikem. Tyto lhůty musí být přiměřené k tomu, k čemu jsou záznamy používány. Kamerové záznamy nesmí být pořizovány v místech, kde můžou urážet lidskou důstojnost nebo zvyšovat nebezpečí úrazu či vzniku škody. O umístění kamer musí být všichni zaměstnanci a další osoby řádně informovány vhodným způsobem. (Navrátil a kol., 2018)

5.1.2 Hlavní zásady pracování osobních údajů

Navrátil a kol. (2018) ve své publikaci uvádí tyto zásady zpracování osobních údajů:

- osobní údaje musí být zpracovány korektně a zákonným transparentním způsobem, to znamená, že při jejich zpracování musí být dodrženy všechny právní předpisy týkající se této problematiky, musí být zpracovány tak, aby bylo jasné, o jaké osobní údaje se jedná a jak byly zpracovány,
- osobní údaje by měly být zpracovány pro výslovně vyjádřené legitimní účely a neměly by být dále zpracovávány způsobem, který se s těmito účely neslučuje,

- mělo by být zachováno pravidlo „minimalizace údajů“, tedy že je zpracován nezbytný, přiměřený a relevantní rozsah ve vztahu k účelu, pro který jsou data zpracovávaná, tedy nesmí být zpracovávány osobní údaje, které nejsou potřebné,
- osobní údaje musí být zpracovány bez chyb a musí být v případě potřeby aktualizované, nepřesné informace musí být bezodkladně vymazány nebo opraveny,
- osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které byly údaje zpracovány, osobní údaje lze uložit i po delší dobu a to, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely historického nebo vědeckého výzkumu anebo pro statistické účely,
- osobní údaje musí být zpracovány, způsobe, který zajistí jejich náležité zabezpečení a musí být chráněny před ztrátou nebo poničením.

Za dodržení výše uvedených pravidel odpovídá správce a musí být dodržování těchto pravidel také schopný doložit. Obecný popis pravidel – zásad můžeme naleznout v této práci v subkapitole číslo 3.5 – Základní kritéria GDPR.

Gobeo a kol. (2018) ve své publikaci k výše zmíněnému doplňují, že všechna komunikace, která probíhá mezi správcem a subjektem údajů o tom, jak jsou tato práva dodržována, musí vyhovovat právu na informace. V praxi to znamená, že komunikace musí být transparentní, stručná a vedena ve snadno srozumitelném jazyku.

5.1.3 Zpracování osobních údajů se souhlasem a bez souhlasu subjektů údajů

Pokud je zpracování osobních údajů založeno na souhlasu subjektu, musí být ten, kdo data zpracovává a uchovává schopen tento souhlas doložit. Pokud je tento souhlas vyjádřen písemným prohlášením, které se týká i jiných skutečností, musí od nich být řádně odlišen. Musí být srozumitelný a snadno přístupný. Souhlas tedy musí být vyjádřen jednoznačně, musí být doložitelný a nesmí být vynucen nebo získán za pomoci lsti. Důležité je také zmínit, že souhlas se zpracováním osobních údajů je dobrovolný a odvolatelný. Výjimkou je, pokud by mělo dojít k odvolání souhlasu v nevhodné době. Za nevhodnou dobu se například považuje taková doba odvolání, která by znemožnila dokončení již probíhající projektu. Odvoláním souhlasu není dotčena zákonnost

zpracování údajů před tímto odvoláním, leda že by již tyto osobní údaje nebyly potřebné. (Navrátil a kol., 2018)

Bártík (2012) se domnívá, že souhlas subjektu údajů se zpracováním je jedním z nejdůležitějších pojmů, pro celou tuto oblast. Zákon o ochraně osobních údajů ho definuje jako vědomý a svobodný projev vůle subjektu údajů. Obecně je poskytnutí souhlasu právním úkonem a to takovým, který je svým charakterem jednoznačně jednostranný.

Mluvíme-li o zpracování osobních údajů bez souhlasu subjektu, je nutné dbát na zákonnost zpracování těchto údajů. Je tedy nezbytné, aby zpracování těchto údajů bylo zákonem dovoleno bez souhlasu subjektů nebo aby byl souhlas řádně udělen. Jedná se například o osobní údaje, které je zaměstnavatel zákonem povinen uchovávat a mít je k dispozici, případně je odesílat veřejným subjektům. Proto, aby mohly být údaje zpracovávány bez souhlasu, musí být splněny určité podmínky nebo alespoň některé z nich. Jedná se zejména o situace, kdy je zpracování údajů nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů. Dále pak pokud je zpracování nutné pro splnění nezbytné právní povinnosti, která se na správce vztahuje. Bez souhlasu subjektů dále mohou být osobní údaje zpracovány, pokud se jedná a ochranu životně důležitých zájmů subjektu údajů nebo fyzické osoby nebo pří výkonu veřejné moci, či úkonu prováděného ve veřejném zájmu. (Navrátil a kol., 2018)

5.1.4 Zpracování citlivých osobních údajů

Zákon zakazuje zpracování osobních údajů, které jsou považovány za citlivé. Mezi takové údaje můžeme zahrnout informace o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení nebo členství v odborech. Dále pak zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o sexuálním životě, sexuální orientaci nebo zdravotním stavu subjektu. Samozřejmě ale existují i výjimky, kdy je možné tyto údaje zpracovávat, jedná se zejména o situace, kdy subjekt udělil výslovný souhlas se zpracováním těchto údajů pro jeden nebo více stanovených účelů. Dále pokud je zpracování těchto údajů nezbytné pro účely plnění povinnosti a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a v oblasti sociálního zabezpečení a sociální ochrany. Další výjimka platí, pokud jsou údaje zpracovávány pro ochranu životně důležitých zájmů subjektu nebo jiné fyzické osoby. Citlivé osobní údaje může

také zpracovávat sdružení, nadace nebo jiný neziskový subjekt, který sleduje cíle, které souvisejí s citlivými osobními údaji jako například náboženství nebo sexuální orientaci. Vždy musí být zaručeno, že tyto údaje nejsou bez souhlasu subjektu poskytovány třetím osobám. Dále mohou být citlivé osobní údaje zpracovány, pokud se jedná o výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí. Zaměstnavatel může tyto údaje zpracovávat, pokud jsou nezbytné pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky nebo preventivního a pracovního lékařství. Pokud je zpracování údajů nebytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako například ochrana před vážnými přeshraničními zdravotními hrozbami nebo pokud je nezbytné pro účely archivace ve veřejném zájmu, pro účely zajištění práv a svobod subjektu. Citlivé údaje mohou být takto zpracovány pro úřední účely, jsou-li zpracovány pracovníkem, který je vázán služebním tajemstvím. (Navrátil a kol., 2018)

Další výjimkou jsou údaje, které se týkají rozsudků v trestních věcech a trestných činů. Tyto údaje sice za citlivé považovány nejsou, ale mohou být zpracovány pouze, pokud na jejich zpracování dohlíží orgán veřejné moci.

5.1.5 Nárok subjektů údajů na přístup k osobním údajům

Subjekt údajů má na základě žádosti právo získat od správce potvrzení, zda osobní údaje, které se ho přímo týkají, jsou či nejsou zpracovávány. Má právo k těmto údajům získat přístup a dále také dle Navrátila a kol. (2018) k těmto informacím:

- pro jaké účely jsou jeho osobní údaje zpracovávány,
- jaké kategorie dotčených osobních údajů jsou o něm zpracovávány,
- kdo jsou kategorie příjemců nebo příjemci, kterým budou nebo jsou osobní údaje zpřístupněny,
- jaká je plánovaná doba uložení osobních údajů nebo podle jakých kritérií budou skartovány,
- zda má právo požadovat od správce výmaz nebo opravu osobních údajů, které se subjektu týkají anebo vznést námitku proti způsobu zpracování těchto údajů,
- zda má právo podat stížnost u dozorového úřadu,

- jaké jsou veškeré dostupné informace o zdroji osobních údajů tazatele, pokud nejsou získány přímo od subjektů údajů,

- zda dochází k automatizovanému rozhodování včetně profilování, a informace týkající se postupu, který byl použit, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

Správce je také povinen poskytnout subjektu údajů kopii zpracovávaných osobních údajů o něm, a to i v elektronické podobě. Právem získat tuto kopii nesmí být samozřejmě nepříznivě dotčena práva a svobody jiných osob.

5.1.6 Výmaz a oprava údajů

Subjekt údajů má právo na opravu údajů bez zbytečného odkladu. Tuto opravu musí provést správce údajů. Zejména se opravují nepřesné údaje, které se subjektu přímo týkají. Zároveň má subjekt nárok na doplnění neúplných osobních údajů. Toto právo najdeme v článku 16 Nařízení.

Dalším důležitým právem je „právo být zapomenut“. Jedná se o právo na výmaz. Subjekt údajů má právo na to, aby bez zbytečných odkladů správce údajů údaje, které se subjektu týkají, vymazal. Správce údajů může osobní údaje podle Nezmara (2017) vymazat pokud:

- již nejsou potřebné pro původní účely,
- subjekt údajů odvolá souhlas, na jehož základě údaje byly zpracovány, v současné době neexistuje žádný další právní důvod pro zpracování, pro který souhlas není potřeba,
- subjekt, kterého se údaje týkají, vznese námitky proti zpracování a neexistují žádné jiné oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- pokud o vymazání osobních údajů rozhodne příslušný orgán,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb nebo zboží.

Pokud údaje byly mezitím zveřejněny a správce je následně povinen je vymazat. Přiměřené kroky použije s ohledem na dostupnou technologii a náklady na provedení. Dále by také měl informovat správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie, či replikace.

Zejména z tohoto důvodu je nanejvýš praktické, aby správce údaje předával na co nejmenší počet míst.

Existují i výjimky z povinnosti výmazu. Povinnost výmazu se neuplatňuje, pokud je zpracování nezbytné. A to zejména pokud jsou údaje důležité pro výkon práva na svobodu projevu a informace. Dále také pokud jsou informace nutné pro splnění právní povinnosti, z důvodu veřejného zájmu v oblasti veřejného zdraví, pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu, či pro statistické účely. Dále pokud se jedná o určení, výkon nebo obhajobu právních nároků. (Nezmar, 2017)

Dále také existuje právo na omezení zpracování. To se uplatňuje, zejména pokud subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit. Dalším důvodem může být, že zpracování těchto údajů je protiprávní, ale subjekt údajů odmítá jejich výmaz a místo toho jen žádá omezení jejich využití. Pokud správce již údaje nepotřebuje pro účely zpracování, ale subjekt je požaduje pro určení, výkon nebo obhajobu právních nároků, nebo pokud subjekt vznesl námitku proti zpracování, poté se na tyto údaje právo na omezení zpracování také vztahuje, a to do chvíle, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů. (Navrátil a kol., 2018)

Pokud bylo zpracování omezeno, mohou být tyto osobní údaje zpracovány pouze se souhlasem subjektu údajů. Výjimku tvoří jejich uložení. Správce je povinen upozornit subjekt údajů předem na to, že omezení na zpracování bude zrušeno, odpadnou-li pro toto omezení důvody. Správce má povinnost oznamovat jednotlivým příjemcům, kterým byly osobní údaje zpřístupněny, veškeré opravy, výmazy nebo omezení zpracování. Výjimku tvoří případy, kdy se toto oznámení jeví jako nemožné, nebo vyžaduje nepřiměřené úsilí. (Navrátil a kol., 2018)

5.1.7 Záznamy o činnostech zpracování

Každý správce a jeho zástupce je povinen vést záznamy o činnostech, které se zpracováním osobních údajů souvisejí. Tyto záznamy by dle Janečkové (2019) měly obsahovat minimálně tyto informace:

- jméno a kontaktní údaje správce, případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů,

- účely zpracování,
- popis kategorií osobních údajů a kategorií subjektů,
- kategorie příjemců, kterým budou nebo byly údaje zpřístupněny, včetně příjemců třetích zemí nebo mezinárodních organizací,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, zahrnuta by měla být i identifikace této třetí země či mezinárodní organizace a doložení záruk řádného zpracování a ochrany osobních údajů,
- pokud je to možné, plánované lhůty pro výmaz jednotlivých údajů, výmaz může být proveden například ve formě výpisu ze skartačního řádu,

Každý zapisovatel dále musí vést záznamy o všech kategoriích činností zpracování prováděných pro správce. Tyto záznamy by měly dle Navrátila a kol. (2018) obsahovat:

- jméno a kontaktní údaje zpracovatele nebo zpracovatelů, dále také každého správce, pro kterého zpracovatel jedná a případně také zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů,
- kategorie zpracování prováděného pro každého ze správců,
- informace o případném předání osobních údajů do třetí země či mezinárodní organizace a doložení vhodných záruk,
- pokud je to možné měly by záznamy také obsahovat obecný popis technických a organizačních bezpečnostních opatření.

Záznamy informací, které jsou výše popsané, musí být vyhotoveny písemně, za což se považuje i elektronická forma. Zároveň je správce nebo zpracovatel povinen tyto záznamy poskytnout na požádání Úřadu pro ochranu osobních údajů.

Jak uvádí článek publikovaný v Cyber Defense Review, který vydal autor Todt (2019), záznamy, které se vedou o zpracování dat a jejich archivování, jsou jedním ze tří klíčových elementů v oblasti ochrany dat u podnikatelských subjektů. Za další dva klíčové elementy je považováno nastavení směrnic na ochranu údajů a plán v případě, že by došlo ke zneužití dat.

5.1.8 PŘEDCHOZÍ KONZULTACE-NOVÝ PRVEK V OCHRANĚ OSOBNÍCH ÚDAJŮ

Novou povinností, která nahrazuje dosavadní povinnost registrace u Úřadu pro ochranu osobních údajů, je povinnost provádět konzultace s Úřadem pro ochranu osobních údajů. Jedná se o velmi účinný nástroj, který napomůže předcházení chybám při správě a zpracování osobních údajů. Správce je povinen konzultovat ochranu osobních údajů a rizika s tím spojená ještě před zpracováním těchto údajů. Pokud Úřad pro ochranu osobních údajů shledá, že by dané zpracování mělo za následek vysoké riziko, musí správce údajů přijmout opatření, která povedou ke zmírnění nebo odstranění tohoto rizika. Takto to nařizuje článek 35 a 36 GDPR. I přesto tento poradenský prvek bude odpovědnost za zpracování veškerých osobních údajů vždy ležet na samotném správci nebo zpracovateli.

5.1.9 POKUTY

Za porušení GDPR mohou dozorové úřady ukládat pokuty. Výše pokuty může dosáhnout až 10 000 000 eur. Pokud by se jednalo o zvlášť závažný případ, mohla by tato pokuta narůst až do výše 20 000 000 eur nebo pokud se jedná o podnik, až do 4% výše celkového ročního obratu celosvětově za předchozí rozpočtový rok. V případě podniku se volí varianta pokuty dle toho, co je vyšší, zda zmiňovaná 4 % anebo stanovená pokuta ve výši 20 000 000. Česká právní úprava zahrnuje pokuty až do výše 10 000 000 Kč. Takto vysoké pokuty slouží zejména jako varování pro ty, kteří nabízejí služby v oblasti ochrany osobních údajů metodou „vystrašit a zkasírovat“. Zároveň nutí subjekty, které se do této doby problematikou víceméně nezabývaly, aby jí věnovaly větší pozornost, což je důležité proto, že se jedná často o soukromé údaje, jejichž zveřejnění by mohlo osobě, které se tyto údaje týkají, ublížit. (Nezmar a kol., 2018)

Při udílení sankce by měla platit zásada přiměřenosti sankce. Měla by se tedy náležitě zohlednit povaha, doba porušení a náležitosti, dále také úmyslný charakter porušení a také kroky, které byly učiněny s cílem zmírnit způsobenou škodu. Dále by mělo být přihlédnuto k míře odpovědnosti nebo k jakémukoli předchozímu relevantnímu porušení a způsobu, jakým se dozorový úřad o porušení dozvěděl a také dalším přitěžujícím nebo ulehčujícím okolnostem. Možností je, místo peněžité sankce, uložit pouze napomenutí. (Praktický manuál GDPR pro každého, 2018)

5.1.10 NÁPRAVNÁ OPATŘENÍ JAKO MOŽNOST TRESTU

Obecné nařízení obsahuje i mechanismy, které mají zajistit spravedlivé ukládání pokut a také umožňuje pokutu vůbec neukládat nebo uložit některé z nápravných pravomocí. Výše jsou zmíněny důvody, pro které může být odstoupeno od peněžní pokuty a může být použit nižší trest. Nyní si tato nápravná opatření přiblížíme. Janečková (2019) uvádí seznam těchto nápravných opatření:

- upozornit správce či zpracovatele, že zamýšlené operace zpracování s největší pravděpodobností porušují Obecné nařízení,
- udělit správci či zpracovateli napomenutí
- nařídit správci nebo zpracovateli, aby uvedl operace zpracování do souladu s Obecným nařízením
- nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů,
- uložit dočasné nebo trvalé omezení zpracování, může být uložen také naprostý zákaz zpracování,
- nařídit opravu, výmaz nebo omezení zpracování a ohlašování takových opatření příjemcům,
- odebrat správci osvědčení nebo nařídit, aby jej subjekt oprávněný k vydávání osvědčení odebral nebo nevydal,
- nařídit přerušení toků údajů příjemci ve třetí zemi nebo mezinárodní organizaci.

Jedná-li se o bagatelní případ, tedy pouze formální porušení Obecného nařízení, ale s minimální společenskou škodlivostí, nemusí být pokuta správci udělena vůbec. Je možné, že bude stačit některé z výše uvedených nápravných opatření nebo pouze informování správce o jeho povinnostech a bude očekáváno, že správce uvede zpracování do souladu s Obecným nařízením sám. Správce se o oblastech, ve kterých udělal chybu, může dozvědět z informativního dopisu.

Přestupky projednává Úřad pro ochranu osobních údajů. Ten také vybírá udělené pokuty. V případě potřeby je také může vymáhat Celní úřad. Promlčecí doba je stanovena v zákoně o odpovědnosti za přestupky a řízení o nich. Pro přestupky, které spočívají v porušení Obecného nařízení, platí tříletá promlčecí lhůta, jelikož se jedná o čin, za který zákon, tedy Obecné nařízení, stanovuje sazbu pokuty, jejíž horní hranice je 100 000 Kč. (Žůrek, 2019)

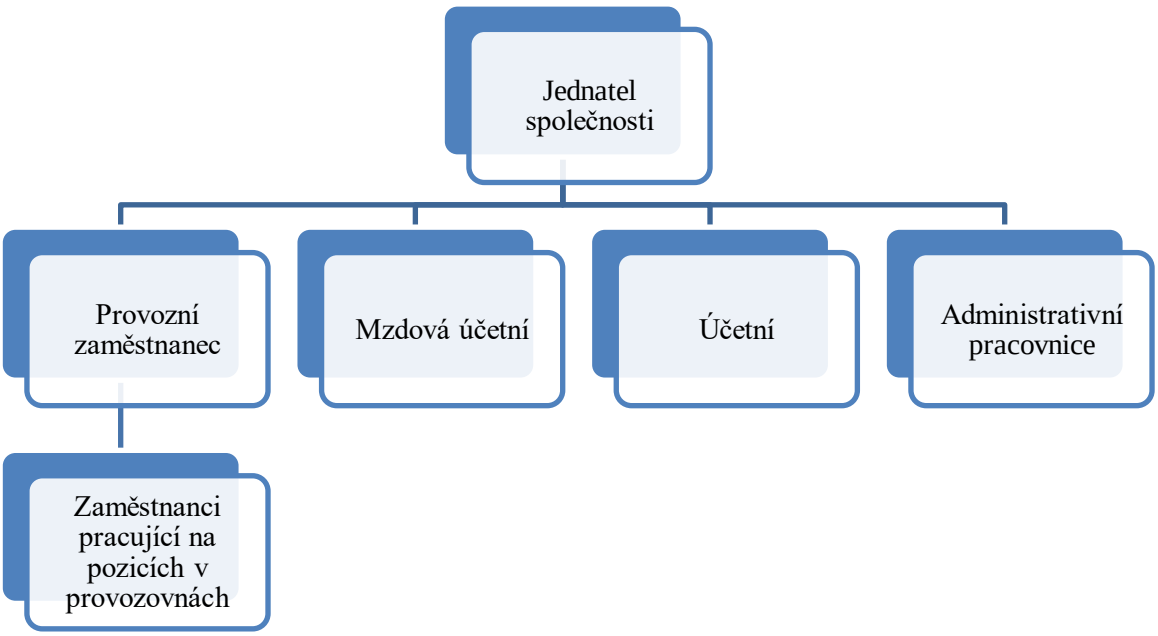
5.2 CHARAKTERISTIKA VYBRANÉHO PODNIKU

Pro praktické přiblížení problematiky GDPR ve vybraném ekonomické subjektu je pro potřeby práce zvolena společnost, která si nepřála být jmenována. V dalším textu bude tato společnost označena jako společnost XY. Zároveň také údaje o společnosti jsou z důvodu zachováni anonymity zkresleny.

Společnost XY je vlastněna fyzickou osobou podnikající. Je zapsána v Obchodním rejstříku. Tato společnost byla založena v roce 2012. Jelikož se jedná o fyzickou osobu podnikající, je tato osoba zároveň také jednatelem celé organizace.

Společnost XY se zabývá prodejem a poskytováním služeb. Jedná se o prodej a služby v oblasti gastronomie. Společnost vlastní několik podniků, mezi které patří zejména restaurace a jiná gastronomická zařízení. V současné době pracuje pro společnost 32 zaměstnanců. Z toho jsou 4 zaměstnanci pracující v administrativě a účetnictví. Zbytek zaměstnanců zastupuje různé pozice ve zmiňovaných provozovnách. Zejména se jedná o pozice číšníků, kuchařů a pomocné síly v kuchyni. Organizační schéma společnosti je znázorněno na obrázku 2.

Obrázek 2: Organizační schéma společnosti XY



Zdroj: Vlastní zpracování, 2020

5.3 SHRNUTÍ KAPITOLY

V první kapitole praktické části práce byla nejprve obecně popsána implementace nařízení na podnikatelský subjekt. Jelikož právě podnikatelský subjekt byl zvolen autorkou práce. Konkrétně je v kapitole popsáno, jaká jsou práva subjektů údajů, jaké jsou povinnosti podnikatelského subjektu, tedy správce těchto údajů a také to, jaké postihy a pokuty správci údajů hrozí, pokud se výše zmiňovanými právy a povinnostmi nebude řídit.

Dále je v této kapitole představen již konkrétní podnik, společnost XY, která se nepřeje být jmenována. Zejména je nastíněna organizační struktura podniku, která je důležitá pro další kapitoly práce.

6. Analýza současné situace ve vybraném podniku v kontextu GDPR

Zdroje informací k praktické části práce

Jelikož autorka práce ve společnosti pracuje od jejího založení, informace k práci čerpala z interních zdrojů společnosti, ke kterým má přístup. Aby tyto informace mohly být použity, bylo požádáno o souhlas jednatele společnosti, se kterým byl v rámci získání informací k vypracování praktické části proveden také rozhovor, který bude v práci dále analyzován. Zároveň byl také se souhlasem majitele proveden dotazník mezi zaměstnanci společnosti mapující jejich znalost o problematice GDPR a spokojenost se způsobem, jakým je problematika GDPR ve společnosti řešena.

6.1 Mapování současného zpracovávání osobních údajů ve společnosti

Jak je zmíněno i v rozhovoru, který byl proveden s jednatelem společnosti a v práci je analyzován v následujících kapitolách, zaměstnanců, kteří pracují v provozovnách společnosti, se problematika zpracování osobních údajů přímo netýká. A to ve smyslu kontaktu se zákazníkem, který do provozovny přijde za účelem konzumace a obsluhujícímu personálu nepodává žádné osobní údaje.

U zbylých zaměstnanců byla provedena analýza, která se zaměřila na získání informací o tom, s jakými osobními údaji tito zaměstnanci přijdou do styku a jak s těmito údaji pracují.

Mzdová účetní – zejména zpracovává údaje zaměstnanců potřebné pro výpočet mezd a také odvod sociálního a zdravotního pojištění a daně z příjmu. Údaje o zaměstnancích jsou uloženy v osobních spisech zaměstnanců a dále také v softwaru, který je pro výpočet mezd využíván. Mezi údaje, které jsou pro tuto agentu potřebné, patří: jméno a příjmení, rodné číslo zaměstnance, datum narození, adresa, telefonní kontakt, číslo bankovního účtu, údaje o dětech a manželce nebo manželovi, které jsou potřebné pro výpočet zálohy na daň z příjmu a ročního zúčtování, dále pak údaje o zdravotním pojištění a údaje o odborné a zdravotní způsobilosti k výkonu zaměstnaní.

Účetní – pracuje zejména s osobními údaji dodavatelů, případně zákazníků. Osobní údaje zákazníků zpracovává pouze ve chvíli, pokud se jedná například o pořádání firemní akce, kde probíhá platba pomocí faktury, pro kterou jsou osobní údaje nezbytné.

Jedná se zejména o údaje, jako jsou jméno a příjmení, datum narození nebo identifikační číslo (IČ), dále daňové identifikační číslo (DIČ), adresa a číslo bankovního účtu. I tyto údaje jsou uloženy v ekonomickém softwaru, který je používán pro vytváření a ukládání faktur pro potřeby účetnictví a dále ve složkách, kde jsou faktury obsahující osobní údaje uloženy v papírové podobě.

Administrativní pracovnice – administrativní pracovnice má přístup k údajům zaměstnanců, které jsou v pracovních smlouvách zaměstnanců, jelikož má tyto smlouvy na starost, dále také zpracovává dokumenty potřebné pro výkon jejich práce, mezi které patří například zdravotní průkaz, který je nutný mít pro kontroly k dispozici a na kterém jsou údaje zaměstnanců jako jméno a příjmení, datum narození, číslo občanského průkazu a adresa bydliště, současně může dojít i k situaci, kdy je na požádání potřeba pomoci s fakturami dodavatelů, může tedy dojít k situaci, kdy má přístup i k údajům o dodavatelích nebo zákaznících tak, jak je zmiňováno výše.

Provozní zaměstnanec – provozní zaměstnanec má přístup k osobním údajům zaměstnanců, zejména potom k údajům potřebným pro výpočet prémií zaměstnanců a dále také k telefonním číslům zaměstnanců, které má uložené ve svém telefonu pro případ, že by bylo nutné s nimi komunikovat ohledně změn v rozpisu směn nebo akutní situace, kdy by bylo potřeba zaměstnance povolat do práce. Provozní zaměstnanec se také stará o nákup a objednávky zboží, má tedy přístup k osobním údajům dodavatelů a jejich zaměstnanců, jedná se o jméno a příjmení, adresu, identifikační číslo, telefonní kontakt, e-mail a číslo bankovního účtu. Informace má uloženy v e-mailu nebo na telefonu, popř. může nahlédnout do systému, který používá účetní ke zpracování faktur dodavatelů. Zároveň může přijít do styku i se zákazníky, kteří si v provozovně chtějí objednat firemní akci a podobně. V takovémto případě může přijít do kontaktu s osobními údaji zákazníků ve stejném rozsahu, jak v případě účetní. Provozní zaměstnanec má dále také přístup ke kamerovým záznamům, které ale může využít pouze za přítomnosti jednatele spolčenosti a pouze pokud je nezbytně nutné záznamy z kamerového systému použít.

Jednatel společnosti – jednatel společnosti má přístup ke všem údajům, ke kterým mají přístup výše zmiňovaní pracovníci. Sám jednatel může jednat s některými dodavateli nebo zákazníky a také nahlížet do údajů zaměstnanců.

6.2 Rozhovor s jednatelem společnosti

V této kapitole je dokumentován rozhovor, který proběhl mezi autorkou práce a jednatelem společnosti XY 23. 3. 2020. Tento strukturovaný rozhovor byl nezbytný pro analýzu současné situace v oblasti problematiky GDPR ve společnosti. Cílem tohoto rozhovoru bylo zejména analyzovat, jaké osobní údaje zaměstnanců jsou ve společnosti zpracovávány a jak je s těmito daty zaházeno. Dále také byly zodpovězeny otázky ohledně problematiky osobních údajů zákazníků. Jednotlivé odpovědi jsou dále v práci analyzovány a jsou použity k analýze rizik v oblasti GDPR.

- **Jaká osobní data svých zaměstnanců sbíráte a zpracováváte?** [1]
  Pokud se jedná o zaměstnance společnosti, zpracováváme zejména data obecného charakteru a organizační údaje. Všechny tyto údaje jsou zpracovávány zejména kvůli pracovním smlouvám a poté pro potřeby mzdové účetní. Zároveň částečně zpracováváme i citlivé údaje, jelikož každý zaměstnanec musí doložit potravinářský průkaz, což je potvrzení o tom, že je zdráv a může pracovat a přicházet do kontaktu s potravinami.
- **Máte stanoveny účely zpracování osobních údajů?**
  Společnost nedisponuje žádným dokumentem, který by stanovoval účely zpracování osobních údajů. Osobní údaje jsou zpracovávány zejména za účelem vytváření pracovních smluv zaměstnanců a mzdových výkazů. Osobní údaje dodavatelů a zákazníků pak za účelem vytváření faktur a pro potřeby účetnictví.
- **Využívá organizace při zpracování osobních dat zpracovatele?**
  Společnost si veškerá data zpracovává sama.
- **Jak jsou údaje zaměstnanců chráněny před zneužitím, ztrátou nebo nepovoleným přístupem?**
  Osobní údaje jsou uchovávány v jednotlivých složkách, které jsou uloženy ve skříních v kancelářích. Společnost si je vědoma toho, že údaje nejsou

[1](Například: Obecné údaje: jméno a příjmení, věk a datum narození, pohlaví, osobní stav, občanství, IP adresa, fotografie nebo jiný obrazový materiál, finanční údaje (čísla kreditních karet, bankovních účtů apod.). Organizační údaje: pracovní a osobní e-mailová adresa, pracovní nebo osobní mobilní telefon, pracovní a osobní adresa, číslo pasu a občanského průkazu, rodné číslo či jiné ověřovací a identifikační údaje. Citlivé údaje: rasa či etnický původ, náboženské, politické či filozofické vyznání, členství v odborech, sexuální orientace, zdravotní stav, trestní delikty či pravomocné odsouzení, genetické údaje (krevní rozbory, DNA profil, rentgenové snímky, důvěrné lékařské zprávy atd.), biometrické údaje (podpis, daktyloskopické údaje, snímky obličeje či jiných částí těla, hlasové záznamy apod.))

dostatečně chráněny před ztrátou nebo nepovoleným přístupem. Je to tedy něco, co je nutné zdokonalit.

- **Jaký typ souhlasu užíváte od jedinců před použitím údajů?**
  Všichni zaměstnanci před nástupem do pracovního poměru podepisují písemný souhlas se zpracováním osobních údajů, který je poté uchován v jejich složce společně s ostatními dokumenty.
- **Jak a kde osobní údaje zaměstnanců uchováváte?**
  Osobní údaje zaměstnanců jsou uchovány ve dvojí podobě. Ve fyzické, papírové formě se jedná o jednotlivé složky zaměstnanců, ale nejen jejich, i dodavatelů a zákazníků. Dále potom v počítačové podobě, kde jsou údaje uloženy v softwaru, který je pro jednotlivé úkony, ať už vytváření pracovních smluv nebo faktur a účetnictví používán.
- **Existuje v organizaci zaměstnanec, který má na starost pouze problematiku GDPR?**
  Takový zaměstnanec ve společnosti neexistuje. Naše administrativní pracovnice byla na problematiku GDPR školena v roce 2018 a pokud je tedy nějaký problém nebo někdo ohledně této problematiky potřebuje informace, obrací se právě na ni.
- **Máte vytvořenu sestavu interních směrnic za účelem ochrany osobních údajů? Kde jsou uloženy? Jak jsou zpřístupněny zaměstnancům a třetím stranám?**
  Společnost žádné takové směrnice vytvořené nemá. Pokud nastupuje nový zaměstnanec, všechny tyto informace jsou komunikovány pouze ústně. Stejně tak je to v případě, kdy má někdo ohledně této problematiky jakýkoliv dotaz. Toto vidím jako problémové, protože zaměstnanci by měli mít přístup k takovýmto informacím neustále, proto by bylo dobré takovýto manuál vytvořit a dát jej zaměstnancům k dispozici.
- **Jak často osobní údaje aktualizujete?**
  Osobní údaje jsou většinou aktualizovány na požádání konkrétního zaměstnance, u kterého se změnily. Je tedy zejména na zaměstnancích, aby takovéto změny hlásili. Žádné pravidelné kontroly neprobíhají.
- **Kdo všechno v organizaci má přístup k osobním údajům zaměstnanců?**
  K osobním údajům má přístup „vedení společnosti“. V našem případě se jedná o mě, jako jednatele společnosti, mzdovou účetní, účetní, administrativní

pracovnici a provozního zaměstnance, který je v přímém kontaktu se zaměstnanci, kteří pracují v jednotlivých provozech. Tito zaměstnanci k osobním údajům přístup nemají.

- **Jak jsou chráněny osobní údaje zákazníků?**

  V případě, kdy zákazník přijde do provozu, tedy restaurace, pouze za účelem konzumace, žádné osobní údaje personálu neposkytuje. K obsloužení zákazníka žádné takové údaje nejsou potřeba. Tedy v tomto případě nedochází k tomu, že by zákazník jakékoliv údaje poskytoval, a tedy ani není nutná ochrana. Jiná situace vzniká v případě, jedná-li se o zákazníka, který chce uspořádat v provozovně například firemní akci. Většinou se jedná o firmy, případně vedoucí pracovníky těchto firem. V tuto chvíli má personál povinnost takového zákazníka odkázat buď na provozního restaurace, nebo na administrativní pracovnici. Ti pak se zákazníkem domlouvají veškeré podrobnosti a v rámci toho pracují i s jeho osobními údaji, které jsou potřeba například pro vystavení faktury a podobně. V tomto případě jsou tedy osobní údaje chráněny tak, že k nim má přístup pouze omezené množství zaměstnanců.

- **V jednotlivých provozovnách společnosti je instalován kamerový systém, po jak dlouhou dobu jsou záznamy uchovávány? Uchovává se i zvukový záznam nebo je používán software pro porovnávání biometrických charakteristik subjektů?**

  Záznamy z kamerového systému jsou uchovávány po dobu sedmi dní, poté se automaticky přetáčejí. Kamerové záznamy zvuk nenahrávají a ve společnosti neexistuje ani žádný vámi výše zmiňovaný software. Všechny provozovny jsou patřičně označeny tak, aby i zákazník věděl, že se v nich kamerový systém nachází.

6.2.1 Analýza rozhovoru s jednatelem společnosti

Z rozhovoru s jednatelem společnosti je patrné, že společnost má dobré povědomí o tom, se kterými osobními údaji pracuje. Zároveň je také zřejmé, že je ve společnosti nastaven určitý systém v tom, kdo s jakými osobními údaji pracuje a z jakých důvodů jsou zpracovávány.

Na druhé straně je nutné zdůraznit, že problémová situace nastává v oblasti dokumentů, které by nějakým způsobem všechny postupy a informace o zpracování osobních údajů shrnovaly a byly dostupné zaměstnancům tak, aby měli přehled, jak tyto

procesy ve společnosti probíhají. Zároveň chybí manuál pro zaměstnance, kteří s údaji přímo pracují, který by obsahoval informace o tom, jak údaje chránit, jak s nimi pracovat a komu je za určitých podmínek poskytnout. Další problém autorka práce vidí v uchovávání osobních údajů zaměstnanců, dodavatelů a zákazníků. Tyto údaje nejsou dostatečně chráněny před zneužitím nebo ztrátou. I zde je tedy prostor pro zlepšení.

Rozhovor s jednatelem společnosti byl využit k analýze rizik, která bude provedena v následujících kapitolách.

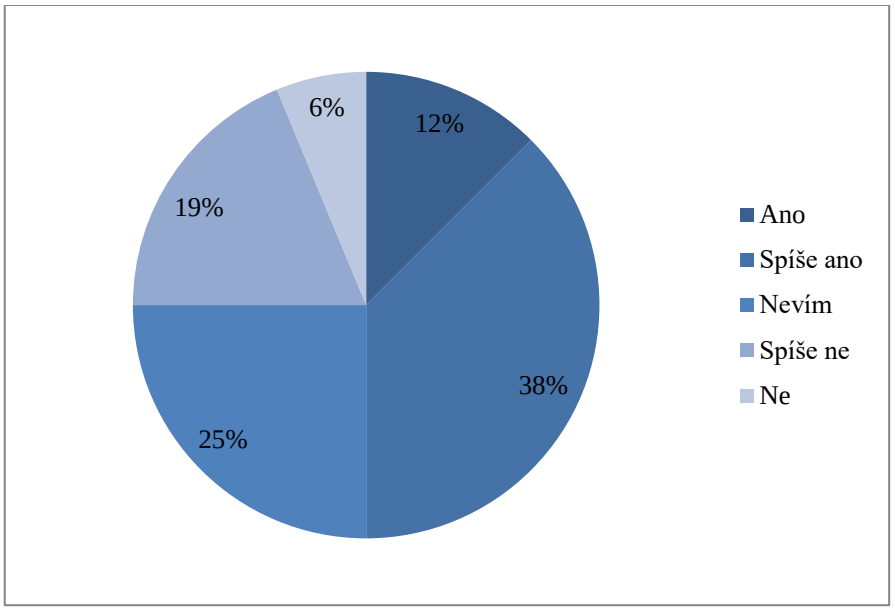
6.3 DOTAZNÍK PRO ZAMĚSTNANCE

V rámci získávání informací k vyhodnocení situace bylo ve společnosti provedeno dotazníkové šetření. Dotazníkové šetření probíhalo ve společnosti v týdnu 23. – 29. 3. 2020. Dotazník byl předložen k anonymnímu vyplnění všem 32 zaměstnancům společnosti a zaměřil se právě na hodnocenou problematiku GDPR. Cílem tohoto dotazníkového šetření bylo zjistit, jaké povědomí o této problematice zaměstnanci mají, zda mají pocit, že je s jejich osobními údaji zacházeno správně a bezpečně.

Níže na obrázcích 3–7 jsou vypracovány grafy, které znázorňují strukturu odpovědí u uzavřených otázek, na které odpovídali zaměstnanci pomocí Likertovy škály.

- **Myslíte si, že máte dobré znalosti o problematice GDPR?**

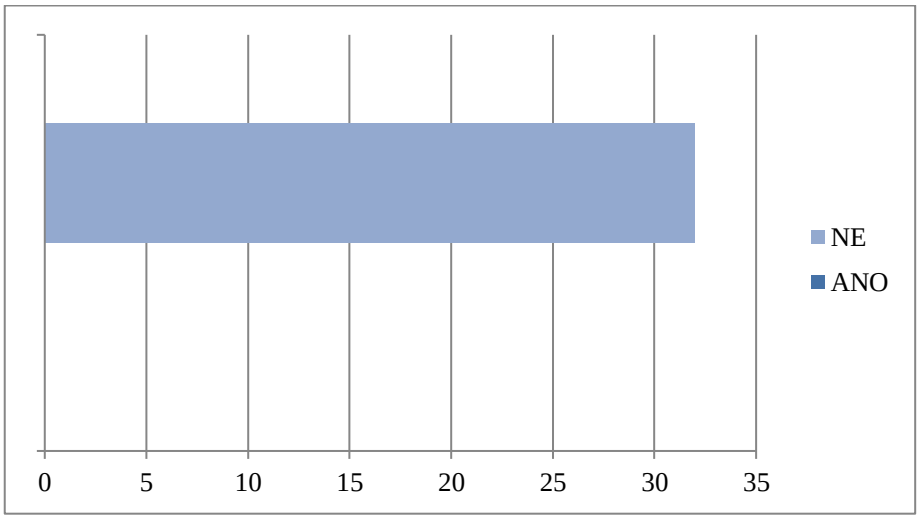
Obrázek 3: Vyhodnocení dotazníku – otázka č. 1



Zdroj: vlastní zpracování, 2020

- **Byla Vám při nástupu do práce k dispozici příručka shrnující informace ohledně GDPR?**[2]

Obrázek 4: Vyhodnocení dotazníku – otázka č. 2

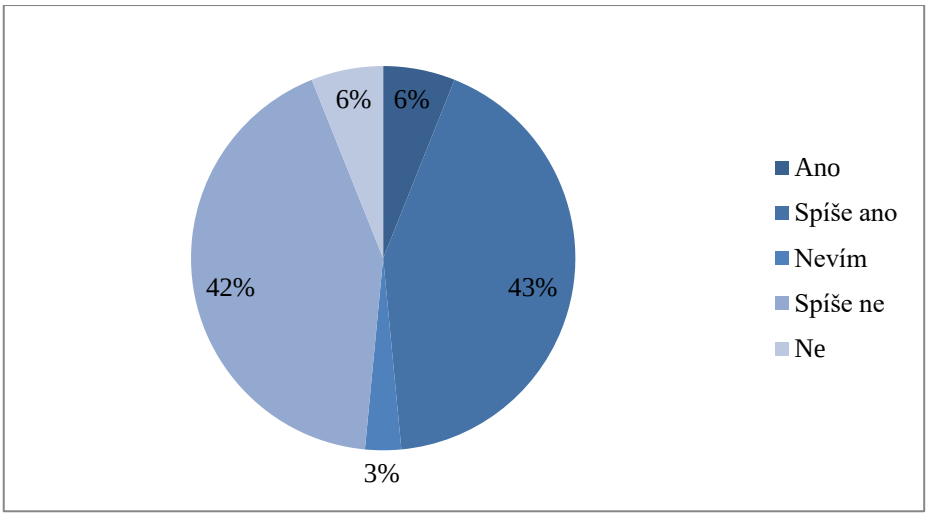


[2] Odpověď pouze ANO/NE

Zdroj: vlastní zpracování, 2020

- **Jste spojen/a se způsobem, jakým jste informován/a o tom, jak je s Vašimi osobními údaji pracováno?**

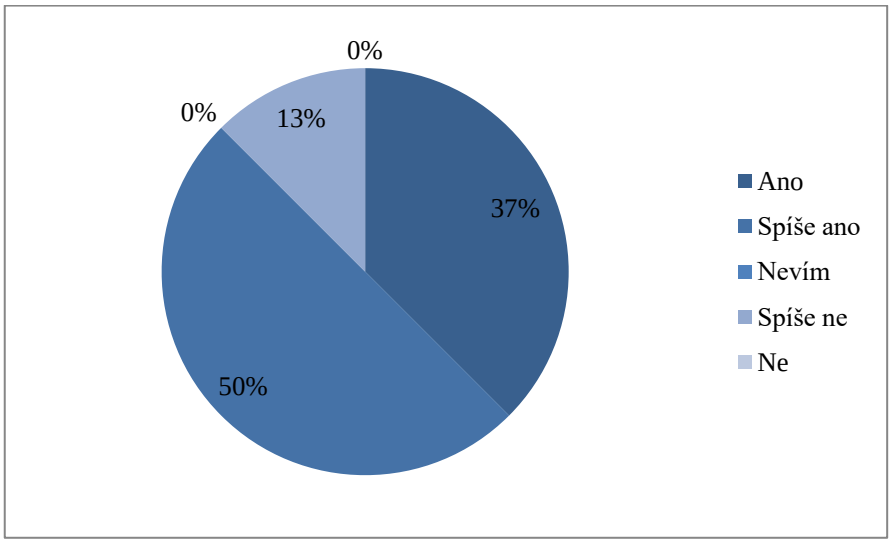
Obrázek5:Vyhodnocení dotazníku – otázka č. 3



Zdroj: vlastní zpracování, 2020

- **Máte pocit, že jsou u správce údajů, tedy zaměstnavatele Vaše údaje v bezpečí?**

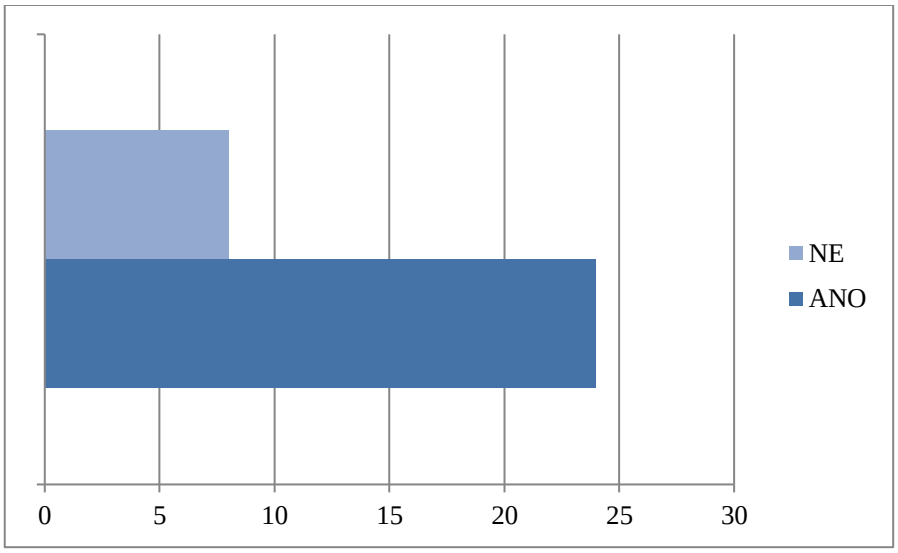
Obrázek6: Vyhodnocení dotazníku – otázka č. 4



Zdroj: vlastní zpracování, 2020

- **Měl/a byste zájem o školení v oblasti GDPR?**[3]

Obrázek7:Vyhodnocení dotazníku – otázka č. 5



Zdroj: vlastní zpracování, 2020

6.3.1 Analýza a hodnocení výsledků dotazníkového šetření

Z dotazníku, který byl předložen všem 32 zaměstnancům, je patrné že zaměstnanci si myslí, že mají dobré znalosti o problematice GDPR. Je ale poměrně těžké zhodnotit, do jaké míry se jedná pouze o subjektivní pocit jednotlivých zaměstnanců. Bohužel není možné zaměstnance podrobit testu, který by ukázal, jak jsou na tom s těmito znalostmi ve skutečnosti. Pro potřeby práce je tato odpověď dostačující v kontextu odpovědí na poslední otázku dotazníku, kdy bylo zjišťováno, zda by zaměstnanci měli zájem o školení v této oblasti. Z grafu vyplývá, že většina zaměstnanců by zájem měla.

Co se týká ochrany osobních údajů zaměstnanců, mají dotázaní pocit, že jsou jejich údaje chráněny dostatečně. Což ukazuje, že v podstatě důvěřují svému zaměstnavateli. Přesto existuje několik jedinců, kteří mají pocit, že by jejich data měla být chráněna lépe.

V čem vidí autorka práce největší problém, který z provedeného dotazování vyplývá? Je to fakt, že zaměstnanci mají pocit, že nejsou dostatečně informování o tom,

[3] Odpověď pouze ANO/NE

jak je s jejich daty pracováno. S tímto problémem souvisí i zjištění, že ani jeden zaměstnanec neodpověděl kladně na otázku, zda byl při nástupu do práce seznámen s konkrétním manuálem, který by tuto problematiku upravoval.

6.4 SHRNUTÍ KAPITOLY

V této kapitole již dochází k analýze současné situace, která je velice důležitá, jelikož na základě této analýzy bude dále docházet k hodnocení celkové situace a poté k návrhům na možná zlepšení. V kapitole je nejprve mapována současná situace práce s osobními údaji. Je tedy upřesněno, kdo jaké údaje a jak zpracovává. Poté je v této kapitole přepsán rozhovor s jednatelem společnosti, kde se autorka práce zajímá zejména o to, jaké osobní údaje jsou ve společnosti zpracovávány, jak jsou tyto údaje archivovány a chráněny. Nejprve se jedná o údaje zaměstnanců společnosti a poté o osobní údaje zákazníků společnosti.

Další částí této práce je analýza dotazníkového šetření, které bylo provedeno ve společnosti a zúčastnili se jej všichni zaměstnanci. Na grafech jsou znázorněny výsledky šetření, které jsou poté jedním ze zdrojů pro následné zhodnocení současné situace.

7. HODNOCENÍ SITUACE A NÁVRH MOŽNÝCH ZLEPŠENÍ V OBLASTI GDPR

7.1 HODNOCENÍ SOUČASNÉ SITUACE A ANALÝZA RIZIK

Správce osobních údajů je povinen osobní údaje adekvátně zabezpečit proti jejich zneužití. Pokud chceme analyzovat a hodnotit rizika spojená se zneužitím údajů, je podstatné vycházet z toho, kde jsou údaje uloženy a kdo má k těmto údajům přístup. Zejména pro tyto účely byl zmapován systém současného zpracování osobních údajů, který se nachází výše.

Data, která jsou zpracovávána pomocí softwaru, jsou uložena na serveru společnosti. Tento server je v uzamčené místnosti, ke které mají přístup všichni zaměstnanci, kteří s daty přicházejí do kontaktu. Tento server by měl být dostatečně zabezpečen proti zničení dat nebo riziku vnějšího napadení. Data jsou dále zaměstnancům zpřístupněna pomocí jejich počítačů. Většina zaměstnanců má tyto počítače chráněny přístupovým heslem. Problémem ale je, že společnost nedisponuje vnitřním předpisem nebo směrnicí, která by se zabývala způsoby, jakými je potřeba data zabezpečit. V současné době tedy společnost spoléhá na úsudek svých zaměstnanců o podobě konkrétních opatření v oblasti zabezpečení počítačů, případně mobilních telefonů.

Veškeré osobní údaje ve fyzické podobě, ať už se jedná o údaje o zaměstnancích, dodavatelích nebo zákaznících, jsou uloženy ve skříních, které se nacházejí v prostoru kanceláří. V případě údajů o dodavatelích a zaměstnancích se jedná o kancelář, ve které pracuje zejména mzdová účetní a účetní. V případě smluv zaměstnanců a ostatních dokumentů, které jsou potřebné pro výkon práce, se jedná o kanceláře v jednotlivých provozovnách. Dokumenty se nenacházejí v uzamčených skříních a přístup k nim má tedy každý, kdo má klíče od těchto kanceláří.

V případě kanceláře pro účetní se jedná o obě účetní pracovnice, administrativní pracovnici, provozního pracovníka a jednatele společnosti. V případě ostatních kanceláří je situace taková, že v některých provozovnách slouží část kanceláří zároveň také jako skladový prostor pro zboží, ke kterému musí mít přístup zaměstnanci pracující v provozovnách. Tím vzniká riziko, neboť zaměstnanci, kteří by k těmto údajům přístup neměli mít, jej mají. Zároveň není dostatečně hlídáno, zda zaměstnanci dodržují svou povinnost, tyto kanceláře zamykat. Zde tedy může být riziko velmi vysoké.

Autorka práce má dojem, že celkové zpracování osobních údajů je poměrně chaotické. Tento dojem budí zejména skutečnost, že ze všech provedených analýz vyplývá, že ke zpracovávaným osobním údajům má přístup v podstatě kdokoliv, kdo ve společnosti pracuje. Složky, ve kterých se osobní údaje nacházejí ve fyzické podobě, nejsou dostatečně chráněny.

Kladně autorka hodnotí nástroje, které jsou pro zpracování dat používány, zejména softwary, se kterými zaměstnanci pracují a server, který data zpracovává. Jedná se o kvalitní produkty, které v sobě mají zabudovány prvky ochrany osobních údajů. Zároveň také není nutné se zabývat kamerovým systémem, který je v provozovnách nainstalován, jelikož je, jak vyplývá z rozhovoru s jednatelem společnosti, přístupný pouze v počítači, který je chráněn heslem a přístup k němu má pouze provozní pracovník za přítomnosti jednatele společnosti. Kamerový systém automaticky přehrává záznamy aktuálnějšími, tudíž data nejsou nikde uchovávána.

Dobré je také zmínit, že společnost od většiny svých zákazníků nezískává žádné osobní údaje. Jelikož nejsou pro poskytnutí služeb třeba. Proto nejsou pro potřeby této analýzy tyto informace podstatné i přesto, že je na ně jednatel společnosti v rozhovoru dotazován. Samotná otázka ale důležitá byla, jelikož jednorázových zákazníků má společnost nejvíce, bylo tedy potřeba analyzovat, zda v tomto případě mohou hrozit nějaká rizika.

7.2 Návrhy možných zlepšení současné situace

7.2.1 Zabezpečení osobních údajů

Jak vyplývá z teoretické části a z kapitoly, která se specificky zaměřuje na technická opatření k zajištění ochrany osobních údajů, je nezbytné, aby písemnosti byly uchovány v uzamykatelných místnostech a uzamykatelných skříních. Z analýzy současné situace je patrné, že místnosti uzamykatelné jsou, ale klíče k těmto místnostem, tedy kancelářím, má většina zaměstnanců. Proto je nezbytné zajistit, aby byli skříně uzamykatelné. Klíče od těchto skříní by měli mít mimo jednatele společnosti pouze ti zaměstnanci, kteří potřebují mít k těmto údajům přístup. V případě údajů, které souvisejí se zpracováním mezd, by měla mít tyto klíče pouze mzdová účetní. Pokud se jedná o smlouvy zaměstnanců, smlouvy s dodavateli a zákazníky a fakturační údaje, v tomto případě musí mít k těmto údajům přístup i účetní, administrativní pracovnice a provozní zaměstnanec. Tímto opatřením bude zamezeno přístupu k těmto údajům pro

ostatní zaměstnance. Díky tomu bude jednodušší chránit údaje před zneužitím a také před ztrátou.

Elektronické datové soubory jsou, jak vyplývá z analýzy, v tuto chvíli také přístupné veškerému vedoucímu personálu bez výjimky. Jednou z možností, jak tyto soubory ochránit a zároveň mít přehled o tom, kdo do dokumentů nahlížel, je nastavit přístup k těmto údajům doménovým jménem. Z analýzy není patrné, zda dochází k pravidelnému zálohování těchto dat, proto by bylo vhodné data zálohovat. Dle získaných informací ohledně softwarů, které jsou ve firmě používány, je patrné, že tyto softwary určitou ochranu údajů mají v sobě zabudovanou, zde tedy autorka žádný problém nenachází.

7.2.2 MANUÁLY A VNITŘNÍ SMĚRNICE

Kde vidí autorka práce velký problém a nedostatek, to je oblast manuálů a směrnic, které by sloužily zaprvé jako návod pro zaměstnance, kteří s daty pracují a zadruhé pro ně byly jakousi příručkou obsahující informace o tom, kdo a jak s jejich daty pracuje.

Proto je nezbytné vytvořit manuál, ve kterém bude uvedeno, s jakými osobními údaji se pracuje a kdo konkrétní s nimi pracuje, a tedy k nim má přístup. Zároveň by tento manuál měl uvádět nezbytná opatření, která je nutné dodržovat v zájmu ochrany osobních údajů. Mezi tato opatření patří zejména ochrana počítačů zaměstnanců pomocí hesla, ochrana telefonu, ve kterém jsou údaje uloženy a také upozornění, že by zaměstnanec pracovní počítač neměl využívat k jiným než pracovním účelům tak, aby se eliminovalo riziko ztráty, poškození nebo odcizení těchto dat.

Dále by měla být vytvořena specifická příručka pro zaměstnance, která by popisovala, jak je s osobními údaji zaměstnanců pracováno, k čemu se používají a jak jsou chráněny a ukládány. Ze zpracované teorie dále vyplývá, že je nezbytné, aby bylo uvedeno, jaké kategorie údajů jsou zpracovávány, kdo jsou příjemci těchto údajů, po jak dlouhou dobu budou údaje uloženy a jestli má zaměstnanec právo na výmaz nebo opravu. Součástí této příručky by také měla být informace o pravidelné aktualizaci osobních údajů, která by zajistila, že osobní údaje zaměstnanců jsou správné. Společnost se v současné době spoléhá pouze na to, že zaměstnanci sami ohlásí, pokud dojde ke změně některého z osobních údajů, k čemuž ne vždy musí dojít. Zároveň jak vyplynulo z dotazníku, který zaměstnanci vyplňovali, řada z nich o skutečnosti, že by

měli své osobní údaje aktualizovat, ani nevěděla. Automatickým aktualizováním minimálně jednou ročně by se těmto nesrovnalostem předešlo.

Správce osobních údajů je povinen vést záznamy o činnostech, které se zpracováním osobních údajů souvisejí. Zaměstnanci společnosti, kteří s těmito údaji pracují, jsou schopni teoreticky tyto činnosti popsat, i přesto by měl vzniknout záznam, který by obsahoval především jméno a kontaktní údaje správce, dále účely zpracování těchto údajů a plánované lhůty pro výmaz. Problematika lhůt výmazu těchto údajů je v tomto případě poměrně komplikovaná, jelikož k výmazu údajů by mělo dojít ve chvíli, kdy bude například ukončen pracovní poměr s konkrétním zaměstnancem, kterého se údaje týkají nebo obchodní vztah s dodavatelem, se kterým společnost spolupracuje. Proto by tyto lhůty měly být uvedeny alespoň takto rámcově, tedy v tom smyslu, že výmaz dat je závislých na těchto výše zmiňovaných situacích. V případě zákazníka, který využívá služby společnosti, by k výmazu dat mělo dojít ve chvíli, kdy již proběhla domluvená služba a byla i fakturována, a tedy tyto údaje již nejsou potřebné.

7.2.3 Školení zaměstnanců

Z provedené analýzy je patrné, že jediný zaměstnanec, který byl ve společnosti na problematiku GDPR vyškolen je administrativní pracovnice, která slouží jako poradce pro ostatní zaměstnance, pokud si s něčím v této oblasti nevědí rady. Jelikož zájem o školení projevila dle dotazníku i určitá část zaměstnanců, autorka by navrhovala společnosti toto školení zajistit. Díky provedenému školení dojde k zastupitelnosti administrativní pracovnice. Zaměstnanci získají větší povědomí o důležitosti chránění osobních údajů a je tedy pravděpodobné, že na jejich ochranu budou také více dbát. U zaměstnanců, kteří s osobními údaji přímo nepracují, ale přesto mají zájem o školení, muže mít toto školení přínos v tom, že se více v problematice vzdělají a budou mít přehled o tom, jak by mělo být s jejich daty pracováno, že by měla být aktualizována a že je nutné je chránit.

7.3 Finanční požadavky na návrhy zlepšení

Z návrhů zlepšení je patrné, že nejdůležitějším úkolem je vytvořit manuály pro problematiku GDPR: Autorka práce navrhuje pro tyto účely najmout externího pracovníka, který by tyto manuály vypracoval tak, aby byly v požadovaném rozsahu a kvalitě. Zároveň využitím externího zdroje nebude společnost zatěžovat současné zaměstnance. Dle dostupných informací na stránkách společnosti Sensio, která se mimo

jiné zabývá zpracováním těchto dokumentů pro společnosti, vypracování požadovaného manuálu stojí 14 250,- Kč. Cena je uvedena za veškeré dokumenty, tedy metodické pokyny, vnitřní směrnice na ochranu osobních údajů, informované souhlasy pro zaměstnance a návrhy smluv s externími dodavateli. Současně autorka navrhuje využít i služby auditora přímo ve společnosti, jedná se o osobní konzultaci, při které budou ujasněny požadavky na zpracování těchto dokumentů. Dle dostupného ceníku je cena této konzultace 7 260,- Kč. (Ceník GDPR, 2020)

Výše zmiňovaná společnost nabízí také možnost školení. Je patrné, že o školení zaměstnanci zájem projevili. Autorka práce se domnívá, že je logické pro školení vybrat stejnou firmu, která dokumenty zpracovává. A to s ohledem na předpoklad, že bude schopna vše vysvětlit právě na tomto konkrétním příkladu a zároveň zaměstnance se všemi dokumenty velmi podrobně seznámit. Cena školení uvedena za jednoho zaměstnance je 423,50,- Kč.

V rámci lepšího zabezpečení je nutné zajistit možnost zamykat skříně, ve kterých se dokumenty obsahující osobní údaje nacházejí. Díky tomu, že autorka práce ve společnosti pracuje, ví, jak tyto skříně vypadají a že je naprosto dostačující koupit klasické visací zámky, které splní účel. V průměru jeden takovýto zámek stojí 150,- Kč.

Celková kalkulace všech výše zmíněných nákladů je přehledně zpracována v tabulce 2.

Tabulka 2: Kalkulace nákladů

Produkt	Cena
Zpracování požadovaných dokumentů	14250 Kč
Návštěva auditora	7260 Kč
Školení zaměstnanců	24 x 423,50 = 10164 Kč
Nákup visacích zámků	10 x 150 = 1500 Kč
Celkem	**33174,-**

Zdroj: vlastní zpracování, 2020

Z výpočtů je patrné, že celkové náklady na požadovaná zlepšení jsou ve výši 33 174,- Kč. Aby částka nezasáhla razantním způsobem do měsíčního rozpočtu společnosti, navrhuje autorka využít služby auditorské firmy ve dvou etapách. Nejprve by proběhla osobní návštěva a konzultace s auditorem, až následně by proběhlo školení.

Pokud by i tak byly náklady příliš vysoké, školení je možné provést ve dvou termínech s menším počtem zaměstnanců, a tedy i menšími náklady.

7.4 PŘÍNOSY PRÁCE

Aby bylo možné zpracovat praktickou část práce, tedy provést analýzu současné situace v oblasti GDPR ve vybrané společnosti XY, bylo nejprve nutné vypracovat teoretickou část práce. Přínos teoretické části, tedy zpracování problematiky GDPR, pojmenování základních úkolů a kritérií a vysvětlení některých důležitých pojmů, vidí autorka práce zejména v tom, že umožňuje lepší pochopení celé problematiky. Zároveň jsou tyto znalosti v práci také aplikovány konkrétněji při popisu zavádění GDPR do činnosti podnikatelských subjektů. Tento popis je využíván při hodnocení analýzy, která je součásti praktické části práce.

Hlavním přínosem celé práce je dle autorky tedy zejména analýza, hodnocení a navržení možných zlepšení pro společnost XY. Díky analýze, která ve společnosti proběhla za pomoci rozhovoru s jednatelem společnosti a dotazníkového šetření, bylo možné definovat rizikové oblasti v souvislosti s problematikou GDPR. Na základě těchto rizikových oblastí jsou i za pomoci poznatků získaných z teoretické části práce v poslední kapitole práce formulovány návrhy, které mohou vést ke zlepšení současné situace. Jelikož se jedná o poměrně malou společnost, bylo nutné uvést v souvislosti s návrhy i jejich finanční náročnost. Ta je upravena tak, aby co možná nejméně zatížila měsíční rozpočet společnosti a bylo tak možné jednotlivé procesy zrealizovat.

ZÁVĚR

Zpracovaná diplomová práce se zabývá problematikou GDPR a poté hodnotí situaci ve vybraném ekonomickém subjektu.

První stanoveným cílem bylo teoreticky popsat tuto problematiku a vysvětlit všechny pojmy, které s ní souvisejí. V prvních kapitolách práce proto dochází k popsání historického kontextu problematiky GDPR. Jsou vysvětleny základy ochrany osobních údajů a definovány tři pilíře, na kterých stojí cíle GDPR. Aby bylo možné lépe popsat, proč bylo přijetí nového nařízení v této oblasti tolik potřebné, dochází v této části práce také ke srovnání původní právní úpravy problematiky s touto novou.

V další teoretické části práce jsou popsány základní úkoly a kritéria GDPR. Základní úkoly jsou popsány v souvislosti s tím, na koho se nařízení o ochraně osobních údajů vztahuje a jak může dát subjekt, jehož osobní údaje se zpracovávají, svůj souhlas k tomuto zpracování. Kritéria GDPR jsou v této kapitole rozdělena do dvou částí. V první jsou popsána práva subjektů osobních údajů. Tato práva musí správce osobních údajů respektovat, jelikož jsou pro subjekt zárukou, že s jeho osobními údaji bude pracování bezpečně a ohleduplně. Tato práva dávají subjektu údajů také možnost své osobní údaje měnit, upravovat, či požádat správce o jejich výmaz, pokud k tomu subjekt má zákonný důvod. Jako druhé jsou popsány zásady GDPR. Tyto zásady jsou klíčové, jelikož definují veškeré povinnosti, které z nařízení vyplývají.

Poslední kapitolou teoretické části práce je pak vysvětlení pojmů, které jsou pro pochopení problematiky GDPR zásadní. Jedná se zejména o vysvětlení pojmů osobní údaj, správce a zpracovatel osobních údajů. V kapitole je vysvětleno, co se za osobní údaj považuje a jsou zmíněna úskalí, která mohou v oblasti definování osobních údajů nastat. Konkrétně v případě rodného čísla, které není přímo považováno za citlivý údaj, ale i přesto se na ně vztahují zákonem stanovené podmínky využití. Dále občanský průkaz, jelikož se jedná o dokument, který obsahuje množství údajů, které je možno zneužít například pro krádež identity. V souvislosti s tím jsou v této kapitole zmíněny obecné možnosti ochrany osobních údajů. V poslední části je vysvětlen institut správce a zpracovatele osobních dat a jsou definována jejich práva a povinnosti.

V praktické části práce nejprve dochází k implementaci poznatků získaných ze studia, které bylo provedeno k zpracování teoretické části, na konkrétní skupinu správců osobních údajů – podnikatelských subjektů, jelikož autorka si pro zpracování

praktické části práce vybrala právě podnikatelský subjekt. Jsou konkrétně vymezena práva a povinnosti v oblasti GDPR u těchto subjektů a také jsou zpracovány postihy, které hrozí za jejich nedodržení. Současně dochází k představení vybraného ekonomického subjektu a nastínění zejména organizační struktury, která je důležitá pro další kapitoly práce.

V následující kapitole práce analyzuje současnou situaci související s problematikou GDPR ve vybrané subjektu. Tato analýza je provedena nejprve za pomoci popisu osobních údajů, které jsou zpracovávány na konkrétních pozicích ve společnosti a je také uvedeno, jak jsou tyto údaje zpracovávány. Další metodou, která je použita pro analýzu je rozhovor, který autorka práce vedla s jednatelem společnosti. V rozhovoru jsou otázky zaměřené právě na kategorie osobních údajů, které jsou ve společnosti zpracovávány. Dále na způsob, jak jsou tyto údaje zpracovávány, jak jsou chráněny a kdo k nim má přístup. Dalším tématem rozhovoru jsou dokumenty, které by ve společnosti problematiku GDPR definovaly, nastavovaly by v této oblasti pravidla a informovaly zaměstnance o všem důležitém, co se zpracováním jejich osobních údajů souvisí. Poslední částí analýzy je vyhodnocení dotazníkového šetření, které bylo ve společnosti provedeno, a účastnili se jej anonymně všichni zaměstnanci.

Poslední kapitola praktické části diplomové práce hodnotí poznatky, které byly získány z předešlé kapitoly. Zaměřuje se zejména na rizika, která z analýzy a následného zhodnocení vyplývají. Tato rizika jsou v kapitole definována. Z hodnocení rizik vyplynulo, že největším problémem je způsob, jakým jsou data uchovávána a jak jsou o celém procesu zpracování osobních údajů informováni zaměstnanci. Na základě těchto definic jsou pak navrženy kroky, které by bylo vhodné implementovat v kontextu žádoucího zlepšení situace.

Vypracovaná diplomová práce je zejména přínosná pro společnost XY, a to díky tomu, že praktická část je zpracována tak, aby byla využitelná pro jednatele společnosti. Na základě analýzy, definování rizik a zhodnocení současné situace v oblasti problematiky GDPR ve společnosti, jsou navrhnuty výše zmíněné kroky, mezi které patří zavedení větší ochrany dat, zhotovení směrnic a postupů, jak s daty pracovat, vypracování příručky pro zaměstnance, aby i oni měli přehled o tom, jak je s daty pracováno a návrh na provedení školení v oblasti problematiky GDPR. Ke všem těmto krokům je také vypracována analýza jejich finanční náročnosti. Díky tomu může jednatel společnost sám

zhodnotit, pokud by se rozhodl pro implementaci postupů, které jsou v této práci navržené, zda jsou pro něj realizovatelné, či nikoli.

SEZNAM POUŽITÝCH ZDROJŮ

Bartík V., & Janečková. E. (2012). Ochrana osobních údajů z pohledu zvláštních právních úprav k 1. 8. 2012. Olomouc, Česko: ANAG

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

Burri, M., & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy, 6*, 479-511. doi:10.5325/jinfopoli.6.2016.0479

Calder, A. (2017). *EU GDPR: A Pocket Guide (European)*. (2. vyd.) Cambridgeshire, United Kingdom: IT Governance Publishing.

Calder, A. (2018). *EU GDPR: A Pocket Guide, School's edition*. Cambridgeshire, United Kingdom: IT Governance Publishing.

Ceník GDPR (2020). Dostupné 22. 4. 2020 z: https://www.izus.cz/gdpr/ke_stazeni/Cenik_GDPR_Sensio.pdf

Denley, A., & kol. (2019). *GDPR: How to Achieve and Maintain Compliance*. Routledge, New York, USA: Taylor & Francis Group.

Drożdż, A. (2020). *Protection of natural persons with regard to automated individual decision making in the GDPR.* Netherlands, Alphen aan den Rijn: Kluwer law internetional.

Foulsham, M., & Hitchen, B., (2018) *GDPR: Guiding Your Business to Compliance: How the NewData Protection Regulation Affect You*. (2. vyd.). Independently Published

Gawronski, M. (2019). *Guide to the Gdpr*. Netherlands, Alphen aan den Rijn: Kluwer Law International B.V.

IT Governance Privacy Team. (2019). *Eu General Data Protection Regulation (Gdpr)* (3. vyd.). Cambridgeshire, United Kingdom: IT Governance Publishing.

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

Janotová, M. (2018). *Ochrana osobních údajů podle GDPR*. Materiál pro účastníky školení pořádaného Integra Centrum v Brně.

Klosek. J. (2000). *Data privacy in the information age*. Westport, USA: Quorum Books

Krzysztofek, M. (2019). *GDPR: General Data Protection Regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*. Netherlands, Alphen aan den Rijn: Kluwer law internetional

Nařízení Evropského parlamentu a Rady Evropské Unie 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ao zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Navrátil, J. (2018). *GDPR pro praxi*. Plzeň, Česko: Vydavatelství a nakladatelství Aleš Čeněk.

Nezmar, L. (2017). *GDPR: praktický průvodce implementací*. Praha, Česko: Grada Publishing.

Nulíček M., & kol. (2018). *GDPR: obecné nařízení o ochraně osobních údajů*. Praha, Česko: Wolters Kluwer.

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

Sharma, S. (2020). *Data Privacy and GDPR Handbook*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Six privacy principles for General Data Protection Regulation compliance (2020). Dostupné 25.4. 2020 z: https://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance

Stanovisko č. 3/2016 Evidence návštěvníků při vstupech do budov a kopírování dokladů, vydal: Úřad pro ochranu osobních údajů

Todt, K. (2019). Data Privacy and Protection: What Businesses Should Do. *The Cyber Defense Review, 4*(2), 39-46. doi:10.2307/26843891

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): a Practical Guide*. Cham, Switzerland: Springer International Publishing.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. doi:10.2307/1321160

Základní příručka k ochraně osobních údajů (2020) Dostupné 22. 4. 2020 z: https://www.uoou.cz/zakladni-prirucka/ds-4744/archiv=1&p1=1061

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

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

Zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů

Žůrek, J. (2018). *Praktický průvodce GDPR: včetně úplného znění GDPR*. (2. vyd.). Olomouc, Česko: ANAG.

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha č. 1: Strukturovaný rozhovor s jednatelem společnosti XY

Otázky pro strukturovaný rozhovor s jednatelem společnosti

1. Jaká osobní data svých zaměstnanců sbíráte a zpracováváte?
   (Například: Obecné údaje: jméno a příjmení, věk a datum narození, pohlaví, osobní stav, občanství, IP adresa, fotografie nebo jiný obrazový materiál, finanční údaje (čísla kreditních karet, bankovních účtů apod.). Organizační údaje: pracovní a osobní e-mailová adresa, pracovní nebo osobní mobilní telefon, pracovní a osobní adresa, číslo pasu a občanského průkazu, rodné číslo či jiné ověřovací a identifikační údaje. Citlivé údaje: rasa či etnický původ, náboženské, politické či filozofické vyznání, členství v odborech, sexuální orientace, zdravotní stav, trestní delikty či pravomocné odsouzení, genetické údaje (krevní rozbory, DNA profil, rentgenové snímky, důvěrné lékařské zprávy atd.), biometrické údaje (podpis, daktyloskopické údaje, snímky obličeje či jiných částí těla, hlasové záznamy apod.))
2. Máte stanoveny účely zpracování osobních údajů?
3. Využívá organizace při zpracování osobních dat zpracovatele?
4. Jak jsou údaje zaměstnanců chráněny před zneužitím, ztrátě nebo nepovolenému přístupu?
5. Jaký typ souhlasu užíváte od jedinců před použitím údajů?
6. Jak a kde osobní údaje zaměstnanců uchováváte?
7. Existuje v organizaci zaměstnanec, který má na starost pouze problematiku GDPR?
8. Máte vytvořenu sestavu interních směrnic za účelem ochrany osobních údajů? Kde jsou uloženy? Jak jsou zpřístupněny zaměstnancům a třetím stranám?
9. Jak často osobní údaje aktualizujete?
10. Kdo všechno v organizaci má přístup k osobním údajům zaměstnanců?
11. Jak jsou chráněny osobní údaje zákazníků?
12. V jednotlivých provozovnách společnosti je instalován kamerový systém, po jak dlouhou dobu jsou záznamy uchovávány? Uchovává se i zvukový záznam nebo je používán software pro porovnávání biometrických charakteristik subjektů?

Příloha č. 2: Dotazník pro zaměstnance společnosti XY

Dotazník pro zaměstnance společnosti

Anonymní dotazník slouží k analýze v rámci diplomové práce na téma „*General Data Protection Regulation ve vybraném ekonomické subjektu*", kterou zpracovává Zuzana Stará.

U každé otázky prosím zakroužkujte nejvhodnější odpověď podle míry souhlasu.

1 – Ano

2 – Spíše ano

3 – Nevím

4 – Spíše ne

5 - Ne

V případě otázek s odpovědí ANO/NE používejte prosím pouze 1 nebo 5.

Děkuji za Váš čas.

1. Myslíte si, že máte dobré znalosti o problematice GDPR?

   1 ○ 2 ○ 3 ○ 4 ○ 5 ○

2. Byla Vám při nástupu do práce k dispozici příručka shrnující informace ohledně GDPR? (ANO/NE)

   1 ○ 2 ○ 3 ○ 4 ○ 5 ○

3. Jste spojen/a se způsobem, jakým jste informován/a o tom, jak je s Vašimi osobními údaji pracováno?

   1 ○ 2 ○ 3 ○ 4 ○ 5 ○

4. Máte pocit, že jsou u správce údajů, tedy zaměstnavatele Vaše údaje v bezpečí?

   1 ○ 2 ○ 3 ○ 4 ○ 5 ○

5. Měl/a byste zájem o školení v oblasti GDPR? (ANO/NE)

   1 ○ 2 ○ 3 ○ 4 ○ 5 ○

ABSTRAKT

Stará, Z. (2020). *Problematika General Data ProtectionRegulation ve vybraném ekonomickém subjektu*. (Diplomová práce), Západočeská univerzita v Plzni. Fakulta ekonomická. Předložená práce je zaměřena na problematiku ochrany osobních údajů. Zejména se zabývá nařízením o ochraně osobních údajů v souvislosti s vybraným ekonomickým subjektem. Práce nejprve teoreticky vysvětluje obecnou problematiku ochrany osobních údajů a nařízení Evropské Unie, které tuto problematiku upravuje, tedy General Data Protection Regulation. Na základě poznatků získaných v teoretické části práce je ve zvoleném ekonomickém subjektu provedena analýza implementace GDPR. Tato analýza slouží ke zhodnocení situace v subjektu a navržení možných změn a zlepšení.

Klíčová slova

General Data Protection Regulation (GDPR), osobní údaj, podnikatelský subjekt

ABSTRACT

Stará, Z. (2020) *The issue of General Data Protection Regulation in selected economic entity.* (Master's Thesis). University of West Bohemia in Pilsen. Faculty of Economics. The presented work is focused on the issue of personal data protection. In particular, it deals with the regulation on the protection of personal data in relation to a selected economic operator. The thesis first theoretically explains the general issues of personal data protection and the European Union regulations that regulate this issue - the General Data Protection Regulation. Based on the knowledge gained in the theoretical part of the work, an analysis of the implementation of GDPR is performed in the selected economic entity. This analysis serves to evaluate the situation in the subject and to suggest possible changes and improvements.

Key Words

General Data Protection Regulation (GDPR), personal data, business subject