VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

OCHRANA OSOBNÍCH ÚDAJŮ VE SPOLEČNOSTI

PERSONAL DATA PROTECTION IN THE COMPANY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Eliška Václavková
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Dydowicz, Ph.D.
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Eliška Václavková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Petr Dydowicz, Ph.D.**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Ochrana osobních údajů ve společnosti

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrh řešení, přínos práce
Závěr

Cíle, kterých má být dosaženo:

Posouzení současné ochrany osobních údajů ve společnosti a návrh změn pro efektivnější splnění Evropského nařízení General data protection regulation (GDPR).

Základní literární prameny:

BASL, J. a R. BLAŽÍČEK. Podnikové informační systémy. Podnik v informační společnosti. Praha: Grada, 2008. 283 s. ISBN 978-80-247-2279-5.

MOLNÁR, Z. Automatizované informační systémy. Praha: Strojní fakulta ČVUT, 2000. 126 s. ISBN 80-01-02269-2.

MOLNÁR, Z. Efektivnost informačních systémů. Praha: Grada Publishing, 2000. 142 s. ISBN 80-716--410-X.

PECINOVSKÝ, R. Myslíme objektově v jazyku Java: kompletní učebnice pro začátečníky. Praha: Grada, 2009. 570 s. ISBN 978-80-247-2653-3.

SODOMKA, P. a H. KLČOVÁ. Informační systémy v podnikové praxi. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato práce se zaměřuje na popis ochrany osobních údajů ve firmě. Obsahuje vysvětlení pojmů spojených s ochranou osobních údajů a následný návrh metodiky ochrany osobních údajů ve společnosti. První část práce specifikuje teoretická východiska a popisuje základní pojmy. Další kapitola pojednává o současném stavu ochrany osobních údajů a poslední část práce obsahuje navrhnutá řešení nedostatků zjištěných v analýze současného stavu.

Klíčová slova

GDPR, osobní údaje, ochrana osobních údajů

Abstract

This thesis is focused on the description of the protection of personal data in the company. It includes explanation of terms connected with protection of personal data and subsequent suggestion of methodology of protection of data in company. The first part of the thesis specifies the theoretical basis and describes the basic terms. Next chapter deals with the current state of the protection of personal data and the final part contains suggested solution for the drawbacks found in the analysis of current state.

Key words

GDPR, personal data, personal data protection

Bibliografická citace

VÁCLAVKOVÁ, Eliška. *Ochrana osobních údajů ve společnosti* [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/118385. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Dydowicz.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 9.5.2019

_____

Podpis studenta

Poděkování

Tímto bych chtěla poděkovat vedoucímu své práce za pomoc při tvorbě práce a za všechny cenné rady, které mi během psaní dal.

OBSAH

Úvod 10

Cíle práce, metody a postupy zpracování 11

1 Teoretická východiska práce 12

1.1 Osobní údaje 12

1.2 Vývoj ochrany osobních údajů na území České republiky 12

1.3 GDPR 13

1.4 Informační technologie a ochrana osobních údajů 26

1.5 Sankce a pokuty 29

2 Analýza současného stavu 31

2.1 Popis společnosti 31

2.2 Zpracování osobních údajů 34

2.3 Uložení osobních údajů 41

2.4 Správce a zpracovatel OÚ 42

2.5 Fyzická bezpečnost údajů 42

2.6 Analýza informačního systému 43

2.7 Pověřenec pro ochranu osobních údajů – DPO 43

2.8 Vedení záznamu o činnostech zpracování 44

2.9 Posouzení vlivu 44

2.10 Zavedená opatření splňující GDPR 44

2.11 Požadavky zadavatele 44

2.12 Shrnutí současného stavu 44

3 Vlastní návrhy řešení 47

3.1 Doporučení pro zjištěné nedostatky 47

3.2 Doporučení pro jednotlivá oddělení 51

3.3 Ekonomické zhodnocení 53

3.4 Přínosy navržených řešení 53
Závěr 54
Seznam použitých zdrojů 55
Seznam použitých tabulek a obrázků 57
Seznam příloh 58

ÚVOD

V dnešní době je téma ochrany osobních údajů hojně diskutováno a velmi tomu přispělo i nové Evropské nařízení o ochraně osobních údajů, tzv. GDPR (zkratka anglického názvu General Data Protection Regulation). Nařízení vstoupilo v platnost v květnu roku 2018 a dotýká se každého, kdo nějakým způsobem zpracovává nebo uchovává osobní údaje občanů celé Evropské unie.

Pro každého člověka by mělo být důležité chránit si své osobní údaje. V rámci firem to platí dvojnásob. Je zde nutná ochrana nejen osobních údajů zaměstnanců, ale také ochrana údajů odběratelů a dodavatelů. Firmy by se proto o nařízení GDPR měly zajímat nejen z důvodu hrozby vysokých pokut, ale také z důvodu možné ztráty důvěryhodnosti v dodavatelsko-odběratelských vztazích.

Jelikož s rozvojem dnešní společnosti vzrůstá hodnota informací, mezi které patří i osobní údaje, rozhodla jsem se věnovat tématu ochrany těchto údajů.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem mojí bakalářské práce je zhodnocení současného stavu společnosti z pohledu zpracovávání osobních údajů a jejich ochrany. Cílem je také následný návrh úpravy těchto postupů v návaznosti na nařízení GDPR.

Mým osobním cílem bylo psát práci, která bude mít reálný přínos v praxi. Po dohodě s vedoucím práce jsem kontaktovala firmu, kterou mi doporučil. Na následné schůzce s majitelem firmy jsme se dohodli, že ve své práci vytvořím analýzu současného stavu ochrany osobních údajů. Podle zjištěných informací dále navrhnu doporučení pro společnost tak, aby splňovala požadavky nařízení GDPR, což bude pro firmu vítaným přínosem.

Pro zhodnocení současného stavu je třeba vytvořit analýzu zpracovávání osobních údajů. Tato analýza vychází z údajů vyplněných pověřenými zaměstnanci firmy do předložených dotazníků.

Tyto dotazníky obsahují popis zpracovávaných osobních údajů, důvod potřeby jejich použití a další informace nutné k analýze zpracování osobních údajů ve společnosti. Na základě analýzy vypracované z těchto dotazníků a doplňujících otázek potom zhodnotím nedostatky v ochraně osobních údajů a popíšu zjištěná rizika.

Výstupem práce bude soubor doporučení pro práci s osobními daty, jež by měla zabránit rizikům poškození, ohrožení nebo nedovolené manipulace s osobními údaji.

Dílčí cíle práce:

- Představení nařízení GDPR
- Analýza současného stavu
- Zhodnocení současného stavu
- Popis návrhu změn a doporučení

1 TEORETICKÁ VÝCHODISKA PRÁCE

1.1 Osobní údaje

„Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je ta fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“ (Žůrek, 2017, s. 30).

V současnosti je ochraně osobních údajů věnována velká pozornost. Je to z toho důvodu, že jsou osobní údaje podobně zneužitelné, jako je v rámci firem zneužitelné například obchodní tajemství. Informace, které se o jednotlivých fyzických osobách zpracovávají, jsou stále rozsáhlejší a s rozvojem informačních technologií je snazší nejen jejich zpracovávání a ukládání, ale i jejich nedovolené zneužití. V souvislosti s tímto rozvojem tedy význam ochrany osobních údajů stále narůstá (Navrátil, 2018, s. 22).

Osobní údaje jsou velmi důležitým ekonomickým aktivem. Online platformy jako jsou vyhledávače nebo sociální sítě často shromažďují data od spotřebitelů. Tyto informace pak mohou prodávat, zejména reklamním firmám. Tyto firmy mohou na základě analýz vytvořených ze získaných dat spotřebitelů efektivněji umisťovat personalizované reklamy (Nezmar, 2018, s. 20).

1.2 Vývoj ochrany osobních údajů na území České republiky

Na území České republiky byla ochrana soukromí poprvé upravena zákonem o ochraně svobody osobní a svobody domovní. Po vzniku samostatného Československa byl přijat Ústavní zákon č. 293/1920 Sb., o ochraně svobody osobní, domovní a tajemství listovního. Dalším zákonem upravujícím ochranu osobních údajů byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech a následně Listina základních práv a svobod, která byla vyhlášena Usnesením předsednictva České národní rady.

V roce 2000 vstoupil v platnost zákon č. 101/2000 Sb., o ochraně osobních údajů (Navrátil, 2018, s. 28).

Dne 25. 5. 2018 nabylo účinnosti Nařízení Evropského parlamentu a rady, které částečně nahrazuje zákon č. 101/2000 Sb. Toto Nařízení bude více popsáno v následující kapitole

Na stránkách Ministerstva vnitra se také vyskytuje informace o nově připravovaném zákoně o zpracování osobních údajů. *„Obecné nařízení o ochraně osobních údajů je přímo použitelné, tedy má přímé účinky na území České republiky a nemusí být do českého právního řádu převedeno zákonem. Aktuálně je v legislativním procesu nový zákon o zpracování osobních údajů, který v dílčích ohledech adaptuje právní řád České republiky na nařízení Evropského parlamentu a Rady (EU) 2016/679 a stanoví některé výjimky, které umožňuje nařízení.“* (MVČR, 2019).

1.3 GDPR

Zkratka pro „General data protection regulation“.

„Nařízení Evropského Parlamentu a Rady (EU) 2016/679

Ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)“ (Nulíček et al., 2017, s. 1).

Obecné nařízení GDPR představuje nový právní rámec ochrany osobních údajů v celém Evropském prostoru, tedy nejen v zemích Evropské unie, ale například i na Islandu, v Norsku a Lichtenštejnsku. Stanovuje pravidla pro zpracování osobních údajů, a také práva subjektů údajů. Základní charakteristikou nařízení je jeho aplikovatelnost a univerzální použitelnost ve všech státech Evropské unie. Sjednocení pravidel pro práci s osobními údaji bylo jedním z cílů přijetí nařízení GDPR (Nezmar, 2018, s. 27).

Cíle GDPR

„Cílem GDPR je:

- *přizpůsobení právní regulace ochrany osobních údajů poměrům dnešní doby,*
- *sjednocení práva ochrany osobních údajů ve všech zemích Evropské unie a dalších zemích, na které dopadá,*

- *posílení práv v oblasti ochrany osobních údajů všech osob, které jsou subjekty údajů a dosáhnout sjednoceného výkladu GDPR dozorovými úřady jednotlivých zemí Evropské unie*
- *posílení důvěryhodnosti Evropské unie a jejích členských zemí (i dalších zemí, které pod GDPR spadají) pro jiné země, které mají zájem na rozvoji obchodu s Evropskou unií a s tím souvisícím předáváním osobních údajů mezi zeměmi* (Navrátil, 2018, s. 30).

Novinky proti předchozím právním předpisům

„Nové povinnosti podle GDPR:

- *povinnost vypracovat posouzení dopadu činnosti na ochranu osobních údajů,*
- *provádět předběžné konzultace s Úřadem pro ochranu osobních údajů,*
- *vést záznamy o zpracovávání osobních údajů,*
- *ohlašovat případy narušení bezpečnosti osobních údajů, a to do 72 hodin od doby, kdy se správce osobních údajů o narušení dozví, na Úřad pro ochranu osobních údajů a také dotčeným osobám, o jejichž osobní údaje se jednalo,*
- *umožnit přenositelnost osobních údajů od jednoho správce k jinému, povinnost jmenovat pověřence ochrany údajů“* (Navrátil, 2018, s. 33).

Povinnosti, které GDPR mění

„GDPR navazuje na dosavadní právní úpravu, ve které mnohé věci mění ve větší či menší míře. Hlavní změny pak jsou tyto:

- *ruší se především povinnost registrace správců a zpracovatelů u Úřadu pro ochranu osobních údajů, ale místo toho jim vzniká povinnost provádět předchozí konzultace s Úřadem pro ochranu osobních údajů,*
- *odpadá povinnost zpracování „projektu ochrany osobních údajů“, podle paragrafu 13 odst. 2 zákona č. 101/2000 Sb., o ochraně osobních údajů, ale místo toho vzniká nová povinnost vypracovat posouzení vlivu na ochranu osobních údajů“* (Navrátil, 2018, s. 65).

Definice v obecném nařízení

„Pro účely Obecného nařízení se rozumí:

„zpracováním“ *jakákoliv operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí, či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;*

„omezením zpracování“ *označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;*

„profilováním“ *jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu;*

„pseudonymizací“ *zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;*

„evidencí“ *jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;*

„správcem“ *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Evropské unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;*

„zpracovatelem“ *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;*

„příjemcem“ *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;*

„třetí stranou“ *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem, ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;*

„souhlasem“ *subjektu údajů jakýkoliv svobodný, konkrétní a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;*

„porušením zabezpečení osobních údajů“ *porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;*

„genetickými údaji“ *osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;*

„biometrickými údaji“ *osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, např. zobrazení obličeje nebo daktyloskopické údaje;*

„údaji o zdravotním stavu“ *osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;*

„dozorovým úřadem“ *nezávislý orgán veřejné moci zřízený členským státem podle čl. 51 Obecného nařízení“* (Žůrek, 2017, s. 30).

Působnost obecného nařízení

Tedy vymezení rozsahu a realizace právního předpisu.

Osobní působnost

Stanovuje okruh subjektů, na které se právní předpis vztahuje. Mezi hlavní subjekty Obecného nařízení patří správci, zpracovatelé, subjekty údajů, dozorové úřady a Sbor (skupina WP29). Mezi subjekty je však třeba zařadit i akreditované subjekty pro monitorování kodexů chování nebo subjekty pro vydávání osvědčení (Žůrek, 2017, s. 34).

Věcná působnost

Vymezuje, na co se právní předpis vztahuje a na co se nevztahuje. Obecné nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na automatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

Ochrana osobních údajů je právně založena jako technologicky neutrální, tedy že je nezávislá na použitých technologiích (Žůrek, 2017, s. 34).

Místní působnost

Omezuje působnost právního předpisu na určité území. Obecné nařízení se z geografického hlediska aplikuje na členské státy Evropské unie (Žůrek, 2017, s. 36).

Extrateritoriální působnost

Znamená působnost právního předpisu zasahující mimo území, kde se primárně uplatňuje. Obecné nařízení se v některých případech vztahuje i na správce, kteří jsou usazeni mimo Evropskou unii. Jedná se o případy, kdy správce zpracovává osobní údaje subjektů, jež se nachází v Evropské unii. V případě, že je zpracování časté, ve větším měřítku nebo zahrnuje zpracování zvláštních kategorií osobních údajů, musí správce pocházející ze zemí mimo Evropskou unii jmenovat písemně svého zástupce v Evropské unii (Žůrek, 2017, s. 37).

Časová působnost

Vymezuje dobu, po kterou je právní předpis součástí právního řádu. Je nutno rozlišovat platnost a účinnost právního řádu. Platnost znamená, že právní předpis prošel stanoveným legislativním procesem a stal se součástí právního řádu. Účinnost znamená, že právní předpis je pro adresáty závazný a může být aplikován.

Obecné nařízení vstoupilo v platnost dne 27. 4. 2016. Od tohoto dne běžela přechodná lhůta určená k uvedení zpracování osobních údajů do souladu s Obecným nařízením. Tato lhůta vypršela dnem nabytí účinnosti nařízení dne 25. 5. 2018. Od tohoto data je Nařízení přímo použitelné a aplikovatelné (Žůrek, 2017, s. 38).

Základní zásady pro zpracování osobních údajů

V článku 5 odst. 1 Nařízení jsou uvedeny zásady pro zpracování osobních údajů, za jejichž dodržování odpovídá správce.

*„**Zákonnost** zpracování osobních údajů spočívá v tom, že zpracování musí probíhat v souladu s právem, resp. s právními předpisy. To znamená, že aby bylo zpracování osobních údajů v souladu se zákonem, musí se dít buď na základě souhlasu dotčené osoby, nebo na základě jiného důvodu, který je však přímo stanoven, a to v čl. 6 odst. + písm. b) až f) GDPR. Ke zpracování musí navíc docházet takovým způsobem, aby bylo pro dotčené osoby předvídatelné.“*

*„**Korektnost** zpracování je poctivé zpracování osobních údajů. Bude záležet na jednotlivém případě, co bude možné považovat po zohlednění všech okolností za korektní zpracování. Obecně lze tuto povinnost definovat jako povinnost ohleduplnosti, a tím i zpřesnění zásady přiměřenosti. Odpovědná osoba by měla zohledňovat zájmy a očekávání dotčených osob a nesmí je bezdůvodně přehlížet nebo mylných představ osob využívat.“*

*„**Transparentnost** by měla především zaručit, že dotčené osoby mohou vykonat své právo na informační sebeurčení, tedy rozhodnout o tom, které – v rámci zákonem daných hranic - údaje o sobě poskytnou. Tato zásada je realizována například informačními povinnostmi při sběru osobních údajů, jakož i tím, že dotčená osoba má právo na takové informace.*

Zásada transparentnosti předpokládá, že všechny informace a sdělení ke zpracování osobních údajů budou jednoduše přístupné, srozumitelné a vyhotovené v jednoduché řeči.“

*„**Účelové omezení** doplňuje zásadu transparentnosti a znamená, že účel zpracování osobních údajů musí být znám již při sběru dat. Pozdější změna účelu, resp. jeho*

rozšíření je možná, pokud to není neslučitelné s účelem původního sběru údajů a existuje pro to zákonný podklad."

„Minimalizace údajů *osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány. Tato zásada se skládá ze tří požadavků. Zaprvé data musí být pro sledovaný účel podstatná. Zadruhé, musí být pro sledovaný účel potřebná, tedy zpracování údajů musí být omezeno na nutnou míru odpovídající sledovanému účelu. Zatřetí musí být takové omezení přiměřené."*

„Přesnost *osobní údaje, které jsou předmětem sběru, musí být také věcně správné, a je-li to potřeba, musí být aktuální."*

„Omezení uložení *osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány."*

„Integrita a důvěrnost *osobní údaje musí být zpracovány tak, aby byla zajištěna přiměřená bezpečnost. To znamená i ochranu před neoprávněným nebo nezákonným zpracováním a před nezamýšleným ztracením, zničením nebo poškozením dat."*

*„**Odpovědnost** zásada odpovědnosti je chápána jako zajištění dodržování zásad stanovených Nařízením. K tomu patří povinnost dodržování těchto zásad také prokázat. Odpovědná osoba musí přijmout technická a organizační opatření, aby zajistila a doložila, že zpracování osobních údajů probíhá v souladu s GDPR."*

„Ochrana osob v případě porušení osobnostních práv nebo ochrany osobních údajů

Právo domáhat se ochrany osobních práv má ta osoba, do jejíchž práv bylo zasaženo neoprávněným zásahem. Neoprávněným zásahem je zásah do osobnosti fyzické osoby, který je v rozporu s objektivním právem, tj. s právním řádem. Tento neoprávněný zásah přitom nemusí spočívat v porušení osobnostních práv jiného, ale i v jejich pouhém ohrožení" (Navrátil, 2018, s. 38-53).

Důvody pro zpracování osobních údajů

„K tomu, aby bylo zpracování osobních údajů zákonné, je třeba, aby jejich zpracování bylo buďto dovoleno zákonem bez souhlasu subjektu údajů, nebo aby byl takový souhlas subjektem údajů řádně udělen. Bez souhlasu subjektu osobních údajů lze osobní údaje shromažďovat a zpracovávat jen tehdy, pokud povinnost takového zpracování vyplývá

přímo ze zákona (například osobní údaje zaměstnanců, které musí zaměstnavatel mít podle zákona k dispozici a případně je i podle zákona odesílat veřejným subjektům.

S ohledem na výše uvedené je zpracování osobních údajů zákonné pouze tehdy, pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- *subjekt udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,*
- *zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (tedy smlouvy, kde je alespoň jednou smluvní stranou fyzická osoba),*
- *zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,*
- *zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (například při léčení, nebo záchraně života),*
- *zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,*
- *zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě"* (Navrátil, 2018, s. 113).

Zvláštní kategorie osobních údajů

Do této kategorie patří takové osobní údaje, které mohou subjekt údajů poškodit nebo zapříčinit jeho diskriminaci ve společnosti, v zaměstnání nebo například ve škole.

Tyto údaje jsou taxativně vyčleněny a je vyžadována zvýšená ochrana při jejich zpracování.

Do kategorie citlivých údajů se řadí údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, podle kterých je možné identifikovat fyzickou osobu (Nezmar, 2018, s. 35).

Důvody pro zpracování zvláštní kategorie osobních údajů

- subjekt údajů udělil výslovný souhlas
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů
- zpracování je nezbytné z důvodu významného veřejného zájmu
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče, atd.
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely (Nezmar, 2018, s. 35).

Práva subjektů údajů

Články 12-14 Nařízení upravují korektnost zpracování, tedy komunikaci se subjekty údajů a otevřenost ve věcech zpracování. Nařízení rozšiřuje rozsah informací, které je

nutné subjektům údajů sdělovat a klade velký důraz na jasnost a srozumitelnost těchto sdělení (Nulíček et al., 2017, s. 177).

Informační povinnost správce

V souladu se zásadou transparentnosti je správce povinen informovat subjekt údajů o zpracování jeho osobních údajů. Poskytování těchto informací se uskutečňuje buď písemně, nebo elektronicky. Ke splnění informační povinnosti musí dojít nejpozději v okamžiku získání osobních údajů (Nulíček et al., 2017, s. 190).

Právo na přístup k osobním údajům

Subjekt údajů má právo požadovat po správci, aby mu sdělil informaci o tom, zda zpracovává osobní údaje, které se ho týkají. Pokud správce údaje zpracovává, má subjekt údajů právo tyto osobní údaje a informace o zpracování obdržet (Nulíček et al., 2017, s. 203).

Právo na opravu

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení (Nulíček et al., 2017, s. 206).

Právo na výmaz (právo být zapomenut)

Dává subjektu údajů právo při splnění určitých podmínek požadovat vůči správci, aby zlikvidoval jeho osobní údaje a dál je neuchovával (Nulíček et al., 2017, s. 209).

Právo na omezení zpracování

Dává subjektu údajů možnost požádat správce, aby omezil zpracování osobních údajů, které se ho týkají. Pro vyhovění žádosti subjektu údajů o omezení zpracování musí být splněna některá z podmínek uvedených v nařízení (Nulíček et al., 2017, s. 215).

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů

Stanovuje správcům povinnost oznamovat všechny opravy, výmaz a omezení všem příjemcům, jimž dotčené osobní údaje poskytli (Nulíček et al., 2017, s. 218).

Právo na přenositelnost údajů

Umožňuje převádění osobních údajů mezi správci tak, aby se usnadnilo předávání osobních údajů z jednoho IT prostředí do jiného (Nulíček et al., 2017, s. 221).

Právo vznést námitku

Dává subjektu právo vznést námitku proti zpracování osobních údajů. Jedná se o situace, kdy subjekt neměl možnosti ovlivnit to, že jsou jeho údaje zpracovány a zároveň se nejedná o plnění právní povinnosti nebo životně důležitý zájem. Subjekt údajů má možnost vznést 3 druhy námitek:

- zpracování na základě právního titulu oprávněného zájmu a plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
- zpracování pro účely přímého marketingu na základě právního titulu oprávněného zájmu
- zpracování pro účely vědeckého či historického výzkumu nebo pro statické účely (Nulíček et al., 2017, s. 227).

Povinnosti a odpovědnosti správce a zpracovatele

„Správce je povinen zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s GDPR. Tato opatření musí být podle potřeby revidována a aktualizována“ (Navrátil, 2018, s. 97).

Pověřenec pro ochranu osobních údajů – DPO

Je specifická osoba, která dohlíží na soulad zpracování osobních údajů s Nařízením. Pověřenec zároveň radí správci ohledně různých skutečností souvisejících s ochranou osobních údajů, nenese však zodpovědnost za zpracování prováděné správcem nebo zpracovatelem (Nulíček et al., 2017, s. 332).

Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:

- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících

se rozsudků v trestních věcech a trestných činů uvedených v článku 10 (Nulíček et al., 2017, s. 330).

Záznamy o činnostech

Jsou písemné záznamy o zpracování osobních údajů, které jsou někteří správci a zpracovatelé povinni vyhotovovat. Záznamy vedené správcem by měly obsahovat jméno a kontaktní údaje správce, účely zpracování, popis kategorií subjektů a kategorií osobních údajů, kategorie příjemců, kterým jsou osobní údaje zpřístupněny, informace o případném předání osobních údajů do třetí země a plánované lhůty pro výmaz údajů. Záznamy vedené zpracovatelem by měly obsahovat jméno a příjmení zpracovatele, kategorie zpracování prováděného pro každého ze správců, informace o případném předání osobních údajů do třetí země a obecný popis technických a organizačních bezpečnostních opatření. Tyto záznamy musí být na vyžádání předloženy dozorovému úřadu.

Povinnost vést záznamy o činnostech se netýká správců a zpracovatelů s méně než 250 zaměstnanci.

Výjimkou, kdy je správce či zpracovatel vždy povinen vést záznamy o činnostech bez ohledu na počet zaměstnanců, jsou taková zpracování, která představují riziko pro práva a svobody subjektu, která nejsou příležitostná a taková, která zahrnují zvláštní kategorie údajů nebo údaje týkající se rozsudků trestů (Nulíček et al., 2017, s. 283).

Posouzení vlivu na ochranu osobních údajů

Posouzení se provádí, pokud je pravděpodobné, že nějaké zpracování bude mít s přihlédnutím k rozsahu a povaze zpracování vysoké riziko pro práva a svobody fyzických osob (Nulíček et al., 2017, s. 310).

Posouzení by mělo obsahovat systematický popis zamýšlených operací zpracování a účely zpracování, posouzení nezbytnosti a přiměřenosti zpracování z hlediska účelu, posouzení rizik pro práva a svobody subjektů, plánovaná opatření k řešení těchto rizik a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s Nařízením (Nulíček et al., 2017, s. 311).

Výsledkem tohoto posouzení by měla být dokumentace, která správci umožní přijmout dostatečná opatření ke zmírnění rizika zpracování (Nulíček et al., 2017, s. 312).

Toto posouzení je nutné, zejména když se jedná o systematické a rozsáhlé vyhodnocování osobních údajů, které je založeno na automatizovaném zpracování včetně profilování.

Když jde o rozsáhlé zpracování zvláštních kategorií údajů nebo o rozsáhlé systematické monitorování veřejně přístupných prostor (Nulíček et al., 2017, s. 310).

Dozorový úřad

Dozorovým úřadem je v České republice Úřad pro ochranu osobních údajů (ÚOOÚ). Je pověřen monitorováním a uplatňováním nařízení GDPR s cílem chránit základní práva a svobody fyzických osob.

Dozorové úřady svojí činností a vzájemnou spoluprací přispívají k jednotnému uplatňování nařízení v celé Evropské unii (Nulíček et al., 2017, s. 405).

„Úkoly dozorového úřadu:

- *obecná povinnost sledovat uplatňování Nařízení v praxi a přispívat k němu,*
- *edukace odborné i laické veřejnosti,*
- *dozor v užším smyslu,*
- *mezinárodní spolupráce,*
- *úkoly týkající se konkrétních institucí či procesů*
- *ostatní úkoly"* (Nulíček et al., 2017, s. 420).

„Pravomoci dozorového úřadu

Článek 58 Nařízení upravuje pravomoci dozorového úřadu. Obecně lze říci, že v porovnání se současnými pravomocemi českého ÚOOÚ tak, jak jsou upraveny především zákonem o ochraně osobních údajů, správním řádem a kontrolním řádem, k jeho výraznému posílení nedochází. Nově jsou upraveny zejména kompetence, které mají vztah k novým právním institutům (jako je ohlašování případů porušení zabezpečení osobních údajů, přezkum osvědčení atd.). Z pohledu klasických dozorových nástrojů, za které lze jistě označit především kontrolu a správní řízení, Nařízení dozorový úřad fakticky neposiluje a nezavádí tak nové povinnosti správců a zpracovatelů" (Nulíček et al., 2017, s. 426).

1.4 Informační technologie a ochrana osobních údajů

Digitální přenosy jsou velmi problematickým bodem ochrany osobních údajů. Jedná se nejen o přenosy po internetu, ale i po firemních sítích nebo přenosy na tisková zařízení (Nezmar, 2018, s. 189).

Tisková zařízení

Tiskárny nebo i jiná multifunkční zařízení se mohou často stát místem úniku osobních údajů. Zejména v posledních letech se snaží firmy snižovat náklady centralizováním tiskových zařízení. To znamená, že nepořizují tiskárnu každému zaměstnanci, který ji potřebuje, ale pořídí jedno velké multifunkční zařízení, které umístí na volné, všem přístupné místo, například chodbu (Nezmar, 2018, s. 189). Tím se toto zařízení stává zranitelným.

Uživatel tiskárny vytiskne citlivý dokument a zapomene si jej z tiskárny vyzvednout. Tento dokument si vzápětí může kdokoli přečíst ať už úmyslně, nebo náhodně při tisku vlastního dokumentu. Tímto způsobem mohou být ohroženy různé dokumenty a informace v nich uvedeny. Může se jednat o obyčejné pracovní listy, o výplatní pásky nebo například o detaily investičního plánu celé společnosti (Nezmar, 2018, s. 189).

V okamžiku, kdy dá uživatel pokyn k tisku, je dokument převeden aplikací do formátu, kterému tiskárna rozumí a je odeslán k vytištění. Většina dat do tiskáren putuje přes počítačovou síť. V 99 % případů jsou tato data přenášena bez jakéhokoliv šifrování a zabezpečení. V případě kybernetického útoku lze tato data snadno zachytit a získat pomocí nástrojů, které jsou volně ke stažení na internetu (Nezmar, 2018, s. 190).

Mnohá současná multifunkční zařízení umožňují ukládání dat na pevný interní disk. Pokud má tiskárna svůj vlastní operační systém, může se stát obětí napadení malwarem (Nezmar, 2018, s. 191).

Zabezpečení koncových zařízení

Jelikož platí, že systém je tak bezpečný a spolehlivý jako je jeho nejslabší článek, je nutné zabezpečení stolních počítačů a notebooků. Při budování prostředí splňujícího

požadavky GDPR je nutné dbát na zabezpečení jednotlivých koncových stanic uživatelů (Nezmar, 2018, s. 191).

Prvním krokem v řízení bezpečnosti IT technologie by vždy mělo být fyzické zabezpečení systému. Tím je myšlena ochrana proti krádeži, zničení nebo neoprávněné změně hardwaru. Fyzickou bezpečnost je tedy možné dodržet s opatřeními, jako je správné umístění v prostorech budovy s kamerovým systémem a řízeným přístupem osob (Nezmar, 2018, s. 191).

V některých případech lze využít ekonomicky příznivější variantu uzamčení stolních počítačů klasickým visacím zámkem. Výhodou této varianty je její jednoduchost a snadné pořízení, údržba i nahraditelnost (Nezmar, 2018, s. 192).

Bezpečí přenosných zařízení

Každé odcizené přenosné zařízení – telefon, tablet, notebook, atd. je možným zdrojem úniku osobních dat. Může se jednat nejen o data vlastníka, ale také data o osobách, se kterými dotyčný vedl konverzaci nebo si o nich tvořil poznámky. Hlavním předpokladem ochrany těchto zařízení je nastavení automatického zamykání a nastavení přístupového hesla. Dalším krokem bezpečnosti těchto zařízení je šifrování dat uložených v zařízení. Jednou z důležitých zásad pro bezpečnost přenosných zařízení by měl být zákaz instalace neznámých aplikací (Nezmar, 2018, s. 194).

Kybernetická bezpečnost

Je nedílnou součástí ochrany osobních údajů. Většina dat, tedy i osobních údajů, je v dnešní době ukládána v digitální podobě. Data jsou převáděna do digitální podoby za pomoci skenerů nebo ručním přepisem. Bez dostatečné ochrany těchto dat nelze zajistit bezpečnost osobních údajů (Nezmar, 2018, s. 195).

Bezpečnosti Wi-Fi

Wi-Fi sítě jsou nejméně bezpečným způsobem kybernetické komunikace. V případě přenosu nejsou většinou data šifrována. Útočník tedy může na síti odposlechnout vše, například i heslo (Nezmar, 2018, s. 217).

Heslová politika

Bylo zjištěno, že asi 10 % uživatelů používá pro všechny své služby stejné heslo. A pouze 30 % uživatelů zadává pro každou službu unikátní heslo. Bezpečnost našich dat tedy záleží primárně na zodpovědnosti provozovatele webových stránek (Nezmar, 2018, s. 221).

Kamerové systémy

Fotografie nebo video záznamy jsou z hlediska GDPR chápány jako osobní údaje. To stejné platí i pro informace získané z těchto záznamů jako jsou například registrační značky aut. Nařízení GDPR chápe použití kamerových systémů jako sběr osobních údajů. Instalací kamer se tedy organizace stává správcem těchto osobních údajů. Správce musí být schopen odůvodnit získávání těchto záznamů. Povinností provozovatele těchto kamer je informovat snímané osoby o používání nahrávacích zařízení a o tom, kdo za záznamy zodpovídá (Nezmar, 2018, s. 230).

Správce údajů je povinen na základě žádosti o přístup k osobním datům subjektu tyto záznamy ukázat či poskytnout jejich kopii. Před zobrazením či předáním kopie je správce povinen skrýt či rozmazat jiné osoby než subjekt údajů nacházející se v záběru (Nezmar, 2018, s. 231).

Použití záznamů pro získání údajů bez vědomí snímaných osob je obecně nezákonné. Skryté sledování je povoleno pouze pro případy, kdy jsou údaje získávány za účelem vyšetřování nebo odhalování trestních činů (Nezmar, 2018, s. 231).

Online oznámení o ochraně osobních údajů

Každá organizace splňující GDPR by měla subjekty údajů informovat o ochraně jejich osobních údajů pomocí prohlášení nebo oznámení. Takové oznámení by mělo subjektům poskytnout informace o organizaci, co organizace s jejich osobními daty bude dělat či s kým tato organizace bude tyto údaje sdílet (Nezmar, 2018, s. 237).

Cookies

„Cookies jsou krátké textové soubory vytvářené webovým serverem a ukládané v počítači prostřednictvím prohlížeče. Když se později vrátíte na stejný web, prohlížeč pošle uloženou cookie zpět a server tak získá všechny informace, které si u vás předtím uložil.

Využití cookies

Princip cookies umožňuje odlišit jednotlivé uživatele a uložit si o něm konkrétní údaje. Např. právě díky cookie ví příslušný server, jaké nastavení jazyka jste si při minulé návštěvě vybrali či jaké vám má předvyplnit přihlašovací jméno do formuláře (pamatuje si ho z minulé návštěvy). Cookies tedy usnadňují personalizaci.

Nevýhody a rizika cookies

Se schopností odlišit uživatele souvisí i nevýhoda používání cookies – do určité míry se ztrácí anonymita. Z těchto důvodů umožňují moderní prohlížeče ukládání cookies vypnout, uživatel tím však přijde o výše zmíněné výhody. Cookies je také možné v prohlížeči smazat" (Adaptic, © 2005–2019)

Ochrana osobních údajů podle GDPR se vztahuje i na případy, kdy jsou fyzickým osobám přiřazeny síťové identifikátory, které využívají jejich zařízení, jako například identifikátory cookies. Tyto nástroje mohou být použity k profilování fyzických osob a k jejich identifikaci. V některých situacích musí být pro takové zpracování udělen souhlas od subjektu údajů. Takový souhlas může být vyjádřen v podobě písemného prohlášení, nebo se může jednat například o zaškrtnutí políčka při návštěvě internetové stránky. Nečinnost nebo předem zaškrtnutá políčka nelze považovat za souhlas (Navrátil, 2018, s. 68).

1.5 Sankce a pokuty

„ GDPR vychází z principu, že za jakékoliv jeho porušení by měly být uloženy sankce včetně správních pokut, a to vedle nebo namísto vhodných opatření uložených dozorovým úřadem (ÚOOÚ) podle tohoto Nařízení. V méně závažných případech porušení, nebo pokud by pokuta, která bude pravděpodobně uložena, představovala pro fyzickou osobu nepřiměřenou zátěž, může být namísto pokuty uloženo napomenutí, pokud takovou sankci národní předpis připouští. To znamená, že Úřad pro ochranu

osobních údajů by měl potrestat právnickou osobu vždy, pokud poruší GDPR, u fyzické osoby může ze sociálních důvodů od pokuty upustit" (Navrátil, 2018, s. 91).

„Výše pokut podle GDPR je skutečně velmi vysoká. Může dosáhnout výše až 10 milionů eur, ve zvlášť závažných případech až 20 milionů eur, nebo jedná-li se o podnik, až do výše 4% celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší" (Navrátil, 2018, s. 127).

Připravovaný český zákon o zpracování osobních údajů však stanovuje horní hranici pokut na částku 10 milionů Kč, pokud firma funguje pouze na českém trhu (Navrátil, 2018, s. 127).

2 ANALÝZA SOUČASNÉHO STAVU

V této části práce se budu věnovat popisu společnosti a jejího nynějšího způsobu práce s osobními údaji a jejich ochranou. Po vzájemné dohodě s majitelem společnosti a z důvodu nutné ochrany bezpečnosti firmy budu uvádět pouze smyšlený název.

2.1 Popis společnosti

Pro zpracování praktické části svojí bakalářské práce jsem si vybrala společnost ABCČ a.s. podnikající v oboru informačních technologií. Majitel společnosti ABCČ a.s. byl ochoten mi poskytnout veškeré potřebné informace pro zpracování této práce. Informace uvedené v analýze byly zároveň konzultovány s pověřenými zaměstnanci daných oddělení.

Základní údaje

Společnost byla založena roku 1996 v Brně. Postupně vznikaly další pobočky a s růstem firmy se rozšiřovala i její působnost a zaměření. Hlavním oborem společnosti je prodej a servis výpočetní techniky. Firma poskytuje zákazníkům komplexní i dílčí řešení informačních a komunikačních systémů. Zabývá se dodávkou specializovaných služeb ve výpočetní technice a poskytuje také moderní cloudová řešení. Společnost je součástí holdingu ABCČ holding s.r.o.

Organizační struktura

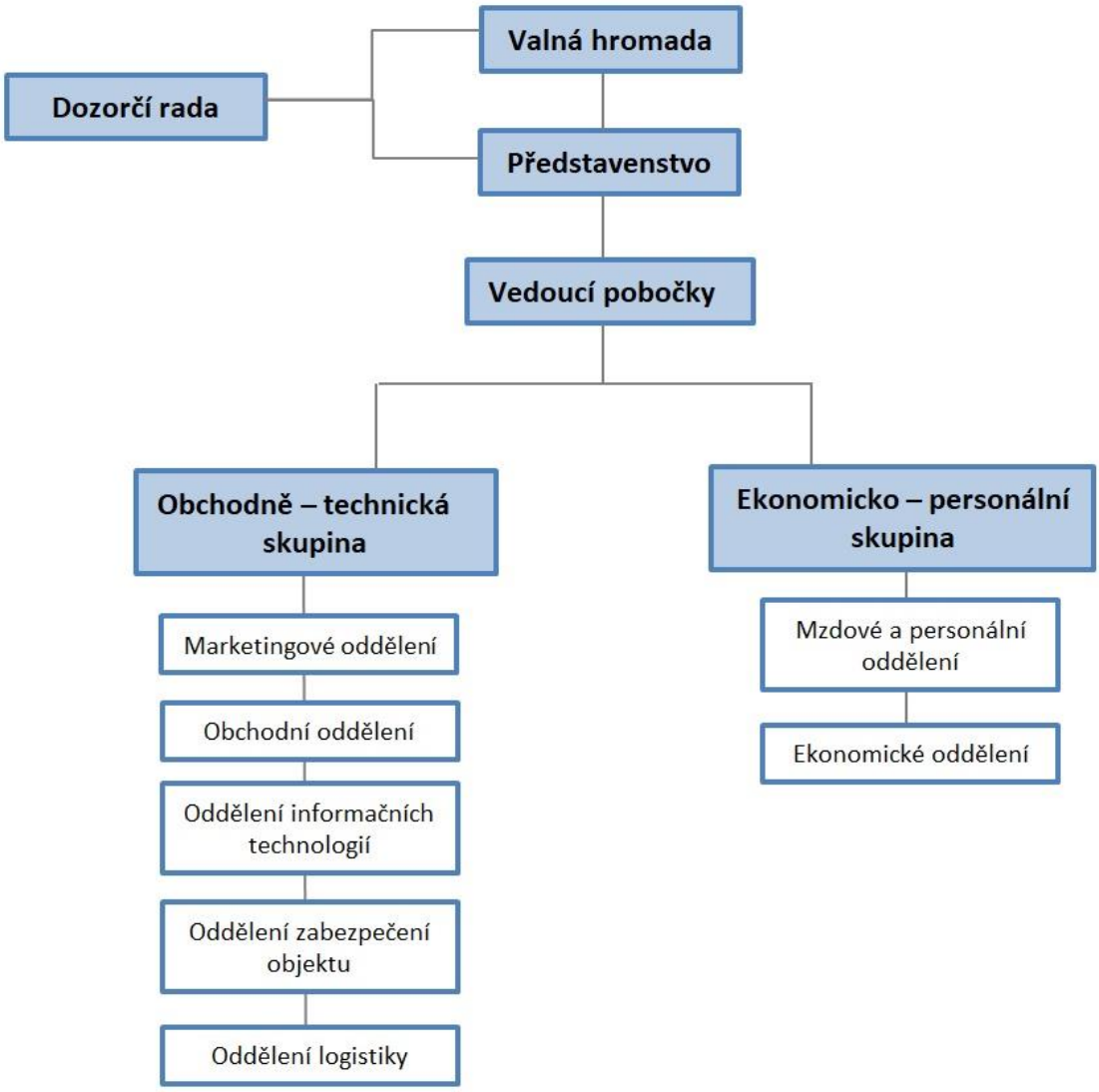
Nejvyšším orgánem ve společnosti je valná hromada, která rozhoduje o nejdůležitějších záležitostech firmy. Valná hromada se schází jednou za rok.

Společnost je rozdělena na 10 poboček. 9 poboček se nachází v České republice a každá z nich sídlí v jiném kraji. Jedna z poboček sídlí na Slovensku.

Každá pobočka má určeného svého vedoucího, který řídí chod pobočky a dohlíží na plnění stanovených cílů a povinností jednotlivých podřízených pracovníků. Dohromady ve všech pobočkách pracuje více než 250 zaměstnanců.

V rámci této bakalářské práce se blíže zaměřím pouze na jednu pobočku, a to hlavní, Brněnskou.

Pobočka má zhruba 50 zaměstnanců a dělí se na několik oddělení. Jednotlivá oddělení pak mají své specifické úkoly. Každé oddělení má stanovenu jednu vedoucí odpovědnou osobu, která odpovídá za správný chod oddělení a za plnění dílčích úkolů. Schůze vedení daných oddělení probíhají podle momentální potřeby.



Obrázek č. 1 : Schéma organizační struktury společnosti

(Zdroj: Vlastní zpracování)

Marketingové oddělení

Má za úkol zpracování reklamy, loga společnosti a celkovou propagaci firmy. Dalším důležitým úkolem je také organizování firemních akcí nebo různých akcí pro zákazníky a firemní partnery. Dále vytváří například letáčky či jiné pozvánky na tyto akce.

Obchodní oddělení

Komunikuje se zákazníky a dodavateli. Zařizuje veškeré objednávky zboží. V případě, že si zákazník objedná zboží, zaměstnanec obchodního oddělení zjistí dostupnost na skladě, nebo objedná toto zboží u dodavatelů. Oddělení se stará také o reklamace zboží.

IT oddělení

IT oddělení se dále dělí na programátory a systémové techniky. Programátoři vytváří nové programy a software pro zákazníky. Nepracují tedy s žádnými osobními údaji. Systémoví technici se starají o bezproblémový chod společnosti, jelikož dnes veškerá komunikace uvnitř i vně firmy probíhá přes počítače. Zajišťují přístupy všech zaměstnanců do interních systémů a potřebných počítačových programů. Starají se o hardware a software celé firmy, jejich funkčnost, opravy nebo případnou výměnu.

Oddělení zabezpečení objektu

Zabývá se vytvářením přístupů do sídla společnosti pro jednotlivé pracovníky. Pro vstup do budovy je třeba znát přístupový pin, nebo mít aktivovaný přístupový čip. Pro přístup do jednotlivých oddělení ve firmě se také využívá těchto dvou možných přístupových metod. Při přijetí nového zaměstnance do pobočky je proto třeba mu vytvořit jednu z těchto dvou přístupových metod ať už pro pohyb uvnitř budovy, nebo i pro samotný vstup do ní. Toto oddělení se zabývá také zabezpečením celého objektu pomocí bezpečnostních kamer.

Oddělení logistiky

Stará se o příjem zboží od doručovatelů či dodavatelů. Příjem probíhá tak, že si pracovník logistiky stáhne z ekonomického softwaru fakturu od dodavatele, zboží převzaté od doručovatele zkontroluje, přepočítá a uloží na připravené místo ve skladě. Z tohoto místa si jej pak vyzvedne obchodník, který si dané zboží objednal. Dále vyřizuje oddělení také expedici zboží ke koncovému zákazníkovi. O výběr a adresaci

zboží se stará pracovník z oddělení obchodu. Pracovník logistiky pouze zabalí žádané zboží a přichystá jej k výdeji.

Mzdové a personální oddělení

Zpracovává mzdovou agendu a vede záznamy o všech zaměstnancích firmy. Vytváří a sepisuje smlouvy pro nové zaměstnance.

Ekonomické oddělení

Zabývá se téměř veškerou agendou ekonomiky holdingu. Řídí papírový tok zboží a správu majetku firmy. Stará se odchozí i příchozí daňové doklady. Řeší docházku a zabývá se problematikou zdravotního a sociálního pojištění.

2.2 Zpracování osobních údajů

V Brněnské pobočce společnosti se zpracovávají osobní údaje o 4 základních skupinách subjektů údajů:

- zaměstnanci
- žadatelé o zaměstnání
- zákazníci
- dodavatelé

Tabulka č. 1 : Zpracovávané osobní údaje

Oddělení	Zpracovávané údaje	Množství OÚ
Marketing	-Jméno -Příjmení -E-mail -Telefonní číslo	500
Obchodní	-Jméno -Příjmení -Adresa -E-mail -Telefonní číslo	10 000
IT	-Jméno -Příjmení -Telefonní číslo -E-mail	250
Zabezpečení budovy	-Jméno -Příjmení	70

Oddělení logistiky	-	-
Mzdové a personální	-Jméno -Příjmení -Titul -Rodné číslo -Číslo OP -Bydliště -Datum narození -Pohlaví -Místo narození -Telefonní číslo -E-mail -Číslo bankovního účtu -Mzdové podmínky -Údaje o dovolené -Jméno, příjmení manžela/ky -RČ manžela/ky -Jméno, příjmení dětí -RČ dětí -Výpis z trestního rejstříku	250
Ekonomické	-Jméno -Příjmení -Bydliště -E-mail -Telefonní číslo -Číslo bankovního účtu	10 000

(Zdroj: Vlastní zpracování)

Zpracování osobních údajů probíhá v papírové i v elektronické formě a dělí se v závislosti na tom, jaké oddělení toto zpracování provádí. Jinak se osobní údaje zpracovávají na ekonomickém oddělení a jinak např. na oddělení marketingu. Z tohoto důvodu je třeba rozdělit zpracování právě podle těchto oddělení.

Výjimkou jsou osobní údaje žadatelů o zaměstnání. Jejich údaje jsou získávány ze životopisů. Životopisy jsou do společnosti přijímány z různých zdrojů. Mohou je posílat sami žadatelé o zaměstnání, nebo různé personální agentury. Životopisy jsou následně uloženy v e-mailové komunikaci, nebo mohou být vytištěny a založeny.

Společnost také využívá portálů www.jobs.cz a www.prace.cz, kde vystaví inzerát a žadatelé se sami následně mohou přes zmíněné portály přihlásit a poskytnout svůj životopis. Přístup k životopisům mají dále pouze oprávnění uživatelé s přístupovým

jménem a heslem pro daný portál. Z portálů si pověřená osoba vybere vhodné kandidáty, které osloví s nabídkou pohovoru. Životopis kandidáta si pro potřeby pohovoru může vytisknout. Po skončení pohovoru mohou být životopisy skartovány nebo uloženy pro možnost dalšího kola přijímacího řízení nebo kvůli oslovení žadatele s jinými nabídkami práce.

Životní cyklus osobních údajů podle jednotlivých oddělení

Marketingové oddělení

Marketingové oddělení zpracovává osobní údaje o zaměstnancích, zákaznících i dodavatelích. Pro oddělení jsou údaje důležité zejména z důvodu potřeby kontaktovat dané subjekty v případě konání firemní akce, akce určené pro firemní partnery či zákazníky. Mezi zpracovávané údaje patří jméno, příjmení, telefonní číslo, e-mail. Tyto údaje získává oddělení přímo od subjektů údajů, a to pomocí formulářů. Tyto formuláře mohou zájemci vyplnit buď na stránkách firmy, nebo je získají od zaměstnance firmy, například od pracovníka marketingového nebo obchodního oddělení. Po skončení akce jsou tyto formuláře odstraněny. Výjimečně se po skončení některých akcí uchovávají soupisy zúčastněných osob z důvodu nutnosti doložit účast sponzorům dané akce.

Tabulka č. 2 : Marketingové oddělení

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Marketing	Oprávněný zájem	Disk	Do skončení akce	-	-
Příjmení	Marketing	Oprávněný zájem	Disk	Do skončení akce	-	-
Telefonní číslo	Marketing	Oprávněný zájem	Disk	Do skončení akce	-	-
E-mail	Marketing	Oprávněný zájem	Disk	Do skončení akce	-	-

(Zdroj: Vlastní zpracování)

Obchodní oddělení

Toto oddělení zpracovává osobní údaje o dodavatelích a odběratelích. Údaje získává zaměstnanec oddělení přímo od subjektů údajů. Komunikace probíhá především přes e-mail. Zákazník odešle zaměstnanci oddělení objednávku zboží, ve které uvede

požadované zboží a rovněž své osobní údaje nutné pro vytvoření faktury. Obchodník poté ověří dostupnost zboží na skladě a vytvoří objednávku v ekonomickém programu. Následně vystaví fakturu na objednané zboží a tu zašle na e-mail zákazníka.

V některých případech je nutné zboží prvně objednat u dodavatelů. Vytvářené objednávky se opět řeší v převážné části přes e-mail. Obchodník v ekonomickém softwaru zjistí, od kterého dodavatele se dané zboží odebírá a vytvoří objednávku. Po dodání zboží od dodavatele je možno vytvořit fakturu pro odběratele a dané zboží mu odeslat.

Po vytvoření faktury předá pracovník obchodního oddělení jednu fakturu pracovníkovi ekonomického oddělení, který s ní dále pracuje. Druhá faktura je předána spolu se zbožím na oddělení logistiky, odkud je poslána k zákazníkovi.

Tabulka č. 3 : Obchodní oddělení

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Objednávka zboží/služeb	Smluvní plnění	Ekonomický software	Do skončení záruky	Archiv společnosti	10 let
Příjmení	Objednávka zboží/služeb	Smluvní plnění	Ekonomický software	Do skončení záruky	Archiv společnosti	10 let
Adresa bydliště	Objednávka zboží/služeb	Smluvní plnění	Ekonomický software	Do skončení záruky	Archiv společnosti	10 let
Telefonní číslo	Objednávka zboží/služeb	Smluvní plnění	Ekonomický software	Do skončení záruky	Archiv společnosti	10 let
E-mail	Objednávka zboží/služeb	Smluvní plnění	Ekonomický software	Do skončení záruky	Archiv společnosti	10 let

(Zdroj: Vlastní zpracování)

IT oddělení

Pracuje pouze s osobními údaji zaměstnanců. Mezi zpracovávané údaje patří jméno, příjmení, telefonní číslo a e-mail. Tyto údaje jsou získávány od personálního oddělení při přijetí nového zaměstnance.

Každý zaměstnanec potřebuje pro výkon své práce přístupy do jiných systémů. Tyto přístupy jsou tedy vytvářeny na základě požadavků od nadřízených jednotlivých

zaměstnanců. Jméno a heslo pro přístup do interních systémů dostávají zaměstnanci v papírové formě. Při prvním přihlášení je po zaměstnanci vyžadována změna přístupového hesla.

Tabulka č. 4 : IT oddělení

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Vytvoření pracovních přístupů	Smluvní plnění	Interní systémy společnosti	Doba trvání pracovního poměru	LTO pásky	6 měsíců
Příjmení	Vytvoření pracovních přístupů	Smluvní plnění	Interní systémy společnosti	Doba trvání pracovního poměru	LTO pásky	6 měsíců
Telefonní číslo	Vytvoření pracovních přístupů	Smluvní plnění	Interní systémy společnosti	Doba trvání pracovního poměru	LTO pásky	6 měsíců
E-mail	Vytvoření pracovních přístupů	Smluvní plnění	Interní systémy společnosti	Doba trvání pracovního poměru	LTO pásky	6 měsíců

(Zdroj: Vlastní zpracování)

Oddělení zabezpečení objektu

Oddělení zabezpečení objektu zpracovává osobní údaje pouze o zaměstnancích firmy. Získá je při přijetí nového zaměstnance do společnosti přímo od subjektů údajů. Informace nutné pro vytvoření přístupů do budovy jsou pouze jméno a příjmení zaměstnance. V případě výpovědi zaměstnance se přístupy zruší a osobní údaje se odstraní.

Tabulka č. 5 : Oddělení zabezpečení objektu

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Monitorování objektu	Oprávněný zájem	Přístupový systém	Doba trvání pracovního poměru	-	-
Příjmení	Monitorování objektu	Oprávněný zájem	Přístupový systém	Doba trvání pracovního poměru	-	-

(Zdroj: Vlastní zpracování)

Oddělení logistiky

Zaměstnanci tohoto oddělení nezpracovávají osobní údaje.

Mzdové a personální oddělení

Mzdové a personální oddělení zpracovává údaje pouze o zaměstnancích společnosti. Osobní údaje zpracovávané tímto oddělením jsou získávány přímo od subjektů údajů. Mezi zpracovávané údaje patří jméno, příjmení, titul, rodné číslo, číslo OP, adresa bydliště, datum narození, místo narození, telefonní číslo, e-mail, číslo bankovního účtu, mzdové podmínky, údaje o dovolené, údaje o manželovi/manželce (jméno, příjmení, rodné číslo) a údaje o dětech (jméno, příjmení, rodné číslo).

Po ukončení pracovního poměru se osobní údaje uchovávají v podobě mzdových listů v archivu společnosti podle zákona po dobu 30 let.

Elektronicky se na tomto oddělení zpracovává pouze jméno, příjmení a e-mail pro potřeby zasílání výplatní pásky na e-mail. E-maily obsahující výplatní pásky jsou vždy po měsíci odstraněny.

Tabulka č. 6 : Mzdové a personální oddělení

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Příjmení	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Titul	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Rodné číslo	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Číslo OP	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Adresa bydliště	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let

Datum narození	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Pohlaví	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Místo narození	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Telefonní číslo	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
E-mail	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Číslo BÚ	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Mzdové podmínky	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Údaje o dovolené	Evidence zaměstnance, zpracování a výplata mezd	Smluvní plnění, zákon	Složka zaměstnance, ekonomický software	Doba trvání pracovního poměru	Archiv společnosti	30 let
Jméno a příjmení manžela/ky	Daňové účely	Smluvní plnění, zákon	Složka zaměstnance	Doba trvání pracovního poměru	Archiv společnosti	30 let
RČ manžela/ky	Daňové účely	Smluvní plnění, zákon	Složka zaměstnance	Doba trvání pracovního poměru	Archiv společnosti	30 let
Jméno a příjmení dítěte	Daňové účely	Smluvní plnění, zákon	Složka zaměstnance	Doba trvání pracovního poměru	Archiv společnosti	30 let
RČ dítěte	Daňové účely	Smluvní plnění, zákon	Složka zaměstnance	Doba trvání pracovního poměru	Archiv společnosti	30 let
Výpis z trestního rejstříku	Hmotná zodpovědnost	Souhlas subjektu	Složka zaměstnance	Doba trvání pracovního poměru		

(Zdroj: Vlastní zpracování)

Ekonomické oddělení

Ekonomické oddělení zpracovává osobní údaje dodavatelů a odběratelů. Po přijetí vystavené nebo přijaté faktury od pracovníka obchodního oddělení zapisuje pracovník ekonomického oddělení informace do ekonomického softwaru. Do systému jsou zapisovány informace o pohybech zboží a zároveň jsou ukládány také informace do firemního adresáře. V tomto adresáři jsou zapsány veškeré potřebné informace o dodavatelích či odběratelích. Po uložení údajů z faktur jsou tyto faktury ukládány po dobu trvání záruky v příručním archivu a poté v archivu společnosti.

Ekonomické oddělení se také stará o ukládání smluv. Tyto smlouvy jsou uloženy v příručním archivu.

Tabulka č. 7 : Ekonomické oddělení
(Zdroj: Vlastní zpracování)

Osobní údaj	Účel zpracování	Zákonnost	Uložení	Doba uložení	Archivace	Doba archivace
Jméno	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let
Příjmení	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let
Adresa bydliště	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let
Telefonní číslo	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let
E-mail	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let
Bankovní spojení	Nákup/prodej zboží a služeb	Smluvní plnění	Ekonomický software	Doba trvání záruky	Příruční archiv, archiv společnosti	10 let

2.3 Uložení osobních údajů

Zpracování osobních údajů ve společnosti probíhá v elektronické i v papírové formě. Elektronické údaje jsou ukládány na disky osobních počítačů nebo na centrální úložiště, které je umístěno na serveru.

Papírové údaje se uchovávají v kanceláři účetního oddělení v příručním archivu. V momentě, kdy pro zaměstnance oddělení není dále nutné mít dokumenty okamžitě přístupné, přenášejí se do archivu, který se nachází v jiné budově patřící společnosti.

Archivace

V archivu jsou dokumenty ukládány po zákonem stanovenou dobu v závislosti na typu jednotlivých dokumentů. Vystavené faktury jsou například uloženy po dobu 10 let, pracovní smlouvy, mzdové listy a podobné dokumenty až po dobu 30 let.

Systém skartování

Skartování se řídí podle vnitřní směrnice firmy.

Vnitřní směrnice firmy

Uvnitř společnosti se aktivně využívá pouze jedna směrnice, a to směrnice pro skartování.

2.4 Správce a zpracovatel OÚ

Správcem osobních údajů je společnost. Zpracovatele společnost nemá.

2.5 Fyzická bezpečnost údajů

Budova společnosti splňuje veškeré bezpečnostní a požární předpisy.

Zabezpečení budovy

Budova se nachází v klidné a odlehlé části města. Je chráněna vnějším i vnitřním kamerovým systémem. Uvnitř budovy jsou nainstalovány snímače a pohybová čidla, která ihned ohlašují neoprávněný pohyb po budově.

2.6 Analýza informačního systému

Společnost má vlastní intranet, na kterém jsou uloženy různé informace. Jedná se například o informace o certifikacích výrobců, certifikáty partnerství, obratové certifikáty, podklady do výběrových řízení nebo reference od zákazníků.

Ve společnosti se používá ekonomický software myWAC. Tento software má rozsáhlé spektrum využitelnosti od jednoduchých fakturačních systémů po veškerou evidenci účetnictví, personalistiky, skladů a prodejů s možností návaznosti na e-shop. Uvnitř společnosti se však používá pouze několik modulů, a to fakturace, účetnictví a personalistika. Tento software nemá zabudovanou ochranu osobních údajů.

Pro každodenní práci, tvorbu tabulek, smluv a cenových nabídek jsou využívány balíčky MS Office. Ve společnosti se také používají různé specializované programy, které jsou nutné pro práci jednotlivých zaměstnanců. Active Directory ve společnosti zajišťuje centrální databázi všech uživatelských účtů.

Server

Nachází se v uzamčené místnosti v nejvyšším patře budovy. Klíč od místnosti má pouze vedoucí pracovník IT oddělení, nikdo jiný se do místnosti nedostane.

Na serveru běží všechny interní systémy firmy a ukládají se v něm veškerá data z těchto systémů. Server má vlastní záložní zdroj pro případ výpadku elektřiny.

Zálohování

Zálohování všech systémů se provádí jednou denně v nočních hodinách. Zálohují se celé systémy i veškerá data. Zálohy se provádí na oddělené diskové pole, kde jsou uloženy půl roku. Zálohy se následně kopírují na LTO pásky. Tyto pásky jsou uloženy v protipožárním trezoru, aby v případě požáru či jiného totálního zničení serveru a diskového pole bylo možné kompletně obnovit firemní systémy. Cloudové služby se ve společnosti nevyužívají.

2.7 Pověřenec pro ochranu osobních údajů – DPO

Společnost nesplňuje ani jedno z kritérií pro jmenování pověřence, mít jej tedy nemusí.

2.8 Vedení záznamu o činnostech zpracování

Společnost má méně než 250 zaměstnanců. Zároveň neprovádí žádná zpracování, která by správci udávala povinnost vést záznamy o činnostech zpracování.

2.9 Posouzení vlivu

Posouzení vlivu společnost dělat nemusí.

2.10 Zavedená opatření splňující GDPR

V rámci splnění nároků Nařízení byla ve firmě již přijata jistá opatření. Mezi tato opatření patří například podpis souhlasu se zpracováním osobních údajů v rámci dlouhodobých obchodních vztahů.

2.11 Požadavky zadavatele

Pro společnost je stěžejní vytvoření analýzy zpracování osobních údajů a jejich současné ochrany. Základním výstupem by tedy mělo být zjištění současného stavu.

Hlavním požadavkem společnosti ABCČ a.s. je, aby tato práce sloužila jako základ k vytvoření metodiky zpracování osobních údajů ve společnosti.

Zadavatel také očekává pomoc při zavádění GDPR do běžného chodu firmy. K tomu je nutné sepsat základní kroky implementace a zajištění souladu budoucího zpracování s GDPR.

Požadavkem společnosti je nutné splnění požadavků dodavatelů a odběratelů na ochranu osobních údajů.

2.12 Shrnutí současného stavu

V rámci analýzy současného stavu byly zjištěny určité nedostatky v ochraně osobních údajů. V této části práce budou tyto chyby pouze stručně vyjmenovány. Následující kapitola pak bude zaměřena na návrhy řešení těchto nedostatků a doporučení pro jejich rychlé a efektivní odstranění. Pro lepší přehlednost na začátku uvedu problémy týkající se celé společnosti a následující část bude rozdělena podle jednotlivých oddělení.

Zjištěné nedostatky:

a) zaměstnanci nejsou dostatečně proškoleni o povinnostech, které GDPR přináší pro práci s osobními údaji,
b) společnost nemá jmenovanou osobu odpovědnou za dohled nad zpracováním osobních údajů ve společnosti,
c) chybí organizační opatření nebo vnitřní směrnice upravující práci s osobními údaji,
d) chybí organizační opatření nebo vnitřní směrnice objasňující postupy při vymáhání práv subjektů údajů (právo na výmaz, právo na přístup),
e) chybí organizační opatření nebo vnitřní směrnice objasňující postupy při narušení bezpečnosti osobních údajů,
f) chybí organizační opatření nebo vnitřní směrnice, která by zajišťovala budoucí soulad s GDPR a jeho trvalé udržení,
g) žadatelé o zaměstnání nejsou informování o způsobu a době zpracovávání jejich osobních údajů,
h) životopisy žadatelů jsou libovolně ukládány bez souhlasu subjektů a k osobním údajům na životopisech mohou mít přístup i neoprávněné osoby,
i) na webových stránkách chybí dokument informující o zpracování osobních údajů ve společnosti a také kontakt na osobu odpovědnou za toto zpracování,
j) dříve uzavřené smlouvy či jiné dokumenty nejsou v souladu s GDPR,
k) společnost nevede žádnou evidenci souhlasů se zpracováním osobních údajů,
l) nejsou dána pravidla pro odesílání a ukládání osobních údajů v e-mailové komunikaci,
m) není ošetřena pravidelná kontrola přístupů do systému a změna přístupových hesel.

Marketingové oddělení

- osobní údaje z akcí jsou uchovávány po delší dobu, než je nezbytně nutné, není nijak ošetřeno jejich odstranění
- společnost nemá k dispozici výslovné souhlasy se zpracováním osobních údajů účastníků akcí

Obchodní oddělení

- zákazníci jsou nedostatečně informováni o zpracování jejich osobních údajů

- zákazníci nejsou informování o zpracování osobních údajů při vytváření objednávky
- osobní údaje zákazníků jsou uchovávány v e-mailové komunikaci bez výslovného souhlasu a po dobu delší než je nezbytně nutná

Mzdové a personální oddělení

- příruční archiv není dostatečně zabezpečený, k jeho obsahu se mohou dostat i neoprávněné osoby
- některé osobní údaje jsou uchovávány po delší dobu, než je pro jejich archivaci nutné

Ekonomické oddělení

- osobní údaje uložené v e-mailové komunikaci jsou dohledatelné po mnohem delší dobu, než je nutné
- zákazníci jsou nedostatečně informováni o zpracování jejich osobních údajů

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V rámci této kapitoly popíšu návrhy na řešení jednotlivých nedostatků v ochraně osobních údajů, které byly zjištěny v analýze současného stavu.

Tato práce se nezabývá implementací GDPR do chodu firmy, pouze vytvořením souboru doporučení pro práci s osobními údaji. Pokud by se firma rozhodla začít projekt implementace GDPR, bylo by vhodné začít rozhodnutím, zda si pro tento projekt najme externí osobu či firmu, nebo zda se o vše postarají interní zaměstnanci.

Implementace GDPR externí firmou by měla velkou výhodu, co se týče zkušeností specializované firmy a také ušetřeného času vlastních zaměstnanců. Proti této výhodě však stojí její vysoká cena. V případě náhlých problémů je nevýhodou, že externí firma nemusí být vždy k zastižení a interní zaměstnanci si s problémy nebudou umět sami poradit.

Pokud se však společnost rozhodne implementovat GDPR vlastními silami, bude mít velkou výhodu v tom, že nebude nutné najímat další osobu, která by se musela dlouze seznamovat s chodem firmy. Společnost si také díky tomuto výběru ve vlastních řadách „vychová“ odborníka na danou problematiku.

Pro projekt implementace GDPR pak může společnost využít doporučení vytvořených v rámci této práce.

3.1 Doporučení pro zjištěné nedostatky

a) Poučení zaměstnanců

Základním kamenem pro dodržování GDPR je znalost tohoto nařízení. Zaměstnanci, kteří jakkoliv pracují s osobními údaji, by proto měli projít školením o GDPR. Školení může provádět externí osoba nebo zaměstnanec firmy, ideálně osoba pověřená ochranou osobních údajů, která má přehled o dané problematice, nebo již prošla školením. Tato školení by měla být rozdělena v závislosti na tom, jaké osobní údaje a v jakém rozsahu školení zaměstnanci zpracovávají.

Základního školení by se měli zúčastnit všichni zaměstnanci. Je to z toho důvodu, aby získali povědomí o tom, co všechno je osobním údajem a proč je nutné tyto údaje

chránit. Školení by mělo dále zaměstnancům přiblížit co vlastně GDPR je, jaké novinky a změny přináší a co hrozí při jeho nedodržení.

Další úrovně školení by již měly být specializované podle potřeb jednotlivých zaměstnanců.

Doporučuji školení provádět pravidelně, jelikož může docházet k různým změnám, ať už legislativním nebo interním změnám ve společnosti (přijímání nových zaměstnanců, povýšení).

b) Jmenování odpovědné osoby

Společnost doposud nemá jmenovanou osobu odpovědnou za ochranu osobních údajů a za korektnost zpracování těchto údajů. Přesto, že společnost nemusí mít pověřence pro ochranu osobních údajů, doporučuji jmenovat alespoň jednoho člověka, který bude odpovídat za soulad ochrany osobních údajů s nařízením GDPR.

Odpovědná osoba by měla:

- dohlížet na zpracování osobních údajů a soulad zpracování s GDPR,
- dohlížet na bezpečnost tohoto zpracování,
- řešit případné narušení bezpečnosti osobních údajů,
- sledovat další legislativní vývoj v rámci ochrany osobních údajů,
- být schopna předávat vědomosti dalším zaměstnancům,
- být uvedena na stránkách společnosti jako kontaktní osoba v případě nejasností o zpracování osobních údajů či vymáhání práv subjekty údajů,
- organizovat školení o GDPR pro zaměstnance

c) Organizační opatření pro práci s osobními údaji

Pro jednodušší a jistější práci s osobními údaji i pro snazší kontrolu, zda zaměstnanci provádí zpracování osobních údajů správně, navrhuji vytvoření interní směrnice o zpracování osobních údajů ve společnosti. V této směrnici je třeba sepsat základní postupy zpracování, a také povinnosti zaměstnanců, kteří s osobními údaji pracují. Jelikož každé oddělení pracuje s osobními údaji jiným způsobem, měl by se na vytvoření této směrnice podílet vždy alespoň jeden zodpovědný člověk z každého oddělení.

d) Organizační opatření pro postup při vymáhání práv subjektů

Další důležitou částí směrnice o zpracování osobních údajů by měl být soubor postupů při vymáhání jednotlivých práv subjektem údajů, tedy srozumitelný popis, jak postupovat, které údaje subjektu údajů poskytnout, případně jakým způsobem.

e) Organizační opatření pro postup při narušení bezpečnosti údajů

Směrnice by měla dále obsahovat i přesně popsané kroky jak postupovat v případě narušení bezpečnosti osobních údajů.

f) Organizační opatření pro budoucí soulad s GDPR

Využívání této směrnice povede i k zajištění trvalého souladu s nařízením GDPR.

g) Informovanost žadatelů o zaměstnání

Žadatelé o zaměstnání by měli být informování, co se děje s jejich osobními údaji po přijetí životopisu do společnosti. Pro tyto případy navrhuji vypracování dokumentu, který bude subjekty informovat o zpracování osobních údajů. Ten bude žadatelům odesílán jako první odpověď na přijatý životopis.

Pro životopisy získávané z internetových portálů je variantou uložení tohoto dokumentu přímo pod inzerát společnosti.

V rámci tohoto dokumentu se žadatel o zaměstnání seznámí s tím, jak jsou jeho osobní údaje zpracovány a kdo má přístup k jeho osobním údajům. Dokument informující o zpracování osobních údajů by měl také obsahovat informaci o uložení či odstranění životopisů po skončení přijímacího řízení, pro které byl životopis poskytnut.

Ukázka tohoto dokumentu je obsažena v příloze. Tento dokument je třeba upravit podle situace, kvůli které je používán.

h) Uložení životopisů a přístup k osobním údajům žadatelů o zaměstnání

Pro uložení životopisů po skončení přijímacího řízení, pro které byl životopis poskytnut by měla mít společnost výslovný souhlas se zpracováním od subjektu údajů. Při souhlasu subjektu osobních údajů společnost může životopis žadatele ukládat i po skončení tohoto přijímacího řízení. Společnost tyto životopisy ukládá z důvodu možného otevření jiné vhodné pozice pro žadatele, kterého pak může na základě jeho osobních údajů kontaktovat s nabídkou této pozice.

V rámci přijímacího řízení doporučuji vždy jmenovat osobu odpovědnou za zpracování osobních údajů žadatelů. Může to být například vedoucí oddělení nebo přímý nadřízený pro pozici, na kterou je vypsaný inzerát. Je to z toho důvodu, aby se zamezilo přístupu neoprávněných osob k těmto osobním údajům.

i) Informace o osobě zodpovědné za zpracování osobních údajů

Na webových stránkách by měla být uvedena osoba, která je odpovědná za zpracování osobních údajů, pro případnou možnost vymáhání práv subjektů údajů či bližší dotazy na zpracování. Na webové stránky společnosti zároveň doporučuji vložit text popisující postup zpracování osobních údajů ve společnosti. Tento text slouží nejen pro přihlášené návštěvníky webu, ale pro všechny, kteří se na daný web dostanou. Je to z toho důvodu, že společnost uchovává cookies. Informace o zpracování osobních údajů na webových stránkách může dále sloužit i pro obchodní partnery, kteří se díky tomu mohou přesvědčit o bezpečnosti svých údajů při spolupráci se společností.

j) Dokumenty

Společnost by měla prohlédnout veškeré uložené smlouvy a další dokumenty a zjistit, zda jsou vypracovány v souladu s nařízením GDPR. Pokud budou v rámci kontroly nalezeny již neplatné smlouvy, měly by být buď skartovány, nebo uloženy do archivu v závislosti na tom, o jakou smlouvu se jedná a zda je její archivace dána zákonem.

Pro archivaci dokumentů by měla být vytvořena interní směrnice, která by určovala postup archivace, její trvání i způsob vyřazení dokumentů.

k) Evidence souhlasů

Pro zpracovávání údajů, které není možné doložit jinými zákonnými důvody (smluvní plnění atd.), je třeba mít jasný a jednoznačný souhlas se zpracováním osobních údajů přímo od subjektů údajů. Společnost by tedy měla vyčlenit údaje, pro které nemá jiné zákonné odůvodnění a získat pro jejich zpracování souhlasy od subjektů. Tyto souhlasy by poté měly být řádně uloženy v příručním archivu pro možnou nutnost jejich doložení. Vzor souhlasu se zpracováním osobních údajů je uveden v příloze.

l) E-mailová komunikace

Během analýzy současného stavu bylo zjištěno, že většina e-mailové komunikace uvnitř firmy není nijak kontrolována a průběžně odstraňována. Tato komunikace obsahuje

velké množství (i zapomenutých) osobních údajů, které již pro firmu nejsou nijak důležité a nemá právo na jejich zpracování ani ukládání.

E-mailová komunikace obsahuje i velké množství citlivých osobních údajů jako jsou například mzdové listy zaměstnanců nebo různé smlouvy. Z tohoto důvodu navrhuji školení pro zaměstnance, které by jim zdůraznilo nutnost průběžného mazání nepotřebných e-mailů a které by je poučilo o bezpečném používání e-mailu v návaznosti na ochranu osobních údajů.

m) Kontrola přístupů a změna přístupových hesel

Uvnitř společnosti mají různí zaměstnanci přístupy do jiných databází a jiných systémů v závislosti na náplni jejich práce. Tyto přístupy se často mění a někdy je potřeba vytvořit přístupy pro jindy neoprávněné uživatele z důvodu práce na krátkodobém projektu. Pro větší bezpečnost navrhuji pravidelné kontroly těchto přístupů do systému. Zároveň je vhodné zavést opatření zajišťující změnu všech přístupových hesel uživatelů alespoň jednou za 3 měsíce. Toto opatření je možné nastavit v Active Directory.

3.2 Doporučení pro jednotlivá oddělení

Marketingové oddělení

Oddělení uchovává osobní údaje účastníků firemních akcí po dobu delší, než je nezbytně nutné. Navrhuji proto odstranit veškeré osobní údaje z předešlých akcí. Pokud je to pro marketingové oddělení nevhodné a trvá na uchování těchto informací, například pro konání budoucích akcí, je třeba získat od subjektů údajů souhlas pro další zpracování a uchování jejich osobních údajů. V tomto případě tedy navrhuji vypracovat souhlas pro každého účastníka. Tento souhlas bude obsahovat popis zpracování, dobu a důvod uložení.

Obchodní oddělení

Z důvodu nedostatečné informovanosti zákazníků o způsobu, době i důvodu zpracování, navrhuji opět vypracování dokumentu informujícího o zpracování osobních údajů. Tento dokument může být posílán všem stálým i budoucím zákazníkům, nebo může být umístěn na webových stránkách společnosti.

Mzdové a personální oddělení

Důležitým bodem ochrany osobních údajů je jejich fyzická bezpečnost. Jelikož bylo zjištěno nedostatečné zabezpečení příručního archivu, ve kterém se nachází citlivé informace všech zaměstnanců, doporučuji pečlivé uzavření těchto dokumentů do uzamykatelné skříně.

Společnost archivuje některé dokumenty déle, než je dané zákonem. Z tohoto důvodu doporučuji pravidelné procházení archivu a odstraňování dokumentů, jejichž archivace není déle nutná. Zákonné lhůty pro archivaci jednotlivých dokumentů obsahujících osobní údaje jsou zobrazeny v následující tabulce.

Tabulka č. 8 : Zákonné lhůty archivace

Zákon	Dokument	Doba archivace
582/1991 Sb., o organizaci a provádění sociálního zabezpečení	Mzdové listy Účetní záznamy pro potřeby důchodového pojištění	30 let
582/1991 Sb., o organizaci a provádění sociálního zabezpečení	Mzdové listy (uživatelé starobního či invalidního důchodu)	10 let
563/1991 Sb., o účetnictví	Účetní závěrka Výroční zprávy	10 let
235/2004 Sb., o dani z přidané hodnoty	Daňové doklady	10 let
589/1992 Sb., o pojistném na sociální zabezpečení	Účetní záznamy pro stanovení pojistného	10 let
563/1991 Sb., o účetnictví	Účetní doklady, knihy Odpisové plány Inventurní soupisy Účtový rozvrh Účetní záznamy	5 let
582/1991 Sb., o organizaci a provádění sociálního zabezpečení	Evidenční listy	3 roky

(Zdroj: Vlastní zpracování)

Ekonomické oddělení

Doporučuji zavést průběžné promazávání e-mailové komunikace. Pro lepší informovanost zákazníků doporučuji uložit na webové stránky dokument informující o zpracování osobních údajů a při vytvoření objednávky zákazníkem mu tento dokument poslat na e-mail.

3.3 Ekonomické zhodnocení

Tato bakalářská práce se nezabývá projektem kompletní implementace GDPR, výstupem jsou pouze návrhy postupů, které by společnost měla zavést do běžného provozu pro splnění nároků Nařízení.

Pokud by se společnost rozhodla pro implementaci GDPR na základě těchto návrhů, znamenalo by to pro ni náklady. Tyto náklady jsou v hrubém odhadu zobrazeny v následující tabulce.

Tabulka č. 9 : Ekonomické zhodnocení

Doporučení	**Částka**
Školení GDPR	4 000,- / osoba
Počet zaměstnanců (každé oddělení + osoba odpovědná za GDPR ve společnosti)	(7+1) * 4 000 = **32 000,-**
Odpovědná osoba, vytvoření interních směrnic, školení o bezpečnosti e-mailové komunikace	V rámci mzdy pověřených pracovníků
Uzamykatelná skříň	**3 000,-**
Konzultace s právníkem	1 500,- / hod
Odhadovaný počet konzultačních hodin	5 * 1 500 = **7 500,-**
Částka celkem	**42 500,-**

(Zdroj: Vlastní zpracování)

3.4 Přínosy navržených řešení

Po zavedení těchto doporučení bude společnost splňovat nároky Nařízení a vyhne se tak hrozbě vysokých pokut i možné ztrátě důvěryhodnosti u obchodních partnerů a budoucích zákazníků. Navržená řešení zajistí dodržování postupů pro práci s osobními údaji a zajistí informovanost všech zaměstnanců, kteří s osobními údaji pracují. Mezi hlavní přínosy pak lze zařadit zabezpečení dostatečné ochrany osobních údajů všech subjektů firmy.

ZÁVĚR

Smyslem práce bylo vytvořit soubor doporučení a návrhů pro společnost, které po jejich zavedení zajistí soulad zpracování osobních údajů ve společnosti s Nařízením. Znalosti k vytvoření této práce jsem získávala postupně souhrnem teorie v první části a následnou praxí ve společnosti. Ta mi byla základním praktickým podkladem pro vypracování těchto doporučení. Díky absolvování této praxe jsem měla možnost nahlédnout do této problematiky hlouběji a v jejím průběhu jsem zjistila, že téma ochrany osobních údajů je velmi rozsáhlé a složité.

Překvapivým zjištěním pro mě bylo, že přesto, že je téma osobních údajů velmi aktuální, má o nutnosti jejich ochrany povědomí jen malá část dnešní populace.

Tato skutečnost byla příčinou toho, že se ochrana osobních údajů v analyzované společnosti doposud příliš neřešila. Majitel společnosti již však v návaznosti na tuto práci přijal určitá opatření, aby v brzké době společnost splňovala veškerá kritéria pro bezpečné zpracování osobních údajů.

Díky této skutečnosti mohu konstatovat, že bylo dosaženo nejen hlavního cíle práce, tedy vytvoření návrhů pro společnost, ale také mého osobního cíle – vytvoření práce, která bude mít pro společnost praktický přínos.

SEZNAM POUŽITÝCH ZDROJŮ

Co jsou Cookies | Adaptic, © 2005–2019. [online]. Adaptic. [cit. 20. 4. 2019]. Dostupné z: http://www.adaptic.cz/znalosti/slovnicek/cookies/

BARTÍK, V. a E. JANEČKOVÁ, 2013. *Ochrana osobních údajů v životě podnikatele.* Moravany u Brna: Anag. ISBN: 978-80-7263-811-6.

BASL, J. a R. BLAŽÍČEK. Podnikové informační systémy. Podnik v informační společnosti. Praha: Grada, 2008. 283 s. ISBN 978-80-247-2279-5.

Ministerstvo vnitra České republiky, 2019 [online]. MVČR. [cit. 25. 4. 2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/gdpr-web-legislativa-legislativa.aspx

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

NAVRÁTIL, J., 2018. *GDPR pro praxi.* 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o.

NEZMAR, L., 2018. *GDPR: Praktický průvodce implementací.* 1. vyd. Praha 7: Grada Publishing, a.s.

NOVÁK, D., 2014. *Zákon o ochraně osobních údajů a předpisy související*. Praha: Wolters Kluwer a.s. ISBN 978-80-7478-665-5

NULÍČEK, M. et al., 2017. *GDPR / Obecné nařízení o ochraně osobních údajů: Praktický komentář.* 1. vyd. Praha: Wolters Kluwert ČR, a.s.

SODOMKA, P. a H. KLČOVÁ. Informační systémy v podnikové praxi. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

Úřad pro ochranu osobních údajů [online]. 2013 [cit. 2019-04-27]. Dostupné z: https://www.uoou.cz/

Zákon č. 563/1991 Sb., o účetnictví ze dne 31. 12. 1991.

Zákon č. 235/2004 Sb., o dani z přidané hodnoty ze dne 23. 04. 2004.

Zákon č. 589/1992 Sb., České národní rady o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti ze dne 17. 12. 1992.

Zákon č. 582/1991 Sb., České národní rady o organizaci a provádění sociálního zabezpečení ze dne 31. 12. 1991.

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech ze dne 01. 06. 1992.

Zákon č. 101/2000 Sb., o ochraně osobních údajů ze dne 04. 04. 2000.

ŽŮREK, J., 2017. *Praktický průvodce GDPR.* 1. vyd. Moravany u Brna: Anag.

SEZNAM POUŽITÝCH TABULEK A OBRÁZKŮ

Obrázek č. 1 : Schéma organizační struktury společnosti……...32

Tabulka č. 1 : Zpracovávané osobní údaje…….....34

Tabulka č. 2 : Marketingové oddělení……...……..36

Tabulka č. 3 : Obchodní oddělení……37

Tabulka č. 4 : IT oddělení ……...38

Tabulka č. 5 : Oddělení zabezpečení objektu……..38

Tabulka č. 6 : Mzdové a personální oddělení…….….39

Tabulka č. 7 : Ekonomické oddělení…….…….....41

Tabulka č. 8 : Zákonné lhůty archivace…….……..52

Tabulka č. 9 : Ekonomické zhodnocení……...53

SEZNAM PŘÍLOH

Příloha č. 1: Dotazník na zpracování osobních údajů ……..…….…….....I

Příloha č. 2: Vzorový souhlas se zpracováním osobních údajů ……..……..……...II

Příloha č. 3: Vzorový dokument informující o zpracování osobních údajů..…...…….III

Přílohy

Příloha č. 1

Dotazník

Zpracování osobních údajů

Oddělení	
Odpovědná osoba	
Počet subjektů OÚ (počet lidí o nichž jsou zpracovávány OÚ)	
Kategorie OÚ (zaměstnanci, žadatelé, zákazníci, dodavatelé)	
Zdroj OÚ (subjekt údajů, intranet…)	
Způsob zpracování (elektronické, papírové)	
Druhy OÚ (jméno, příjmení, e-mail…)	
Účel zpracování (proč jsou OÚ potřeba)	
Zvláštní kategorie OÚ (zdravotní stav, výpis z rejstříku trestů, náboženské vyznání)	
Účel zpracování zvl. kategorie OÚ	
Místo uložení OÚ (archiv, počítačové úložiště)	
Doba uložení	
Archivace	

Příloha č. 2

Souhlas se zpracováním osobních údajů

1 Uděluji tímto souhlas společnosti ABCČ a.s., se sídlem v Brně, IČ: ……., zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl …, vložka …… (dále jen „Správce“), aby ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) (dále jen „Nařízení“) zpracovávala tyto osobní údaje:

- Jméno
- Příjmení
- E-mail

2 Tyto osobní údaje : jméno, příjmení a e-mail je nutné zpracovat za účelem ……..

3 Zpracování osobních údajů je prováděno Správcem po dobu nezbytnou k tomuto účelu tedy po dobu 2 let.

4 S výše uvedeným zpracováním uděluji výslovný souhlas. Poskytnutí osobních údajů je dobrovolné. Tento souhlas je možné vzít kdykoliv zpět (například zasláním e-mailu či dopisu na kontaktní údaje společnosti).

_____

Podpis

Po udělení tohoto souhlasu může subjekt údajů využít svých práv, kterými jsou:

- Vzít souhlas kdykoliv zpět
- Právo na přístup k vlastním osobním údajům
- Právo na opravu osobních údajů
- Právo na výmaz osobních údajů
- Právo na omezení zpracování osobních údajů
- Právo na přenositelnost dat
- Právo vznést námitku proti zpracování osobních údajů

Příloha č. 3

Vzorový dokument informující o zpracování osobních údajů

1. **Správce osobních údajů**

Společnost ABCČ, a.s. se sídlem v Brně, IČ: ……., zapsané ve veřejném rejstříku vedeném u Krajského soudu v Brně, oddíl …, vložka …… (dále jen „Správce“)

Vás tímto informuje o zpracování Vašich osobních údajů a o Vašich právech.

2. **Rozsah zpracování osobních údajů**

Osobní údaje jsou zpracovány v rozsahu, v jakém jej subjekt údajů správci poskytl, nebo které správce shromáždil a zpracovává je v souvislosti s uzavřením smluvního či jiného právního vztahu v souladu s platnými právními předpisy.

3. **Zpracovávané osobní údaje**

Adresní a identifikační údaje (jméno, příjmení, titul, adresa bydliště, kontaktní údaje)

Popisné údaje (bankovní spojení)

Údaje nezbytné pro plnění smlouvy

4. **Zdroj osobních údajů**

Subjekt údajů (e-mailová komunikace, vizitky, webové stránky, telefon aj.)

Veřejně přístupné rejstříky (obchodní rejstřík, živnostenský rejstřík atd.)

5. **Doba zpracování**

Po dobu trvání záruky / Po dobu trvání akce / Po dobu pracovního poměru / Po dobu trvání smlouvy / XY let

7. **Důvod zpracování**

Smluvní plnění / Jednání o smluvním vztahu / Plnění právní povinnosti správce / Oprávněné zájmy správce / Účely obsažené v rámci souhlasu subjektu údajů

8. Způsob zpracování

Zpracování je prováděno správcem v jeho sídle pověřenými zaměstnanci. Ke zpracování dochází prostřednictvím výpočetní techniky / manuálně. Zpracování probíhá za dodržení všech bezpečnostních zásad pro zpracování osobních údajů.

Správce přijal veškerá nutná technickoorganizační opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, jejich změně, zničení, ztrátě, neoprávněným přenosům, k neoprávněnému zpracování či k jinému zneužití osobních údajů. Zpracování tedy probíhá v souladu s platným Nařízením Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Po uplynutí doby nutné pro zpracování poskytnutých osobních údajů jsou tyto údaje kompletně odstraněny z veškerých zdrojů.

9. Subjekt údajů se může domáhat svých práv, která jsou následující:

Právo na přístup k vlastním osobním údajům

Právo na opravu osobních údajů

Právo na výmaz osobních údajů

Právo na omezení zpracování osobních údajů

Právo na přenositelnost dat

Právo vznést námitku proti zpracování osobních údajů

Těchto práv se můžete domáhat u správce na uvedené kontaktní adrese.

V případě jakýchkoliv dotazů, kontaktujte prosím společnost na uvedené adrese.