Projekt implementace GDPR ve vybrané firmě

Bc. Nela Kotrabová

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav podnikové ekonomiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Nela Kotrabová**
Osobní číslo:	**M17049**
Studijní program:	**N6208 Ekonomika a management**
Studijní obor:	**Podniková ekonomika**
Forma studia:	**prezenční**
Téma práce:	**Projekt implementace GDPR ve vybrané firmě**

Zásady pro vypracování:

Úvod

Definujte cíle práce a použité metody zpracování práce.

I. Teoretická část

- **Přehledně zpracujte teoretické poznatky z oblasti General Data Protection Regulation.**

II. Praktická část

- **Charakterizujte vybranou firmu a analyzujte její současný stav ochrany osobních údajů.**
- **Vytvořte projekt implementace GDPR ve vybrané firmě.**
- **Proveďte ekonomickou a rizikovou analýzu projektu.**

Závěr

Rozsah diplomové práce:	**cca 70 stran**
Rozsah příloh:	
Forma zpracování diplomové práce:	**tištěná/elektronická**

Seznam odborné literatury:

CALDER, Alan. EU GDPR: A Pocket Guide. 1st ed. United Kingdom: IT Governance Publishing, 2016, 74 s. ISBN 978-1-84928-833-0.
NAVRÁTIL, Jiří. GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 339 s. Pro praxi. ISBN 978-80-7380-689-7.
NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, 301 s. Právo pro praxi. ISBN 978-80-271-0668-4.
VOIGT, Paul a Axel VON DEM BUSSCHE. The EU general data protection regulation (GDPR). New York: NY: Springer Berlin Heidelberg, 2017, 383 s. ISBN 9783319579580.
ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018, 343 s. Právo. ISBN 978-80-7554-152-9.

Vedoucí diplomové práce:	**Ing. Zuzana Virglerová, Ph.D.** Ústav podnikové ekonomiky
Datum zadání diplomové práce:	**14. prosince 2018**
Termín odevzdání diplomové práce:	**16. dubna 2019**

Ve Zlíně dne 14. prosince 2018

L.S.

doc. Ing. David Tuček, Ph.D.
děkan

Ing. Petr Novák, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ/DIPLOMOVÉ PRÁCE

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen na elektronickém nosiči v příruční knihovně Fakulty managementu a ekonomiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

1. že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
2. že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 12.4.2019

Jméno a příjmení: Neb. Kotrabová

.....

podpis diplomanta

ABSTRAKT

Cílem diplomové práce je implementace Obecného nařízení o ochraně osobních údajů ve vybrané firmě. Diplomová práce je rozdělena na tři části. První část je teoretická, kde jsou zachyceny poznatky týkající se Obecného nařízení od základních pojmů až po případné sankce, následuje analytická část, která popisuje a analyzuje současný stav ochrany osobních údajů vybrané firmy. Na základě této analýzy a stanovení nesouladů s Obecným nařízením je navržený projekt, pomocí kterého budou do firmy implementována opatření, aby tak ochrana osobních údajů zaměstnanců a zákazníků byla v souladu s Obecným nařízením na ochranu osobních údajů.

Klíčová slova: Obecné nařízení o ochraně osobních údajů, zákazníci, profilování, osobní údaj, transparentnost

ABSTRACT

The purpose of the diploma thesis is an implementation of the General Data Protection Regulation (GDPR). The thesis is divided into the three parts. The first part is theoretical, where the data concerning the General Regulation are captured from basic concepts to possible sanctions, followed by an analytical part, which is describing and analysing the current state of protection of the selected company's personal data. Based on these analysis and the determination of inconsistencies with the General Regulation, a project is proposed that will serve to implement measures to protect personal data.

Keywords: General Data Protection Regulation, Customers, Profiling, Personal Data, Transparency

Tímto bych chtěla poděkovat vedoucí mé diplomové práce Ing. Zuzaně Virglerové, PhD. za odborné rady, připomínky, ochotu a veškerou pomoc při zpracování diplomové práce.

OBSAH

ÚVOD

Sjednocení právní úpravy v oblasti ochrany osobních údajů bylo dlouhodobým záměrem Evropské unie. Dne 25. května 2018 se tato snaha proměnila v nařízení, které sjednotilo ochranu osobních údajů fyzických osob. Tímto dnem se 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 stalo účinné a všechny organizace členských států Evropské unie se jím musí řídit. Obecné nařízení je koncipováno především k ochraně osobních údajů fyzických osob. Lze říci, že právní úprava ochrany osobních údajů přišla právě včas, protože většina z nás si bez každodenního online prostředí nedokáže život představit. A právě v online světě hrozí větší nebezpečí ztráty soukromí.

Nejprve je v teoretické části popsáno, co to vlastně Obecné nařízení je, jakou roli hraje Úřad pro ochranu osobních údajů a jak se postupně ochrana osobních údajů historicky vyvíjela. Dále jsou definovány základní pojmy a také zásady, kterými se nyní společnosti musí řídit, aby byly v souladu s Obecným nařízením. Společnosti musí být také schopny zabezpečit, aby v každém případě byla respektována práva, která má každá fyzická osoba v oblasti ochrany osobních údajů. Následují poznatky o posouzení vlivu zpracování osobních údajů a jmenování pověřence, IT zabezpečení a kamerových systémech a v neposlední řadě o sankcích při nezajištění souladu s Obecným nařízením.

Praktická část diplomové práce je rozdělena na popis a analýzu společnosti a samotný projekt implementace. V analytické části je nejprve popsána společnost, čím se zabývá, kolik má zaměstnanců apod., následuje analýza současného stavu ochrany osobních údajů, na jejímž konci je pomocí GAP analýzy shrnuto, jaké kroky jsou nutné udělat, aby společnost prováděla svoji hospodářskou činnost v souladu s Obecným nařízením. Tato analýza je východiskem pro projekt implementace do vybrané firmy.

Projekt implementace je hlavní částí diplomové práce. V projektu jsou popsány všechny kroky, které jsou nutné k zajištění souladu firmy s právním prostředím. Jedná se o stanovení účelu zpracování osobních údajů až po vytvoření dokumentu (vnitřního předpisu), kterým se vybraná společnost musí řídit.

Nakonec je provedena riziková analýza, analýza nákladů projektu a jsou zhodnoceny přínosy projektu. Jsou zde stanovena rizika, se kterými se lze v průběhu projektu setkat. Dále je projekt zhodnocen z hlediska ekonomického, kde jsou stanoveny náklady vynaložené na implementaci GDPR.

CÍLE A METODY ZPRACOVÁNÍ PRÁCE

Hlavním cílem diplomové práce je implementace Obecného nařízení na ochranu osobních údajů do vybrané firmy. Obecné nařízení je účinné od 25. května 2018 a ukládá tak povinnost všem společnostem, které disponují nebo zpracovávají osobní údaje fyzických osob na území Evropské unie, řídit se novými pravidly.

K tomu, aby bylo dosaženo hlavního cíle, je nutno nastudovat danou problematiku a na základě získaných poznatků provést analýzu současné ochrany osobních údajů. Zhodnocení současného stavu ochrany osobních údajů je provedeno pomocí sběru dat. Shrnutí rozdílů současného a požadovaného stavu ochrany osobních údajů je výsledkem GAP analýzy, jejíž výsledky slouží pro projekt implementace Obecného nařízení do vybrané firmy.

Z kvalitativních metod je využita metoda sběru informací, které je využita především ke zjištění, jaké osobní údaje firma spravuje a zpracovává a celkovému přehledu, jak firma nakládá s osobními údaji fyzických osob. Následuje syntéza, pomocí které jsou poznatky z jednotlivých oblastí Obecného nařízení postupně implementovány do vybrané firmy.

Další využitou metodou je metoda PZH, která slouží pro vyhodnocení rizika celého projektu. Je využita i v souboru, který slouží pro vyhodnocení rizik při jednotlivých podobách uchovávání osobní údajů – papírové i elektronické.

Pro zhodnocení projektu z hlediska trvání je využita metoda CPM (Critical Path Method), která určuje nejkratší možnou dobu trvání projektu.

I. TEORETICKÁ ČÁST

1 CO JE TO GDPR

GDPR (General Data Protection Regulation) jako 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 se stalo účinným dne 25. května 2018. Požadavky, které si klade za cíl toto nařízení, musí od tohoto data splňovat každá organizace, instituce, společnost, škola nebo také zdravotnické zařízení, která zpracovává nebo ukládá osobní údaje z kteréhokoliv členského státu Evropské Unie. (Nezmar, 2017, s. 13)

Protože s rychlým technologickým rozvojem a globalizací stoupl i rozsah zpracování a shromažďování osobních dat fyzických osob, je na místě, aby tato oblast byla regulována a byla tak posílena důvěra a jistota fyzických osob, hospodářských subjektů a orgánu veřejné moci. (Nulíček, 2017, s. 3)

Toto nařízení je zásadním krokem posílení základních práv jednotlivců v digitálním věku a usnadnění podnikání pomocí vyjasnění pravidel pro podniky a veřejné subjekty na digitálním jednotném trhu. Jednotný zákon také odstraní současnou roztříštěnost v různých vnitrostátních systémech a zbytečnou administrativní zátěž. (Data protection in the EU, © 2018)

Nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES nahradí v České republice zákon č. 101/2000 Sb., o ochraně osobních údajů. Nyní tedy zákon o ochraně osobních údajů upravuje pouze některé aspekty, které se týkají Úřadu pro ochranu osobních údajů. Jedná se například o ustavení, organizaci a další dílčí záležitosti nutné k doplnění celého rámce ochrany osobních údajů. GDPR se vztahuje na všechny státy Evropské unie, Island, Norsko a Lichtenštejnsko a v rámci České republiky byl ustanoven jako dohledový orgán Úřad na ochranu osobních údajů. (Nezmar, 2017, s 27)

1.1 Úřad pro ochranu osobních údajů

Právo na ochranu občana před neoprávněnými zásahy do soukromého života a shromažďování, zveřejňování nebo zneužívání osobních údajů, které stanovuje Listina základních práv a svobod, je stále více narušováno. Tohle narušování bylo jedním z mnoha důvodů, proč bylo v České republice přijato Obecné nařízení o ochraně osobních údajů.

Jako nezávislý dozor nad dodržování povinností při zpracování osobních údajů byl zvolen Úřad na ochranu osobních údajů. Mezi jeho další činnosti v této oblasti patří například vedení registru povolených zpracování osobních údajů. Dále se jedná o poskytování konzultací a přijímání podnětů i stížností občanů, pokud dojde k porušení zákona. (Úřad, © 2013)

Rozsah působnosti Úřadu pro ochranu osobních údajů se dotýká i dalších zákonů. Pro představu se jedná o Správní řád, Kontrolní řád, Zákon o svobodném přístupu k informacím, Zákon o službách informační společnosti, Zákon o střetu zájmů, Zákon o elektronických komunikacích, Zákon o regulaci reklamy, Zákon o cestovních dokladech, Zákon o evidenci obyvatel a rodných číslech a Zákon o základních registrech. (Působnost úřadu, © 2013)

1.2 Historie a vývoj ochrany osobních údajů

Svým způsobem lze o ochraně osobních údajů hovořit již od samého počátku lidstva, kdy lidé žili ve velmi úzké pospolitosti. Intimní záležitosti, které dnešní společnost považuje za velmi soukromé, prováděli lidé běžně veřejně. Jako další příklad lze uvést i to, že bohatí a významní lidé si své soukromí přece jen více chránili.

Z hlediska významných událostí došlo k narušení soukromí nejprve při náboženských válkách (nevhodní byli lidé s odlišným náboženstvím), Velké francouzské revoluci (problém s rozdílnými názory) a v neposlední řadě při genocidě (rasové zákony v době nacismu).

Asi největší zlom v oblasti ochrany osobních údajů nastal s rozvojem výpočetní techniky od 70. let 20. století. Od této doby přinesla elektronická komunikace, sociální sítě, elektronické obchodování, robotizace apod. velmi mnoho výhod a zjednodušení všedního života, ale také mnoho hrozeb – nejen v oblasti ochrany osobních údajů. (Navrátil, 2018, s. 26)

Jako první dokument, který měl zaručovat právo na soukromí, byla v roce 1948 přijata Všeobecná deklarace lidských práv Valným shromážděním OSN. Pro představu, díky technickému pokroku a celkovému rozvoji společnosti bylo nutné reagovat na zvyšující se míru sběru a zpracování osobních údajů, přijetím dalších dokumentů jako například:

- Evropská úmluva o ochraně lidských práv a základních svobod,
- Vnitrostátní předpisy nebo začlenění ochrany osobních údajů do Ústavy státu,
- Směrnice OECD o ochraně soukromí a přeshraničních tocích osobních údajů,
- Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat.

Úmluva o ochraně osob (Úmluva č. 108) se stala základem ochrany osobních údajů pro další dokumenty, které měly sloužit k ochraně osobních údajů. Byly zde již definovány pojmy, jako je správce nebo zpracování, které budou více definovány v dalších kapitolách. Následoval další dokument s názvem Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která se inspirovala výše zmíněnou Úmluvou č. 108. (Žůrek, 2018, s. 12-16)

Směrnice 95/46/ES zajistila sjednocení a harmonizaci pouze v základních otázkách, proto bylo nutné nadále pokračovat a upravit a sjednotit legislativu. K tomu slouží nyní platné a účinné 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. (Žůrek, 2018, s. 12-16)

1.3 Hodnota osobních údajů

Pro dnešní digitální trh mají osobní údaje fyzických osob ekonomickou hodnotu, zejména pro sociální sítě, vyhledávače, online videa atd. Lze taky osobní údaje považovat za ekonomické aktivum, které je vytvořeno identitou a chováním jedinců. Takto vytvořené aktivum je pak obchodováno výměnou za vyšší kvalitu výrobků, zboží a služeb. (Nezmar, 2017, s. 20)

Takto sesbíraná data přes online platformy slouží k analýze chování spotřebitelů a následně tak může být navržena reklama cílená přímo určitým skupinám osob. Prodávající mohou využívat údaje jako věk, pohlaví, postoje a zájmy uživatelů nebo demografické údaje. Využitím byť jen těchto základních údajů se odstraní asymetrie informací a lze získat vyšší efektivitu online transakcí. (Nezmar, 2017, s. 20)

1.4 Související právní předpisy a pojmy

V oblasti ochrany osobních údajů existují ještě další právní předpisy, kterými je nutno se řídit. Existují také pojmy, které se týkají Obecného nařízení nebo osobních údajů celkově. Níže jsou popsány vybrané pojmy.

Zákon o ochraně osobních údajů

V roce 2000 byl v České republice přijat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který doposud upravoval problematiku zpracování osobních údajů. Nyní jej nahradilo Obecné nařízení o ochraně osobních údajů, ale tento zákon bude

i nadále v platnosti. Upravuje však jen některé oblasti, především se jedná o postavení a organizaci dozorového úřadu, pro Českou republiku se jedná o Úřad pro ochranu osobních údajů. (Navrátil, 2018, s. 31)

Ministerstvo vnitra dodává, že zákon č. 101/2000 Sb. o ochraně osobních údajů bude nadále upravovat ještě další dílčí záležitosti, které jsou nutné k dotvoření celého rámce ochrany osobních údajů, které Obecné nařízení neupravuje. Tímto zákonem lze také upravit některé otázky týkající se ochrany osobních údajů na vnitrostátní úrovni. Důvodem pro revizi právního rámce ochrany osobních údajů byla především skutečnost, že stávající právní úprava již neodpovídala době, zejména pokud se jednalo o prostředky, které byly využívány pro zpracování osobních údajů. (Ochrana osobních údajů, © 2019)

Pracovní skupina WP29

Pracovní skupina WP29 byla poradním orgánem pro Evropskou komisi. Neměla svou vlastní právní subjektivitu a také neměla žádné pravomoci nad osobami nebo dozorovými úřady jednotlivých členských států. Jednalo se tedy spíše o neformální skupinu a její činnost spočívala hlavně ve vydávání doporučení a stanovisek. (Nulíček, 2017, s. 453)

Nezmar (2017, s. 44) dodává, že v souvislosti s Obecným nařízením vydává Pracovní skupina WP29 metodické materiály obsahující vodítka pro správce a zpracovatele. Tato skupina se poté transformovala na Evropský sbor pro ochranu osobních údajů. Úloha skupiny však zůstává stejná.

Evropský sbor pro ochranu osobních údajů (dále jen Sbor) má přímo stanovené úkoly. Má již vlastní právní subjektivitu a musí být nezávislý. Sbor je tvořen vedoucími dozorových úřadů jednotlivých členských států a evropským inspektorem ochrany osobních údajů. Nyní má Evropská komise právo účastnit se činnosti Sboru, ale hlasovací právo nemá. Vydané výkladové materiály nejsou sice závazné, ale jsou podstatnou součástí Obecného nařízení, protože se jím řídí i dozorové úřady. Vodítka jsou vydávána postupně od roku 2016, ale v roce 2018 došlo k revizi. Vodítka jsou k dispozici pro každého na internetových stránkách dozorového úřadu. (Žůrek, 2018, s. 29)

Sbor si volí předsedu, který je klíčovou osobou s řadou pravomocí a dva místopředsedy. Předseda zastupuje Sbor a má rozhodující hlas v případě nerozhodného hlasování. Všechny úkoly, které předseda má, jsou popsány v čl. 74 Obecného nařízení. (Nulíček, 2017, s. 460)

Privacy by Design

Privacy by Design stanovuje, že jakákoli činnost, kterou podnik provádí a která zahrnuje zpracování osobních údajů, musí být prováděna s ohledem na ochranu údajů a soukromí na každém kroku. To zahrnuje interní projekty, vývoj produktů, vývoj softwaru, IT systémy a mnoho dalšího. V praxi to znamená, že IT oddělení nebo jakékoli oddělení, které zpracovává osobní údaje, musí zajistit, aby bylo soukromí integrováno do systému během celého životního cyklu systému nebo procesu. (What is Privacy by Design & Default?, © 2018)

Žůrek (2018, s. 227) dodává, že pokud se týká tento přístup zpracování, lze použít pojem Data Protection by design.

Privacy by Default

Privacy by Default znamená, že jakmile bude produkt nebo služba zveřejněna, měla by být ve výchozím nastavení použita nejpřísnější ochrana osobních údajů bez jakéhokoli manuálního vstupu koncového uživatele. Veškeré osobní údaje poskytnuté uživatelem k zajištění optimálního použití produktu by měly být uchovávány pouze po dobu potřebnou k poskytnutí produktu nebo služby. (What is Privacy by Design & Default?, © 2018)

ePrivacy

ePrivacy je připravované evropské nařízení, které bude doplňovat Obecné nařízení o ochraně osobních údajů. Prozatím se směrnice vztahují pouze na tradiční telekomunikační operátory, ale nově pak budou závazná pravidla platit i pro WhatsApp, Facebook, atd. Ochrana soukromí tak bude zaručena u obsahu i u metadat. (Obecné nařízení o ochraně osobních údajů prakticky, © 2017)

Metadata jsou data, která popisují další data, informace nebo zdroj, ke kterému jsou vázána. (Metadata, © 2018)

2 ZÁKLADNÍ POJMY

Jak uvádí Rob Perry (2019, s. 9-11) ve svém článku s názvem GDPR – Project or Permanent Reality?, to, že je již Obecné nařízení o ochraně osobních údajů účinné, neznamená to, že je všechna práce hotova. Ochrana osobních údajů není jen projektem, který by měl skončit nebo již skončil. I přesto, že se společnosti snažily a vytvořily procesy, které jsou v souladu s celým nařízením, neznamená to konec. Podle Perryho je celé GDPR v dětství a některé části samotného nařízení jsou spíše otázkou názorů než kvantifikovatelné. Je velmi důležité implementovat a integrovat procesy, které budou sloužit k dodržování předpisů a zároveň tak minimalizují riziko případných sankcí.

Proto, abychom mohli vůbec pochopit koncepci ochrany osobních údajů, je důležité se seznámit se základními pojmy, se kterými GDPR pracuje. Neustále je v práci zmiňován pojem osobní údaj, je tedy na místě vysvětlit, co se pod tímto pojmem skrývá.

2.1 Osobní údaje

Pojem osobní údaje je popsán jako veškeré informace týkající se identifikované nebo identifikovatelné fyzické osoby. Identifikovatelnou osobou je myšlena fyzická osoba, která může být buď přímo, nebo nepřímo identifikována. Jako identifikátor může být označeno jméno, identifikační číslo, data o lokalizaci, online identifikátor nebo další identifikátory týkající se fyziologické, duševní, ekonomické, kulturní nebo sociální stránky fyzické osoby. Takto definovaná fyzická osoba se nazývá subjekt údajů. (IT Governance Privacy Team, 2017, s. 20)

Některé společnosti mohou namítat, že získávají pouze informace, ale rozdíl je v tom, že informace se od osobního údaje liší tím, že nejsou spojeny s konkrétní fyzickou osobou. Organizace, která disponuje osobními údaji, si musí dát tedy velký pozor na to, aby byť jen náhodou nezískala taková data, která nebudou pouze informacemi, protože se může stát, že se najde způsob, jakým lze data spojit s konkrétní fyzickou osobou. (IT Governance Privacy Team, 2017, s. 20)

Podle článku 9 Obecného nařízení o ochraně osobních údajů je zakázáno zpracovávat osobní údaje patřící do zvláštní kategorie osobních údajů. Do této kategorie patří například údaje o rasovém a etnickém původu, politických názorech, náboženského nebo filozofického vyznání. Dále taky o členství v odborech, genetických (dědičné nebo získané znaky fyzické osoby) a biometrických údajích (např. zobrazení obličeje), o zdravotním stavu (tě-

lesné i duševní zdraví) nebo taky o sexuální orientaci fyzické osoby. (Nařízení Evropského parlamentu a Rady 2016/679)

Calder (2016, s. 10) dodává, že biometrická dat jsou stále častěji využívány k autentizaci i s dalšími osobními údaji, které by měly být chráněny.

2.2 Zpracování osobních údajů

Další základní pojem se váže přímo k pojmu osobní údaj – jedná se o zpracování. Zpracováním lze rozumět jakoukoliv operaci nebo jejich soubor, které jsou prováděny s osobními údaji. Ke zpracování lze použít automatické i neautomatické prostředky, například sběr, nahrávání, organizování, strukturování, sdílení, změna, mazání dat nebo jen zadávání do počítače nebo chytrého telefonu. (Voigt, 2017, s. 9)

2.3 Evidence

Evidencí se rozumí jakýkoliv strukturovaný soubor s osobními údaji, který má centralizovanou nebo decentralizovanou podobu. Dalším kritériem, podle kterého můžeme rozeznat, že se jedná o evidenci je rozdělení dat podle funkčního nebo zeměpisného hlediska. (Nařízení Evropského parlamentu a Rady 2016/679)

2.4 Třetí strana

Jedná se o fyzickou nebo právnickou osobu, agenturu, orgán veřejné moci nebo jiný subjekt, která je oprávněna ke zpracování osobních údajů. Tato osoba není subjektem osobních údajů, správcem, zpracovatelem ani osobou, která podléhá přímo správci nebo zpracovateli. (Nařízení Evropského parlamentu a Rady 2016/679)

2.5 Souhlas

Nezmar (2017, s. 34) popisuje souhlas jako konkrétní, svobodný, informovaný a hlavně jednoznačný projev vůle. Subjekt může dát souhlas se zpracováním osobních údajů prohlášením nebo jiným zjevným potvrzením. Souhlas musí být aktivní, dobrovolný a je poskytován k určitému účelu zpracování. Jedná se o jeden z právních důvodů, na jehož základě může správce zpracovávat osobní údaje.

Proto, aby vůbec mohl být udělen souhlas, existují podmínky, které jsou obsaženy v článku 7 Obecného nařízení. Asi nejdůležitější je tzv. odlišitelnost souhlasu. To znamená, že poskytnutý souhlas musí být oddělený, například není možné, aby byl součástí obchodních

podmínek. Zároveň nesmí být uzavření smlouvy podmíněno tímto souhlasem. I když subjekt údajů dá souhlas se zpracováním osobních údajů, má právo jej kdykoliv odvolat. Odvoláním souhlasu však neznamená vždy osobní údaje zlikvidovat, ale nastane povinnost přestat je zpracovávat pro ten účel, pro který byl poskytnutý souhlas. (Nezmar, 2017, s. 131)

Nezmar (2017, s. 131) dále uvádí, že odvolání souhlasu musí být stejně snadné jako jeho získání, proto u každé ze tří možností získání souhlasu, musí existovat způsob, jak souhlas odvolat. V následující tabulce se nachází způsob získání souhlasu a s tím spojené odvolání.

Tabulka 1 Způsob získání a odvolání souhlasu se zpracováním osobních údajů (vlastní zpracování podle Nezmara, 2017, s. 132)

Způsob získání souhlasu	**Způsob odvolání souhlasu**
Pomocí online formuláře (například pomocí zaškrtnutí pole se souhlasem)	Odškrtnutí pole povolující zpracování osobních údajů
V písemné formě	Písemné prohlášení o odnětí souhlasu
Ústně, prostřednictvím telefonu, lze jej pak zaznamenat i fyzicky	Ústně – může být uložen v doslovném záznamu, ale komplikací může být objem dat a složité vyhledávání

2.6 Profilování

Všechny formy automatizovaného zpracování osobních údajů, které spočívají v jejich použití k hodnocení některých faktů o fyzických osobách. Jedná se zejména o pracovní výkon, ekonomickou situaci, zdravotní stav, osobní preference nebo zájmy, spolehlivost, chování, místa, kde se nachází a pohybu. (Žůrek, 2017, s. 30)

2.7 Pseudonymizace

Pseudonymizací se rozumí takové zpracování údajů, že již subjektu nemohou být přiřazeny vlastnosti nebo jednotlivé údaje bez použití jakýchkoliv dodatečných informací. Tyto informace by měly být uchovávány odděleně a měla by se na ně vztahovat technická nebo organizační opatření, která zajistí, že nebudou přiřazena zpět identifikovatelné osobě. (Žůrek, 2017, s. 31)

2.8 Správce

Správcem osobních údajů může být každý subjekt, který určuje účel a prostředky, pomocí kterých mohou být osobní údaje zpracovány. Stanovený správce primárně zodpovídá za zpracování osobních údajů a musí existovat řádný právní důvod, aby mohl zpracovávat osobní údaje a zároveň je zabezpečit. Jako správce může vystupovat právnická i fyzická osoba a mezi jeho hlavní úkoly patří odpovědnost za dodržování zásad zpracování a povinností a zabezpečení údajů, které ukládá Obecné nařízení. Mezi další povinnosti můžeme zařadit například jmenování pověřence pro ochranu osobních údajů, posuzovat vliv na ochranu osobních údajů, ohlašovat případy porušení zabezpečení kontrolnímu orgánu a vést záznamy o zpracování pokud musí. (Obecné nařízení o ochraně osobních údajů prakticky, © 2017)

2.9 Zpracovatel

Zpracovatelem osobních údajů se může stát fyzická i právnická osoba, agentura, orgán veřejné moci nebo jiný subjekt. Jeho hlavní náplní je zpracovávání osobních údajů pro správce, který jej pověří nebo vyplývají z jeho činnosti. Velmi nutno zdůraznit, že zpracovatel je zpracovatelem jen těch osobních údajů, které mu správce poskytl. (Obecné nařízení o ochraně osobních údajů prakticky, © 2017)

Výše byly popsány pojmy, které jsou základem pro porozumění Obecného nařízení, ale existují ještě další pojmy, které Obecné nařízení popisuje. Jedná se například o příjemce, porušení zabezpečení osobních údajů, hlavní provozovnu, genetické a biometrické údaje, zástupce, podnik, skupinu podniků, závazná podniková pravidla, dozorový úřad, dotčený dozorový úřad, relevantní a odůvodněná námitka, služba informační společnosti a mezinárodní organizace. (Nařízení Evropského parlamentu a Rady 2016/679)

3 ZÁSADY A PRINCIPY

Obecné nařízení o ochraně osobních údajů obsahuje zásady, které lze označit za základní stavební kameny celého Obecného nařízení. Většina níže vyjmenovaných zásad byla již obsažena v Zákoně o ochraně osobních údajů, v Obecném nařízení je najdeme v článku 5. Změna oproti Zákonu o ochraně osobních údajů spočívá v přímém vyjmenování zásad zpracování osobních údajů a současně stanovení odpovědnosti správce za dodržování povinností a také toto dodržování povinností doložit. Nastavení zpracování osobních údajů v souladu s Obecným nařízením je považováno za nepřetržitý proces, který napomáhá správcům dodržovat, případně dokazovat tento soulad novými standardizovanými nástroji, kterými mohou být například záznamy o činnostech zpracování osobních údajů, různé kodexy chování či osvědčení. (Žůrek, 2018, s. 60)

3.1 Zásada zákonnosti, korektnosti a transparentnosti

Nulíček (2017, s. 105) uvádí **zákonnost** jako jeden z nejdůležitějších principů ochrany osobních údajů. Zásada zákonnosti stanovuje, že zpracování osobních údajů musí vždy probíhat alespoň na základě jednoho z právních titulů, které jsou uvedeny v článku 6, odst. 1. Zpracování osobních údajů může probíhat na základě více titulů a zánik jednoho neznamená, že automaticky musí zpracovatel osobní údaje vymazat. Zásada zákonnosti dále stanovuje, že zpracování nesmí být protiprávní. Za protiprávní zpracování lze považovat takové zpracování, které probíhá za nelegálním či nelegitimním účelem nebo také situaci, kdy zpracování není v souladu s právním řádem obecně (například je v rozporu s Občanským zákoníkem).

Nezmar (2017, s. 50) dodává, že Obecné nařízení zakládá organizacím rozšířenou povinnost při dodržování předpisů a vyžaduje po organizacích zvýšení péče o vytváření a zavádění činností při zpracování osobních údajů.

Korektnost a transparentnost prezentuje Nulíček (2017, s. 106) jako povinnost organizací být otevřený a transparentní ohledně způsobů nakládání s osobními údaji. Nejdůležitějším krokem u respektování této zásady je povinnost informovat subjekt osobních údajů o rozsahu a způsobu zpracování osobních údajů, které jsou popsány v Obecném nařízení.

K **transparentnosti** se vyjadřuje i server podnikatel.cz, který popisuje transparentnost jako povinnost týkající se informování subjektů, komunikaci s nimi a jak správci pomáhají subjektům s jejich právy. Na základě článku 12 Obecného nařízení jsou požadavky na komu-

nikaci se subjekty údajů charakterizována jako stručná, srozumitelná, snadno přístupná, musí být použity srozumitelné jazykové prostředky, musí být písemná (v určitých případech i ústní – například pro slepé osoby) a musí být poskytnuta zdarma. (Langerová, 2018)

3.2 Zásada účelového omezení

Účelové omezení zpracování osobních údajů znamená, že údaje, které jsou získány, jsou zpracovány pouze pro určité, výslovně vyjádřené a legitimní účely (vždy v souladu s právním řádem). Správce má tak povinnost zpracovat jen ty údaje, které jsou v souladu s účelem, za kterým byly shromážděny. Je považováno za nepřístupné, aby správce nebo zpracovatel shromáždil údaje k určitému účelu a poté je zpracoval k jinému účelu. To by totiž znamenalo, že by subjekt zůstal neinformován o účelu zpracování a nemohl by tak rozhodovat, jak bude s jeho osobními údaji naloženo. (Janečková, 2018, s. 7)

Nulíček (2017, s. 108) dodává, že účel by měl být stanoven určitě, ale ne zase úplně úzce, aby správce osobních údajů sám sebe neomezil v možných operacích zpracování a porušil by tak zásadu účelového omezení. Nutno však dodat, že je nutné se vyvarovat obecným frázím, jako je například: zpracování pro „marketingové účely“ nebo třeba „zkvalitnění služeb“.

3.3 Zásada minimalizace údajů

Zásada minimalizace údajů představuje pro správce a zpracovatele osobních údajů povinnost zpracovávat pouze přiměřené, relevantní a v nezbytném rozsahu v souladu se stanoveným účelem zpracování osobních údajů. Respektování této zásady znamená, že správce nesmí požadovat více údajů po subjektu než je opravdu nutné. Zásada minimalizace údajů může působit jako univerzální, ale existují jiné právní prameny, které tuto zásadu konkretizují. Jedná se například o zákon č. 262/2006 Sb., zákoník práce, který uvádí, že zaměstnavatel nemůže požadovat po zaměstnanci informace, které bezprostředně nesouvisí s náplní práce. Povinností správců je zajištění vhodného technického a organizačního opatření, které zajistí, že budou zpracovány pouze nezbytné osobní údaje a ty, které jsou v souladu se stanoveným účelem. (Žůrek, 2018, s. 63)

3.4 Zásada přesnosti

Povinnost mít správné a přesné osobní údaje je již vymezena v Zákoně o ochraně osobních údajů. Obecné nařízení dále stanovuje, že data, která máme, musí být přesná a v případě

potřeby aktualizovaná. Přestože zní zásada přesnosti jasně, existují situace, kdy nemusí být proveditelné zajistit správnost každého osobního údaje, který organizace má. Neexistuje žádná definice přesnosti, ale nepřesnou informací se rozumí taková informace, která je nesprávná nebo zavádějící. K zajištění požadavku přesnosti mohou organizacím pomoci následující kroky:

- realizovat přiměřené opatření k získání a zpracování osobních údajů,
- zajistit jasný a nezpochybnitelný zdroj osobních údajů,
- uvážit, zda existují problémy nebo nejasnosti osobních údajů,
- promyslet, zda nutné osobní údaje aktualizovat, nebo jak často. (Nezmar, 2017, s. 63)

3.5 Zásada omezení uložení

Získaná osobní data by měla být uchovávána pouze po nezbytně dlouho dobu, která je vytyčena účelem. Dobu, po kterou jsou data uchovávána, určuje většinou sám správce a za toto rozhodnutí nese odpovědnost. (Janečková, 2018, s. 9)

3.6 Zásada integrity a důvěrnosti

Podle této zásady musí být osobní údaje zpracovávány tak, aby bylo zajištěno náležité zabezpečení před neoprávněným nebo protiprávním zpracování. Dále také například před ztrátou, zničením či poškozením. Zejména v dnešní době, kdy se množí kauzy s úniky dat, je zabezpečení osobních údajů klíčovou povinností. (Nulíček, 2017, s. 118)

3.7 Zásada odpovědnosti

Správce údajů musí zajistit soulad se všemi zásadami, které jsou zahrnuty v Obecném nařízení a musí být schopný doložit způsob, jakým jsou zásady plněny. Musí zajistit, aby bylo vše v souladu tam, kde dochází ke zpracování osobních údajů. (Nezmar, 2017, s. 81)

Nulíček (2017, s. 119) dodává, že ochrana osobních údajů bude muset být proaktivní a ne reaktivní. Správce musí sám zavádět vhodné systémy pro ochranu osobních údajů a musí vést řádnou dokumentaci.

4 PRÁVA A POVINNOSTI

Obecné nařízení stanovuje práva, která mají subjekty údajů v souvislosti se svými osobními údaji. Správcům a zpracovatelům je tak umožněno lépe porozumět a mít tak nad osobními údaji větší kontrolu. Stanovená práva dávají subjektům údajů pocit kontroly nad tím, kde se objevují jejich osobní data. Klíčovým problémem je celkové porozumění právům a povinnostem jak ze strany subjektu, tak i ze strany správce a zpracovatele. (ITGP Privacy Team, 2017, s. 190)

Právo být informován

Právo na informace je základním právem, které naplňuje zásadu transparentnosti. Pro subjekty údajů se jedná o pasivní právo, pro správce údajů o aktivní povinnost, protože musí automaticky (ne na požádání) informovat subjekt o zpracování. Informace musí být napsány jednoduše a srozumitelně. (Žůrek, 2018, s. 132-135)

Právo přístupu

Obecné nařízení dává subjektu právo získat potvrzení o zpracování osobních údajů, přístup a další doplňující informace ohledně osobních údajů. Důvodem pro přístup je možnost ověření zákonnosti zpracování osobních údajů, a zda vůbec takové zpracování existuje. Správce musí první kopii zpracovávaných údajů poskytnout bezplatně, za další kopii si může naúčtovat přiměřený poplatek. Informace musí být poskytnuty neprodleně a nejpozději do jednoho měsíce od obdržení žádosti. (Nezmar, 2017, s. 86)

Právo na opravu

Správce by měl bez zbytečného odkladu opravit nepřesné nebo nesprávné údaje týkající se subjektu. Podle účelu zpracování osobních údajů má subjekt právo na doplnění osobních údajů i pomocí dodatečného prohlášení. (Navrátil, 2018, s. 118)

Nulíček (2017, s. 206) dodává, že správce poskytne subjektu údajů informace o opatřeních písemně nebo v některých případech i elektronicky. V elektronické formě může dojít k doplnění údajů prostřednictvím vyplnění nepovinných polí.

Právo výmazu (být zapomenut)

Právo na výmaz je novým právem v oblasti zpracování osobních údajů a ukládá správci povinnost neprodleně vymazat osobní údaje subjektu. Důvody pro smazání osobních údajů jsou následující:

- pominutí účelu zpracování osobních údajů,
- odvolání souhlasu (pokud byl udělen) nebo neexistuje žádný právní důvod,
- podání námitky ze strany subjektu údajů,
- protiprávním zpracování,
- neudělení rodičovského souhlasu se zpracováním osobních údajů dětí,
- právní povinnosti stanovené Evropskou unií. (Obecné nařízení o ochraně osobních údajů prakticky, © 2017)

Právo omezit zpracování

Právo omezit zpracování osobních údajů je popsáno v článku 18 Obecného nařízení. Jsou zde vyjmenovány všechny případy, kdy správce musí omezit zpracování. Za takový případ je například považováno:

- popření přesnosti osobních údajů subjektem,
- protiprávní zpracování, ale subjekt si z nějakého důvodu nevyžaduje smazání osobních údajů,
- správce již údaje nepotřebuje (ale subjekt ano – pro právní nároky),
- vznesení námitky do ověření důvodů zpracování. (Nařízení Evropského parlamentu a Rady 2016/679)

Právo na přenositelnost dat

Právo na přenositelnost dat (právo na portabilitu) si klade za cíl umožnit převádět osobní údaje mezi správci tak, aby měl subjekt méně práce s kopírováním a přesouváním osobních údajů z jednoho IT prostředí do druhého. Právo na přenositelnost lze uplatnit pouze u automatizovaně zpracovávaných osobních údajů a zároveň musí být založeno na souhlasu nebo plnění smlouvy. Správce musí poskytnout osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu. Pokud je to možné, je vyžadováno, aby data byla předána správcem přímo druhému správci. (Nulíček, 2017, s. 221-223)

Právo vznést námitku (právo na stížnost)

Díky tomuto právu má subjekt osobních údajů právo vznést námitku proti zpracování jeho konkrétních osobních údajů. Pokud správce neprokáže závažné a oprávněné důvody pro zpracovávání osobních údajů a tyto důvody nepřevažují nad zájmy, právy a svobodami subjektu, nesmí správce dále osobní údaje zpracovávat. V případě využívání osobních údajů pro účely přímého marketingu můžu subjekt osobních údajů vznést kdykoliv námitku

proti tomuto zpracování a vše musí proběhnout zdarma. Na možnost vznést námitku týkající se zpracování osobních údajů by měl být subjekt údajů výslovně upozorněn. Především by toto právo mělo být odlišeno od ostatních informací. (Žůrek, 2018, s. 147)

Práva související s automatizovaným rozhodováním a profilováním

Pro společnosti je profilování velmi vhodný nástroj pro zvýšení prodeje a zisku, určení nejziskovějších i rizikových zákazníků apod. Pomocí profilování lze zjistit demografické nebo psychologické údaje, chování subjektů nebo předchozí nakupování atd. Pomáhá tak firmám efektivněji cílit marketing a umožňuje personalizaci nabídek. Pro určení, že se opravdu jedná o profilování, musí být splněny dvě podmínky, a to:

- údaje musí být zpracovávány automatizovaně,
- osobní údaje jsou používány k vyhodnocení některých osobních aspektů. (Nezmar, 2017, s. 92-94)

I pokud je zapojen do zpracování osobních údajů lidský faktor, jedná se v některých případech o automatizované zpracování. Například tabulky v Excelu obsahující osobní údaje zákazníků, kde jsou zákazníci hodnoceni a na jejich základě je pak rozhodnuto, jsou předmětem automatizovaného zpracování. (Nezmar, 2017, s. 92-94)

5 POSOUZENÍ VLIVU OCHRANY OSOBNÍCH ÚDAJŮ A POVĚŘENEC OSOBNÍCH ÚDAJŮ

Obecné nařízení ukládá povinnost Úřadu pro ochranu osobních údajů vypracovat seznam operací zpracování, které budou podléhat posouzení vlivu ochrany osobních údajů. Při posouzení vlivu ochrany osobních údajů je využívána zkratka DPIA (Data Protection Impact Assessment). ÚOOÚ se rozhodl stanovit operace s klasifikací rizikovosti operací – velmi rizikové, rizikové a ostatní. Zda společnost bude muset posuzovat vliv ochrany osobních údajů, je nutno zjistit, jestli zpracování osobních údajů má za následek vznik vysokého rizika pro práva a svobody fyzických osob, pokud zároveň přihlédne k povaze, rozsahu, účelu a kontextu zpracování a s využitím nových technologií. Vypracovaný dokument stanovuje několik obecných kritérií, podle kterých lze stanovit vysokou rizikovost zpracování osobních údajů. Firma by měla provádět posouzení vlivu pokud:

1. hodnotí bonitu fyzických osob, včetně profilování a předpovědi,
2. provádí automatické rozhodování s právním nebo obdobným významným účinkem,
3. systematicky monitoruje (včetně monitorování veřejně přístupných prostor),
4. zpracovává citlivé údaje a provádí zpracování velkého rozsahu,
5. kombinuje nebo propojuje data různých zpracování,
6. provádí zpracování údajů, které se týkají zranitelných subjektů údajů,
7. dochází k inovativnímu využití nebo aplikaci technologických nebo organizačních řešení,
8. provádí zpracování s obtížně uplatnitelnými právy subjektů údajů – v rámci veřejné oblasti, které se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy. (Dozorová činnost, © 2013)

Obecné nařízení ukládá některým správcům a zpracovatelům povinnost nominovat pověřence osobních údajů, tzv. DPO (Data Protection Officer). Postavení pověřence je podle Obecného nařízení klíčové, proto stanovuje podmínky, úkoly a postavení, kdy musí být pověřenec jmenován. (Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, © 2018)

Pověřenec by měl plnit pomocnou funkci nebo koordinovat ochranu osobních údajů správce nebo zpracovatele. Další jeho funkcí je zajištění komunikace s dozorovým orgánem, tedy Úřadem na ochranu osobních údajů. Hlavním úkolem pověřence je sledovat soulad

praxe s Obecným nařízením. Ke splnění tohoto úkolu využívá sběr informací, analýzu a kontrolu stanovených opatření k ochraně osobních údajů. Měl by informovat, radit a poskytovat doporučení správcům a zpracovatelům osobních údajů. (DPO, © 2019)

Ferrara a Spoto (© 2018) dodávají, že jmenovaný pověřenec osobních údajů pro svou práci potřebuje široký rozhled a především legální pohled na to, jak celý softwarový systém pracuje s osobními daty.

Nutnost jmenovat pověřence a další informace o pověřencích jsou zakotvena v Obecném nařízení v článku 37. Obecné nařízení ukládá povinnost jmenovat pověřence v případě, že správce nebo zpracovatele monitoruje rozsáhle a systematicky osobní údaje nebo zpracovává zvláštní kategorii údajů (trestní věci a trestné činy). Pověřenec musí být jmenován podle svých profesních kvalit (znalost práva a dostatečná praxe v oblasti ochrany osobních údajů) a může být jmenován i pro skupinu podniků. Zvolený pověřenec může být pracovníkem správce nebo zpracovatele, případně může tuto činnost provozovat na základě smlouvy. Nutností správce nebo zpracovatele je zveřejnění kontaktních údajů pověřence a sdělit je dozorovému úřadu. (Nařízení Evropského parlamentu a Rady 2016/679)

Nezmar (2017, s. 174) dodává, že pověřenec musí být nezávislý i když je podřízen vrcholovému managementu. Zájmy managementu nesmí nařizovat, jak řešit danou situaci, jakých výsledků má být dosaženo nebo jak má postupovat při vyšetřování stížnosti, případně zda vůbec konzultovat s dohledovým orgánem.

Aby správce mohl doložit dozorovému orgánu, že provedl všechny kroky k zajištění souladu se zpracováním osobních údajů, doporučuje se mít vypracovaný dokument, který prokáže, že nemusí být jmenován pověřenec a posouzení vlivu na ochranu osobních údajů. Tento dokument by měl obsahovat relevantní důvody, proč pověřenec nebyl jmenován. (Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, © 2018)

6 IT ZABEZPEČENÍ A KAMEROVÝ SYSTÉM

V současné době si nelze představit jakékoliv podnikání bez informačních technologií. To jaké informační technologie si společnosti zvolí, může mít vliv na celkový chod podnikání. Některé společnosti považují využívání nejnovějších technologií za nejlepší nástroj pro boj s konkurenceschopností, díky kterému mohou rychle a účinně reagovat na tržní prostředí a chování zákazníků. (Mulačová Věra a kol., 2013, s. 355)

Správce nebo zpracovatel bude muset osobní údaje zabezpečit a udělat všechny potřebné kroky k tomu, aby zamezil možnému úniku dat. Nutností je provést analýzu současného stavu ochrany osobních údajů a posoudit, zda například některá přístupová oprávnění jsou opravdu nutná pro jednotlivé činnosti. Při zjištění, že určitá osoba nebo skupina lidí nepotřebuje mít přístup k některým datům, je nutné omezit jejich přístup a toto rozhodnutí zdokumentovat v záznamech o činnostech zpracování. (IT a zabezpečení, © 2017)

Nezmar (2017, s. 221) uvádí, že bezpečnost dat uživatelů závisí na tom nejslabším článku. Takovým článkem může být vyplnění dat na nezabezpečeném formuláři (bez protokolu HTTPS). Tímto jsou data odeslána v textovém souboru a kdokoliv si je může přečíst. Velmi důležitým krokem je správné nastavení heslové politiky. Heslo by mělo mít velká a malá písmena, číslice a speciální znak. Používání dostatečně dlouhých a složitých hesel napomáhá k eliminaci úniku osobních dat a prodlužuje se doba nutná k prolomení hesla. Platí zde přímá úměra, čím složitější kombinace čísel, písmen a znaků, tím je potřebná doba pro prolomení hesla delší.

K ochraně hesla lze využít tzv. hashování. Jedná se o algoritmus, který si bere na vstupu zprávu jakékoliv velikosti a výstupem je pak kratší hodnota. Výstup se nazývá „hash“ a může být bez obav zveřejněn. Hashovací funkce jsou jednosměrné, takže nelze zjistit, vstupní data, která souvisí s heslem. (Sosinsky, 2016, s. 682)

Společnosti by se měly bránit i před viry. Nejlepším řešením je používání antivirového programu. Techniku, kterou hackeři využívají pro zašifrování dat, v zařízeních se nazývá ransomware. Po zašifrování dat požadují hackeři výkupné za vyzrazení přístupového hesla. Jedná se o sofistikovaný program, kterým se zařízení může infikovat při spuštění zavirované přílohy v e-mailu, webového prohlížeče nebo prohlížením webu, kde se tento vir nachází. Pro ochranu dat je doporučeno mít antivirový program, který obsahuje nástroj k odstranění ransomware. Obranou před napadením je pravidelná aktualizace všech programů,

operačního systému, prohlížečů a v neposlední řadě antivirového programu. (Ransomware, © 2016)

Instalace kamerového systému musí mít právní důvod, neboť je neoddělitelně spjatá s ochranou soukromí osob. Používání kamerového systému je již zakotveno v Občanském zákoníku, ale jelikož se bude jednat o zpracování údajů, musí se dále společnosti řídit i Obecným nařízením. (Janečková, 2018, s. 205)

Dalším zákonem, který upravuje kamerové systémy, je Zákoník práce. Zde jsou uvedeny důvody, pro které zaměstnavatel nesmí sledovat zaměstnance, aby nedošlo k narušení soukromí, až na zvláštní výjimky. Sledování osob a pořizování záznamů musí být nezbytné pro naplnění konkrétního účelu a vše musí být přiměřené vzhledem k okolnostem a ochraně soukromí osob. Za menší zásah do soukromí může být například považováno monitorování bez záznamu před zaznamenáváním pohybu se záznamem. Důležitou roli hraje také umístění kamery. (Dostál, © 2018)

Pokud se tedy správce osobních údajů rozhodne o využívání kamer, bude jeho povinností sdělit osobám, které mohou být předmětem monitorování, že jsou sledovány a musí být informováni, kdo za to zodpovídá. Informování musí být vždy jasné a srozumitelné, může být využito například piktogramu s uvedeným kontaktem na provozovatele. (Nezmar, 2017, s. 230)

Pro ty, kteří využívají kamerový systém, platí, že by měly vést záznamy o činnostech zpracování, které slouží jako doklad dozorovému úřadu, že podnik jedná v souladu s Obecným nařízením. Záznamy o činnostech zpracování jsou interní dokumenty, kde jsou uvedeny kontaktní údaje správce, účely zpracování, subjekty údajů a příjemců, případně lhůty pro výmaz a měly by být obecně popsány organizační a technické bezpečnostní opatření. (Hruška, © 2017)

7 SANKCE PŘI NEDODRŽENÍ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Cílem Obecného nařízení je zajištění soudržnosti a především zajištění vysoké ochrany osobních údajů. Jelikož ne všichni rozumí GDPR, u většiny firem se zvýší náklady na zavedení opatření, aby vše v podniku probíhalo v souladu s Obecným nařízením. Je možnost, že implementaci nebudou firmy z tohoto důvodu dělat dobrovolně, proto jsou sankce nastaveny poměrně vysoce. Na druhou stranu, výše sankce musí respektovat zásadu, která říká, že v každém případě musí být sankce účinná, přiměřená a odrazující. (Janečková, 2018, s. 105)

Krystlik (© 2017) uvádí, že nedodržování pravidel stanovených GDPR nebude tolerováno, proto společnosti mohou dostat pokutu až 4 % celosvětového obratu a až 20 milionů EUR.

Výše sankce bude záviset na mnoha faktorech. Jako příklad lze uvést povahu, délku a závažnost porušování, míra škody a počet poškozených občanů. Ke zmírnění/zvýšení sankce mohou pomoci kroky, které byly provedeny ke zmírnění škod atd. Mimo to, že bude společnost (správci osobních údajů) sankcionována, fyzické osoby je navíc mohou žalovat a požadovat náhradu škody. (Obecné nařízení o ochraně osobních údajů prakticky, © 2017)

Varováním může být sankce 50 milionů EUR udělená společnosti Google, protože neposkytla uživatelům odpovídající informace a nezískala souhlas pro personalizaci reklamy. Šetření této situace probíhalo několik měsíců na základě dvou neziskových firem ve Francii. Společnosti uvedli, že Google ztěžoval nalezení a nastavení týkající se zpracování osobních dat, zejména u cílené reklamy. Pokuta má být udělena za nedostatek transparentnosti, nedostatečné informace a nezískání platného souhlasu týkající se personalizace reklamy. Google je také vyšetřován kvůli údajnému porušení GDPR ve Švédsku kvůli údajnému shromažďování údajů o poloze uživatelů Android. V článku také stojí, že osm měsíců po zavedení GDPR byl počet stížností 95 000. Důvody pro stížnosti byly na telemarketing, propagační e-maily a video sledování. Během stejného období organizace provedly více než 41 000 oznámení dozorovým orgánům o narušení dat. (Computer Fraud & Security, © 2019)

Nezmar (2017, s. 43) dodává, že ne vždy musí být udělena pokuta. Správce může být nejprve upozorněn, že zpracování osobních údajů pravděpodobně porušuje Obecné nařízení, poté může být uděleno napomenutí, případně mu může být nařízeno dát vše do pořádku.

8 RIZIKOVÁ ANALÝZA

Ještě před samotným začátkem projektů by měla být brána v potaz rizika a nejistoty. Zvážení a integrace možnosti rizika do projektu je základním faktorem kvalitní přípravy. Taková příprava, hodnocení a výběr projektu proto vyžaduje:

- identifikaci rizika, které mohou ovlivnit výsledky projektu,
- stanovit a vyhodnotit dopad rizik na budoucí výsledky projektu,
- uvažovat o možných opatřeních, která by mohla snížit například náklady způsobené rizikem. (Fotr, Hnilica, 2014, s. 15)

Jelikož u pojmu riziko neexistuje pouze jedna definice, je nutné si uvést pro lepší chápání, alespoň některé z nich:

- *„pravděpodobnost či možnost vzniku ztráty, obecně nezdaru,*
- *odchýlení skutečných a očekávaných výsledků,*
- *nebezpečí chybného rozhodnutí,*
- *kombinace pravděpodobností a jejího následku.“* (Smejkal, Rais, 2013, s. 90)

Pro analýzu a následné vyhodnocení rizik existuje spousta metod. Smejkal, Rais (2013, s. 113) uvádí a popisují některé metody pro hodnocení rizik. Příkladem je například metoda Delphi, která je postavena na souboru otázek. Tyto otázky jsou rozděleny na pevnou a variabilní část. Variabilní část je využita podle postavení respondenta nebo podle průběhu rozhovoru. Dalšími metodami, které autoři popisují, jsou například CRAMM, @Risk, RiskPac nebo RiskWatch. Všechny tyto metody patří mezi kvantitativní metody a jedná se především o počítačové systémy nebo programy, které sice dokáží přesněji vyjádřit míru rizika, ale jsou dostupné za poněkud vyšší cenu než jiné metody.

Výběr metody vždy záleží na získaných informacích, možnostech hodnotitelů nebo na účelu posuzovaných rizik, případně druhu ohrožení. Jednou z metod pro hodnocení rizik je i jednoduchá polokvantitativní metoda „PZH“, která bere v potaz tři složky rizika a to:

- pravděpodobnost vzniku a existence rizika (P),
- závažnost možného následku rizika (Z),
- názor hodnotitele na riziko (H). (Nezmar, 2017, s. 126)

Každá složka (pravděpodobnost, závažnost a názor hodnotitele) je ohodnocena body od 1 do 5. Číslo 1 znamená nejnižší pravděpodobnost ohrožení i závažnosti rizika, naopak číslo

5 udává největší pravděpodobnost (téměř jisté) ohrožení. U stanovení následku je využita opět stupnice 1 až 5 a udává poškození údajů bez následku až po poškození údajů s fatálními následky. U poslední složky, názoru hodnotitelů, je nutné brát v potaz například počet ohrožených subjektů, míru závažnosti, dynamičnost rizika, vliv pracovního systému, úroveň zabezpečení dat a jiné. Události mohou mít zanedbatelný vliv na míru nebezpečí až po více významných a nepříznivých vlivů na závažnost u konkrétního rizika. Součinem všech tří složek ohodnocených stupnicí 1 až 5, dostaneme výsledné číslo hodnoty rizika (R). Výpočet tedy vypadá následovně: P*Z*H = R. (Nezmar, 2017, s. 126)

Nezmar (2017, s. 127) také uvádí konkrétní hodnoty rizika, a k těmto hodnotám přiřazuje míru rizika, viz následující tabulka.

Tabulka 2 Vyhodnocení rizik (vlastní zpracování podle Nezmara, 2017, s. 127)

Celkové riziko R	**Míra rizika**
> 100	Nepřijatelné
51-100	Nežádoucí
11-50	Mírné
3-10	Akceptovatelné
< 3	Bezvýznamné

9 SHRNUTÍ POZNATKŮ TEORETICKÉ ČÁSTI

Teoretická část je rozdělena na 8 kapitol, které mají za úkol popsat Obecné nařízení o ochraně osobních údajů. V první kapitole je definováno, co je to GDPR, jakou roli hraje Úřad pro ochranu osobních údajů při zpracování osobních údajů, stručná historie a vývoj ochrany osobních údajů a také hodnota osobních údajů.

V následující kapitole jsou vyjmenovány a popsány základní pojmy související s Obecným nařízením, např. osobní údaj, správce, zpracovatel nebo profilování. Dále jsou popsány zásady a principy, které musí společnosti implementovat do svých pravidel a kultury firmy, aby uspokojila podmínky zpracování osobních údajů zakotveného v Obecném nařízení.

Další kapitola se zabývá právy a povinnostmi. Jedná se o práva, která má každá fyzická osoba vůči jakékoliv organizaci ve smyslu zpracování osobních údajů. Povinnostmi se rozumí, co musí správce osobních údajů udělat pro to, aby uspokojil práva fyzických osob.

Následující kapitola popisuje podmínky pro vypracování posouzení vlivu ochrany osobních údajů a podmínky, zda musí správce nebo zpracovatel osobních údajů jmenovat pověřence, který ji bude radit v oblasti GDPR a zajišťovat soulad praxe s Obecným nařízením.

Jelikož většina firem (správců) využívá ke svému podnikání informační technologie, je nutné zmínit, jakých oblastí se GDPR dotýká v oblasti informačních technologií a jak zabezpečit, aby nedošlo k úniku dat.

Výše popsané kapitoly jsou důležité pro správnou analýzu osobních údajů v jednotlivých společnostech. Na základě popsaných pojmů, práv a povinností bude provedena analýza a následně projekt implementace Obecného nařízení do vybrané firmy.

V rámci předposlední kapitoly jsou zmíněny sankce, které mohou být uloženy správcům osobních údajů v případě nesouladu s Obecným nařízením. Zmíněna je také již první sankce, která byla udělena společnosti Google.

Poslední kapitola je věnována charakteristice rizikové analýze, která by měla být provedena u každého projektu pro zjištění hrozeb a případně stanovit, jak dané problémové situace řešit. Zejména je popsána metoda PZH, která bude využita i v projektové části diplomové práce.

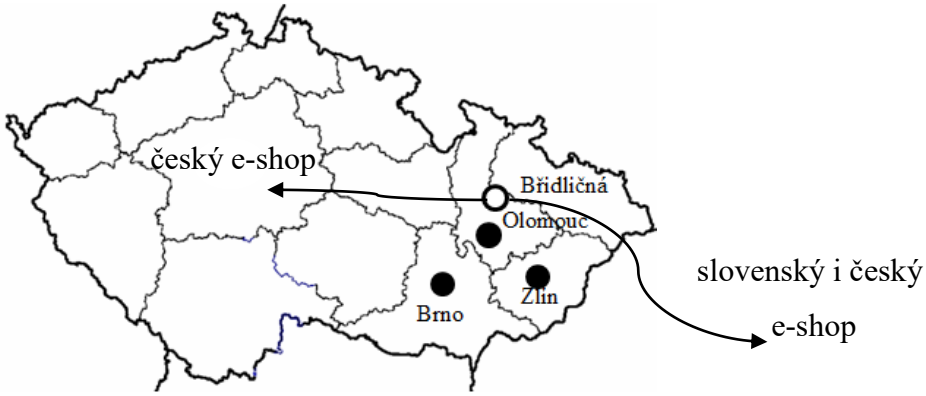
II. PRAKTICKÁ ČÁST

10 O SPOLEČNOSTI

Celé podnikání začalo již v roce 2012 formou živnostenského podnikání. Nejprve byl hlavní náplní prodej ořechů a sušeného ovoce přes e-shop, v dalších letech byly otevřeny tři prodejny. Protože podnikatelé chtěli získat ještě více zákazníků, rozšířili svůj sortiment a začali spolupracovat s firmami s podobným zaměřením.

10.1 Charakteristika společnosti

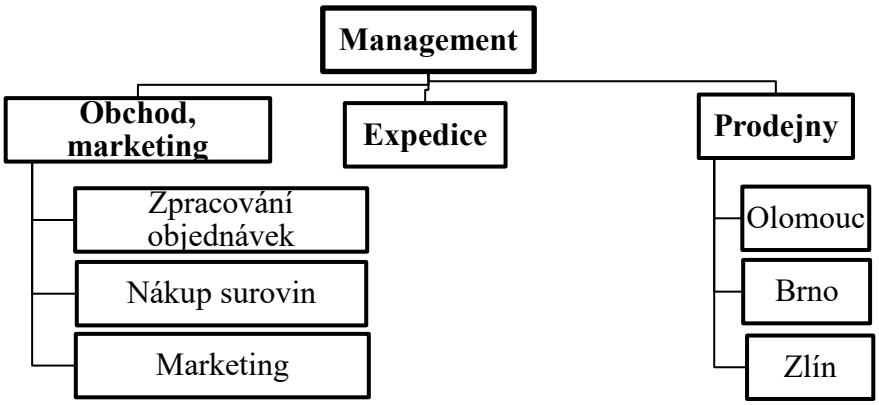
Nyní je právní forma vybrané firmy společnost s ručením omezeným, v obchodním rejstříku je zapsána od roku 2016. Sídlo firmy se nachází v Břidličné, okres Bruntál. Hlavním předmětem podnikání je prodej ořechů, přírodního sušeného ovoce, mrazem sušeného ovoce, semínek, superpotravin, vlastních výrobků z těchto surovin a ostatního sortimentu, do kterého lze zařadit například vanilkové lusky, kakaové produkty, čokolády, sušené houby nebo třeba přírodní potravinářská barviva. Společnost si pronajímá tři prodejny – ve Zlíně, Olomouci a nově od března 2019 také v Brně. Sklad se nachází v Břidličné, všechny objednávky jsou expedovány právě odtud. Další formou prodeje jsou dvě platformy e-shopu (česká a slovenská). Zákazníci mohou nakoupit i na české platformě v eurech a dodání na Slovensko je taky možné. Neznamená to, že pokud není objednávka provedena na slovenské platformě, že nemůže být dodána na Slovensko. Následující obrázek ukazuje rozložení prodejen a skladu, odkud putuje zboží k zákazníkům.



Obrázek 1 Rozmístění prodejen a skladu (vlastní zpracování)

Společnost vlastní dva muži, kteří jsou zároveň i jednateli a společnost zastupují každý samostatně. Základní kapitál je 200 000 Kč, a jejich podíly jsou stejné (každý 50 %). Celý management společnosti tvoří čtyři lidé – dva výše zmínění jednatelé, vedoucí prodejny ve Zlíně a vedoucí prodejny v Olomouci. Ostatní zaměstnanci pracují ve skladu, na prodej-

nách a jako administrativní pracovníci zodpovídající za chod e-shopu na obou platformách a marketing. Většina z nich jsou brigádníci studující na vysokých školách. Celkový počet zaměstnanců je 9 a počet brigádníků se průběžně pohybuje okolo 20 osob. Celou organizační strukturu znázorňuje následující obrázek.



Obrázek 2 Organizační struktura společnosti (vlastní zpracování)

Strategií společnosti je zaměřovat se na prodej přírodních produktů a stálé rozšiřování sortimentu trvanlivých potravin. Hlavním cílem společnosti je tedy rozšíření vysoce kvalitních potravin v oblasti oříšků a sušeného ovoce na českém a slovenském trhu. Nákupce vyhledává a nakupuje pouze kvalitní potraviny, proto se občas bohužel stane, že některé potraviny nejsou déle dostupné. Aby si společnost nepokazila pověst u zákazníků, nesnaží se sehnat zboží za každou cenu na úkor kvality suroviny. Jelikož se vybraná firma snaží ztotožnit s konceptem bezobalových prodejen, dala si za cíl používat co nejméně obalů a neplýtvat zbytečně potravinami ani obalovým materiálem. Na e-shopu si i zákazníci mohou vybrat, zda chtějí zboží balit do fólie nebo se rozhodnou šetřit materiál a nechají si balíček doručit bez spousty obalu. Tato možnost je hojně využívána.

Vybraná firma si velmi váží svých zákazníků a proto každá připomínka, pochvala nebo jakákoliv zpětná vazba je pro firmu stěžejní pro další rozvoj, ale také pro úspěšný boj s konkurencí.

10.2 Zákazníci

Společnost si rozděluje zákazníky na dva segmenty, a to na korporátní klienty (B2B) a spotřebitele (B2C).

V oblasti B2B zákazníků jsou největšími odběrateli cukrárny, restaurace, prodejny se zdravou výživou, bezobalové prodejny, čajovny, bistra, případně i některá fitness centra. Tito

zákazníci většinou nakupují ve velkých baleních, protože jsou cenově výhodnější a mnoho z nich se také přiklání k ochraně životního prostředí a používání co nejméně obalového materiálu, zejména plastu. U některého zboží jsou k dispozici až 25kg balení, ale jsou k dispozici i menší varianty balení (3 kg, 5 kg, 10 kg, 20 kg nebo například u kešu ořechů základní obchodní světový lot vážící 22,68 kg).

Co se týká B2C zákazníků, společnost odhaduje, že nejpočetnější skupinou jsou lidé ve věku 30-45 let. Na své si přijdou skupiny lidí jako vitariáni, vegetariáni, vegani, zájemci o zdravý životní styl nebo jen lidé, kteří preferují potraviny bez aditiv. Balení, která většinou tito zákazníci nakupují, jsou v rozmezí 50g až po 1kg balení. Nákup však není nijak omezen, takže kdokoliv si může zakoupit balení, které právě vyžaduje.

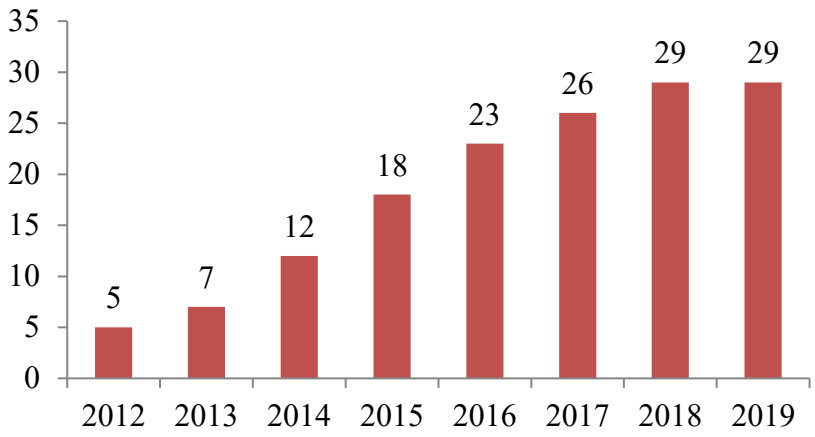
Při nákupu nad 3000 Kč má zákazník nárok na dopravu zdarma. Při nákupu nad 10 000 Kč má zákazník nárok na slevu. S tou však souvisí splnění dalších podmínek jako nákup velkých balení nebo nákup stanoveného počtu malých balení.

Pro zákazníky se tým mladých lidí společnosti snaží udělat maximum pro jejich spokojenost a formou zasílaných ochutnávek ke každé objednávce jim minimálně zlepšit den a navnadit k dalšímu nákupu a spolupráci.

10.3 Společnost v číslech

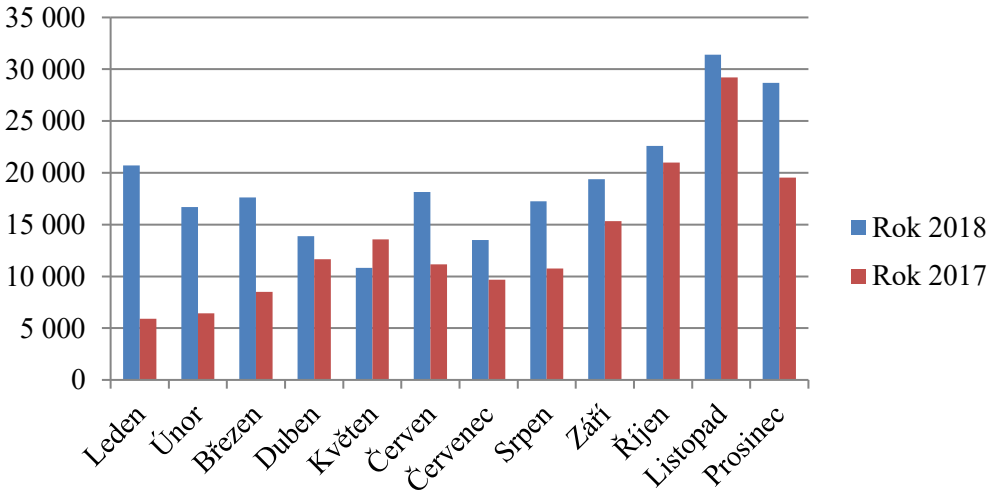
Od začátku podnikání stojí za celou činností podniku několik lidí. Při zahájení podnikání bylo ve firmě 5 zaměstnanců, kteří byli schopni zabezpečit celý chod firmy. Pro naplnění zvoleného cíle (v té době minimálně zdvojnásobit měsíční obrat) bylo nutné postupně navyšovat počet zaměstnanců, protože narůstal objem prodeje. Od roku 2016, kdy bylo živnostenské podnikání změněno na obchodní společnost, se společnost více zaměřila na marketing, za kterým stojí především externisté. Společnosti se stále zvětšoval objem prodeje a tak bylo nutné přijmout další pracovníky na administrativní činnost i do expedice. Nyní je počet pracovníků 29. Tento počet zahrnuje jak zaměstnance, brigádníky tak i externí pracovníky. V roce 2019 společnost neplánuje přijmout další pracovníky. Následující graf zachycuje celkový vývoj zaměstnanců.

Graf 1 Počet zaměstnanců v letech 2012 – 2019 (vlastní zpracování)



Vybraná společnost provádí svoji prodejní činnost ve třech prodejnách a přes internetový obchod, který je provozován přes dvě platformy. Pro představu, následující graf zobrazuje počet návštěvníků e-shopu v letech 2017 a 2018 v jednotlivých měsících. Údaje jsou sledovány a vyhodnocovány pro konkrétní zdroje vstupu uživatelů, v následujícím grafu jsou však údaje zobrazeny celkově za všechny zdroje za měsíc.

Graf 2 Počet návštěvníků eshopu v letech 2017 a 2018 (vlastní zpracování)



Z grafu 2 vyplývá, že oproti roku 2017 se v roce 2018 zvýšil počet návštěvníků v každém měsíci kromě května, kdy návštěvnost poklesla. V roce 2018 bylo zvýšení návštěvnosti způsobeno pravděpodobně lepší reklamou, které se společnost začala více věnovat. Z pozorování na prodejnách a případného zjišťování při rozhovoru bylo zjištěno, že pokud je v měsíci významná událost či svátek, lidé nakupují produkty vybrané společnosti více. Příkladem může být mírné zvýšení návštěvnosti v březnu 2018, kdy lidé slavili Velikonoce. Dalším příkladem může být měsíc červen, kdy začínaly prázdniny a lidé více nakupo-

vali dárková balení. Největší návštěvnost a celkově i prodejnost, nastala v říjnu, listopadu a prosinci, kdy největším motivem nákupu byly Vánoce jak u B2B zákazníků, kteří se chtěli především dobře zásobit, tak i B2C zákazníků, kteří nakupovali zboží jako dárek.

Vybraná společnost si nepřála zveřejnit žádné finanční výsledky, proto nejsou v práci uvedeny.

10.4 SWOT analýza

V rámci představení společnosti je provedena i SWOT analýza, která popisuje silné a slabé stránky společnost a také její příležitosti a hrozby, se kterými se potýká. Vše zachycuje následující tabulka.

Tabulka 3 SWOT analýza (vlastní zpracování)

Silné stránky	**Slabé stránky**
Prodej kvalitního zboží a široká nabídka	Nedodělané platformy e-shopu a nejednotnost
Vzdělání a zkušenosti v oblasti nákupu a prodeje ořechů a sušeného ovoce	Ne všichni zaměstnanci jsou zainteresováni do chodu firmy
Osobní přístup k zákazníkům, věrní zákazníci	
Výroba kvalitních produktů	
Dobré hodnocení od zákazníků na internetu	
Příležitosti	**Hrozby**
Rozvíjející se trh s ořechy a sušenými plody	Konkurence velkých a známějších firem
Větší zájem o zdravý životní styl a jiná životní přesvědčení (veganství apod.)	Legislativní změny
Větší zájem o potraviny bez aditiv	Ztráta důležitého dodavatele
Větší zájem o kvalitnější potraviny	Ztráta zájmu zaměstnanců vzdělávat se
	Změna preferencí ve stravování zákazníků

Na základě SWOT analýzy lze říci, že nejsilnější stránkou společnosti je především prodej a výroba kvalitních potravin v oblasti ořechů a sušeného ovoce a jejich široká nabídka. Další silnou stránkou je osobní přístup k zákazníkům založený na komunikaci a zájmu o ně. Díky tomu má společnost dobré (lze říci i velmi dobré) hodnocení na internetu. Další silnou stránkou je velký zájem, ochota a odborné znalosti majitelů a nákupčího společnosti ze světa ořechů a sušeného ovoce.

Mezi slabé stránky především patří to, že společnost nemá ještě úplně dokončený e-shop a zkouší ostatní provozovatele e-shopů. Slabou stránkou je i to, že někteří zaměstnanci berou svoji práci jako nutné zlo a nejsou zainteresování tak jako ostatní, které práce baví.

Jako příležitosti lze vyhodnotit celkově dnešní dobu, kdy lidé kladou větší důraz na to, co jedí a zajímají se o složení produktů a jejich kvalitu. Zejména lidé zajímající se o zdravý životní styl nebo různé formy životních stylů jako jsou vegani, vegetariáni apod.

Hrozbou pro společnost je, jako u každé jiné společnosti, její konkurence. Především se jedná o velké firmy nebo ty, které jsou lidem známější nebo cenově dostupnější (hlavně supermarkety). Dále lze považovat hrozbu i legislativní změny, především takové, které by mohly vybranou firmu stát celé podnikání (například zmiňované Obecné nařízení o ochraně osobních údajů). Nezájmem zaměstnanců vzdělávat se v oblasti prodeje, surovin a dalších souvisejících oblastí může společnost ztratit výhody, které lze mít díky odborným znalostem. V případě, že by se změnily stravovací návyky lidí, mohlo by dojít k úbytku zákazníků a tím by mohla být existence firmy ohrožena nebo alespoň by jí klesly zisky.

11 ANALÝZA SOUČASNÉHO STAVU OCHRANY OSOBNÍCH ÚDAJŮ

Tato kapitola se zabývá popisem a analýzou současného stavu ochrany osobních údajů. Na základě této analýzy bude zpracován projekt, pomocí kterého se do společnosti implementuje nařízení regulující ochranu osobních údajů fyzických osob. Pro účely diplomové práce se tedy jedná o osobní data B2C zákazníků a zaměstnanců firmy, ale v některých případech i o B2B zákazníky.

11.1 Jaká data jsou zpracovávána

V první řadě je nutno zmínit, že firma nemá zpracován žádný dokument, který by jakkoliv upravoval sběr, shromažďování nebo jakoukoliv manipulaci s osobními údaji. Proto, aby mohl být vůbec vytvořen nějaký dokument, který bude upravovat zpracování osobních údajů, je nutné zjistit, jaká data jsou vlastně nutná k poskytnutí služby a prodeji výrobků a zboží. Pro lepší zobrazení budou data rozdělena na zákaznický segment a zaměstnanecký segment.

11.1.1 Zaměstnanec

Ještě předtím, než se člověk stane zaměstnancem firmy, zasílá životopis na email firmy, popřípadě donese životopis osobně do kanceláře nebo na prodejnu. Pokud je uchazeč přijat, záleží ještě na tom, zda se bude jednat o brigádníka, který bude mít pouze dohodu o provedení práce nebo dohodu o pracovní činnosti, anebo se z něj stane zaměstnanec na hlavní pracovní poměr.

V případě, že je uzavřena pracovní smlouva, firma vyžaduje mít následující informace:

- jméno a příjmení (příp. jméno za svobodna),
- datum a místo narození,
- adresa trvalého bydliště,
- rodné číslo,
- zdravotní pojišťovna,
- telefon a email,
- číslo bankovního účtu,
- rodinný stav,
- děti,

- a zda bude uplatňován odpočet na děti.

V případě brigádníka se osobní údaje omezují pouze na jméno a příjmení, datum narození, telefon a email.

11.1.2 Zákazník

Zákazník, který nakupuje na prodejně, neuvádí žádné osobní údaje. Po zákazníkovi, který nakupuje přes e-shop, jsou vyžadována tato data:

- jméno a příjmení,
- telefon a email,
- fakturační adresa (ulice a číslo popisné, město, PSČ),
- případně doručovací adresa, pokud je rozdílná od fakturační adresy.

Výše uvedená data stačí k tomu, aby byla objednávka v pořádku vyřízena. Zákazník se může na e-shopu i registrovat, ale data, která vyplňuje při registraci, jsou totožná s těmi, která potřebuje pro obyčejnou objednávku. Zatím je společnost nijak nevyužívá. Pokud však dojde k reklamaci a zákazník se například rozhodne pro vrácení peněz, je již společnosti poskytnuto zákazníkovo číslo bankovního účtu.

11.2 Uložení dat

Co se týká ukládání dat osobních údajů, vyskytují se ve společnosti dokumenty jak v tištěné podobě tak i v elektronické.

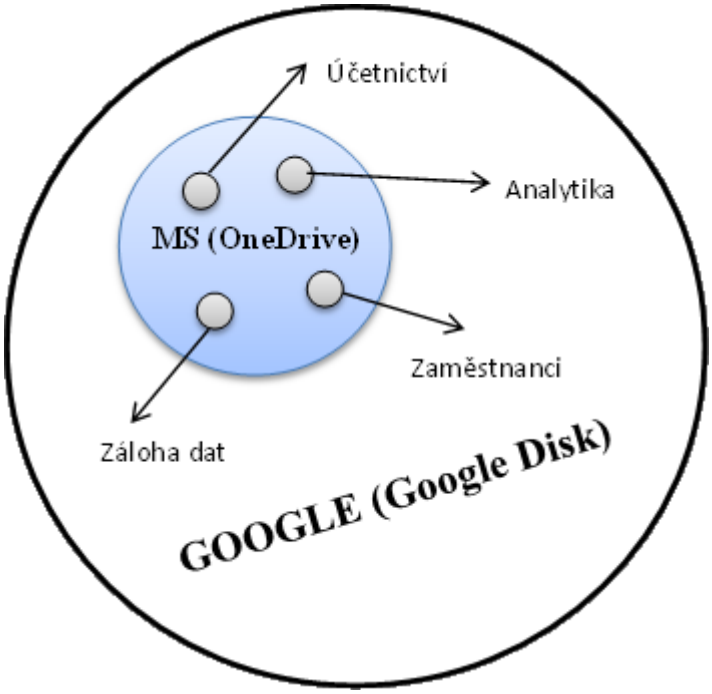
11.2.1 Zaměstnanec

Osobní údaje o zaměstnancích a brigádnících jsou uchovávána u účetní v šanonu v tištěné podobě. Pro případ ztráty nebo jakéhokoliv zničení jsou data uložena ještě na externím harddisku.

11.2.2 Zákazník

Zákazníkova osobní data vstupují do firmy při první provedené objednávce vyplněním formuláře, do kterého musí uvést údaje, které jsou zmíněny v kapitole 11.1.2. Tato data jsou pak uložena u poskytovatelů e-shopu shop.cz a eshop-rychle.cz, následně zálohována na externí harddisk a jsou také stále k dispozici na emailu. K dalším úložištím patří Google Disk.

Přehled o zpracovávaných datech a osobních údajů znázorňuje následující obrázek. Management pracuje na licencovaných MS aplikacích, na kterých jsou uložena data z oblasti účetnictví, analytiky, data o zaměstnancích a jsou zde zálohována všechna data, která se nacházejí na Google Disku. Na Google disku jsou pouze data, která jsou potřebná pro zpracování administrativy a objednávek. K těmto datům mají přístup všichni. Záloha na MS OneDrive se uskutečňuje ručně každý měsíc.



Obrázek 3 Schéma uložených dat (vlastní zpracování)

11.3 Přístup a ochrana dat

K osobním údajům zaměstnanců, brigádníků a zákazníků mají přístup čtyři lidé, kteří tvoří management společnosti. Jedná se o dva majitele, vedoucí prodejny ve Zlíně a v Olomouci. Ostatní členové týmu (administrativní pracovníci, provoz a expedice, obchod a marketing) i externí pracovníci mají k dispozici osobní údaje zákazníků, které jsou uloženy na platformách e-shopu a mají přístup i k některým dokumentům, které se nachází na Google Disku. K těmto datům se dostanou pomocí uživatelského jména a hesla. Existují však dokumenty a aplikace, ke kterým má přístup pouze management společnosti (například internetové bankovnictví – zabezpečení přes telefon). Mezi externí pracovníky patří například účetní, která má dostupné všechny dodavatelské a odběratelské faktury a osobní údaje o zaměstnancích.

11.4 Systémy a aplikace

Dalším bodem, který je nutné zjistit a analyzovat jsou všechny systémy a aplikace, ve kterých se osobní údaje zákazníků nebo zaměstnanců nacházejí. Ve vybrané společnosti se jedná o 3 platformy e-shopu (česká, slovenská a velkoobchod), přičemž platforma velkoobchodu je již ukončena, ale stále na ní jsou uloženy osobní údaje zákazníků, kteří pomocí ní uskutečnili nákup. Kompletně by měla být smazána tato platforma i s veškerými údaji ke konci května. Podle informací o zpracování osobních údajů jedna platforma získává a zpracovává pouze jméno, adresu a kontaktní informace a tyto informace jsou následně uchovávány 15 let po ukončení smluvního vztahu. Osobní údaje slouží k plnění smlouvy a online marketingu. Na dalších dvou (velkoobchodní a slovenská) mají pouze e-mailovou adresu, kterou zpracovávají pouze za účelem zasílání newsletteru.

Jako další aplikaci, která zpracovává osobní údaje zákazníků, lze uvést MailChimp. Pomocí této aplikace zasílá společnost svým B2B i B2C zákazníkům hromadné e-maily s novinkami nebo různými slevami a akcemi, aby tak zvýšila prodejnost. B2B zákazníci jsou umístěni v databázích podle toho, zda se jedná o bezobalové prodejny nebo retailové prodejny. Jelikož Obecné nařízení je zaměřeno na fyzické osoby, je nutné se nyní zaměřit především na B2C zákazníky, ale bude nutné získat souhlas i od B2B zákazníků, které lze identifikovat například pomocí emailu. Pro účely marketingu jsou vytvořeny databáze zákazníků podle částky, za kterou v minulosti nakoupili (např. skupina, která zakoupila během určitého období nad 3000 Kč). Jelikož se jedná o profilování, které bylo popsáno v kapitole 2.6 Profilování, bude nutné získat výslovný souhlas s profilováním.

Pro potřeby účetnictví má externí účetní k dispozici účetní program, kde účtuje všechny faktury a jsou dostupné i informace o zaměstnancích.

Pro komunikaci se zákazníky používá firma internetový chat – SmartsUpp. V této aplikaci jsou uvedeny osobní údaje zákazníka, konkrétně jméno a příjmení a místo, odkud píše. Někteří zákazníci, kteří se dotazují, vystupují pod číslem, které jim je přiděleno, pokud neuvedou své kontaktní údaje. Pokud je chat vypnutý, dotaz přijde na email a je zde uvedeno veškeré prohlížení eshopu zákazníkem.

Nedílnou součástí celého procesu nákupu na internetu je také platba a doprava za zboží. Pro tyto účely mají zákazníci k dispozici platbu pomocí dobírky, převodem, pomocí bitcoinu a nebo přes GoPay. Právě tento způsob platby vyžaduje další údaje, které by mohly být zneužity. Zákazníci jsou přesměrováni na další internetovou stránku, kde vyplňují in-

formace platební karty. Zabezpečení těchto údajů již nespadá do povinností společnosti, ale je nutné, mít správně nastaveny smluvní podmínky.

Co se týká dopravy, má společnost uzavřenou smlouvu se skupinou dopravců. Na všech platformách dopravců jsou zadávány informace, které jsou nutné k nákupu zboží, konkrétně doručovací adresa a kontaktní údaje jako e-mail a telefonní číslo. Přístup je omezen pomocí uživatelského jména a hesla.

Pro marketingové účely využívá firma Google Analytics, nástroj, který umožňuje získat osobní data týkající se návštěvnosti, chování uživatelů a prodeje. Od společnosti Google využívá společnost ještě Google Adwords, která je využívána za účelem zvýšení prodejnosti. Tato služba využívá klíčových slov a inzerenti tak mohou zvýšit návštěvnost a vyhledávání svých webových stránek. Jako nástroj využívaný v rámci internetové reklamy využívá společnost hlavně PPC (pay-per-click), kdy inzerent platí za reklamu až tehdy, pokud na ni někdo klikne.

Společnost dále využívá pro marketingové účely ještě Sklik a FacebookAds. Obojí slouží pro reklamní účely, kde jsou lidem zobrazovány stránky podle toho, o co se zajímají. Například Facebook.com má funkci, kde si uživatel může nastavit přímo oblasti, o které se zajímá, a následně jsou mu zobrazovány reklamy z této oblasti. Reklamní články nebo upozornění jsou na sociální síti Facebook označeny slovy „*sponzorováno*“.

Propagaci provádí firma pomocí účtu na sociální síti Facebook a Instagram. Obě sociální sítě používá k propagaci a informování zákazníků o různých novinkách či akcích.

11.5 Ochrana osobních dat v obchodních podmínkách

Doposud podléhalo zpracování osobních údajů Zákonu o ochraně osobních údajů. Na základě tohoto zákona firma informovala zákazníky a návštěvníky eshopu prostřednictvím obchodních podmínek. Pravidla, která měla společnost stanovena, vypadají následovně:

8.1. Ochrana osobních údajů kupujícího, který je fyzickou osobou, je poskytována zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

8.2. Kupující souhlasí se zpracováním těchto svých osobních údajů: jméno a příjmení, adresa bydliště, identifikační číslo, daňové identifikační číslo, adresa elektronické pošty, telefonní číslo a (dále společně vše jen jako „osobní údaje“).

8.3. Kupující souhlasí se zpracováním osobních údajů prodávajícím, a to pro účely realizace práv a povinností z kupní smlouvy a pro účely vedení uživatelského účtu. Nezvolí-li kupující jinou možnost, souhlasí se zpracováním osobních údajů prodávajícím také pro účely zasílání informací a obchodních sdělení kupujícímu. Souhlas se zpracováním osobních údajů v celém rozsahu dle tohoto článku není podmínkou, která by sama o sobě znemožňovala uzavření kupní smlouvy.

8.4. Kupující bere na vědomí, že je povinen své osobní údaje (při registraci, ve svém uživatelském účtu, při objednávce provedené z webového rozhraní obchodu) uvádět správně a pravdivě a že je povinen bez zbytečného odkladu informovat prodávajícího o změně ve svých osobních údajích.

8.5. Zpracováním osobních údajů kupujícího může prodávající pověřit třetí osobu, jakožto zpracovatele. Kromě osob dopravujících zboží nebudou osobní údaje prodávajícím bez předchozího souhlasu kupujícího předávány třetím osobám.

8.6. Osobní údaje budou zpracovávány po dobu neurčitou. Osobní údaje budou zpracovávány v elektronické podobě automatizovaným způsobem nebo v tištěné podobě neautomatizovaným způsobem.

8.7. Kupující potvrzuje, že poskytnuté osobní údaje jsou přesné a že byl poučen o tom, že se jedná o dobrovolné poskytnutí osobních údajů.

8.8. V případě, že by se kupující domníval, že prodávající nebo zpracovatel (čl. 9.5) provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života kupujícího nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může:

- požádat prodávajícího nebo zpracovatele o vysvětlení,
- požadovat, aby prodávající nebo zpracovatel odstranil takto vzniklý stav.

8.9 Požádá-li kupující o informaci o zpracování svých osobních údajů, je mu prodávající povinen tuto informaci předat.

11.6 IT vybavení a zabezpečení

Ve firmě jsou čtyři notebooky, na kterých je přístup úplně ke všem informacím. Jedná se o notebooky managementu. Několik dalších notebooků, které vlastní firma je určena pracovníkům expedice. V případě ostatních pracovníků, převážně brigádníků a externistů, jsou používány jejich vlastní notebooky a zařízení. Firma ke své práci využívá také několik

tiskáren a chytrých telefonů. K veškeré komunikaci je využíváno WiFi připojení, které je dle smlouvy s poskytovatelem šifrováno. Pokud dojde k výpadku internetového připojení, lze využít hotspot přes mobilní telefon, pokud má některý z pracovníků dostupná internetová data. Vyskytují se ale i situace, kdy pracovník využívá veřejné WiFi připojení. Jako prvek zabezpečení komunikace lze vnímat šifrování pomocí HTTPS. Pomocí HTTPS je zajištěna bezpečná komunikace zákazníkům, kteří provádí objednávku na e-shopu. Do budoucna společnost plánuje zapojení a využívání kamerového systému na prodejnách k ochraně majetku před krádeží zboží nebo jiného vybavení.

Zabezpečení dat je prováděno pomocí Microsoft Defender, integrovaného antiviru ve Windows 10. U některých notebooků jsou nainstalovány ještě free verze různých dostupných antivirů, bohužel u některých chybí jakákoliv ochrana. K ochraně osobních dat, která jsou uložena jak na Google Disku tak i na One Drive úložišti, slouží pouze přihlašovací jméno a heslo, které je stanoveno a dosud se aktualizuje jednou za rok. Změna ostatních hesel, na stránky dopravců, poskytovatele e-shopu i internetové bankovnictví, probíhá taky jednou ročně nebo v případě nějakého problému. Firma již má stanovenou osobu, která bude za tuto problematiku zodpovídat a zároveň má za úkol stanovit, jak často bude docházet k aktualizaci hesel. K zálohování dat dochází pouze ručně po týdnu, kdy z Google Disku jsou data zkopírována na One Drive.

12 PŘEHLED NESOULADŮ – SHRNUTÍ GAP ANALÝZY

Po provedené analýze současného stavu ochrany osobních údajů je potřeba zjistit, s jakými nedostatky se firma potýká v souvislosti s Obecným nařízením. K tomuto účelu bude využita GAP analýza, která bude podkladem pro projektovou část. Součástí analýzy bude i popis nutných kroků k odstranění nesouladů. Pro úspěšnou implementaci GDPR bude nutné udělat následující kroky.

1. Přesně a výstižně stanovit účel zpracování osobních údajů.

Přesné a výstižné stanovení účelu zpracování osobních údajů bude prvním krokem, od kterého se budou následující kroky a opatření odvíjet. Stanovené účely musí být transparentně vyvěšeny.

2. Vytvořit záznamy o činnostech zpracování.

Záznamy o činnostech zpracování budou sloužit pro dozorový úřad v případě kontroly. Především budou vypracovány z důvodu využívání kamerového systému, ale budou vytvořeny i pro ostatní účely zpracování.

3. Při zavedení kamerového systému informovat zaměstnance a vyvěsit na vstupní dveře informování zákazníků o monitorování.

I přesto, že zatím kamery na prodejně nejsou, bude součástí projektu alespoň příprava informačního listu, který po zavedení kamerového systému bude vyvěšen na hlavních dveřích každé prodejny, která bude monitorována. Poté musí následovat informování zaměstnanců o umístění kamery a fungování kamery.

4. Získat souhlas s profilováním.

Získání souhlasu s profilováním souvisí s předchozím bodem, kdy firma musí získat výslovný souhlas, že subjekt údajů souhlasí s profilováním – v tomto případě se jedná o zařazení subjektu do kategorie s nákupem nad určitou částku nebo kategorie B2B a B2C zákazníků, aby mohly být těmto subjektům zasílány například informace o produktech, které by mohly být vhodné pro jejich použití, případně dražší produkty, které běžně každý nenakupuje.

5. Stanovit rozsah zpracovávaných osobních údajů pro každou jednotlivou činnost.

V rámci GDPR je důležité myslet i na minimalizaci dat. V tomto kroku bude muset být stanoven rozsah, jaké osobní údaje budou zpracovávány pro každou jednotlivou činnost.

6. Vytvořit databázi získaných souhlasů.

Společnost bude muset mít vytvořenou databázi, kde budou evidovány všechny získané souhlasy, jejich doba platnosti, případně odvolání souhlasu. Zároveň pak neudělený souhlas nesmí být podmínkou neposkytnutí služby.

7. Upravit obchodní podmínky.

V obchodních podmínkách již nemůže být zahrnuta problematika ochrany osobních údajů.

8. Vytvořit informační memorandum pro zákazníky.

Obecné nařízení nařizuje transparentní informovanost subjektů o zpracování jejich osobních údajů, proto bude pro tento účel vyvěšeno na stránky e-shopu informační memorandum.

9. Vytvořit informační memorandum pro zaměstnance.

Zaměstnanci musí být informování o rozsahu a účelech zpracování jejich osobních údajů podobně jako zákazníci. Proto musí být vytvořeno memorandum, se kterým budou seznámeni stávající zaměstnanci a bude přidáváno k nově podepisovaným pracovním smlouvám nebo jiným dohodám týkající se pracovní činnosti.

10. Nastavit a zavést kontrolní mechanismy.

Doposud ve společnosti neexistují kroky nebo mechanismy, které by měly za úkol kontrolovat, zda je s osobními údaji nakládáno v souladu s Obecným nařízením, případně jiným nařízením nebo zákonem.

11. Nastavit pravidla pro zabezpečení osobních údajů – zabezpečení dat.

Je nutné revidovat stávající zabezpečení osobních údajů a pravidla užívání mobilních zařízení a přístupu k datům.

12. Stanovit odpovědnosti za zpracování osobních údajů a nastavit pravidla přístupů.

U každého účelu zpracování je nutné nastavit odpovědnou osobu, která za zpracování osobních údajů bude zodpovídat, případně bude provádět kontrolní mechanismy. Nově by také mělo být určeno, kdo bude mít přístup k jednotlivým datům.

13. Zavést pravidla pro případné využití práv subjektů údajů a vypracovat návrh vzorových odpovědí.

V případě, že by subjekt údajů (v případě vybrané firmy se jedná o zákazníky a zaměstnance) využil některých z práv, která mu Obecné nařízení uděluje, je vhodné mít přichys-

táno řešení, jak postupovat při jednotlivém uplatňovaném právu a mít k dispozici vzorové odpovědi.

14. Vypracovat dokument pro ohlášení porušení zabezpečení osobních údajů.

V případě úniku dat je důležité mít vypracovaný postup i vzorovou zprávu, která umožní kontaktovat a informovat dozorový úřad co nejrychleji při porušení zabezpečení osobních údajů či jejich úniku.

15. Vypracovat vzorovou zprávu pro subjekt údajů v případě porušení zabezpečení.

Při porušení zabezpečení dat je nutné informovat také subjekty údajů, proto je nutné mít k dispozici zprávu, která se pak jen odešle subjektu údajů a o případném úniku jejich osobních údajů je informuje.

16. Vypracovat soubor pro vyhodnocení rizik.

Nutností je zhodnotit rizika, která souvisí se zpracováním osobních údajů ať už v elektronické nebo papírové podobě a taky konkrétní možný způsob v rámci způsobu zpracování, jak mohou data uniknout.

17. Vypracovat vzorové odpovědi pro dotazy týkající se osobních údajů.

Je pravděpodobné, že dotazy, kterou budou na správce nebo zpracovatele mířeny, se budou opakovat, proto pro zjednodušení a urychlení jejich práce, budou připraveny vzorové odpovědi na nejčastější dotazy ohledně Obecného nařízení a zpracování osobních údajů.

18. Vytvořit vnitřní předpis pro uchovávání jednotlivých osobních údajů.

Vnitřní předpis stanoví, jak bude nakládáno s osobními údaji a jak dlouho budou uchovávány jednotlivé dokumenty.

19. Vypracovat dokument, který analyzuje nutnost zpracování DPIA a vytvoření nové pracovní pozice DPO.

Pro případnou kontrolu dozorovým úřadem bude vytvořen dokument, který odůvodňuje mít nebo nemít jmenovaného pověřence a provádět nebo neprovádět DPIA.

20. Informovat a proškolit zaměstnance.

Nutností je informování zaměstnanců jak nakládat s osobními údaji zákazníků a především v tomto bodě sdělit zaměstnancům, jaká jejich data jsou zpracovávána a jak jsou chráněna. Zaměstnanci budou proškoleni.

13 PROJEKT IMPLEMENTACE GDPR

Poslední částí diplomové práce je samotný projekt implementace Obecného nařízení. Doposud fungovala vybraná firma podle zákona o ochraně osobních údajů i přesto, že Obecné nařízení o ochraně osobních údajů je účinné již od 25. května 2018. Jako podklad pro projekt slouží výše provedená GAP analýza, která určuje, jaké kroky musí být provedeny, aby firma prováděla svoji činnost podle platné legislativy v oblasti ochrany osobních údajů. Protože některé dokumenty nebo texty budou určeny pouze pro interní potřeby, nebudou tyto dokumenty zveřejněny v diplomové práci.

13.1 Stanovení cílů a postupu implementace

Cílem projektu je provést taková opatření, aby ochrana osobních údajů, které vybraná firma spravuje a zpracovává, bylo v souladu s Obecným nařízením o ochraně osobních údajů. Prvním krokem, který je nutný provést je stanovit účel, za jakým jsou osobní údaje subjektů spravovány a zpracovávány. Dalším krokem, který bude také základním krokem k úspěšné implementaci GDPR, je stanovení rozsahu zpracování osobních údajů pro jednotlivé činnosti. Dále se bude jednat o vytvoření databáze získaných souhlasů, informačního memoranda pro zákazníky i zaměstnance. Nutností je také zavedení kontrolních mechanismů a nastavení pravidel zabezpečení. Z Obecného nařízení také vyplývá, že musí být stanovena odpovědná osoba a musí být určena pravidla pro přístup k osobním údajům subjektů. Pro zjednodušení budou vytvořeny vzorové odpovědi a dokumenty, které budou sloužit v případě, že subjekt osobních údajů využije svá práva a bude vyžadovat informace o zpracování jeho osobních údajů. Pro případné porušení ochrany osobních údajů bude vytvořeno hlášení pro dozorový úřad a pro subjekty údajů, které informuje o možném ohrožení. Důležité je také vypracování analýzy zpracování DPIA, jmenování DPO a provedení analýzy rizik. Všechny informace, pravidla a postupy budou zakotveny ve vnitřním předpisu vybrané společnosti, která bude na závěr celého projektu proškolena, jak nakládat s osobními údaji zákazníků a zaměstnanců. Nakonec bude vypracována ekonomická a riziková analýza celého projektu.

13.2 Stanovení účelu zpracování osobních údajů

Jak již bylo zmíněno výše, stanovení účelu zpracování osobních údajů je základním a také nejdůležitějším krokem pro úspěšnou implementaci Obecného nařízení. Přesně a výstižně

stanovený účel bude vyvěšen na webových stránkách společnosti, aby byla splněna podmínka transparentnosti a informovanosti subjektů osobních údajů.

Zpracování osobních údajů subjektů se provádí za účelem zpracování objednávky, vyřízení jakéhokoliv dotazu nebo poptávky a pro zasílání newsletterů. Tyto účely jsou posuzovány jako právní důvody, na jejichž základě může společnost spravovat a zpracovávat osobní údaje bez udělení souhlasu. Z online marketingu jsou využívány nástroje Google Analytics, Sklik a FacebookAds. K účelu zpracování se váže pouze využívání Google Analytics, protože ostatní nástroje jsou placené a ochrana osobních údajů je přenesena na společnosti poskytující tyto nástroje, proto nejsou předmětem projektu. Nastavení zpracování osobních údajů lze nastavit v prohlížeči každého subjektu, zda souhlasí nebo nesouhlasí se zpracováním cookie souborů, které jsou spravovány právě pro účely Google Analytics.

Účel zpracování osobních údajů se vyskytuje i ve vytvořených dokumentech s názvem „**Záznamy o činnostech zpracování**“. Tento dokument je vytvořen pro účel zpracování a vyřízení objednávky, vedení účetnictví, zasílání obchodních sdělení, pro využívání kamerového systému, který společnost zatím nevyužívá, ale jelikož použití plánuje na prodejnách, bude jej mít k dispozici, a další. Záznamy o činnostech zpracování jsou interním dokumentem, ale návrh k jednomu účelu zpracování je k dispozici níže v tabulce. Tyto záznamy pak budou sloužit pro dozorový úřad jako doklad, jak je s osobními údaji nakládáno u jednotlivého účelu zpracování.

Tabulka 4 Návrh záznamu o činnostech zpracování (vlastní zpracování)

Záznamy o činnostech zpracování na základě 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
Účel zpracování osobních údajů – ZPRACOVÁNÍ OBJEDNÁVKY
Titul zpracování – splnění smlouvy
1. Kdo je správcem osobních údajů k tomuto účelu?
Název společnosti, sídlo, IČO
2. Kdo je zpracovatelem osobních údajů?
Dopravci, banky

3. Kterých subjektů se tento účel týká?
Stávající i noví zákazníci
4. Které konkrétní osobní údaje jsou zpracovávány za tímto účelem?
Jméno, příjmení, fakturační a doručovací adresa, e-mailová adresa, telefonní číslo, informace o předchozích objednávkách, reklamacích či dotazech (pro vyřízení reklamace i číslo bankovního účtu)
5. Odkud jsou osobní údaje subjektů získány?
Na e-shopu prostřednictvím provedené objednávky
6. Jaká je podoba uložení osobních údajů?
Elektronická i papírová
7. Kdo má přístup k osobním údajům?
Všichni zaměstnanci (kromě zaměstnanců na prodejnách)
8. Kdo má odpovědnost za osobní údaje?
Jednatel
9. Jaká je doba uchování osobních údajů?
Doba uchování je 10 let
10. Jaké jsou provedeny technické a organizační opatření?
Přijetí potvrzovacího e-mailu při provedené objednávce, zabezpečení archivu, zamezení přístupu neoprávněným osobám k osobním údajům, zabezpečení e-mailu i e-shopu pomocí přihlašovacího jména a hesla

13.3 Stanovení rozsahu zpracovávaných osobních údajů

S ohledem na zásadu minimalizaci dat musí být určen také rozsah zpracování osobních údajů. Pro zákazníky, kteří provádí objednávku přes e-shop, se jedná o osobní údaje potřebné pro vyřízení objednávky – konkrétně o osobní údaje jako je jméno a příjmení, telefon, e-mail a adresní údaje, které jsou nutné pro doručení zásilky. Všechny údaje budou uchovávány po dobu 10 let.

13.4 Získání souhlasu k profilování a jeho evidence

Pro zpracování dat pomocí profilování je nutné získat výslovný souhlas subjektu osobních údajů. Pro tento účel se však společnost rozhodla neprovádět profilování, tudíž nebude

získávat souhlas se zpracováním osobních údajů a nemusí tak vést ani evidenci (databázi) získaných souhlasů, která by v případě získávání souhlasu byla povinná.

13.5 Obchodní podmínky

Vše, co se týkalo ochrany osobních údajů, bylo zapsáno v obchodních podmínkách. Nyní již tento způsob informování nestačí a dokonce je i protiprávní. Pro tento účel je vytvořeno Informační memorandum pro zákazníky, které je podrobněji popsáno v následující kapitole. Část, týkající se ochrany osobních údajů, byla tedy smazána z obchodních podmínek.

13.6 Informační memorandum

Protože zákazníci i zaměstnanci musí být informování o tom, kdo je správcem jejich osobních údajů, jaké údaje jsou o nich zpracovávány, jak dlouho se uchovávají, za jakým účelem jsou data zpracovávána, komu jsou osobní údaje předávány, zda jsou používány soubory cookie, jaká jsou práva subjektů údajů, jak společnost zabezpečuje jejich osobní údaje, jakým způsobem mohou vznést námitku a především kontakt, na který se mohou obrátit v případě využití práv nebo jakéhokoliv dotazu týkající se ochrany osobních údajů, jsou vytvořeny dva dokumenty – konkrétně s názvem Informační memorandum (pro zákazníky i pro zaměstnance).

13.6.1 Informační memorandum pro zákazníky

Tento dokument bude vyvěšen na webových stránkách společnosti. Bude sloužit pro informování zákazníků, kteří budou provádět objednávku, poptávku či jakoukoliv komunikaci, při které uvedou své osobní údaje. Informování se týká následujících bodů:

1. Kdo je správcem a zpracovatelem osobních údajů?
2. Za jakým účelem jsou zpracovávány osobní údaje?
3. Jaké údaje jsou zpracovávány?
4. Komu jsou předávány osobní údaje?
5. Jsou používány soubory Cookie?
6. Jak dlouho jsou zpracovávány osobní údaje?
7. Zpracování osobních údajů se souhlasem a bez něj.
8. Zabezpečení osobních údajů.
9. Práva subjektů osobních údajů.
10. Jakým způsobem lze vznést námitku proti zpracování osobních údajů?

11. Kontakt na správce při jakémkoliv dotazu ohledně ochrany osobních údajů.

Část dokumentu je k dispozici také v příloze č. 1, avšak údaje o vybrané firmě nejsou k dispozici.

13.6.2 Informační memorandum pro zaměstnance

Informování zaměstnanců ohledně ochrany osobních údajů proběhne prostřednictvím školení. Následně bude vytvořen dokument, ve kterém je stručně shrnutý obsah školení. Obsahem školení i dokumentu jsou informace o konkrétních právních důvodech zpracování, jaké údaje jsou uchovávány a zpracovávány, je definován účel zpracování osobních údajů, komu jsou poskytovány osobní údaje subjektů, jak dlouho jsou osobní údaje uchovávány. Dalším bodem je, že zaměstnanec bere na vědomí, že v případě přístupu k osobním údajům třetích osob je zavázán mlčenlivostí a především k ochraně osobních údajů třetích osob z důvodu ztráty, změně, zničení atd. Podpisem tohoto dokumentu zaměstnanec souhlasí se všemi podmínkami v něm uvedených a zavazuje se tyto podmínky dodržovat. Podpis dokumentu je tedy brán jako informování subjektu osobních údajů o zpracování jeho osobních údajů a také o jeho právech. V případě jakékoliv změny bude muset být vypracován nový dokument, který musí následně zaměstnanci znovu podepsat.

Část návrhu informačního memoranda pro zaměstnance se nachází v příloze č. 2.

13.7 Nastavení a zavedení kontrolních mechanismů

Kontrolní mechanismy lze chápat jako nástroj, pomocí kterého bude ověřováno, zda jsou stanovená pravidla k ochraně osobních údajů dodržována. Kontroly se budou provádět jednou za čtvrtletí. Každé čtvrtletí bude zvolena jedna osoba managementu společnosti, která provede kontrolu dodržování zákonného zpracování osobních údajů u zákazníků a u zaměstnanců. Kontrolu nemůže provádět jakýkoliv zaměstnanec, protože by mohlo dojít k úniku dat o jednotlivých zaměstnancích, proto mohou kontrolu provádět jen ty osoby, které mají přístup ke všem osobním údajům společnosti. Především je toto rozhodnutí postaveno na tom, že vedení společnosti má zájem na zákonném postupu a nemělo by tak docházet ke kontrolám, jen aby se splnily. Pro účel kontrolních mechanismů bude vytvořen dokument, ve kterém bude popsáno, co se má provádět, jak často a budou se zde zaznamenávat i případné problémy nebo návrhy na nové kontrolní mechanismy či opatření. Následující tabulka ukazuje návrh na přehledné zaznamenávání kontrol osobních údajů, který je částí vytvořeného dokumentu.

Tabulka 5 Návrh na zaznamenávání kontrol osobních údajů (vlastní zpracování)

Datum	Kdo provedl kontrolu	U jakého zaměstnance	Počet zákazníků	Návrh na změnu/zjištěný problém	Podpis

13.8 Nastavení pravidel pro zabezpečení dat

Nejlepší způsobem, jakým zajistit ochranu osobních údajů je preventivní zabezpečení. První krok, který byl společnosti navrhnutý, bylo nastavení hesel při vstupu do počítače nebo notebooku. Každý počítač tedy bude vyžadovat zadání hesla. Bylo stanoveno, že heslo bude desetimístné a musí obsahovat velká a malá písmena, číslice a nějaký speciální znak. Jedná se i o notebooky a počítače, které jsou majetkem pracovníků, kteří provádí zpracování osobních údajů zákazníků. V případě odejití od počítače se bude muset pracovník odhlásit. Hesla se budou měnit čtvrtletně, ale v případě, že bude mít pracovník jakékoliv (i to nejmenší tušení), že mohlo dojít k vyzrazení přístupových údajů, neprodleně změní heslo.

Co se týká mobilních telefonů, každý telefon bude mít nastavené buď heslo při odemčení telefonu, nebo určený znak, pomocí kterého se telefon odemkne.

V případě tiskáren a ostatních zařízení bude zavedeno pravidlo, že ten, kdo nemá oprávněný přístup k osobním údajům subjektů, nesmí být v místnosti při provádění činnosti.

13.9 Stanovení odpovědnosti a pravidel přístupů

Stanovení odpovědné osoby za zpracování osobních údajů je nedílnou součástí projektu. Určená osoba bude zodpovídat za dodržování nastavených pravidel, která budou v souladu s Obecným nařízením. Tato osoba je zapsána ve vnitřním předpisu a v případě kontroly dozorovým úřadem, nebo pokud dojde k porušení ochrany zabezpečení dat, bude povinna situaci řešit. Jelikož odpovědná osoba bude jedna osoba z managementu společnosti, mezi další povinnosti zodpovědné osoby je občasné provádění kontrolních mechanismů, které jsou představeny a popsány v kapitole 13.6 Nastavení a zavedení kontrolních mechanismů.

Co se týká pravidel přístupů, ty jsou popsány taktéž ve vnitřním předpisu ochrany osobních údajů. Jsou stanoveny jednotlivé kategorie (složky nebo dokumenty), ke kterým mají pří-

stup opravdu jen lidé, kteří ke své práci tyto údaje potřebují. Dojde tak k zamezení přístupu neoprávněným osobám a zúží se tak možnost úniku nebo ztráty dat.

13.10 Pravidla a vzorové odpovědi pro subjekty osobních údajů

Další částí projektu bylo vytvoření vzorových odpovědí pro subjekty osobních údajů. V této části byly sepsány také pravidla, především lhůty, kterými je nutno se řídit v případě uplatnění práv subjektů. Byly vypracovány odpovědi na dotazy subjektů, které společnost považuje za nejčastější. Níže je uveden příklad jednoho dotazu a vypracované vzorové odpovědi.

Dotaz: *„Co se děje s mými osobními údaji, když už je mi objednané zboží doručeno?“*

Odpověď:

„Dobrý den, pane/paní …,

Vaše osobní údaje máme v elektronické i papírové podobě uloženy, protože se nacházejí na fakturách, které jsou zasílány ke každé objednávce. Jedná se konkrétně o tyto údaje:

- jméno a příjmení,
- fakturační a doručovací adresa,
- telefonní číslo a emailová adresa.

Doba uchování těchto dokumentů je 10 let. Dále zpracováváme Vaše osobní údaje k zasílání newsletteru. Pokud si to již nepřejete, můžete se odhlásit na webových stránkách. K jiným účelům Vaše osobní údaje nevyužíváme.

V případě nejasností nás neváhejte kontaktovat.

S pozdravem (*název firmy, odpovědná osoba, která dotaz vyřizuje*)“

Jedná se o návrh odpovědi, kterou může brát společnost jako základ pro ostatní odpovědi. Ne vždy budou dotazy stejné nebo konkrétní, proto bude nutné na jednotlivé dotazy vzorovou zprávu upravovat podle potřeby. Pro dotazy je vytvořená i databáze, ve které se bude evidovat, kdo se dotazoval, e-mail, datum doručení dotazu, kdo a kdy odpověděl. Tato databáze bude především sloužit k tomu, aby se předešlo případnému nedodržení lhůty, které jsou stanoveny pro vyřízení dotazů ohledně osobních údajů. Následně, pokud bude mít jedna osoba více dotazů či nepřiměřené dotazy, mohou být výpisy zpoplatněny. Návrh evidence je zobrazen níže.

Tabulka 6 Návrh evidence dotazů (vlastní zpracování)

Evidence dotazů					
Tazatel	**E-mail**	**Datum**	**Kdo odpovídal**	**Datum**	**Poplatek**
Jméno	*jmeno@jmeno.cz*	*Datum dotazu*	*Odpovědná osoba*	*Datum odpovědi*	*Ano/Ne*

13.11 Dokumenty pro ohlášení porušení zabezpečení

V případě, že dojde k porušení zabezpečení osobních údajů, je správce povinen kontaktovat dozorový úřad a informovat jej o možnosti narušení ochrany dat. Povinností je provést tento krok bezodkladně, nejpozději však do 72 hodin od zjištění problému. Pro tuto situaci jsou vytvořeny dva dokumenty, které budou sloužit pro informování dozorového úřadu a pro informování subjektů, kterých se bude narušení ochrany dat týkat.

13.11.1 Dokument pro ÚOOÚ

Pro informování Úřadu na ochranu osobních údajů o možném incidentu jsou dvě možnosti. První možností je vyplnění dokumentu přímo na webových stránkách tohoto úřadu. Tento formulář je poměrně dlouhý, ale zato jsou zde předepsány informace, které jsou nutné pro další řízení.

Druhou možností je mít připravený formulář k tomuto účelu, který bude stručnější, ale bude také splňovat požadavky, které musí být uvedeny při incidentu. Jelikož v případě porušení zabezpečení ochrany osobních údajů není moc času na vyplňování dlouhých formulářů, bude vypracován kratší dokument. Následující tabulka ukazuje návrh zkráceného formuláře pro ohlášení incidentu pro dozorový úřad.

Tabulka 7 Návrh formuláře pro ohlášení incidentů dozorovému úřadu (vlastní zpracování)

Identifikační údaje společnosti	Název společnosti, adresa, IČO
Typ oznámení	1. Úplné oznámení (v případě všech dostupných informací) 2. Postupné ohlášení (nejsou k dispozici všechny údaje k učinění úplného oznámení)
Povaha porušení	Kategorie a počet možných ohrožených subjektů

Příčina porušení zabezpečení	Krádež, hackerský útok apod.
Popis provedených opatření	Organizační a technická opatření provedená, aby nedošlo k porušení zabezpečení (případně jaká nová opatření budou zavedena, aby se incidenty neopakovaly)
Pravděpodobné důsledky porušení ochrany osobních údajů	
Datum, čas a místo porušení ochrany osobních údajů	

13.11.2 Dokument pro subjekty údajů

V případě porušení zabezpečení ochrany osobních údajů je nutno informovat i subjekty osobních údajů o tom, že by mohlo, nebo že došlo k ohrožení jejich osobních údajů. Pro tento případ je nachystána vzorová zpráva, která bude v případě incidentu rozeslána dotčeným subjektům osobních údajů.

Vypracovaná vzorová zpráva obsahuje informaci, že mohlo dojít nebo došlo k ohrožení osobních údajů, dále přesný popis události, co se stalo, kdy k incidentu došlo a jaké osobní údaje jsou (nebo by mohly být) předmětem ohrožení a především kontakt na správce osobních údajů v případě jakéhokoliv dotazu dotčených subjektů.

Následuje návrh vypracované zprávy pro subjekty údajů v případě porušení ochrany osobních údajů.

„Vážený pane/paní……..,

protože nám záleží na spolupráci s Vámi a zavázali jsme se respektovat Vaše soukromí, spravovat a zpracovávat Vaše osobní údaje podle 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 (GDPR), dovolujeme si Vás upozornit v rámci preventivního opatření, že MOHLO DOJÍT/DOŠLO k ohrožení Vašich osobních údajů.

K události (*přesný popis události, která způsobila narušení bezpečnosti osobních údajů*) došlo dne……. Osobní údaje, které by mohly být předmětem ohrožení, jsou následující: (*vyjmenovat konkrétně, pokud je možné, že některé údaje neunikly, vyjmenovat taky*).

Pravděpodobné důsledky narušení Vašich osobních údajů mohou být …(*popsat*).

K narušení bezpečnosti osobních údajů došlo za těchto okolností: …(*popsat*).

Proto, abychom ochránili Vaše osobní údaje jsme provedli ... (*přijatá opatření, i opatření, která byla provedena ke zmírněn možných nepříznivých účinků*)

V případě jakéhokoliv dotazu nás neváhejte kontaktovat na email ……. nebo na telefonu ……

S pozdravem

(*název firmy*)“

13.12 Vyhodnocení rizik

Pomocí metody PZH popsané v kapitole 8 Riziková analýza, bude vypracován systém hodnocení rizik. Hodnocení rizik se týká jednotlivých podob zpracování osobních údajů, tzn. osobní údaje v papírové a elektronické podobě. Následující tabulka zachycuje vyhodnocení rizik spojených s papírovou podobou uchování osobních údajů.

Tabulka 8 Hodnocení rizik uchování osobních údajů v papírové podobě (vlastní zpracování)

Zdroj rizika	**Konkrétní nebezpečí**	**Hodnocení rizika (P*Z*H)**	**Bezpečnostní opatření**
Ztráta dokumentů obsahující data zákazníků nebo zaměstnanců	Nesprávná archivace, nepřehledné uspořádání, přístup neoprávněným osobám	3*3*3 = **27**	Správná archivace, nový přístup k uspořádání dokumentů, zabezpečení vstupu pouze oprávněným osobám
Odcizení nebo zneužití osobních údajů	Neoprávněný přístup k údajům	3*3*4 = **36**	Zabezpečení vstupu pouze oprávněným osobám
Zničení nebo poškození dokumentů	Nedbalost zaměstnance (nehoda, chyba)	3*3*4 = **36**	Informování a školení zaměstnance jak zacházet s dokumenty

Zdroj rizika	**Konkrétní nebezpečí**	**Hodnocení rizika (P*Z*H)**	**Bezpečnostní opatření**
Zničení nebo poškození dokumentů	Přírodní katastrofa (vichřice, požár, záplavy)	2*3*2 = **12**	Vést záznamy v elektronické podobě, záloha
Zničení nebo poškození dokumentů	Nekvalitní tisk nebo vyblednutí dokumentu	2*2*2 = **8**	Vést záznamy v elektronické podobě, záloha
Neoprávněný přístup k osobním údajům	Zaslání zásilky s fakturou jiné osobě	3*3*3 = **27**	Dvojitá kontrola, školení

Z výše uvedené tabulky je patrné, že největším rizikem u papírového uchovávání osobních dat subjektů je odcizení, zničení nebo poškození osobních údajů v důsledku nedbalosti zaměstnance nebo umožněním přístupu k osobním údajů neoprávněným osobám. Následují rizika spojená se ztrátou dokumentů způsobenou nesprávnou archivací nebo nepřehledným uspořádáním. Dalším rizikem je neoprávněný přístup k osobním údajům, který může být způsobem například zasláním zásilky s fakturou jiné osobě. Ve všech případech jsou stanovena konkrétní bezpečnostní opatření, aby se předešlo stanoveným rizikům.

Následující tabulka znázorňuje zdroje rizika, nebezpečí, hodnocení a bezpečnostní opatření při uchovávání dat v elektronické podobě.

Tabulka 9 Hodnocení rizik uchování osobních údajů v elektronické podobě (vlastní zpracování)

Zdroj rizika	**Konkrétní nebezpečí**	**Hodnocení rizika (P*Z*H)**	**Bezpečnostní opatření**
Ztráta dat	Hackerský útok	2*3*3 = **18**	Vhodné hardwarové a softwarové vybavení a zabezpečení
Vyzrazení/únik/ ztráta přístupových hesel	Přístup neoprávněným osobám k osobním údajům zaměstnanců a zákazníků	3*3*4 = **36**	Školení zaměstnanců, nastavená heslová politika,
Ztráta či záměna dat zákazníka	Chyba způsobená softwarovým nebo hardwarovým selháním	3*4*4 = **48**	Častá aktualizace, nové IT vybavení, vhodné IT zabezpečení, potvrzovací email
Ztráta, poškození nebo přístup k osobním údajům	Napadení virem	3*3*2 = **18**	Dostatečná ochrana antivirovým programem
Únik dat	Zasílání dat mezi pracovníky přes sociální sítě	4*3*4 = **48**	Upraveno ve vnitřním předpisu - zákaz zasílat jakékoliv údaje týkající se subjektů údajů přes sociální sítě

Uchovávání a zpracování osobních údajů v elektronické podobě s sebou nese největší riziko ztráta nebo záměna dat zákazníka způsobená softwarovým nebo hardwarovým selháním. Toto riziko je hodnoceno 48 body. Dalším, stejně ohodnoceným rizikem, je únik dat způsobený zasíláním interních informací přes sociální sítě. Následuje riziko spojené s vyzrazením nebo únikem přístupových hesel s ohodnocení 36 bodů. I v těchto případech

jsou stanovena bezpečnostní opatření, především se jedná o školení zaměstnanců, zavedení dobré heslové politiky, častou aktualizací a opatření týkající se IT vybavení. Potvrzovací e-mail řeší problematiku záměny dat zákazníka, například při registraci či změně osobních údajů.

Pro posouzení o jak velké riziko se jedná, je použita stupnice, která je uvedená v kapitole 8 Riziková analýza. Pro přehlednost je umístěna tatáž tabulka i zde.

Tabulka 10 Stupnice pro vyhodnocení rizik (vlastní zpracování podle Nezmara, 2017, s. 127)

Celkové riziko R	Míra rizika
> 100	Nepřijatelné
51-100	Nežádoucí
11-50	Mírné
3-10	Akceptovatelné
< 3	Bezvýznamné

Na základě výše uvedené stupnice se nejedná o nežádoucí nebo nepřijatelná rizika. Maximální stanovené riziko je vyhodnoceno jako mírné. I takto označená rizika však nelze brát na lehkou váhu. Doporučuje se mít vypracovaný plán opatření podle rozhodnutí managementu společnosti.

13.13 Analýza potřeby DPIA a DPO

Pro některé společnosti vyplývá z Obecného nařízení provádět DPIA (Posouzení vlivu ochrany osobních údajů) a mít jmenovaného DPO (Pověřence osobních údajů). Vybraná společnost nespadá do kategorie organizací, které budou muset mít jmenovaného pověřence na ochranu osobních údajů nebo provádět Posouzení vlivu ochrany osobních údajů. Vyplývá to z analýzy, která byla provedena na základě poznatků z kapitoly 5 Posouzení vlivu na ochranu osobních údajů a pověřenec na ochranu osobních údajů a také na základě schválených pokynů Evropským sborem pro ochranu osobních údajů (Pracovní skupiny WP29) popsaného v kapitole 1.4. Související právní předpisy a pojmy.

Vypracovaná analýza bude sloužit pro dozorový úřad při případné kontrole nebo jako důkazní materiál v případě porušení zabezpečení osobních údajů. Následující tabulky ukazují část dokumentu vypracovaného v rámci této analýzy.

Tabulka 11 Část analýzy na posouzení vlivu na ochranu osobních údajů (vlastní zpracování)

DPIA (posouzení vlivu na ochranu osobních údajů)	
Podmínka	**ANO/NE**
Provádí se ohodnocení nebo hodnocení bonity fyzických osob, včetně profilování a předpovědi	NE
Provádí se automatické rozhodování s právním nebo obdobným významným účinkem	NE
Provádí se systematické monitorování, včetně monitorování veřejně přístupných prostor	NE
Provádí se zpracování citlivých údajů	NE
Provádí se zpracování velkého rozsahu	NE
Provádí se kombinace nebo propojování dat různých zpracování	NE
Provádí se zpracování osobních údajů týkající se zranitelných subjektů údajů	NE
Dochází k inovativnímu využití nebo aplikaci technologických nebo organizačních řešení	NE
Provádí se zpracování s obtížně upravitelnými právy subjektů údajů – pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy	NE

Další tabulka je také součástí vypracované analýzy, tentokrát se týká potřeby mít jmenovaného pověřence. Existují zde také podmínky, které mohou pomoci k rozhodnutí, zda je potřeba mít jmenovaného DPO.

Tabulka 12 Část analýzy o jmenování pověřence osobních údajů (vlastní zpracování)

DPO (pověřenec pro ochranu osobních údajů)	
Podmínka	**ANO/NE**
Zpracování osobních údajů provádí orgán veřejné moci nebo veřejný subjekt	NE
Hlavní činností správce nebo zpracovatele v operacích zpracování je vyžadováno rozsáhlé pravidelné a systematické monitorování subjektů údajů	NE
Hlavní činností správce nebo zpracovatele je rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů	NE

13.14 Vnitřní předpis

Výstupem projektu je i vnitřní předpis, ve kterém je vše podrobně popsáno. Každý bod uvedený v GAP analýze je zachycen a popsán ve vnitřním předpisu. Jedná se například o stanovený účel a rozsah zpracování osobních údajů, záznamy o činnostech zpracování, jsou zde zahrnuta i informační memoranda, informace ke kontrolním mechanismům, zabezpečení dat, stanovení odpovědné osoby a pravidla přístupů k osobním údajům, vzorové odpovědi na nejčastější dotazy, postup pro ohlašování porušení zabezpečení osobních údajů, vzorová zpráva pro subjekt v případě porušení zabezpečení, návrh formuláře pro dozorový úřad, vypracovaná analýza nutnosti zpracování DPIA a vytvoření nové pozice DPO. Na základě tohoto dokumentu bylo sestaveno i školení.

13.15 Školení zaměstnanců

Pro úspěšné dokončení implementace bylo na základě vnitřního předpisu provedeno školení, které mělo za úkol informovat zaměstnance, co nového Obecné nařízení přináší a jaké další povinnosti jim toto nařízení ukládá. Nejde jen o taxativní vymezení, co vše musí pracovníci dělat, ale každý pracovník by měl pochopit podstatu celého nařízení. Proto bylo na začátku školení alespoň stručně shrnuto, co je Obecné nařízení, koho se týká a byly také objasněny pojmy týkající se ochrany osobních údajů. Školení vycházelo z vypracovaného vnitřního předpisu a pracovníkům tak bylo vysvětleno, jak se k osobním údajům chovat. Dalšími částmi školení byl například způsob zpracování dat, jak postupovat v případě dotazů subjektů osobních údajů, jak postupovat při porušení zabezpečení údajů, seznámení

s heslovou politikou. Všichni zaměstnanci pak svým podpisem potvrdili, že byli proškoleni a seznámeni s povinnostmi týkající se Obecného nařízení.

14 ZÁVĚREČNÉ ZHODNOCENÍ

Po všech provedených krocích implementace je na řadě zhodnocení celého projektu. Zhodnocení proběhne z hlediska času, rizik, nákladů a budou níže popsány také přínosy celého projektu.

14.1 Časové zobrazení trvání projektu

Zhodnocení z hlediska času bylo provedeno pomocí metody CPM (Critical Path Method), která je jednou z metod síťové analýzy. Metoda pomocí „kritické cesty“ zobrazuje trvání projektu. Prvním krokem je stanovení:

- jednotlivých aktivit,
- doby trvání aktivit,
- všech předchozích aktivit (všechny činnosti předcházející jednotlivým aktivitám).

Stanovení výše jednotlivých kroků shrnuje následující tabulka.

Tabulka 13 Jednotlivé aktivity projektu (vlastní zpracování)

Označení aktivity	Aktivita	Počet dnů	Předchozí aktivity
A	Stanovení účelu zpracování osobních údajů	1	-
B	Stanovení rozsahu zpracování osobních údajů	1	A
C	Rozhodování o profilování, získávání souhlasu a evidence těchto souhlasů	1	A, B
D	Vytvoření informačního memoranda pro zákazníky	1	A, B, C
E	Vytvoření informačního memoranda pro zaměstnance	1	A, B, C
F	Nastavení pravidel zabezpečení	2	A, B
G	Stanovení odpovědnosti a nastavení pravidel přístupů	2	A, B, F
H	Stanovení pravidel při využití práv + vzorové zprávy	1	A, B, E

Označení aktivity	Aktivita	Počet dnů	Předchozí aktivity
I	Nastavení a zavedení kontrolních mechanismů	2	A, B, G
J	Vypracování dokumentu pro dozorový úřad v případě porušení zabezpečení dat	1	A, B, F, G, I, M, N
K	Vypracování vzorové zprávy pro subjekty v případě porušení zabezpečení dat	1	A, B, G
L	Vyhodnocení rizik jednotlivých podob zpracování	2	A, B, G, I
M	Analýza potřeby DPIA a DPO	1	A, B
N	Vytvoření vnitřního předpisu	3	A, B, F, G, I, L, M
O	Školení zaměstnanců	3	N

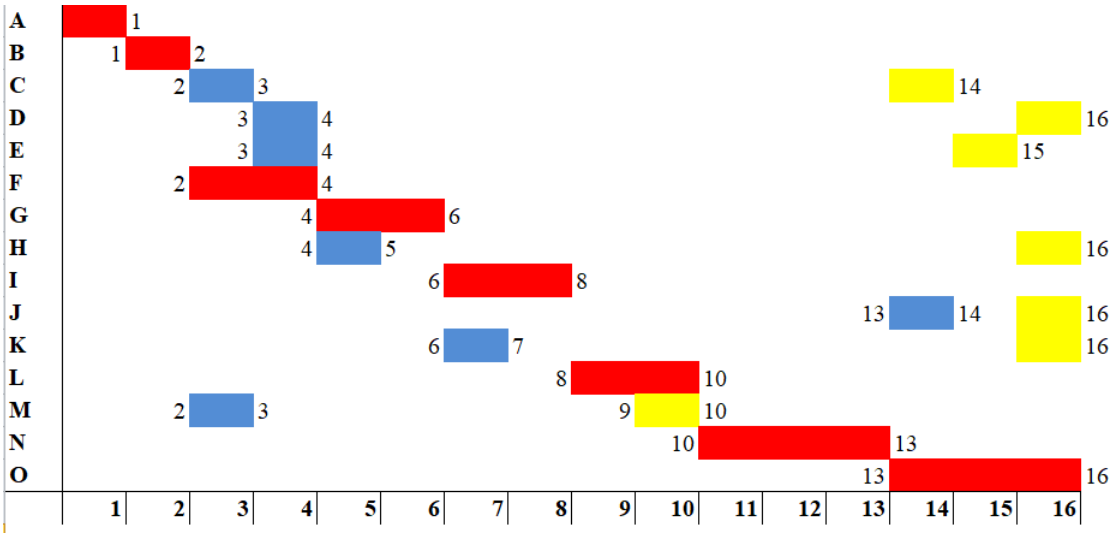
Po zadání vstupních dat do programu QM for Windows je získána kritická cesta. Kritická cesta (nejkratší možná doba projektu) je vyznačena červeně, konkrétně se jedná o činnosti A, B, F, G, I, L, N, O. V případě, že by se zpozdila některá z činností kritické cesty, celý projekt by se zpozdil. Následující obrázek znázorňuje kritickou cestu.

Activity	Activity time	Early Start	Early Finish	Late Start	Late Finish	Slack
Project	16					
A	1	0	1	0	1	0
B	1	1	2	1	2	0
C	1	2	3	13	14	11
D	1	3	4	15	16	12
E	1	3	4	14	15	11
F	2	2	4	2	4	0
G	2	4	6	4	6	0
H	1	4	5	15	16	11
I	2	6	8	6	8	0
J	1	13	14	15	16	2
K	1	6	7	15	16	9
L	2	8	10	8	10	0
M	1	2	3	9	10	7
N	3	10	13	10	13	0
O	3	13	16	13	16	0

Obrázek 4 Aktivity projektu (vlastní zpracování v QM for Windows)

Pomocí programu QM for Windows byla určena nejkratší možná doba, za kterou mohlo být Obecné nařízení na ochranu osobních údajů implementováno do společnosti. Nejkratší doba projektu byla po výpočtu softwarovým programem stanovena na 16 dnů. Program také vypočítal nejdříve možné začátky a konce jednotlivých činností a v posledním sloupci je vyobrazena celková rezerva (obrázek 4). Tato rezerva znamená, o kolik dní lze jednotlivou činnost posunout, aby nebyl ovlivněn průběh projektu.

Výstupem z programu QM for Windows je také grafické zobrazení průběhu projektu na následujícím obrázku. Následující obrázek znázorňuje graficky kritickou cestu (červená), nejdříve možné začátky a konce (modrá), nejpozději možné začátky a konce (žlutá).



Obrázek 5 Kritická cesta projektu (vlastní zpracování na základě QM for Windows)

Celková doba implementace ale trvala déle, konkrétně 22 dnů (169 hodin), tento údaj je zobrazen v tabulce 14, ve které jsou uvedeny náklady projektu.

14.2 Riziková analýza

Každý projekt s sebou nese určitá rizika. Pro zhodnocení projektu z hlediska rizik je použita metoda PZH, která již byla jednou využita v kapitole 13.11 Vyhodnocení rizik. Jedná se o analýzu situací, které mohou ohrozit projekt, jejich zdroj a následně jsou stanovena opatření, pomocí kterých lze zmírnit nebo úplně odstranit možné riziko.

Tabulka 14 Riziková analýza projektu (vlastní zpracování)

Zdroj rizika	**Konkrétní nebezpečí**	**Hodnocení rizika (P*Z*H)**	**Bezpečnostní opatření**
Špatná implementace	Zatajení informací	3*4*4 = **48**	Vysvětlení podstaty Obecného nařízení
Špatná implementace	Nedostatečná analýza, špatná spolupráce vedení nebo ostatních zaměstnanců	4*4*3 = **48**	Zaměření se na detaily, vysvětlení podstaty Obecného nařízení
Špatná implementace	Nepochopení Obecného nařízení	4*4*4 = **64**	Prostudování a získání znalostí Obecného nařízení, proškolení
Incident	Porušení zabezpečení dat v průběhu projektu	4*4*5 = **80**	Správné zabezpečení osobních údajů
Sankce	Kontrola dozorovým úřadem ještě před implementací GDPR do podnikové praxe	5*5*5 = **125**	Okamžité zavedení Obecného nařízení
Sankce	Špatné nebo nedostatečné zabezpečení dat, nesprávná implementace	4*4*4 = **64**	Získání znalostí Obecného nařízení

Z rizikové analýzy vyplývá, že největším rizikem je udělení sankce, která může být způsobena opožděnou implementací. Riziko je ohodnoceno 125 body. Toto riziko je největší z toho důvodu, že Obecné nařízení je již účinné téměř rok a vybraná společnost neprovedla žádný krok k tomu, aby splnila stanovené požadavky. V takovém případě by pak mohla být výše sankce pro vybranou společnost likvidační, protože dozorový úřad by nemohl brát v úvahu žádnou snahu ani provedené opatření k zabezpečení osobních údajů zákazníků a zaměstnanců. Druhým největším rizikem, souvisejícím s tím předchozím, je taktéž uděl-

lení sankce, ale z důvodu, že dojde k porušení zabezpečení (úniku) dat. Následují rizika způsobená nepochopením Obecného nařízení, špatnou nebo nedostačující vstupní analýzou, která je podkladem pro správnou implementaci. Mezi opatření tedy lze zařadit nejprve vysvětlení podstaty Obecného nařízení, aby byl každý motivován spolupracovat a nedošlo tak například k zatajení některých informací.

14.3 Analýza nákladů projektu

U každého projektu se musí počítat s vynaloženými náklady. Záleží na managementu společnosti, kolik peněžních prostředků jsou ochotni vložit do jednotlivých projektů. Vybraná společnost, jako většina ostatních, přemýšlí, kde ušetřit a proto vybírá variantu s nejnižšími náklady. Jinak tomu není ani u tohoto projektu.

Proto, aby proběhla správná implementace, je nutné stanovit správný základ, ze kterého bude projekt vycházet. Nejprve tedy bylo důležité se seznámit s prostředím vybrané firmy a poté provést analýzu dosavadního stavu ochrany osobních údajů. Nutností byla i cesta do skladu, aby došlo k úplnému seznámení procesů v rámci vyřizování objednávky a kdo má přístup k osobním údajům zákazníků. Celá analýza trvala 110 hodin, hodinová sazba činila 100 Kč. Na základě analýzy byly provedeny kroky k zajištění souladu s Obecným nařízením. Implementace GDPR trvala 160 hodin, hodinová sazba zůstala stejná, tedy 100 Kč. Dále bylo nutné provést školení, které se uskutečnilo v Brně, Břidličné a ve Zlíně. Každé školení trvalo 3 hodiny. V Olomouci školení neproběhlo, zaměstnanci přijeli do Břidličné. Cena zahrnuje cestu Břidličné a do Brna. Celkem jsou tedy náklady projektu 30 750 Kč a lze říci, že je to cena podstatně nižší, než kdyby byl projekt proveden společností zabývající se právním poradenstvím. Následující tabulka podává přehled o vynaložených nákladech.

Tabulka 15 Náklady projektu (vlastní zpracování)

Činnost	Částka
Analýza ochrany osobních údajů (110 h)	11 000 Kč
Návštěva expedice v rámci analýzy - cestovné (220 km, cena benzínu 15.1.2019 je 31,07 Kč/litr)	550 Kč
Implementace GDPR (160 h)	16 000 Kč

Činnost	Částka
Školení (9 h)	900 Kč
Náklady na cestovné v rámci školení (Břidličná, Brno + zaměstnanci z Olomouce do Břidličné)	2 300 Kč
Celkem	**30 750 Kč**

14.4 Přínosy projektu

Největším přínosem projektu je samotná implementace Obecného nařízení do podnikové praxe vybrané společnosti. Správnou a co nejrychlejší implementací lze předejít sankcím, které by se mohly vyšplhat až do závratných, pro firmu likvidujících, částek. Nyní již má vybraná firma v rukou vnitřní předpis, který popisuje nejen nakládání s osobními údaji, ale upravuje také ostatní aspekty týkající se Obecného nařízení.

Další výhodou je právě zmíněný vnitřní předpis, který bude sloužit především pro správné zacházení s osobními údaji, ale také v případě porušení zabezpečení dat, je tento dokument důkazním materiálem pro dozorový úřad.

Nespornou výhodou je zjištění, jaké osobní údaje vlastně společnost zpracovává, kdo má k jakým údajům přístup apod. Proškolení zaměstnanci pak mohou získané poznatky využít i ve svém soukromém životě (u jiných zpracovatelů, e-shopů) z pohledu zákazníka. Budou již vědět, jaká mají práva a budou jistější při případném konfliktu s jinými zpracovateli.

Velkým přínosem jsou i nízké náklady v porovnání s externími společnostmi, které se Obecným nařízením zabývají.

ZÁVĚR

Hlavním cílem diplomové práce bylo navrhnout a provést takové kroky, ale vybraná společnost byla v souladu s Obecným nařízením na ochranu osobních údajů, které je účinné od 25. května 2018.

Projekt implementace vycházel z analýzy současného stavu ochrany osobních údajů, která byla nutná provést na samotném začátku. Na základě této analýzy pak bylo pomocí GAP analýzy zjištěno, co je špatně nebo jaká opatření a dokumenty chybí.

V projektové části byly nejprve stanoveny cíle a postup implementace. Poté následovaly jednotlivé kroky k zajištění souladu s Obecným nařízením na ochranu osobních údajů. Jednalo se o stanovení účelu zpracování, vytvoření záznamů o činnostech zpracování, analýzu potřeby DPIA a DPO, vnitřní předpis, analýzu rizik, informační memoranda pro zákazníky i zaměstnance, stanovení kontrolních mechanismů, atd. Nakonec byla využita síťová analýza pro znázornění časového harmonogramu projektu a také nejkratší možné doby, za kterou mohl být projekt uskutečněn. Celý projekt byl poté ještě vyhodnocen z hlediska nákladů a rizik.

Projekt je zakončen zhodnocením přínosů. Pro vybranou společnost je největším přínosem právě samotná implementace, za kterou se navíc v praxi platí nemalé peníze. Výhodou tedy je, že společnost ušetřila a především byly provedeny podstatné kroky k tomu, aby firmě nebyly uděleny vysoké sankce.

I přesto, že Obecné nařízení na ochranu osobních údajů je účinné již téměř rok, stále existují společnosti, které spoléhají na štěstí, že je konkurence nebo kdokoliv jiný nenahlásí dozorovému úřadu. Díky tomuto projektu tak vybraná firma má v rukou dokumenty, které budou sloužit pro dozorový úřad jako důkazní materiál při každém problému, který nastane v oblasti ochrany osobních údajů a především provádí svoji hospodářskou činnost podle platných právních předpisů.

SEZNAM POUŽITÉ LITERATURY

COMPUTER FRAUD & SECURITY, 2019, Google is first company hit with major GDPR fine, ScienceDirect [online]. vol. 2019, issue 2, s. 1-3 [cit. 2019-03-14] ISSN 1361-3723

Data protection in the EU, 2018. European Commission [online]. [cit. 2019-03-09]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

DOSTÁL, Dalibor. GDPR ovlivní také kamerové systémy ve firmách. Na co si podniky musí dát pozor?. Businessinfo.cz. [online] Leden 9, 2018, [cit. 2019-02-11] Dostupné z: https://www.businessinfo.cz/cs/clanky/gdpr-ovlivni-take-kamerove-systemy-ve-firmach-na-co-si-podniky-musi-dat-pozor-99784.html

DPO, [online] © 2019. GDPR bez obav. [cit. 2019-03-11]. Dostupné z: http://www.gdprbezobav.cz/dpo/

FERRARA, P., Spoto, F.: Static analysis for GDPR compliance. In: ITASEC 2018, CEUR Workshop Proceedings, vol. 2058. s. 8 [cit. 2019-03-11] Dostupné z: http://ceur-ws.org/Vol-2058/paper-10.pdf

FOTR, Jiří a Jiří HNILICA. 2014, Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 299 s. Expert. ISBN 978-80-247-5104-7.

HRUŠKA, Vít. Právní úprava kamerových systémů podle GDPR. In. Maceklegal.cz. [online] Září 5, 2017, [cit. 2019-02-14] Dostupné z: https://www.maceklegal.cz/pravni-uprava-kamerovych-systemu-podle-gdpr.html

IT a zabezpečení, 2017. GDPRsafe [online]. [cit. 2019-04-10]. Dostupné z: https://gdprsafe.cz/ukazka/it-a-zabezpeceni/

IT Governance Privacy Team, 2017. EU General Data Protection Regulation (GDPR) - An Implementation and Compliance Guide. Second edition. United Kingdom. ISBN 978-1-84928-836-1.

JANEČKOVÁ, Eva. 2018, GDPR: praktická příručka implementace. Praha: Wolters Kluwer, xiii, s. 119. ISBN 978-80-7552-248-1.

KRYSTLIK, Jocelyn, 2017, With GDPR, preparation is everything, ScienceDirect [online]. vol. 2017, issue 6, s. 5-8 [cit. 2019-02-14]. ISSN 1361-3723

LANGEROVÁ, Jana. Jak je to s GDPR a transparentností? In: Podnikatel.cz. [online] Bře 3, 2018, [cit. 2019-02-14]. Dostupné z: https://www.podnikatel.cz/clanky/jak-je-to-s-gdpr-a-transparentnosti/

Metadata, 2018. IT-slovnik [online]. [cit. 2019-04-10]. Dostupné z: https://it-slovnik.cz/pojem/metadata

MULAČOVÁ, Věra a Petr MULAČ. 2013, Obchodní podnikání ve 21. století. Praha: Grada, 520 s. ISBN 978-80-247-4780-4.

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). In: *Úřední věstník Evropské unie* [online]. L 119/1 [cit. 2019-02-14]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN

NAVRÁTIL, Jiří. 2018, GDPR pro praxi. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 339 s. Pro praxi. ISBN 978-80-7380-689-7.

NEZMAR, Luděk. 2017, GDPR: praktický průvodce implementací. Praha: Grada Publishing, 301 s. Právo pro praxi. ISBN 978-80-271-0668-4.

NULÍČEK, Michal. 2017, GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 525 s. Praktický komentář. ISBN 978-80-7552-765-3.

Obecné nařízení o ochraně osobních údajů prakticky, [online] ©2017. *GDPR*. [cit. 2019-02-14]. Dostupné z: https://www.gdpr.cz/gdpr/

Ochrana osobních údajů, 2019. MVCR [online]. [cit. 2019-04-10]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

PERRY, Rob, 2019 GDPR – project or permanent reality?, ScienceDirect [online]. vol. 2019, issue 1, s. 9-11 [cit. 2019-02-14]. ISSN 1361-3723.

Pověřenec pro osobní údaje dle GDPR: kdy, koho a jak pověřit?, 2018. Epravo [online]. Praha 1 [cit. 2019-04-10]. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-osobni-udaje-dle-gdpr-kdy-koho-a-jak-poverit-107265.htmlv

Působnost úřadu, [online] © 2013. Úřad pro ochranu osobních údajů. [cit. 2019-02-04]. Dostupné z: https://www.uoou.cz/pusobnost-uradu/ds-1269/archiv=0&p1=1059

Ransomware, 2016. Avast [online]. [cit. 2019-04-10]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

SMEJKAL, Vladimír a Karel RAIS. 2013, Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 483 s. Expert. ISBN 978-80-247-4644-9.

SOSINSKY, Barrie. 2016, Mistrovství – počítačové sítě. Brno: Computer Press, 840 s. ISBN 978-80-251-3363-7

Úřad, [online] © 2013. Úřad pro ochranu osobních údajů. [cit. 2019-02-04]. Dostupné z: https://www.uoou.cz/urad/ds-1059/p1=1059

VOIGT, Paul a Axel VON DEM BUSSCHE, 2017. The EU general data protection regulation (GDPR). New York: NY: Springer Berlin Heidelberg, 383 s. ISBN 9793319579580.

What is Privacy by Design & Default?, 2018. ICS [online]. [cit. 2019-04-10]. Dostupné z: https://www.ics.ie/news/what-is-privacy-by-design-a-default

ŽŮREK, Jiří. 2018, Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 343 s. Právo. ISBN 978-80-7554-152-9.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

B2B Business to business

B2C Business to customer

CPM Critical Path Method (metoda pro zobrazení časového průběhu projektu)

DPIA Data Protection Impact Assessment (Posouzení vlivu ochrany osobních údajů)

DPO Data Protection Officer (Pověřenec pro ochranu osobních údajů)

GDPR General Data Protection Regulation

OSN Organizace spojených národů

PPC Pay Per Click (druh internetové reklamy)

ÚOOÚ Úřad na ochranu osobních údajů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK A GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: INFORMAČNÍ MEMORANDUM PRO ZÁKAZNÍKY

INFORMAČNÍ MEMORANDUM PRO ZÁKAZNÍKY

Zde najdete informace, základní principy a přehled o zpracování osobních údajů zákazníků na základě 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.

1. Kdo je správcem a zpracovatelem Vašich osobních údajů?

Správce a zpracovatelem osobních údajů je , který provozuje společnost , s. r. o., se sídlem , se spisovou značkou vedená u , IČO: .

2. Za jakým účelem zpracováváme Vaše osobní údaje?

V rámci našeho podnikání dochází ke zpracování osobních údajů, které jsou nutné k vyřízení Vaší objednávky, dotazu, případně poptávky, dále taky pro zasílání newsletterů. Vaše osobní údaje jsou zpracovávány také pro uskutečnění dopravy dopravcem a další zpracování osobních údajů probíhá pomocí souborů cookie.

3. Jaké údaje o Vás zpracováváme?

Zpracováváme Vaše osobní údaje, které zadáte při objednávce na této stránce nebo při poptávce či jakéhokoliv dotazu, který napíšete na naše e-maily.
Jedná se konkrétně o jméno, příjmení, telefon, fakturační a doručovací adresa, e-mailová adresa, informace o předchozích objednávkách, reklamacích či dotazech. V případě reklamace můžeme po Vás vyžadovat číslo bankovního účtu pro vrácení peněz. Při zvoleném způsobu platby přes GoPay nemáme přístup k údajům o Vaší kartě.

4. Komu předáváme Vaše osobní údaje?

Vaše osobní údaje předáváme pouze dopravcům za účelem doručení Vámi objednaného zboží nebo výrobků na našem e-shopu. Jedná se o kontaktní údaje a případně částku, pokud jste si zvolili platbu dobírkou. Vaše údaje pak dále zpracovává i externí účetní. Existují však zvláštní podmínky, které jsou zákonem definovány a my jsme povinni předat některé Vaše osobní údaje Policii ČR, Úřadu na ochranu osobních údajů, orgánům veřejné správy a dalším orgánům činných v trestním řízení.

5. Používáme soubory Cookie?

Soubory Cookie slouží pro zaznamenání informací o návštěvě webu, nikoliv ke zjištění Vašich citlivých údajů. Tyto soubory umožní na webu zaznamenat informace o tom, že jste navštívili web a příští návštěva může být pro Vás příjemnější například díky uložení nastavení, které si zvolíte (částka, jazyk, apod.)
V případě, že souhlasíte s využíváním cookie, stiskněte dole na stránce tlačítko „*ROZUMÍM*“, tím dáváte souhlas s využíváním cookie. Účel využití cookie je pouze pro použití nástroje Google Analytics.

V případě, že si nepřejete ukládat cookie, změňte nastavení přímo ve Vašem prohlížeči.

6. Jak dlouho zpracováváme Vaše osobní údaje?

Vaše osobní údaje zpracováváme od provedení objednávky až po vystavení faktury a předání dopravci, poté po dobu 10 let. V případě, že jste nám udělili souhlas se zpracováním osobních údajů, jsou Vaše osobní údaje zpracovávány po dobu 10 let od data udělení souhlasu. Našim zákazníkům zasíláme e-mailem obchodní sdělení s novinkami. Pokud si již nepřejete, abychom dále zpracovávali Vaše osobní údaje a nezasílali Vám obchodní sdělení, můžete se jednoduše odhlásit od jejich odběru.

7. Zpracování osobních údajů se souhlasem a bez něj

Vaše osobní údaje zpracováváme i bez souhlasu, a to konkrétně ty, které jsou nutné pro vyřízení objednávky a její doručení k Vám.
Dále pak podle zákona 480/2004 Sb., o některých službách informační společnosti Vám můžeme zasílat obchodní sdělení. To však pouze za předpokladu, že jste náš zákazník nebo nám k tomu dáte souhlas. Souhlas můžete kdykoliv odvolat, případně uvést, že nemáte zájem o obchodní sdělení.

8. Jak jsou Vaše osobní údaje zabezpečeny?

Při pohybu na e-shopu jsou Vaše data chráněna protokolem HTTPS. Vaše osobní údaje jsou zabezpečeny před neoprávněným přístupem, zneužitím či ztrátou pomocí. Jako ochranu před porušením zabezpečení využíváme především omezený přístup do prostor podnikání a minimalizaci počtu pracovníků, kteří přijdou s Vašimi údaji do kontaktu. V případě vypršení lhůty pro zpracování jsou Vaše osobní údaje smazány, v papírové podobě jsou skartovány.

9. Jaká máte práva v souvislosti s Vašimi osobními údaji

V rámci Obecného nařízení na ochranu osobních údajů máte následující práva:

- právo na informace,
- právo na přístup k Vašim osobním údajům,
- právo na přenositelnost Vašich osobních údajů,
- právo na opravu nepřesných osobních údajů nebo jejich doplnění,
- právo na omezení zpracování Vašich osobních údajů,
- právo vznést námitku proti zpracování osobních údajů,
- právo na výmaz osobních údajů bez zbytečného odkladu (pouze pokud neexistuje jiný zákonný důvod),
- právo na odvolání souhlasu se zpracováním osobních údajů,
- právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování včetně profilování,
- podat stížnost dozorovému orgánu, kterým je Úřad na ochranu osobních údajů

PŘÍLOHA P II: INFORMAČNÍ MEMORANDUM PRO ZAMĚSTNANCE

Informační memorandum pro zaměstnance

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 (dále jen Obecné nařízení) se stalo účinným dne 25. května 2018. Požadavky, které si klade za cíl toto nařízení, musí od tohoto data splňovat každá organizace, instituce, společnost, škola nebo také zdravotnické zařízení, která zpracovává nebo ukládá osobní údaje z kteréhokoliv členského státu Evropské Unie.

Zaměstnavatel (, IČO: , se spisovou značkou vedená u) je považován za správce osobních údajů a zaměstnanec je subjektem osobních údajů.

Zaměstnavatel zpracovává tyto osobní údaje: jméno, příjmení (příp. jméno za svobodna), telefonní číslo, emailovou adresu, datum a místo narození, trvalé bydliště, případně adresu pro doručování, bankovní spojení, zdravotní pojišťovnu, údaje o dětech v případě odpočtu na děti a rodinný stav z důvodu slevy na manžela/manželku. Tyto osobní údaje jsou získávány ze životopisu, případně z dotazníku, který slouží pro doplnění osobních údajů.

Účelem zpracování osobních údajů je plnění povinností zaměstnavatele na základě pracovní smlouvy (dohody o pracovní činnosti či dohody o provedení práce) a plnění povinností zaměstnavatele na základě příslušných právních předpisů (výpočet daní, mzdového účetnictví, archivační povinnost).

Osobní údaje subjektů jsou poskytovány těmto příjemcům:

- účetní (*doplnit jméno, IČO*)
- Státní správě sociálního zabezpečení,
- Zdravotním pojišťovnám,
- v určitých případech Policii ČR a ostatním orgánům veřejné správy.

Zaměstnavatel přijal potřebná organizační a technické zabezpečení pro zpracování osobních údajů tak, aby předešel jejich náhodnému nebo protiprávnímu zničení, ztrátě, pozměněním či jejich zneužití třetími osobami.

Osobní údaje subjektů jsou zpracovávány pouze po dobu nezbytnou k naplnění účelu zpracování. Poté budou osobní údaje zlikvidovány.

Zaměstnanec svým podpisem pod tímto textem potvrzuje, že byl ze strany zaměstnavatele plně informován o zpracování osobních údajů, a také o jeho právech ve vztahu ke zpracovávaným údajům.

Zaměstnanec bere na vědomí, že v rámci jeho práce bude mít přístup k osobním údajům třetích osob. Zaměstnanec je povinen se při nakládání s osobními údaji řídit pokyny zaměstnavatele a nejednat v jejich rozporu.

Zaměstnanec je povinen osobní údaje nikomu neprozradit a nezpřístupnit třetí osobě.
Zaměstnanec je dále povinen počínat si tak, aby nedošlo k neoprávněnému nebo nahodilému