Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Diplomová práce

Implementace GDPR do podnikatelské činnosti malých firem

Bc. Jan Krejčí

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Jan Krejčí

Podnikání a administrativa

Název práce

Implementace GDPR do podnikatelské činnosti malých firem

Název anglicky

Implementation of GDPR into the business activity of small businesses

---

Cíle práce

Hlavním cílem této práce je navržení postupu implementace Nařízení (EU)2016/679 (GDPR) do podnikatelské činnosti malých firem z hlediska časové,personální, organizační a ekonomické náročnosti. Dílčími cíli je zpracování vzorového Záznamu o činnostech zpracování pro jednu konkrétní činnost správce osobních údajů a návrhu dodatku k již uzavřeným smlouvám s dodavateli pro dodržení GDPR v obchodní praxi. Dále je dílčím cílem práce zjištění nedostatků v procesu zavádění GDPR do praxe. Výstupem práce je vyhodnocení zjištěných nedostatků spojených se zaváděním GDPR a navržení opatření k jejich nápravě.

Metodika

Práce bude zpracována na základě prostudování a následné obsahové analýzy odborné literatury, studia internetových odkazů, studia právních předpisů, vlastního zjištění a konzultací. Dále bude využito metod popisu, analýzy, kompilace z odborné literatury a judikatury. V praktické části práce je hlavně použita metoda komparační a statistická, dále je použito metody porovnání. Na závěr práce budou shrnuty výsledky s vyhodnocením zjištěných skutečností.

Doporučený rozsah práce

60-80 stran

Klíčová slova

GDPR, osobní údaj, informace, pověřenec, správce osobních údajů, zpracovatel osobních údajů, Úřad pro ochranu osobních údajů, malé podniky

---

Doporučené zdroje informací

EU General Data Protection Regulation (GDPR) – An Implementation and Compliance Guidce, Privacy team, ITGP, 2016

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016

NEZMAR, L. GDPR : Praktický průvodce implementací, GRADA, 2017, ISBN: 978-80-271-0668-4

NULÍČEK, M a kol.: GDPR – Obecné nařízení o ochraně osobních údajů, Wolters Kluwer ČR, 2017, ISBN: 978-80-7552-765-3

Ochrana osobních údajů – vybrané otázky, příručka pro podnikatele, Masarykova univerzita, 2011, ISBN: 978-80-210-5572-8

Příručka evropského práva v oblasti ochrany údajů, Agentura Evropské unie pro základní práva, 2014, ISBN: 978-92-871-9933-1

The Data Protection Officer: Profession, Rules, and Role, Paul Lambert, CRC Press, 2017

The EU General Data Protection Regulation (GDPR) – A Practical Guide, Paul Voight, Axel von dem Bussche, Springer, 2017

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

Zákon č. 40/2009, trestní zákoník

Předběžný termín obhajoby

2019/20 ZS – PEF (únor 2020)

Vedoucí práce

Ing. JUDr. Eva Daniela Cvik, Ph.D. et Ph.D.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 24. 10. 2019

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 30. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 26. 11. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Implementace GDPR do podnikatelské činnosti malých firem" jsem vypracoval samostatně pod vedením vedoucí diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30. 11. 2019 _____

Poděkování

Rád bych touto cestou poděkoval Ing. JUDr. Evě Daniele Cvik, Ph.D. et Ph.D. za odborné vedení diplomové práce a vybraným podnikatelům za spolupráci.

Implementace GDPR
do podnikatelské činnosti malých firem

Abstrakt

Tato práce řeší implementaci Nařízení GDPR do podnikatelské činnosti malých firem a živnostníků.

V teoretické části je nejprve popsán význam osobních údajů a vývoj jejich ochrany. Následně jsou popsány důležité pojmy z Nařízení GDPR uplatněné v praktické části práce. Teoretickou část uzavírají metodické postupy implementace nařízení vybrané z odborné literatury a příruček institucí Evropské unie a českých ministerstev a úřadů.

V praktické části práce byla zhodnocena implementace GDPR ve dvou vybraných firmách. Pro zajištění souladu s GDPR byla dána doporučení a tato doporučení byla aplikována do podnikatelské praxe.

Z teoretických znalostí a praktických zkušeností bylo vycházeno při formulování obecného postupu implementace Nařízení GDPR do činnosti malých firem. Tento postup byl formulován dvěma způsoby. Prvním způsobem je posloupnost jednotlivých kroků ke kompletní implementaci od začátku do konce. Druhý způsob je formou otázek, předem formulovaných odpovědí a z nich plynoucích doporučení pro odstranění nesouladu s nařízením GDPR.

Klíčová slova: GDPR, osobní údaj, zpracování osobních údajů, ochrana osobních údajů, Úřad pro ochranu osobních údajů, ÚOOÚ, správce osobních údajů, zpracovatel osobních údajů, souhlas se zpracováním osobních údajů, zabezpečení

Implementation of GDPR into the business activity of small businesses

Abstract

This diploma thesis focuses on the implementation of the GDPR into the business activity of small businesses and freelancers.

In the theoretical part is in the beginning described the importance of personal data and the development of their protection. Subsequently, important terms from the GDPR applied in the practical part of the thesis are described. The theoretical part is concluded by methodical procedures for the implementation of the regulation selected from the literature and manuals of the institutions of the European Union and Czech ministries and authorities.

In the practical part, the implementation of GDPR in two selected companies was evaluated. Recommendations have been made to ensure compliance with GDPR and have been applied to business practice.

The theoretical knowledge and practical experience were based for the formulation of the general procedure for the implementation of the GDPR into the activities of small companies. This procedure was formulated in two ways. The first is the sequence of steps to complete implementation from start to finish. The second is in the form of questions, pre-formulated answers and the resulting recommendations for addressing inconsistency with GDPR.

Keywords: GDPR, personal data, personal data processing, personal data protection, The Officer for Personal Data Protection, Czech DPA, data controller, data processor, consent to personal data processing, security

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

BOZP	bezpečnost a ochrana zdraví při práci
DPIA	Data Protection Impact Assessment / posouzení vlivu na ochranu osobních údajů
EU	Evropská unie
GDPR	General Data Protection Regulation
GPS	Globální polohový systém
Nařízení GDPR	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES
OSVČ	osoba samostatně výdělečně činná
PO	požární ochrana
s. r. o.	společnost s ručením omezeným
Společnost	vybraná s. r. o. (pro vlastní práci)
ÚOOÚ	Úřad pro ochranu osobních údajů
Živnostník	vybraná OSVČ (pro vlastní práci)

1 Úvod

Oblast ochrany osobních údajů je v posledních letech velmi často diskutované téma. Je tomu kvůli rozvoji informačních a komunikačních technologií který umožnil vznik a rozvoj obrovských nadnárodních korporací, jejichž hlavní příjem souvisí se sběrem, zpracováním, analyzováním a využitím nebo prodáním osobních údajů.

Zákony připravované a přijaté většinou v devadesátých letech na tuto situaci nebyly připraveny, a tak docházelo velmi často ke zneužití osobních údajů.

Pro nadnárodní korporace je důležité, aby základní pravidla byla postavena na stejných základech po celém světě a nemusely své služby výrazně odlišovat v různých zemích. Pro lidi jejichž osobní údaje jsou zpracovávány je důležité, aby věděli, jaké osobní údaje o nich firma sbírá a jak je hodlá použít.

Na druhé straně rozvoj komunikačních technologií umožňuje efektivnější přenos dat, který lidem zjednodušuje život a umožňující, aby si firmy předaly jejich osobní údaje mezi sebou a člověk nemusel znovu zadávat veškeré osobní údaje, pokud například mění poskytovatele bankovních služeb.

Technologický vývoj je tedy hlavním důvodem, proč se Evropská unie rozhodla přijmout nařízení o ochraně osobních údajů. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (dále Nařízení GDPR) je komplexní a velmi obsáhlý dokument který nastavuje jasná a jednotná pravidla v celém Evropském hospodářském prostoru. Jeho obsáhlost je zároveň problémem pro malé firmy a osoby samostatně výdělečně činné, proti kterým není přijetí nařízení primárně namířeno, ale musí se jím řídit. Tito podnikatelé mají časově a finančně velmi omezené možnosti celé nařízení prostudovat a pochopit.

Na jaře 2018 nebylo možné uniknout před zprávy o přijetí Nařízení GDPR a ochraně osobních údajů. Vysoce medializovaná byla především možná výše pokut. Této situace využily některé poradenské firmy a nabídly vystrašeným podnikatelům zařízení všech povinností za vysoké částky. Po několika týden tento mediální humbuk ustal, a i kvůli nízkému počtu kontrol Úřadem pro ochranu osobních údajů (76 zahájených kontrol v roce 2018) velká část podnikatelů Nařízení GDPR do své činnosti neimplementovala. (ÚOOÚ, 2019, s. 8).

Cílem této práce bylo najít jednoduchý a pokud možno co nejvíce univerzální postup pro osoby samostatně výdělečně činné a malé firmy, jak splnit požadavky definované Nařízením GDPR s nízkými náklady svépomocí.

Prostředkem, jak k tomuto cíli dojít bylo studium odborné literatury a platné legislativy. Dále byly využité příručky českých ministerstev a institucí Evropské unie. Více než roční praktické zkušenosti s Nařízením GDPR umožnily čerpat i ze zkušeností podnikatelských subjektů s implementací, kontrolní činnosti a aktuálních rozhodnutí Úřadu pro ochranu osobních údajů a nových metodických postupů vydaných většinou právě tímto úřadem.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem této práce je navržení postupu implementace Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES do podnikatelské činnosti malých firem a osob samostatně výdělečně činných z hlediska časové, personální, organizační a ekonomické náročnosti.

Dalším cílem je zhodnocení souladu zpracování osobních údajů s Nařízením GDPR u dvou vybraných menších podnikatelských subjektů a zpracování vzorového Záznamu o činnostech pro jednu konkrétní činnost správce osobních údajů a návrhu dodatku k již uzavřeným obchodním smlouvám pro dodržení GDPR v obchodní praxi.

Dále je dílčím cílem práce zjištění nedostatků v procesu zavádění GDPR do praxe.

Výstupem práce je vyhodnocení zjištěných nedostatků spojených se zaváděním GDPR a navržení opatření k jejich nápravě a univerzální návrh postupu implementace pochopitelný pro malé podnikatele.

2.2 Metodika

První část práce je zaměřena na vymezení teoretických východisek vlastní práce. Práce je vytvořena na základě prostudování a následné obsahové analýzy a komparace odborné literatury, studia internetových odkazů, studia právních předpisů, studia příruček vydaných institucemi EU, ministerstvy a Úřadem pro ochranu osobních údajů, vlastního zjištění, a konzultací. Dále bylo využito metod popisu, analýzy, kompilace z odborné literatury a judikatury.

V praktické části práce byla vybrána jedna osoba samostatně výdělečně činná a jedna společnost s ručením omezeným. Oba podnikatelské subjekty si nepřály být jmenovány a v práci jsou nazývány jako živnostník a společnost. U nich byl hodnocen soulad ochrany zpracovávaných osobních údajů s Nařízením GDPR. K tomuto hodnocení byl využit rozhovor s živnostníkem a jednatelem společnosti cílem tohoto rozhovoru byla identifikace sběrných uzlů osobních údajů, jejich typ a účel zpracování, a dále kontrola zpracovaných dokumentů GDPR těmito subjekty.

Sběrné uzly osobních údajů a jejich datové toky byly znázorněny pomocí diagramů datových toků.

Následně byly živnostníkem i jednatelem společnosti za přítomnosti autora práce vyplněny dotazníky pro zpracování GAP analýzy vytvořené na základě odborné literatury.

Pro posouzení, zda je nutné zpracovat posouzení vlivu na ochranu osobních údajů byla použita metodika hodnocení rizikovosti vydaná Úřadem pro ochranu osobních údajů.

Pomocí komparace zjištěného stavu s požadavky Nařízení GDPR byly zjištěny nedostatky a navržena opatření pro zajištění souladu.

Na základě prostudované literatury a legislativy a poznání činnosti vybraných podnikatelských subjektů byl vypracován vzor dodatku k existujícím smlouvám a vzor záznamu o činnostech.

3 Teoretická východiska

V části teoretická východiska byl nejprve shrnut vývoj zpracování a ochrany osobních údajů ve světě, Evropské unii a na území České republiky.

Další část se zabývá Nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES. V práci jsou popsány principy, na kterých je nařízení založeno a vysvětleny pojmy využité ve vlastní práci.

Další část, zaměřená na implementaci GDPR do činnosti menších správců osobních údajů, popisuje metody doporučené v odborné literatuře a v příručkách vydaných Úřadem pro ochranu osobních údajů.

3.1 Vývoj ochrany osobních údajů

Mezi základní lidská práva vždy patřilo právo na soukromí. Toto právo se neustále vyvíjí s postupujícím vývojem lidské společnosti. Z práva na soukromí byla odvozena potřeba chránit fyzické osoby před případnými negativními vlivy při zpracování osobních údajů. V době internetu, moderních technologií a sledovacích zařízení je sběr dat mnohem jednodušší, jejich rozsah větší a sdílení rychlejší. Zároveň je zde mnohem větší riziko jejich zneužití. (Žůrek, 2017, s. 12)

3.1.1 Historie ochrany osobních údajů ve světě a současný stav

Právo na soukromí bylo poprvé definováno ve všeobecné deklaraci lidských práv. Tato deklarace, přijatá v roce 1948 v San Franciscu, zakazovala svévolné zasahování do soukromého života a korespondence. Evropská úmluva o ochraně lidských práv sjednaná v Římě roku 1950 zaručovala právo na respektování rodinného a soukromého života. Otázky práva na ochranu osobních údajů při jejich zpracování byly řešeny v obou těchto dokumentech. (Žůrek, 2017, s. 13)

Reakcí práva na vývoj společnosti a nástup automatizace do oblasti zpracování osobních údajů byla zvýšená pozornost a postupné vyčlenění této oblasti. Zlomovým datem byl 28. leden 1981, kdy byla přijata Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat. V této úmluvě byly poprvé definovány pojmy osobní údaj, správce a automatizované zpracování apod. Také stanovila zásady pro zpracování a zabezpečení osobních údajů. Z této úmluvy se vycházelo při tvorbě pozdějších evropských dokumentů

a den jejího přijetí je považován za mezinárodní den ochrany osobních údajů. (Žůrek, 2017, s. 13-14)

S nástupem globalizace a rozvojem technologií v 80. a 90. letech se osobní údaje stále častěji předávaly do třetích zemí. Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů reagovala na tento vývoj a regulovala jak neautomatizované, tak plně nebo částečně automatizované zpracování osobních údajů. (Žůrek, 2017, s. 14)

Po schválení směrnice v Evropské unii, musely členské státy přijmout do právních řádů odpovídající předpisy. Tento harmonizační účinek byl z počátku úspěšný. Postupem času byly národní předpisy novelizovány a původně dosažená harmonizace klesla na nižší úroveň. Novely přibývaly čím dál častěji také kvůli rozvoji internetu a nástupu sociálních sítí. (Žůrek, 2017, s. 15)

Po roce 2010 byla proto nutná revize legislativy ochrany osobních údajů. Protože směrnice 95/46/ES splnila požadavek harmonizace pouze částečně, bylo rozhodnuto revidovat právní rámec zpracování osobních údajů pomocí nařízení. Nařízení má vyšší sjednocovací účinek, protože platí pro všechny právní subjekty působící v Evropské unii, zatímco směrnice pouze členským státům nařizuje do určité doby upravit vlastní předpisy. (Žůrek, 2017, s. 15-16)

Dne 27. dubna 2016 bylo přijato Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES. Toto nařízení někdy nazývané jako GDPR (zkratka z anglického General Data Protection Regulation) je právě reakcí na vývoj společnosti a technologií v posledních dvaceti letech. Účinnost Obecného Nařízení GDPR nastala 25. května 2018. (Žůrek, 2017, s. 16)

3.1.2 Historie ochrany osobních údajů v České republice a současný stav

Na území České republiky začala být ochrana osobních údajů řešena zákonem č. 256/1992 Sb. o ochraně osobních údajů v informačních systémech. Tento zákon ovšem neřešil papírové evidence, které byly v té době mnohem více rozšířené. O několik měsíců později byla přijata Listina základních práv a svobod. Ta garantuje nedotknutelnost soukromí osoby v čl. 7 odst. 1 a právo na ochranu před neoprávněným shromažďováním,

zveřejňováním nebo jiným zneužíváním údajů o jeho osobě v čl. 10 odst. 3. (Žůrek, 2017, s. 18)

Čl. 10 odst. 3 Listiny základních práv a svobod nebyl v České republice řešen zákonem a až do 1. června 2000. V tento den nabyl účinnosti zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, který zřizoval dozorový orgán nad dodržováním povinností při zpracování osobních údajů nazvaný Úřad pro ochranu osobních údajů. Zákon byl novelizován před vstupem České republiky do Evropské unie kvůli nutnosti transpozice Směrnice 95/46/ES. (Žůrek, 2017, s. 18-19)

24. dubna 2019 byl vyhlášen zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon adaptoval obecné nařízení o ochraně osobních údajů do české legislativy, některé záležitosti byly upřesněny nebo zjednodušeny. Zákon je účinný dnem vyhlášení. (Úřad pro ochranu osobních údajů, 2019)

3.2 Hodnota osobních údajů

Na osobní údaje, zejména v digitálním prostoru, se dá dívat jako na ekonomické aktivum. Je to soubor tvořený chováním jedinců na internetu. Tyto údaje jsou shromažďovány na online platformách, které je využívají pro zlepšení svých služeb a prodávají reklamním firmám, které díky jejich analýze personifikují inzerci na internetu. Pokud není zajištěna ochrana uživatelů internetu, klesá jejich ochota sdílet osobní údaje. (Nezmar, 2017, s. 20)

Příkladem využití databáze osobních údajů firmami jsou kromě příjmů plynoucích z reklamy také uživatelské recenze a komentáře na sociálních sítích nebo údaje o používání aplikací a zařízení, které pomáhají k úsporám a inovacím. Pro spotřebitele je výhodou zobrazování relevantní reklamy nebo slevy a odměny nabízené výměnou za ochotu sdílet své osobní údaje. (Nezmar, 2017, s. 23-25)

Osobní údaje tedy mají hodnotu jak pro firmy, které je sbírají, tak pro spotřebitele, kteří dostanou za jejich sdílení určitou hodnotu. Aby byl užitek maximalizován pro obě strany, je nutné, aby bylo chráněno soukromí spotřebitelů před zneužitím pomocí právních předpisů. (Nezmar, 2017, s. 25-26)

3.3 GDPR

Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES nepřináší do současné legislativy zásadní změny spíše, než revolucí

ho jde označovat jako evoluci odpovídající na vývoj společnosti. Jeho důležitost je především ve sjednocení legislativy v zemích Evropského hospodářského prostoru (Evropská unie, Island, Lichtenštejnsko a Norsko). Z nařízení vyplývají povinnosti, které se musí plnit každý subjekt který zpracovává osobní údaje. Dále se podle něj řídí dozorové orgány a z nařízení všem fyzickým osobám, jejichž osobní údaje jsou zpracovávány vyplývají určitá práva. (Úřad pro ochranu osobních údajů, 2019)

Nejvíce nařízení ovlivní subjekty, které zpracovávají velká množství osobních údajů nebo zvláštní kategorie osobních údajů. Jde především o banky, nemocnice, telekomunikační operátory. Menším firmám a živnostníkům, které zpracovávají osobní údaje svých zaměstnanců, klientů a obchodních partnerů přináší toto nařízení také nové povinnosti, ale nemělo by je zásadně ovlivnit. Zpracování osobních údajů výhradně pro osobní nebo domácí účely je stejně jako zpracování orgány pro prevenci, odhalování a vyšetřování trestných činů z nařízení vyjmuto. (Úřad pro ochranu osobních údajů, 2019)

3.3.1 Zásady zpracování osobních údajů

Všechna pravidla upravující zpracování definovaná v Obecném nařízení jsou odvozena od zásad uvedených v čl. 5. Jedná se o zákonnost, korektnost, transparentnost, omezení účelu, minimalizaci údajů, přesnost, omezení uložení, integritu a důvěrnost. (Žůrek, 2017, s. 58)

3.3.1.1 Zásada zákonnosti, korektnosti a transparentnosti

Aby byla splněna zásada zákonnosti při zpracování osobních údajů, musí být pro zpracování alespoň jeden právní důvod. Zpracování musí probíhat v souladu s obecným nařízením i ostatními zákony. (Nulíček, 2017, s. 105-107)

Právními důvody jsou udělení souhlasu se zpracováním osobních údajů; nezbytnost zpracování pro splnění smlouvy se subjektem údajů; nezbytnost pro splnění právních povinností správce; nezbytnost pro ochranu životně důležitých zájmů subjektu nebo jiné fyzické osoby; nezbytnost pro výkon veřejné moci nebo úkolu ve veřejném zájmu; nezbytnost zpracování pro účely oprávněných zájmů správce nebo třetí strany (Nezmar, 2017, s. 53)

Zásada transparentnosti požaduje informování subjektu o veškerých důvodech zpracování osobních údajů a jejich přístupnost. (Žůrek, 2017, s. 59-60)

Pokud subjekt udělí souhlas se zpracováváním pro jeden účel a správce se rozhodne osobní údaje využít k jinému účelu, musí požádat o nový souhlas. Pak je splněna zásada korektnosti (Nezmar, 2017, s. 31-32)

3.3.1.2 Zásada účelového omezení

Správce může zpracovávat osobní údaje pouze k účelu, který sdělí subjektu nejpozději při počátku jejich shromažďování. Výjimkou je situace, kdy je povinnost daná zákonem. Účel zpracování musí být určitý, výslovně vyjádřený a legitimní. (Žůrek, 2017, s. 60)

Určitým vyjádřením účelu nemůže být např. marketingové využití. Správce by měl zvolit např. informování o aktuálních speciálních nabídkách. Výslovné vyjádření znamená, že účel zpracování musí subjekt, správce i případný zpracovatel pochopit stejně. Účel by měl tedy být správcem jasně vysvětlen. Zásada legitimity znamená, že účel musí být v souladu s Nařízením i ostatními právními předpisy. Pokud dochází ke zpracování za jiným účelem, jedná se o další zpracování. To je povoleno pouze ve čtyřech případech uvedených v čl. 6 Nařízení. (Nulíček, 2017, s. 108-109)

3.3.1.3 Zásada minimalizace údajů

Správce může shromažďovat pouze ty osobní údaje, které jsou přiměřené účelu jejich zpracování. Příkladem může být využití rodného čísla jako jedinečného identifikátoru člověka. Vyžadování rodného čísla je v tomto případě nepřípustné, protože správce si může zvolit vlastní jedinečný identifikátor. (Nulíček, 2017, s. 109-110)

3.3.1.4 Zásada přesnosti

Shromažďované osobní údaje musí být přesné. Pokud správce zjistí, že jsou nepřesné, musí je opravit. Není určeno, jak často by měl správce údaje kontrolovat, ale důležitá je závažnost chyby pro subjekt. Pro kontrolu a aktualizaci údajů, by měl správce zvolit vhodnou metodu. Např. nevyžádaný email nejspíš nezpůsobí subjektu žádnou škodu, naopak chybně uvedená dlužná částka v registru dlužníků, může zamezit uzavření úvěrové smlouvy. Se zásadou přesnosti souvisí právo subjektu na opravu. Pokud subjekt upozorní na chybný osobní údaj, má správce povinnost upozorněním se zabývat a údaje aktualizovat nebo opravit. (Nulíček, 2017, s. 110-113)

3.3.1.5 Zásada omezení uložení

Zásada omezení uložení znamená, že pokud pomine účel, pro který správce zpracovával osobní údaje, musí je zlikvidovat nebo anonymizovat. Výjimkou je zpracování pro vědecké nebo statistické účely (Nulíček, 2017, s. 113-114)

3.3.1.6 Zásada integrity a důvěrnosti

Zásada integrity a důvěrnosti se týká zabezpečení dat před jejich neoprávněným či protiprávním zpracováním, poškozením, ztrátou nebo zničením. Tyto zásady jsou více rozebrány v čl. 32 nařízení. Zásady integrity a důvěrnosti jsou uvedeno přímo mezi zásadami nově. Z toho je zřejmé, že na zabezpečení je nyní zaměřena vyšší pozornost. (Nulíček, 2017, s. 118)

3.3.1.7 Zásada odpovědnosti

Stejně jako v původní legislativě je správce odpovědný za dodržení všech povinností. Nově však má povinnost doložit soulad všech procesů s GDPR. Správcem přijatá opatření vyplývají z míry rizika vyhodnocené v závislosti na technice zpracování, druhu zpracovávaných osobních údajů, potenciální škodě subjektu apod. Prokazování souladu podrobněji rozebírá čl. 24 Nařízení. (Nulíček, 2017, s. 118-119)

3.3.2 Důležité pojmy v GDPR

Pojmy jsou definovány v čl. 4 odst. 1 Obecného nařízení. Některé pojmy jsou nové, některé jsou převzaté ze starších předpisů.

3.3.2.1 Osobní údaj

Každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor např. jméno, identifikační číslo nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Příklad osobních údajů v tabulce Tabulka 1. (Nezmar, 2017, s. 31-32)

Anonymizované údaje, jsou takové údaje, které se netýkají identifikované nebo identifikovatelné osoby, případně byli upraveny tak, aby je nebylo možné osobu podle nich identifikovat. Anonymizované údaje nejsou považovány za osobní údaje. Příklad anonymizovaných údajů v tabulce Tabulka 1. (Nulíček, 2017, s. 83)

Naopak pseudonymizované údaje se za osobní údaje považují. Tyto údaje není možno přiřadit ke konkrétní osobě bez použití jiných informací umístěných jinde. Příklad pseudonymizovaných osobních údajů v tabulce Tabulka 1. (Nulíček, 2017, s. 87-88)

Tabulka 1 Příklad osobních, pseudonymizovaných osobních a anonymních údajů

Jméno	Příjmení	Město	Věk	Vzdělání	
Martin	Nový	Praha	25	SŠ	Osobní údaje
001		Praha	25	SŠ	Pseudonymizované osobní údaje
		Praha	25	SŠ	Anonymní údaje

Zdroj: vlastní zpracování

Zvláštní skupinou osobních údajů jsou údaje genetické, biometrické a údaje o zdravotním stavu. O jejich zpracování pojednává čl. 9 Nařízení. (Nulíček, 2017, s. 94-95)

3.3.2.2 Zvláštní kategorie osobních údajů

Do zvláštní kategorie osobních údajů, často označované také jako citlivé údaje patří informace o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby a genetické a biometrické údaje, pokud jsou zpracovávány za účelem jedinečné identifikace fyzické osoby. Pokud např. fotografie není určena pro zpracování citlivých údajů, mezi citlivé údaje nepatří.

Tyto osobní údaje mohou subjektu zpracování způsobit diskriminaci nebo ho jinak poškodit ve společnosti, zaměstnání nebo škole. Tyto osobní údaje je zakázáno zpracovávat kromě případů uvedených v článku 9 odst. 2 obecného nařízení. (Úřad pro ochranu osobních údajů, 2019)

3.3.2.3 Zpracování osobních údajů

Jakákoliv operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů s pomocí i bez pomoci automatizace. Jedná se např.

o shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení, pozměnění, vyhledání, nahlédnutí, použitá, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. (Žůrek, 2017, s. 30)

3.3.2.4 Profilování

Forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu. (Nezmar, 2017, s. 32)

Většinou se jedná o využití osobních údajů k předpovědi chování konkrétní osoby a zacílení reklamy. Využití profilování má ale mnohem větší rozsah použití. (Nulíček, 2017, s. 86-87)

3.3.2.5 Správce

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů. Jsou-li účely a prostředky tohoto zpracování určeny právem Evropské unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. (Žůrek, 2017, s. 31)

Správcem je ta osoba, která rozhodla o vykonávání činnosti, pro kterou je nutné zpracovávat osobní údaje, nebo jí to bylo nařízeno zákonem. Nezaleží na tom, jestli osobní údaje zpracovává. (Nulíček, 2017, s. 89)

Jmenováním pověřence pro zpracování osobních údajů nebo zpracovatele se správce nemůže zcela zbavit odpovědnosti. (Žůrek, 2017, s. 86)

3.3.2.6 Zpracovatel

Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. (Žůrek, 2017, s. 31)

Zpracovatel má správcem určený způsob a účel zpracování osobních údajů. Pokud zpracovatel zpracovává osobní údaje i pro svůj vlastní účel, (např. údaje nutné pro zaměstnávání svých zaměstnanců) je v tomto případě správcem. Zpracovatele se týkají

především povinnosti ohledně zabezpečení osobních údajů, školení zaměstnanců, záznamech o činnosti. Pro zpracování osobních údajů zpracovatelem nepotřebuje správce souhlas subjektu údajů, protože je zpracovatel povinen zpracovávat osobní údaje podle správcových pokynů. Zpracovatelé jsou nejčastěji využíváni, pokud je to pro správce ekonomicky výhodné, nebo zpracování správcem není možné z personálních či technických důvodů. (Žůrek, 2017, s. 87-88)

Pokud zpracovatel zapojí do zpracování osobních údajů dalšího správce, jedná se o řetězení zpracovatelů. Řetězení zpracovatelů není Nařízením GDPR zakázáno, ale je pro něj nutné povolení správce. Podmínky zapojení dalšího správce můžou být součástí smlouvy o zpracování osobních údajů. (Žůrek, 2017, s. 90-91)

Zpracovatel musí postupovat podle smlouvy o zpracování osobních údajů uzavřené mezí ním a správcem, součástí smlouvy by mělo být především:

- předmět a doba trvání zpracování,
- povaha a účel zpracování,
- typ osobních údajů a kategorie subjektů údajů,
- povinnosti a práva správce

(Úřad pro ochranu osobních údajů, 2018)

3.3.2.7 Souhlas se zpracováním osobních údajů

Souhlas subjektu údajů je jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. (Žůrek, 2017, s. 31)

Oproti původnímu zákonu je nutný aktivní souhlas. Souhlasem není aktivní užívání (např. webové stránky) nebo předvyplněný souhlas. (Nulíček, 2017, s. 93)

Souhlas je jedním z právních důvodů pro zpracování osobních údajů. Je vyžadován pouze v případech, že nelze zpracování osobních údajů právně odůvodnit jinak. Typickými případy, kdy není souhlas nutný je např. zpracování osobních údajů pro plnění pracovně právní smlouvy nebo dodání zboží zákazníkovi. (Úřad pro ochranu osobních údajů, 2019)

3.3.2.8 Dozorový úřad

Dozorovým úřadem je nezávislý orgán veřejné moci zřízený členským státem podle článku 51 Nařízení GDPR. (Nulíček, 2017, s. 76)

Oblast ochrany osobních údajů v České republice dozoruje Úřad pro ochranu osobních údajů (ÚOOÚ). (Nulíček, 2017, s. 98)

Hlavními úkoly úřadu pro ochranu osobních údajů je monitorování a vymáhání uplatňování obecného Nařízení GDPR a jiných předpisů regulujících oblast ochrany osobních údajů. Kromě dozorové role má také za úkol zvyšovat povědomí veřejnosti o ochraně osobních údajů.

Dozorová funkce úřadu je plněna především zpracováváním stížností subjektů zpracování osobních údajů, kontrolní činností a různými úkoly které zkvalitňují oblast ochrany osobních údajů v Evropském hospodářském prostoru.

Osvětovou a konzultační roli plní úřad především prostřednictvím konzultací se zástupci profesních, odborných a průmyslových sdružení, Parlamentu ČR, případně přímo se správci nebo subjekty zpracování osobních údajů. Dalším způsobem je publikování využitelných výstupů z těchto konzultací, překladů a vlastních metodických materiálů na svých internetových stránkách. Zaměstnanci ÚOOÚ se také zúčastňují konferencí a vzdělávacích projektů. (Úřad pro ochranu osobních údajů)

3.3.3 Práva subjektu údajů

Pro vybalancování pozice mezi správcem a subjektem jsou v Nařízení GDPR (stejně jako v dříve platném zákonu č. 101/2000 Sb., o ochraně osobních údajů) přiznána subjektům zpracování práva. Většina práv uvedených v dříve platné legislativě byla převzata a aktualizována v obecném Nařízení GDPR. Právo na přenositelnost a některá jiná práva byla definována nově.

Práva subjektu údajů:

- právo být informován
- právo na přístup k osobním údajům
- právo na opravu, resp. doplnění
- právo na výmaz
- právo na omezení zpracování
- právo na přenositelnost údajů
- právo vznést námitku
- právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování.

Právo být informován je základním právem, které zaručuje splnění zásady transparentnosti. Jde o právo pasivní – to znamená, že je povinností správce informovat subjekt před zpracováním osobních údajů.

Právo na přístup k osobním údajům předpokládá aktivní žádost subjektu. Subjekt může žádat informace o účelu zpracování; kategoriích dotčených osobních údajů; příjemci nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny; plánované době, po kterou budou osobní údaje uloženy; existenci práva požadovat od správce opravu nebo výmaz osobních údajů, právu vznést námitku; právu podat stížnost u dozorového úřadu; o zdroji osobních údajů, pokud nejsou získány od subjektu údajů; skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Právo na opravu nebo doplnění údajů plyne ze zásady přesnosti. Pokud subjekt upozorní správce, že zpracovávané osobní údaje jsou nepřesné nebo nekompletní, musí se tím správce zabývat a případné nepřesnosti bez zbytečných odkladů opravit nebo doplnit.

Právo na výmaz je známé tako jako právo být zapomenut. Správce musí osobní údaje smazat nastane-li alespoň jeden z následujících případů:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování
- osobní údaje byly zpracovány protiprávně
- osobní údaje musí být vymazány ke splnění právní povinnosti
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 obecného nařízení

Nové právo na přenositelnost údajů dává subjektu možnost získat osobní údaje ve strojově čitelném formátu od správce. Na požádání subjektu, má povinnost poskytnout tyto osobní údaje také jinému správci. (Úřad pro ochranu osobních údajů, 2019, s. 99-110)

3.3.4 Zabezpečení

Nařízení ukládá správci povinnost přijmout adekvátní bezpečnostní opatření. Vzhledem rozdílné povaze, rozsahu a účelu zpracování u různých správců není způsob

zabezpečení definován. Správce však musí být schopen doložit soulad zpracování s obecným nařízením. Vhodnými způsoby zabezpečení elektronických dokumentů je např. pseudonymizace nebo šifrování. Listinné dokumenty by měly být zamčené vždy, když se s nimi nepracuje. (Úřad pro ochranu osobních údajů, 2019)

3.3.5 Sankce

Jedním z důvodů velké medializace přijetí Nařízení GDPR je výška pokut. Ne každé porušení musí být trestáno pokutou. Alternativou může být napomenutí, nařízení vyhovět žádosti subjektu údajů nebo plnit požadavky Nařízení GDPR. Za porušení s vyšší intenzitou zásahu do práva na ochranu osobních údajů je výše pokuty až 20 000 000 eur nebo 4% celosvětového ročního obratu. Tato pokuta může být udělena za porušení povinností upravujících zásady a zákonnost zpracování, podmínky souhlasu se zpracováním osobních údajů a podmínky zpracování zvláštních kategorií osobních údajů a práva subjektu údajů apod. Nižší sazba až 10 000 000 eur nebo 2% celosvětového ročního obratu může být vyměřena např. za porušení v oblasti záznamů o činnostech zpracování nebo posouzení vlivu na ochranu osobních údajů. Výše pokut musí být účinná, přiměřená a odrazující. (Úřad pro ochranu osobních údajů, 2019)

3.3.6 Nové povinnosti

Nové povinnosti jsou odvozeny od přístupu založeném na riziku. Ty nahrazují původní oznamovací povinnost. Podle něj musí správce od počátku uvažovat o rizicích pro práva fyzických osob a přizpůsobit tomu zabezpečení osobních údajů. Pokud zpracování nebo selhání zabezpečení představuje riziko pro práva a svobody dotčených fyzických osob, vznikají správcům nové povinnosti:

- záznamy o činnostech zpracování
- jmenování pověřence pro ochranu osobních údajů
- posouzení vlivu na ochranu osobních údajů
- předchozí konzultace s dozorovým úřadem

Pokud dojde k porušení zabezpečení, ze kterého plyne riziko, je správce povinen tuto skutečnost ohlásit subjektu údajů a dozorovému úřadu. U správců, kteří mají pověřence pro ochranu osobních údajů, by právě on měl dbát o soulad s obecným nařízením. (Úřad pro ochranu osobních údajů, 2019)

3.3.6.1 Záznamy o činnostech zpracování

Záznam o činnostech je základním prostředkem většiny správců pro prokázání souladu zpracování osobních údajů s Nařízením GDPR. Jedná se o obecné záznamy zpracování provedené správcem. Nejde o záznamy konkrétních činností prováděných každodenně. Forma, jak by měl záznam vypadat není v nařízení definována. Vzor využitelný pro malé typy správců zhotovil ÚOOÚ (Tabulka 2). (Úřad pro ochranu osobních údajů, 2018)

Tabulka 2 Záznam o činnostech zpracování pro nejmenší podnikatele

Záznam o činnostech zpracování pro nejmenší podnikatele

jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů	*název a kontaktní údaje na svou firmu (na sebe)*
účely zpracování	*důvody, proč zpracovává osobní údaje (nabízení služeb bývalým zákazníkům, kontakt na objednatele služby apod.)*
popis kategorií subjektů údajů	*čí osobní údaje zpracovává (zákazníci, zaměstnanci, dodavatelé atd.)*
popis kategorií osobních údajů	*jaké osobní údaje zpracovává (jméno a příjmení, bydliště, číslo mobilního telefonu, e-mailová adresa apod.)*
kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích	*příjemce údajů (osoba, které jsou údaje předávány)*
informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk	*při zpracování prováděném nejmenšími podnikateli a živnostníky by k předávání do třetích zemí zpravidla nemělo docházet*
je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů	*předpokládaný čas výmazu údajů (po 3 letech od zakázky apod.)*
je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.	*např. uzamčená skříň pro listinné dokumenty, přístupová práva k počítači, v němž jsou osobní údaje uloženy*

Zdroj: Úřad pro ochranu osobních údajů, 2018

3.3.6.2 Jmenování pověřence pro ochranu osobních údajů

Nově zavedeným nástrojem je pověřenec pro ochranu osobních údajů. Povinnost správce jmenovat pověřence, vzniká ze tří důvodů:

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

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

V jiných případech není správce ani zpracovatel povinen jmenovat pověřence pro ochranu osobních údajů. Správce a zpracovatel mohou jmenovat pověřence pro ochranu osobních údajů i dobrovolně v případech, že jim to nařízení přímo nepřikazuje. (Úřad pro ochranu osobních údajů, 2019)

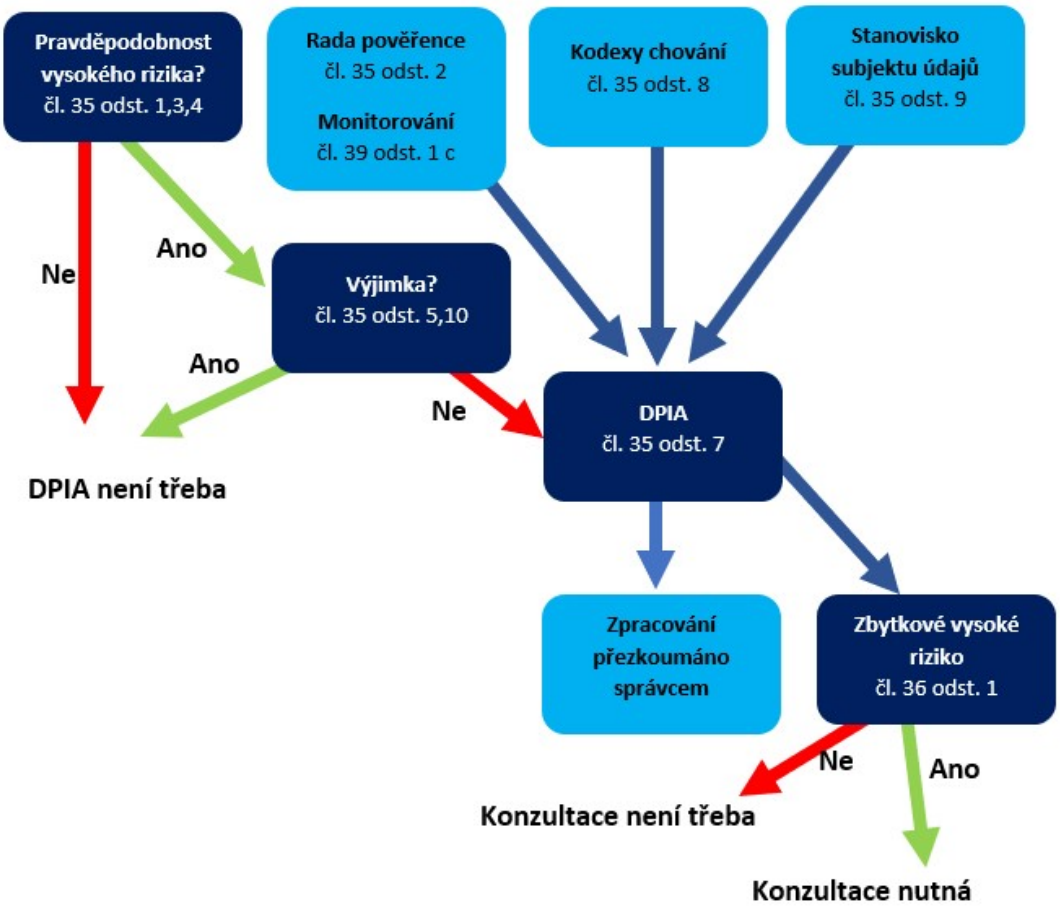
3.3.6.3 Posouzení vlivu na ochranu osobních údajů a konzultace s dozorovým úřadem

Pokud je během zpracování pravděpodobné vysoké riziko ohrožení práv a svobod subjektu zpracování osobních údajů musí správce provést posouzení vlivu na ochranu osobních údajů. Jde především o vyhodnocování pomocí automatizovaného zpracování a na nich založeném rozhodování ovlivňující fyzické osoby; rozsáhlé zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech; rozsáhlé monitorování veřejně přístupných prostor; zpracování splňující kritéria seznamu vydaným ÚOOÚ.

Pokud z posouzení vyplyne, že dané zpracování má za následek vysoké riziko, musí správce přijmout opatření, které riziko zmírní a konzultovat situaci s dozorovým úřadem. (Úřad pro ochranu osobních údajů, 2019)

Rozhodování je-li potřeba zpracovat DPIA a konzultovat situaci s dozorovým orgánem je znázorněno na Obrázku 1. (Nezmar, 2017, s. 100-101)

Obrázek 1 Rozhodování o DPIA



Zdroj: Nezmar, 2017, s. 101

ÚOOÚ také vydal návrh seznamu operací, které nepodléhají posouzení vlivu na ochranu osobních údajů. Při zpracování vycházel z dozorové praxe a jeho hlavním úkolem je zmenšit administrativní zátěž menších a středních správců. ÚOOÚ hodlá tento seznam aktualizovat podle své dozorové praxe a budoucích stanovisek Evropského sboru pro ochranu osobních údajů.

Mezi tyto operace patří:

1. Plnění zákonných povinností při vedení účetnictví, personální a mzdové agendy, sociálního a zdravotního pojištění na základě právních předpisů.
2. Zpracování týkající se obchodní činnosti (včetně zasílání newsletterů), zpracovávající pouze nezbytné osobní údaje, pokud se nejedná o zpracování zvláštních kategorií osobních údajů.

3. Přímý marketing a s tím spojené profilování zákazníků, založené na zákaznickém výběru či zobrazování položek z nabídky zboží, výrobků a služeb umístěných na webové stránce správce při jedné návštěvě zákazníka.
4. Zpracování nebo soubor operací zpracování, která upravují platné právní předpisy.
5. Poskytování zdravotních služeb osobou, která není v zaměstnaneckém poměru.
6. Využití nezbytných osobních údajů pouze k zajištění právních služeb pro subjekt údajů.
7. Zpracování zajišťovaná jednotlivými podnikajícími fyzickými osobami poskytujícími sociální služby využívající nezbytné osobní údaje pouze k zajištění sociálních služeb pro subjekt údajů.
8. Snímání veřejné komunikace kamerou umístěnou na vozidle, monitorující nezbytný prostor před, nebo za vozidlem, a to za účelem dokumentace nehody a jejím šetřením příslušnými orgány.

(Úřad pro ochranu osobních údajů, 2019, s. 1-2)

3.3.7 Kamerový systém

Pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru a zároveň je účelem pořizovaných informací a záznamů využití k identifikaci fyzických osob v souvislosti s určitým jednáním podléhá Nařízení GDPR. Stejně jako pro jakékoliv jiné zpracování osobních údajů musí být i pro provozování kamerového systému právní důvody. Pro kamerový systém jde prakticky o zpracování nezbytné pro splnění právní povinnosti správce; zpracování nezbytné pro oprávněné zájmy správce nebo třetí strany; nebo je povinnost provozovat kamerový systém dána jiným zákonem. Kamerový systém by neměl být použit tam, kde jde oprávněný zájem splnit prostředky s menším zásahem do soukromí. (Žůrek, 2017, s. 206-208)

3.3.8 Zabezpečení IT technologií

V současné době téměř každý používá informační a komunikační technologie plné vlastních osobních údajů, nebo pro správu cizích osobních údajů. Proto je důležité dbát na jejich bezpečnost.

3.3.8.1 Tiskárny

Trendem poslední doby je využívání multifunkčních tiskáren se vzdáleným přístupem umístěných na chodbách nebo jiných společných prostorech. Ty představují riziko pro osobní údaje z důvodu zapomenutí vytisknutých dokumentů. Tento problém jde řešit odloženou aktivací tisku, dokud osoba, která tisk zadala nepotvrdí tisk přímo na tiskárně. To jde pomocí čipu, otisku prstů apod. Moderní tiskárny jsou vlastně počítačem s procesorem a harddiskem, a tak by měly být chráněny i proti zavirování. (Nezmar, 2017, s. 189-191)

3.3.8.2 Koncová a přenosná zařízení

U zabezpečení stolních počítačů a notebooků je potřeba řešit fyzické zabezpečení pomocí zámků i zabezpečení firmwarové výbavy BIOSu a operačního systému. Nejslabším článkem soustavy je často člověk, a proto je třeba dbát na používání silných hesel a využívat zabezpečení pomocí biometrických údajů. (Nezmar, 2017, s. 191-194)

3.3.8.3 Elektronické dokumenty

Stále více dokumentů je v současnosti v digitální podobě. Výhodou je lepší zabezpečení proti ztrátě dokumentů. Zatímco listinné dokumenty se dají chránit pouze uzamčením. Elektronické dokumenty se efektivněji sdílejí a zároveň se dají zašifrovat a zpřístupnit pouze heslem. Podle Nezmara je důležité při řešení správy elektronických dokumentů zvažovat následující hlediska:

- Řízená distribuce dokumentů
- Zabezpečený přístup k souborům
- Žádné postrádané dokumenty
- Respektování zákonných nařízení
- Obnova po havárii
- Archivace vzácných nebo zvláště citlivých papírových dokumentů

(Nezmar, 2017, s. 216-217)

3.3.8.4 Cloud computing

Při používání cloudových služeb k záloze a sdílení dokumentů s osobními údaji je podle skupiny WP29 poskytovatel cloud computingu zpracovatelem a zákazník správcem osobních údajů. Poskytovatel cloudových služeb tedy musí zachovat důvěrnost a soubory ke kterým má přístup musí zpracovávat podle pokynů správce. (Nezmar, 2017, s. 251)

Společnosti Google a Microsoft provozující cloudové služby Disk Google, Google Fotky, OneDrive apod. garantovaly soulad svých služeb s Nařízením GDPR. Podle Škorničkové převezmou velkou část povinností za své klienty. (GDPR.cz, 2017)

3.3.9 Zaměstnanci

Nezbytnou podmínkou při zaměstnávání osob je vedení personální evidence s osobními údaji zaměstnanců. K vedení evidence není nutný souhlas pracovníků, ale organizace je musí informovat o tom, jak bude záznamy používat a komu budou zpřístupněny. Organizace by měla kontrolovat, jestli jsou záznamy správné a aktuální, ale také by měla mazat údaje které nezbytně nepotřebuje. Záznamy musí být zabezpečeny – tištěné pod zámkem, elektronické zaheslované. Citlivé údaje a informace o zdravotním stavu by měly být uchovávány odděleně nebo v pseudonymizované podobě. Na soukromí zaměstnanců je třeba myslet především při zpracování zdravotních informací a používání monitorovacích zařízení. (Nezmar, 2017, s. 183-187)

3.4 Implementace GDPR

Proces implementace Nařízení GDPR do činnosti firem je složitým procesem a velmi se liší v závislosti na typu a objemu zpracovávaných osobních údajů a riziku.

3.4.1 GAP Analýza

Prvním krokem implementace požadavků GDPR do činností organizace by měla být GAP analýza. Její doslovný překlad (analýza mezery) naznačuje že výsledkem této analýzy by měl být popis rozdílu mezi současným a požadovaným stavem a návrh opatření, jak tohoto stavu dosáhnout. Požadovaným stavem je takový stav, který odpovídá Nařízení GDPR. GAP analýza by měla zjistit:

- Kde dochází v organizaci ke sběru osobních dat
- Jaká struktura dat je shromažďována

- Jaké nástroje jsou ke sběru dat používány
- Jaký je formální obsah nástrojů
- Jestli a jak byl získán souhlas se zpracováním osobních údajů
- Kdo může k osobním údajům přistupovat a na základě jakých oprávnění
- Jak jsou data uchovávána a zabezpečena
- Jaké systémy jsou pro práci s daty používány
- Jaké jsou procesy, ve kterých data figurují a soulad či nesoulad těchto procesů s Nařízením GDPR
- Stav smluvních závazků týkajících se osobních údajů
- Vazby a smlouvy třetích stran
- Přístup k dopadům zpracování na soukromí
- Proces řízení incidentů a schopnost reakce
- Jaké jsou návrhy na zlepšení v případě nesouladu

Na počátku provádění GAP analýzy je potřeba identifikovat sběrné uzly osobních dat a vytvořit jejich seznam včetně odpovědných osob. Dalším krokem je identifikace jednotlivých zpracování pomocí dotazníku. (Nezmar, 2017, s. 96-98)

3.4.2 Posouzení vlivu na ochranu osobních údajů (DPIA)

Pro účely posouzení, zda je nutné provést posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assesment - DPIA) vydal Úřad pro ochranu osobních údajů příručku pro sebehodnocení správce osobních údajů nazvanou „K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)“. Sebehodnocení v příručce se skládá z deseti kritérií zpracování, kritéria jsou dále rozčleněny do třech způsobů zpracování osobních údajů, které nabývají kritické hodnoty, významné hodnoty nebo nízké hodnoty s popisky jednotlivých případů zpracování. Správce na základě těchto kritérií přiřadí své zpracování k těmto hodnotám. Správce musí zpracovat posouzení vlivu na ochranu osobních údajů, pokud jsou alespoň dvě odpovědi v kritických hodnotách nebo pokud je v kritických hodnotách jedna a alespoň pět v hodnotách významných.

3.4.2.1 10 kritérií pro sebehodnocení

1. Zpracování osobních údajů zahrnuje monitorování subjektů údajů;
2. Zpracování údajů, které umožňují přímou identifikaci a/nebo těch, které mají vysoce osobní povahu pro subjekty údajů;
3. Zpracování údajů, jenž může subjekty údajů vystavit ohrožení z okolního prostředí;
4. Zpracování velkého rozsahu osobních údajů;
5. Zpracování, které zahrnuje monitorování veřejně přístupných prostor;
6. Zpracování osobních údajů, které mohou subjekty údajů ovlivnit v omezeném rozsahu;
7. Zpracování osobních údajů, které jsou veřejně přístupné;
8. Zpracování osobních údajů, využívající složité nebo pokročilé technické infrastruktury či platformy;
9. Zpracování osobních údajů jinými správci či zpracovateli;
10. Zpracování osobních údajů prostřednictvím nových technologických či organizačních řešení.

V říjnu 2019 vydal Úřad pro ochranu osobních údajů pracovní verzi příručky „Metodika obecného posouzení vlivu na ochranu osobních údajů“ ta by měla pomoci správcům osobních údajů vypracovat posouzení vlivu na ochranu osobních údajů (DPIA). (Úřad pro ochranu osobních údajů, s. 1-13)

3.4.3 Desatero zpracování pro správce

Jako návod pro malé správce údajů, živnostníky a malé podniky vydal ÚOOÚ základní pravidla shrnuté do následujícího desatera.

1. Zpracování údajů, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, musí být legitimní a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování údajů musí být založeno na některém ze základních důvodů (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.

3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr - účel zpracování údajů.
4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být vždy přiměřené účelu zpracování.
5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít jasný zákonný podklad, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
6. Správce i zpracovatel osobních údajů musí osobní údaje patřičně zabezpečit a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno férově, korektně a transparentně. Informace o zpracování poskytované subjektu údajů musí být zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci.
8. Zpracování nesmí nadměrně zasahovat do soukromí. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
9. Po naplnění účelu zpracování je dána povinnost osobní údaje zlikvidovat. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
10. V rámci EU je v každé členské zemi zaručena unifikovaná ochrana osobních údajů, kterou stanoví obecné nařízení (GDPR). Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.

(Úřad pro ochranu osobních údajů)

4 Vlastní práce

Vlastní práce je zaměřená na zhodnocení implementace GDPR do podnikatelské činnosti jedné osoby samostatně výdělečně činné a jedné společnosti s ručením omezeným.

Nejprve jsou představeny podnikatelské činnosti těchto vybraných subjektů, jejich oprávnění a okruh jejich klientů.

Dalším bodem je popis přijatých opatření v souvislosti s přijetím Nařízení GDPR a případných změn u jejich klientů které ovlivnily i vybrané podnikatelské subjekty.

Nařízení GDPR přináší nové povinnosti. Bylo zjištěno, jestli oba podnikatelské subjekty musí zpracovávat záznamy o činnostech zpracování, jestli musí jmenovat pověřence pro ochranu osobních údajů, zpracovat posouzení vlivu na ochranu osobních údajů a konzultovat ho s dozorovým úřadem.

K tomuto účelu byla provedena GAP analýza oblasti zpracování osobních údajů a hodnocení rizika zpracování osobních údajů. Těmito analýzami bylo zjištěno, zda podnikatelské subjekty splňují všechny nároky plynoucí z Nařízení GDPR.

V závěru práce byla oběma subjektům dána doporučení, jaká provést opatření, aby jejich zpracovávání bylo v souladu s Nařízením GDPR.

4.1 Charakteristika vybrané osoby samostatně výdělečně činné

Prvním vybraným subjektem pro zhodnocení aktuálního stavu je osoba samostatně výdělečně činná podnikající na základě živnostenského oprávnění. (dále živnostník)

Živnosti ohlašovací vázané

- Technicko - organizační činnost v oblasti požární ochrany
- Poskytování služeb v oblasti bezpečnosti a ochrany zdraví i při práci

Živnost ohlašovací řemeslná

- Kominictví

Živnosti ohlašovací volné

Hlavní činností živnostníka je zajištění zákonných povinností na úseku bezpečnosti a ochrany zdraví při práci a požární ochrany svým klientům v soukromém i veřejném sektoru. Jedná se o školy, mateřské školy, obce, sportovní areály, výrobní firmy, zemědělce apod. Klientům také prodává zboží související s obory bezpečnosti a ochrany zdraví při práci a požární ochrany – především bezpečnostní tabulky a jiné značení.

Další činností jsou kontroly a revize spalinových cest.

Živnostník má platnou kvalifikaci odborně způsobilé osoby v prevenci rizik, odborně způsobilé osoby v požární ochraně a revizního technika spalinových cest.

V několika posledních letech živnostník spolupracuje s jinou osobou samostatně výdělečně činnou, která ho může zastupovat u klientů kde vykonává technicko - organizační činnost v oblasti požární ochrany a poskytuje služby v oblasti bezpečnosti a ochrany zdraví při práci.

4.2 Změny provedené živnostníkem v souvislosti s přijetím Nařízení GDPR

V době před počátkem účinnosti Nařízení GDPR se na sledovaného živnostníka obraceli klienti (správci osobních údajů svých zaměstnanců) s prosbou o navržení nebo podpis smlouvy o zpracování osobních údajů. Jednalo se především o klienty, kteří měli jmenovaného pověřence pro ochranu osobních údajů. Živnostník tuto smlouvu vytvořil a postupně dodal svým klientům, se kterými má uzavřenou obchodní smlouvu.

Obecně lze říci, že živnostník i jeho klienti začali brát oblast ochrany osobních údajů v této době více vážně, s postupem času tento zájem trochu opadl. Dokumenty pro oblast bezpečnosti a ochrany zdraví při práci a požární ochrany týkající se zdravotní způsobilosti a profesní kvalifikace zaměstnanců byly přemístěny do uzamčených skříní a živnostník k nim má nyní složitější přístup. Problémem je dříve běžný krátkodobý přesun některých dokumentů klientů do kanceláře živnostníka kvůli vypracování prověrky bezpečnosti a ochrany zdraví při práci nebo zaslání některých dokumentů emailem. Živnostník nyní více využívá přenosný počítač a potřebné údaje zpracuje přímo u klienta.

4.3 Zpracování osobních údajů živnostníkem

V této části jsou identifikovány činnosti, při kterých dochází ke zpracování, typ zpracovávaných osobních údajů a způsob jakým jsou zpracovávány.

4.3.1.1 Školení o bezpečnosti a ochrany zdraví při práci a požární ochraně

- Jméno a příjmení
- Profese
- Pracovní náplň
- Datum narození
- Podpis

Údaje o profesi a pracovní náplni jsou nezbytné pro zvolení vhodného obsahu školení.

Datum narození je vyžadováno pouze u vedoucích pracovníků. Součástí jejich školení je také test a po jeho absolvování pracovníci obdrží osvědčení. Pro jasnou identifikaci v případě kontroly klienta státními inspekčními orgány, pojišťovnami apod. je na testu i osvědčení uvedeno datum narození.

Pro potvrzení účasti na školení a jeho porozumění je od všech přítomných zaměstnanců požadován podpis na prezenční listině. Prezenční listina je podepsána také živnostníkem nebo vedoucím zaměstnancem, který školení provedl.

Informace jsou většinou získány před školením od personalisty nebo zaměstnance klienta zodpovědného za bezpečnost a ochranu zdraví při práci elektronickou formou emailem, zpracovány na počítači živnostníkem, vytištěny, po školení podepsány a uloženy pod zámkem. Z pohledu živnostníka jde o data nutná pro plnění obchodní smlouvy, z pohledu správce jde o plnění právních povinností souvisejících se zaměstnáváním osob.

4.3.1.2 Provádění prověrky bezpečnosti a ochrany zdraví při práci:

- Jméno a příjmení
- Profese
- Pracovní náplň
- Datum narození
- Výsledek prohlídky lékařem pracovnělékařské péče
- Profesní kvalifikace
- Podpis (členů komise)

Prověrku bezpečnosti a ochrany zdraví při práci zpracovává komise vybraná vedoucím zaměstnancem firmy. Její součástí jsou obvykle vedoucí pracovník, odborně způsobilá osoba v prevenci rizik a několik zaměstnanců zodpovědných za bezpečnost na pracovišti.

Kromě stavu pracoviště posuzuje komise také zda jsou zaměstnanci způsobilí k provádění úkolů v rámci jejich pracovní náplně. Pro určité činnosti musí pracovník absolvovat kurz, školení nebo dosáhnout určité vzdělání, nebo úspěšně absolvovat určitou zkoušku. Pravidelně musí zaměstnanci také absolvovat prohlídku lékařem pracovnělékařské péče. Jejich platnost se odvíjí od pracovní náplně, zařazení do kategorie práce podle § 37 z. č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů a na věku zaměstnance. Pracovní náplň, datum narození a datum a výsledek zdravotní prohlídky jsou tedy spolu s kategorizací prací nutnými osobními údaji pro správné posouzení zdravotní způsobilosti k pracovním úkonům.

Po dokončení je prověrka vytištěna a podepsána všemi členy komise a vedoucím zaměstnancem, který potvrzuje její převzetí.

Informace dodá elektronicky, ústně, nebo písemně jiný člen komise a následně jsou zpracovány na počítači živnostníkem. Tyto osobní údaje jsou nutné pro splnění obchodní smlouvy, resp. pro splnění povinností vyplývajících ze zákona č. 262/2006 Sb. Zákoníku práce z pohledu správce.

4.3.1.3 Vypracování a aktualizace dokumentace požární ochrany

- Jméno a příjmení
- Telefonní číslo
- Podpis

Rozsah dokumentace požární ochrany závisí na požárním nebezpečí objektů a činností. Pro činnosti se zvýšeným požárním nebezpečím musí být vypracovány řád ohlašovny požárů, požární poplachové směrnice a dokumentaci zdolávání požáru. Součástí těchto dokumentů jsou telefonní čísla na pracovníky, které je nutné kontaktovat v případě nouze při požárech, haváriích a jiných nebezpečných situacích. Telefonní čísla jsou sdělena většinou ústně přímo od subjektu údajů nebo vedoucího pracovníka.

Dokumenty jsou podepsány živnostníkem a vedoucím zaměstnancem, který dokument schválil.

Tyto dokumenty jsou zveřejněny pracovišti, aby se jimi mohl kdokoliv řídit v případě požáru nebo jiné nebezpečné situace. Dokumentace zdolávání požáru je uložena i u hasičského záchranného sboru.

Z pohledu zpracovatele jde o nezbytné údaje pro plnění obchodní smlouvy. Z pohledu správce jde o zajištění požární prevence podle zákonu č. 133/1985 Sb. Zákonu o požární ochraně.

4.3.1.4 Poradenská činnost a komunikace

- Jméno a příjmení
- Emailová adresa
- Telefonní číslo

Pro bezproblémovou komunikaci s klienty živnostník využívá emailovou adresu a telefonní číslo na zaměstnance s kterými komunikuje.

Důvodem pro zpracování je plnění obchodní smlouvy. Obchodní smlouvy živnostník uchovává v zamčené skříni.

4.3.1.5 Provádění revizí a kontrol spalinových cest

- Jméno a příjmení
- Adresa bydliště
- Telefonní číslo
- Emailová adresa
- Podpis

Pro zajištění revizí a kontrol spalinových cest je nutné znát vlastníka a provozovatele spalinové cesty a adresu objektu. Pro komunikaci s objednatelem je nutné znát jeho emailovou adresu nebo telefonní číslo.

Revizní zpráva, technická zpráva a zpráva o kontrole spalinové cesty je živnostníkem vyhotovená vždy minimálně ve dvou kopiích. Předání je potvrzeno podpisem subjektu údajů na kopii zprávy pro živnostníka. Tato kopie je archivována v zamčené skříni živnostníka.

Zpracovávání osobních údajů je nutné pro splnění požadavků na provoz spalinových cest provozovaných subjektem osobních údajů podle zákonu č. 133/1985 Sb. Zákona o požární ochraně.

4.3.1.6 Další zpracování

V některých případech živnostník spolupracuje s jinou osobou samostatně výdělečně činnou, která ho může zastupovat. Tuto spolupráci uvedl živnostník ve smlouvě se svými klienty. Podle obchodní smlouvy jsou obě osoby u některých klientů jedním zpracovatelem, u jiných klientů jde o dalšího zpracovatele.

Pro zálohu dokumentů a vzdálený přístup k dokumentům živnostník používá cloudovou službu OneDrive společnosti Microsoft.

4.3.2 Diagram toku osobních údajů

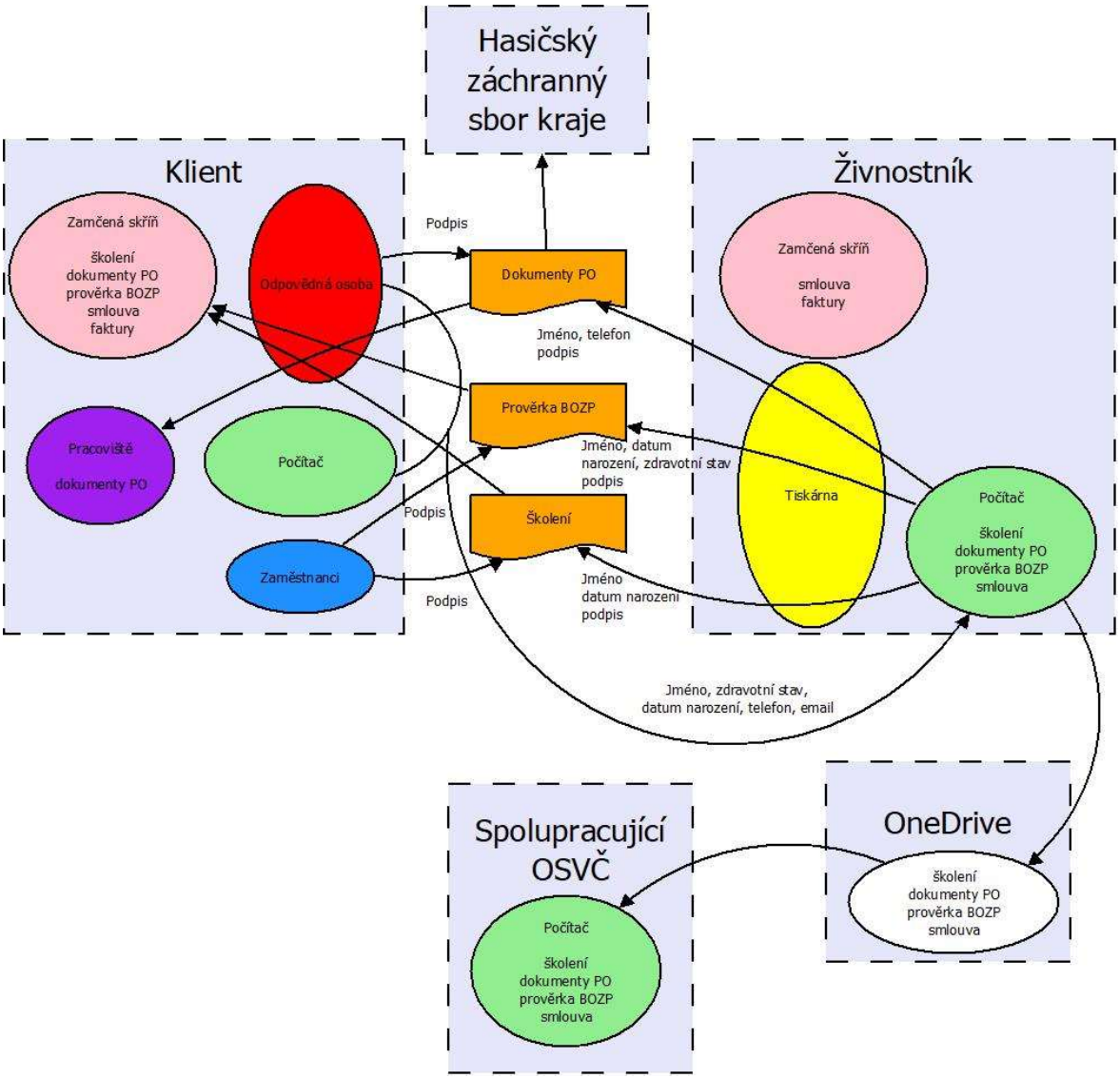
Na Obrázku 2 je zobrazen diagram toku osobních údajů. Pro zjednodušení a lepší přehlednost je předpokládáno, že všechny dokumenty jsou vytištěny živnostníkem. V praxi jsou někdy poslány elektronicky klientovi k vytištění. Dále je předpokládáno, že klient má pouze vytištěné verze dodaných dokumentů. V praxi má některé dokumenty i v elektronické verzi. Klient má osobní údaje obsažené v dodaných dokumentech v jiné podobě uložené elektronicky (v elektronické podobě byly dodány živnostníkovi). Dalším zjednodušením je

předpoklad, že všechny dokumenty byly dodány živnostníkem. V praxi jsou některé dokumenty dodány spolupracující OSVČ. Také budou vynechány všechny operace, kde je jediným zpracováním uvedení zodpovědné osoby, podepsání a poslání nebo předání dokumentu mezi zpracovatelem a správcem (předpisy BOZP a PO, faktury, smlouvy). Protože je řešen především zpracovatel, není podstatné, jak správce zjistil osobní údaje svých zaměstnanců. Posledním zjednodušením je sloučení údajů jméno, příjmení a titul a jejich uvedení pouze jako jméno.

Na Obrázku 2 je vidět, že odpovědná osoba klienta předává živnostníkovi osobní údaje svých zaměstnanců. Veškeré údaje jsou zpracovávány za účelem vypracování dokumentů. Tyto dokumenty jsou ve vytištěné podobě podepsány a předány odpovědné osobě klienta. Všechny dodané dokumenty jsou uloženy v zamčené skříni klienta. Některé dokumenty PO jsou zveřejněny na pracovišti klienta nebo předány hasičskému záchrannému sboru. Tyto dokumenty obsahují kontaktní údaje využitelné v případě požáru a jiných nouzových situací. Elektronická verze je uložena na počítači živnostníka a s využitím synchronizace služby OneDrive společnosti Microsoft i na počítači spolupracující OSVČ.

Pro živnost kominictví není diagram vypracován. V tomto případě se jedná o předání osobních údajů, jejich zpracování do zprávy, uložení v počítači a na OneDrive (bez synchronizace na jiný počítač). Následně jsou vytištěny a podepsány dvě kopie. Jedna je předána klientovi a druhá uložena v zamčené skříni živnostníka.

Obrázek 2 Datové toky osobních údajů zpracovávaných živnostníkem



Zdroj: Vlastní zpracování

4.3.3 GAP analýza

Po identifikaci datových toků byla zpracována GAP analýza pro zjištění souladu zpracování osobních údajů s Nařízením GDPR. Údaje týkající se výhradně kominictví jsou napsané zeleně. Analýza byla zpracována společným vyplněním dotazníku s živnostníkem. Její výsledek je v Tabulce 3. Bylo zjištěno, že živnostník využívá všechny osobní údaje, které získává od správce nebo subjektu údajů. Při analýze bylo zjištěno, že živnostník nezpracovává záznamy o činnostech, ty byly nově zpracovány pro činnost kominictví i BOZP a PO.

Tabulka 3 GAP analýza činností - BOZP a PO a kominictví

Identifikace zpracování

Název zpracování: BOZP a PO Kominictví		**Počet zaměstnanců organizace:**	**0**
Vymezení vztahu organizace ke zpracování:			
Správce	Ne		
Zpracovatel	Ano	*Správce* – klienti služeb v oblasti BOZP a PO	
Jsou využíváni subzpracovatelé?	Ano	Spolupracující OSVČ Microsoft OneDrive	
Subjekty údajů:			
Klienti a zaměstnanci klientů			
Jiné osoby, které řeší oblast BOZP a PO u klienta (zde jde z pravidla o jméno, příjmení a osvědčení revizních techniků a osob vykonávajících kontroly státních úřadů)			
Sběrné uzly:			
Komunikace se správcem / subjektem: Email Telefon Ústně Flashdisk			
Právní základ zpracování:			
Osobní údaje:	Ano	Zvláštní kategorie osobních údajů:	Ano
Plnění smlouvy Plnění právní povinnosti (správce) Oprávněný zájem (fakturace)		Plnění povinností a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany (správce)	
Rozsah zpracování:			
Kolik subjektů údajů zpracování zahrnuje?	Cca 60 klientů / 1000 osob Cca 200 majitelů / provozovatelů spalinových cest		
Systematické zpracování:			
Jedná se o systematické zpracování?	Ano Ne		
Identifikátory:			
Jméno, Příjmení	Ano		
Titul	Ano		
Datum narození	Ano	Pro zjištění platnosti zdravotní způsobilosti	
Vzdělání	Ano	Pouze u profesí, kde je nutná speciální kvalifikace (elektrikáři, revizní technici apod.)	
Email	Ano	Pouze pro zajištění komunikace s několika zaměstnanci klienta	
Telefon	Ano	Pro zajištění komunikace s několika zaměstnanci klienta Pro zajištění požární prevence (týká se několika odpovědných pracovníků)	
Podpis	Ano	Potvrzení účasti na školení a převzetí dokumentů	

Adresa bydliště	Ano		
Zvláštní kategorie osobních údajů:			
Zdravotní stav	Ano	Pro zjištění platnosti zdravotní způsobilosti	
Informování subjektu údajů:	Ano/Ne		Ano/Ne
Povinné	Ne	Pokud ano, proběhlo?	
Je v rámci zpracování prováděno:	Ano/Ne		
Profilování	Ne		
Generalizace	Ne		
Odvozování	Ne		
Technická a organizační opatření:	Ano/Ne		
Pseudonymizace	Ne		
Anonymizace	Ne		
Šifrování	Ano		
Uložení osobních údajů:	Ano/Ne		Ano/Ne
Manuální	Ano	Elektronické	Ano
Dokumentace BOZP a PO správce Hasičský záchranný sbor kraje (některé dokumenty PO) Majitel/provozovatel spalinové cesty		Stolní počítač Přenosný počítač Přenosný počítač spolupracující OSVČ Poslání emailem správci Hasičský záchranný sbor kraje (některé dokumenty PO) Microsoft OneDrive	
Doba zpracování:			
Po jakou dobu je potřebné osobní údaje shromažďovat?	Po dobu platnosti smlouvy		
Interní odpovědnost za zpracování:	-		

Zdroj: vlastní zpracování

4.3.4 Posouzení rizika

Podle metodiky vydané ÚOOÚ byla vytvořena Tabulka 4 a následně vyplněna společně s živnostníkem. Z tabulky vyplývají významné a kritické hodnoty některých kritérií, na která je nutno klást zvýšenou pozornost. Kritická hodnota je způsobena zpracováváním zdravotních osobních údajů zaměstnanců klientů pro posouzení způsobilosti vykonávat práci. Významnou hodnotou je ohodnoceno zpracování veřejně přístupných dokumentů k zajištění požární prevence s kontaktními údaji. Další zvýšená hodnota je způsobena zapojením dalšího zpracovatele do řetězce zpracování osobních údajů. Jedná se o OSVČ se stejnou kvalifikací, který může živnostníka zastupovat. Zpracování DPIA není nutné, protože jde o jednu kritickou a dvě významné hodnoty.

Tabulka 4 Posouzení významu zpracovávaných osobních údajů živnostníkem

#	Kritérium	Hodnota
1	Zpracování osobních údajů zahrnuje monitorování subjektů údajů	Nízká
2	Zpracování údajů, které umožňují přímou identifikaci a/nebo údajů, vysoce osobní povahy pro subjekty údajů	Kritická
3	Zpracování údajů, které mohou subjekty údajů vystavit ohrožení z okolního prostředí	Nízká
4	Zpracování osobních údajů velkého rozsahu	Nízká
5	Zpracování zahrnující snímání veřejně přístupných prostor	Nízká
6	Zpracování osobních údajů, které mohou subjekty údajů v omezeném rozsahu ovlivnit	Nízká
7	Zpracování osobních údajů, které jsou veřejně přístupné	Významná
8	Zpracování osobních údajů, využívající složité nebo pokročilé technologické infrastruktury či platformy	Nízká
9	Zpracování osobních údajů jinými správci či zpracovateli	Významná
10	Zpracování osobních údajů prostřednictvím nových technologických nebo organizačních řešení	Nízká

Zdroj: vlastní zpracování podle ÚOOÚ

4.4 Charakteristika vybrané společnosti s ručením omezeným

Druhým vybraným podnikatelským subjektem je společnost s ručením omezeným (společnost). Předmětem podnikání společnosti jsou následující činnosti uvedené v přílohách živnostenského zákona

Živnosti ohlašovací řemeslné

- Truhlářství, podlahářství
- Malířství, lakýrnictví, natěračství
- Zednictví
- Pokrývačství, tesařství

Živnosti ohlašovací volné

Společnost se orientuje na práci s vysoce kvalitními materiály a nabízí především:

- hydroizolace střech, dlažeb, teras
- odolné lité podlahy
- renovace schodišť a PVC fólií
- sanace betonu
- prodej vysoce kvalitních materiálů

Aktuálně společnost zaměstnává celkem 11 zaměstnanců.

V oblasti ochrany osobního údajů je společnost nejčastěji v roli správce osobních údajů svých zaměstnanců nebo zpracovatelem osobních údajů klientů se kterými je v obchodním vztahu a lidí kteří společnost kontaktují skrze webový formulář nebo jiné cesty. Společnost také provozuje kamerový systém ve svém skladu a obchodě a sleduje služební osobní automobily pomocí systému GPS.

4.5 Změny provedené v souvislosti s přijetím Nařízení GDPR

V době před začátkem účinnosti Nařízení GDPR společnost přestěhovala personální evidenci z budovy skladu a obchodu do zamčené skříně v sídle společnosti. Společnost také přidala zaškrtávací políčko souhlasu se zpracováním osobních údajů ke kontaktnímu formuláři na svých webových stránkách. Společnost také upravila své smlouvy a dokumentaci o zpracování osobních údajů pomocí kamerového systému a systému GPS.

4.6 Zpracování osobních údajů společností

V této části jsou identifikovány činnosti, při kterých dochází ke zpracování, typ zpracovávaných osobních údajů a způsob jakým jsou zpracovávány.

4.6.1 Zaměstnávání lidí

Pro plnění právních požadavků na zaměstnávání lidí společnost zpracovává tyto osobní údaje svých zaměstnanců:

- Jméno a příjmení
- Všechna dřívější příjmení
- Datum a místo narození
- Rodné číslo
- Místo trvalého pobytu
- Číslo občanského průkazu
- Jméno, příjmení a rodné číslo dětí zaměstnanců
- Rodinný stav zaměstnance a jméno, příjmení, název a adresu zaměstnavatele manžela nebo manželky
- Předchozí zaměstnání
- Vzdělání
- Druh pobíraného důchodu
- Počet dětí (u žen)
- Zdravotní pojišťovna
- Zdravotní stav
- Telefon
- Email

Pracovní smlouva obsahuje jméno, příjmení, datum a místo narození, místo trvalého pobytu. Pracovní smlouvy jsou uloženy v zamčené skříni v sídle společnosti.

Pro výpočet mzdy, hlášení na sociálním úřadě, odvod sociálního a zdravotního pojištění společnost zpracovává jméno, příjmení (a dřívější příjmení), datum a místo narození, rodné číslo, číslo občanského průkazu. Dále jméno, příjmení a rodné číslo dětí zaměstnanců; rodinný stav zaměstnance a jméno, příjmení, název a adresu zaměstnavatele manžela nebo manželky (pro vyplnění daňového přiznání). Tyto osobní údaje také zpracovává účetní, Okresní správa sociálního zabezpečení, zdravotní pojišťovna a finanční úřad.

Pro zjištění věku odchodu do starobního důchodu společnost zpracovává údaje o počtu dětí svých zaměstnankyň.

Pro placení zdravotního pojištění zjišťuje společnost zdravotní pojišťovnu svých zaměstnanců. (Úřad pro ochranu osobních údajů, 2013)

Pro zjištění, zda je pracovník schopen vykonávat práci má společnost uzavřenou smlouvu s lékařem o poskytování pracovnělékařské péče. Na zdravotním posudku jsou uvedeny jméno, příjmení, datum narození, pracovní náplň a kategorie práce a zdravotní stav. Tyto údaje zpracovává společnost a lékař. Lékař je správcem osobních údajů.

Pro zajištění komunikace se zaměstnanci zpracovává společnost telefonní a emailové kontakty svých zaměstnanců.

Personální evidenci vede jednatel společnosti spolu s jedním dalším zaměstnancem. Složky s těmito osobními údaji v listinné podobě nejsou uloženy na provozovně společnosti, ale v sídle společnosti v zamčené skříni.

4.6.2 Kamerový systém

Společnost zpracovává osobní údaje prostřednictvím obrazového záznamu kamerového systému, provozovaného za účelem ochrany majetku.

Osobní údaje mohou být zpřístupněny v případě mimořádných událostí orgánům činným v trestním řízení nebo správním orgánům pro vedení přestupkového řízení apod.

Kamerový systém se skládá ze čtyř kamer umístěných v provozovně společnosti:

- ve venkovním prostoru před vchodem do budovy
- v prostoru hlavního vchodu
- ve dvou skladech

Záznamy jsou v programu pravidelně přepisovány po dosažení kapacity paměti. Provoz kamerového systému je na základě detekce pohybu.

Zaměstnanci společnosti udělili souhlas se zpracováním na dobu neurčitou a byli informováni o právu na přístup k osobním údajům, právu žádat vysvětlení nebo odstranění vzniklého stavu.

4.6.3 GPS

Služební osobní vozidla společnosti jsou sledována zaměstnavatelem pomocí systému GPS za účelem ochrany majetku. Zařízení zaměstnavateli umožní sledování pohybu vozidla, spotřebu paliva a vystopování v případě krádeže. GPS systém dále slouží k jednodušší tvorbě knihy jízd, nemusí být tedy vyplňována ručně.

K informacím má přístup pouze jednatel firmy a budou uchovávány v souladu s povinností archivovat data sloužící k daňové kontrole příjmových a výdajových dokladů, tedy po dobu 5 nebo 10 let.

Zaměstnanci společnosti udělili souhlas se zpracováním na dobu neurčitou a byli informováni o právu na přístup k osobním údajům, právu žádat vysvětlení nebo odstranění vzniklého stavu.

4.6.4 Komunikace s klienty, fakturace

- Jméno a příjmení
- Emailová adresa
- Telefonní číslo

Pro bezproblémovou komunikaci s klienty a fakturaci živnostník využívá emailovou adresu a telefonní číslo na lidi s kterými komunikuje.

Důvodem pro zpracování je plnění obchodní smlouvy.

4.6.5 Kontaktování přes kontaktní formulář na webových stránkách

Na svých internetových stránkách má společnost vytvořený kontaktní formulář. Jeho prostřednictvím kromě zprávy společnost také zpracovává následující osobní údaje:

- Jméno
- Příjmení
- Email

- Telefon

Pro odeslání zprávy musí její odesílatel souhlasit se zpracováním osobních údajů pro účely zpětného kontaktování. Tento souhlas je zajištěn zaškrtnutím tlačítka. Bez zaškrtnutí nelze zprávu odeslat.

4.6.6 Záloha dokumentů a informační systém

Pro zálohování a vzdálený přístup k dokumentům využívá společnost službu Disk Google společnosti Google. Firma také využívá informační systém pro účetnictví a jiné činnosti.

4.6.7 Zpracovatelé

Zpracovateli osobních údajů je účetní a poskytovatel služeb BOZP a PO a společnost Google prostřednictvím produktu Disk Google.

4.7 Diagram toku osobních údajů

Na Obrázku 3 je zobrazen diagram toku osobních údajů ve společnosti. Pro zjednodušení jsou osobní údaje zaměstnanců vypsány pouze jednou, při převzetí osobních údajů zaměstnanci jednatelem a zapsání do přenosného počítače jednatele (toto může proběhnout i na počítači v provozovně nebo počítači účetní). Dále není přesně specifikováno, které osobní údaje jsou zpracovávány a není blíže specifikována veřejná správa (to je popsáno v předchozím textu). Jednatele může v některých činnostech zastoupit i jiný zaměstnanec. Tečkovanou čarou je naznačeno sdílení dat mezi počítači. Oblast bezpečnosti práce a požární ochrany je zde vynechána, protože vypadá podobně, jako na obrázku živnostníka, který se na tuto oblast specializuje.

Pro plnění právních požadavků na zaměstnávání lidí společnost zpracovává osobní údaje svých zaměstnanců. Tyto osobní údaje jsou získány během přijetí zaměstnance do práce a jsou zadány do informačního systému společnosti. Složky zaměstnanců jsou v listinné podobě uloženy v zamčené skříni v sídle společnosti.

Do informačního systému má přístup kromě několika zaměstnanců přístup i účetní. Výstupy z účetnictví jsou předávány veřejné správě a v listinné podobě uloženy v zamčené skříni v sídle společnosti.

Při přijetí a periodicky po několika letech absolvují zaměstnanci prohlídku lékařem pracovnělékařské péče. O jejím výsledku je sepsán lékařský posudek, který je součástí

personální evidence a je uložen v zamčené skříni v sídle společnosti. Lékař není zpracovatelem, ale dalším správcem.

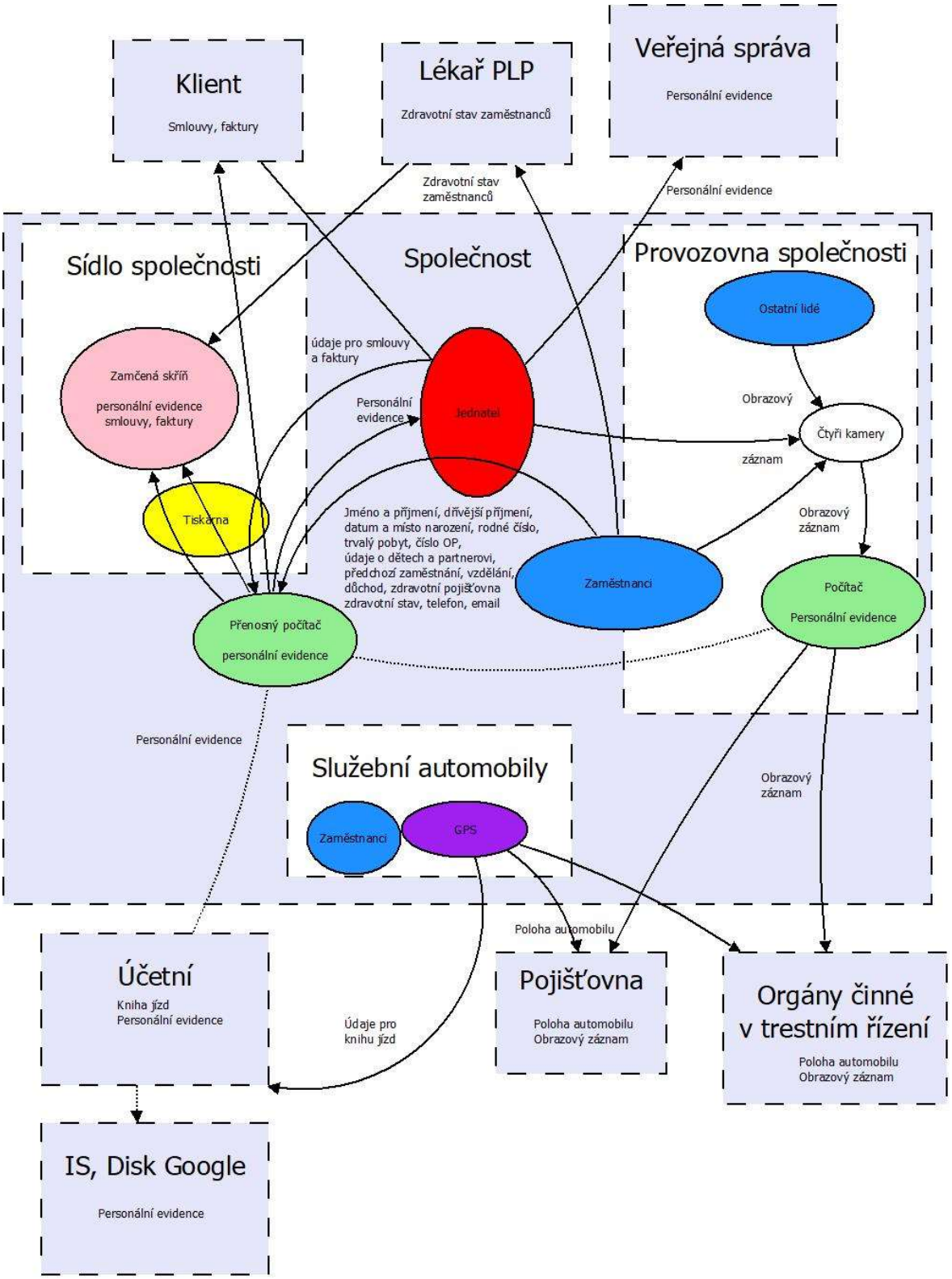
Společnost zpracovává osobní údaje klientů nutné pro komunikaci, podepsání smlouvy a fakturaci. Vydané faktury a uzavřené obchodní smlouvy jsou předány klientovi a uloženy v zamčené skříni v sídle společnosti.

Provozovna společnosti je z bezpečnostních důvodů vybavena kamerovým systémem. Záznamy z něj jsou uchovávány běžně maximálně jeden týden. V případě incidentů mohou být data z kamerového systému uložena jednatelem a předána pojišťovně a orgánům činným v trestním řízení.

Služební automobily společnosti jsou vybaveny systémem GPS. Data získaná tímto systémem jsou využívána pro vedení knihy jízd. Dalším důvodem je bezpečnost. V případě incidentů mohou být údaje o poloze automobilu (a zaměstnance) předány pojišťovně a orgánům činným v trestním řízení.

Kromě informačního systému používá společnost pro sdílení a zálohu některých osobních údajů službu Disk Google. Touto službou je synchronizováno několik počítačů společnosti.

Obrázek 3 Datové toky osobních údajů ve společnosti



Zdroj: Vlastní zpracování

4.8 GAP analýza

Po identifikaci datových toků byla zpracována GAP analýza pro zjištění souladu zpracování osobních údajů s GDPR. Analýza byla zpracována společným vyplněním dotazníků s jednatelem společnosti.

4.8.1 Zaměstnávání osob

Výsledek analýzy je v Tabulce 5. Bylo zjištěno, že společnost nezískává žádné osobní údaje, které nepotřebuje. Zaměstnanci byli seznámeni se zpracováním osobních údajů a záznamy o činnostech zpracování byly v pořádku.

Tabulka 5 GAP analýza činností - zaměstnávání

Identifikace zpracování

Název zpracování: Zaměstnanci		**Počet zaměstnanců organizace:**	**11**
Vymezení vztahu organizace ke zpracování:			
Správce	Ano	Zpracovatelé	Ano
		Poskytovatel služeb BOZP a PO Účetní Jiní zpracovatelé zajišťující legislativní požadavky Disk Google	
Zpracovatel	Ne		
Subjekty údajů:			
Zaměstnanci			
Sběrné uzly:			
Zaměstnanci: Dotazník Rozhovor Lékař Účetní			
Právní základ zpracování:			
Osobní údaje:	Ano	Zvláštní kategorie osobních údajů:	Ano
Plnění právní povinnosti		Plnění povinností a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany Zpracování je nezbytné pro účely preventivního nebo pracovního lékařství	
Rozsah zpracování:			
Kolik subjektů údajů zpracování zahrnuje?	11		
Systematické zpracování:			

Jedná se o systematické zpracování?	Ano		
Identifikátory:			
Jméno, Příjmení	Ano		
Dřívější příjmení	Ano		
Titul, vzdělání	Ano		
Datum narození	Ano		
Místo narození	Ano		
Místo trvalého pobytu	Ano		
Děti	Ano	Jméno, příjmení, rodné číslo (počet dětí u žen)	
Manžel/manželka	Ano	Jméno, příjmení, zaměstnavatel	
Zdravotní pojišťovna	Ano		
Předchozí zaměstnání	Ano		
Rodné číslo	Ano		
Vzdělání	Ano		
Email	Ano		
Telefon	Ano		
Podpis	Ano		
Zvláštní kategorie osobních údajů:			
Zdravotní stav	Ano	Pro zjištění platnosti zdravotní způsobilosti	
Informování subjektu údajů:	Ano/Ne		Ano/Ne
Povinné	Ano	Pokud ano, proběhlo?	Ano
Je v rámci zpracování prováděno:	Ano/Ne		
Profilování	Ne		
Generalizace	Ne		
Odvozování	Ne		
Technická a organizační opatření:	Ano/Ne		
Pseudonymizace	Ne		
Anonymizace	Ne		
Šifrování	Ano		
Uložení osobních údajů:	Ano/Ne		Ano/Ne
Manuální	Ano	Elektronické	Ano
Personální evidence Lékař		Účetní systém Stolní počítač Přenosný počítač Flashdisk Disk Google Lékař Státní správa Účetní Poskytovatel služeb BOZP a PO	
Doba zpracování:			
Po jakou dobu je potřebné osobní údaje shromažďovat?	5-10 let		
Interní odpovědnost za zpracování:	Jednatel + jeden zaměstnanec		

Zdroj: vlastní zpracování

4.8.2 GPS ve služebních autech

Vyplněný dotazník GAP analýzy pro monitorování polohy služebních automobilů je v Tabulce 6. Bylo zjištěno že společnost neaktualizovala souhlas se zpracováním osobních údajů podle nové legislativy. Z obsahového hlediska je však v pořádku, a proto není nutné ho se stávajícími zaměstnanci podepisovat znovu. Pokud firma přijme nové řidiče, musí vypracovat novou verzi. Záznam o činnostech pro systém GPS byl vypracován v průběhu psaní této diplomové práce.

Tabulka 6 GAP analýza činností - GPS

Identifikace zpracování

Název zpracování: GPS		**Počet zaměstnanců organizace:**	**11**
Vymezení vztahu organizace ke zpracování:			
Správce	Ano	Zpracovatelé	Ano
		Účetní (kniha jízd)	
Zpracovatel	Ne		
Jsou využíváni subzpracovatelé?	Ne		
Subjekty údajů:			
Zaměstnanci - řidiči			
Sběrné uzly:			
GPS systém v autě			
Právní základ zpracování:			
Osobní údaje:	Ano	Zvláštní kategorie osobních údajů:	Ne
Souhlas Oprávněný zájem (ochrana majetku)			
Rozsah zpracování:			
Kolik subjektů údajů zpracování zahrnuje?	4		
Systematické zpracování:			
Jedná se o systematické zpracování?	Ano		
Identifikátory:			
Jméno, Příjmení	Ano		
Lokalita	Ano		
Zvláštní kategorie osobních údajů:			
	Ne		
Informování subjektu údajů:	Ano/Ne		Ano/Ne
Povinné	Ano	Pokud ano, proběhlo?	Ano
Je v rámci zpracování prováděno:	Ano/Ne		
Profilování	Ne		
Generalizace	Ne		
Odvozování	Ne		
Technická a organizační opatření:	Ano/Ne		

Pseudonymizace	Ne		
Anonymizace	Ne		
Šifrování	Ano		
Uložení osobních údajů:	Ano/Ne		Ano/Ne
Manuální	Ne	Elektronické	Ano
		Účetní systém Stolní počítač Přenosný počítač Flashdisk Disk Google Orgány činné v trestním řízení (pouze ve zvláštních případech)	
Doba zpracování:			
Po jakou dobu je potřebné osobní údaje shromažďovat?	5-10 let		
Interní odpovědnost za zpracování:	Jednatel, účetní		

Zdroj: vlastní zpracování

4.8.3 Kamerový systém

Také při GAP analýze kamerového systému zpracované v Tabulce 7 bylo zjištěno, že společnost neaktualizovala souhlas podle GDPR. Nový souhlas bude nutné zpracovat při přijetí nových zaměstnanců. Záznam o činnostech pro kamerový systém byl vypracován v průběhu psaní této diplomové práce.

Tabulka 7 GAP analýza činností - kamerový systém

Identifikace zpracování

Název zpracování: Kamerový systém		**Počet zaměstnanců organizace:**	**11**
Vymezení vztahu organizace ke zpracování:			
Správce	Ano	Zpracovatelé	ne
Zpracovatel	Ne		
Jsou využíváni subzpracovatelé?	Ne		
Subjekty údajů:			
Zaměstnanci – především skladníci a řidiči Jiné osoby – zákazníci, kolemjdoucí			
Sběrné uzly:			
4 kamery			
Právní základ zpracování:			
Osobní údaje:	Ano	Zvláštní kategorie osobních údajů:	Ne
Souhlas Oprávněný zájem (ochrana majetku)			
Rozsah zpracování:			

Kolik subjektů údajů zpracování zahrnuje?	Až 9 zaměstnanců		
Systematické zpracování:			
Jedná se o systematické zpracování?	Ano		
Identifikátory:			
Obrazový záznam	Ano		
Lokalita	Ano		
Zvláštní kategorie osobních údajů:			
	Ne		
Informování subjektu údajů:	Ano/Ne		Ano/Ne
Povinné	Ano	Pokud ano, proběhlo? Zaměstnanci podpisem souhlasu Ostatní upozorněni tabulkou	Ano
Je v rámci zpracování prováděno:	Ano/Ne		
Profilování	Ne		
Generalizace	Ne		
Odvozování	Ne		
Technická a organizační opatření:	Ano/Ne		
Pseudonymizace	Ne		
Anonymizace	Ne		
Šifrování	Ano		
Uložení osobních údajů:	Ano/Ne		Ano/Ne
Manuální	Ne	Elektronické	Ano
		Paměť zařízení Orgány činné v trestním řízení a jiné paměťové médium (pouze ve zvláštních případech)	
Doba zpracování:			
Po jakou dobu je potřebné osobní údaje shromažďovat?	Obvykle do vyčerpání paměťové kapacity zařízení (maximálně několik dní) Pokud dojde k porušení majetkových práv majitele společnosti, bude záznam předán policii.		
Interní odpovědnost za zpracování:	Jednatel		

Zdroj: vlastní zpracování

4.9 Posouzení rizika

Podle metodiky vydané ÚOOÚ byla vytvořena Tabulka 8 a následně vyplněna společně s jednatelem společnosti. Z tabulky vyplývají významné a kritické hodnoty některých kritérií, na která je nutno klást zvýšenou pozornost. Kritická hodnota je způsobena vedením personální evidence zaměstnanců obsahující i údaje o zdravotním stavu. Významnou hodnotou je ohodnoceno provozování kamerového systému v prodejním skladu a sledování služebního automobilu pomocí systému GPS. Další významná hodnota je způsobena zapojením dalšího zpracovatele do řetězce zpracování osobních údajů. V tomto případě jde o externí účetní, případně jiné zpracovatele pomáhající vést jednateli personální evidenci a veřejnou správu. Zpracování DPIA není nutné, protože jde o jednu kritickou a dvě významné hodnoty.

Tabulka 8 Posouzení významu zpracovávaných osobních údajů společností

#	Kritérium	Hodnota
1	Zpracování osobních údajů zahrnuje monitorování subjektů údajů	Významná
2	Zpracování údajů, které umožňují přímou identifikaci a/nebo údajů, vysoce osobní povahy pro subjekty údajů	Kritická
3	Zpracování údajů, které mohou subjekty údajů vystavit ohrožení z okolního prostředí	Nízká
4	Zpracování osobních údajů velkého rozsahu	Nízká
5	Zpracování zahrnující snímání veřejně přístupných prostor	Nízká
6	Zpracování osobních údajů, které mohou subjekty údajů v omezeném rozsahu ovlivnit	Nízká
7	Zpracování osobních údajů, které jsou veřejně přístupné	Nízká
8	Zpracování osobních údajů, využívající složité nebo pokročilé technologické infrastruktury či platformy	Nízká
9	Zpracování osobních údajů jinými správci či zpracovateli	Významná
10	Zpracování osobních údajů prostřednictvím nových technologických nebo organizačních řešení	Nízká

Zdroj: vlastní zpracování podle ÚOOÚ

5 Výsledky a diskuze

Oba dva podnikatelské subjekty se začaly vážněji zajímat o problematiku ochrany osobních údajů v době mezi schválením a účinností Nařízení GDPR. V rámci práce byl hodnocen soulad současného stavu ochrany osobních údajů s požadavky platné legislativy.

5.1 Zhodnocení implementace Nařízení GDPR do činnosti živnostníka

Živnostník měl už před počátkem účinnosti Nařízení GDPR dobrý přehled o tom, které osobní údaje potřebuje k plnění povinností vyplývajících z uzavřených obchodních smluv. Byly-li mu poskytnuty osobní údaje, které nepotřeboval, neukládal je.

Během psaní diplomové práce byly uzavřeny zpracovatelské smlouvy s klienty – správci osobních údajů a vypracovány záznamy o činnostech.

5.1.1 Časová náročnost

Identifikace získávaných osobních údajů, jejich sběrných uzlů, účelů a důvodů zpracování byla pro živnostníka velice jednoduchá a zabrala mu pouze několik minut.

Několik hodin zabralo vytvoření vzoru smlouvy o zpracování osobních údajů jako dodatku k dříve uzavřeným obchodním smlouvám pro jednotlivé klienty. Živnostník vycházel ze vzorů smluv, které dostal od některých klientů. Pro oblast kominictví nemá živnostník uzavřené žádné obchodní smlouvy a nebylo nutné vypracovat žádné dodatky.

Nejvíce času zabralo upravení zpracovatelských smluv pro přibližně 60 klientů, jejich vytištění, a podepsání. Úprava a vytištění smlouvy pro každého klienta zabrala přibližně 10-15 minut – jde celkově přibližně o jeden pracovní den.

Smlouvy byly distribuovány a podepsány správci průběžně během preventivních kontrol pracovišť klientů. Vzhledem k obvyklé časové náročnosti kontroly u klienta je tento čas zanedbatelný.

Záznamy o činnostech zpracování byly vytvořeny v rámci této diplomové práce pro činnost BOZP a PO i pro kominictví. Jejich vypracování zabralo asi 1 hodinu.

5.1.2 Personální náročnost

Živnostník veškeré úkoly zvládl plnit sám, případně s pomocí autora diplomové práce. Jeho informačními zdroji byly především internetové články a vzory smluv dodané některými klienty.

5.1.3 Organizační náročnost

Živnostník začal více využívat svůj přenosný počítač k práci přímo u klientů. Dříve běžná praxe, kdy si dokumentaci odvezl k práci domů není možná z důvodu zabezpečení.

Živnostník také založil pořadač pro zakládání zpracovatelských smluv a nově dokumenty s osobními údaji uložil do zamčené skříně.

5.1.4 Ekonomická náročnost

Nejvyšším nákladem jsou přibližně dva pracovní dny, které živnostník věnoval veškeré práci. Dalšími náklady je jeden pořadač na zpracovatelské smlouvy a náklady na vytištění zpracovatelských smluv a záznamů o činnostech zpracování pro poskytování služeb v oblasti BOZP a PO a kominictví.

5.2 Zhodnocení implementace Nařízení GDPR do činnosti společnosti

Společnost již před implementací GDPR měla podepsané souhlasy se zpracováním osobních údajů se svými zaměstnanci pro provozování kamerového systému a systému GPS ve služebních osobních automobilech. Tyto souhlasy nebylo potřebné upravovat a znovu podepisovat. Dále měla společnost zpracovaný záznam o činnostech pro zaměstnávání osob. Záznamy o činnostech zpracování pro GPS systém, kamerový systém a evidenci klientů byly zpracovány během psaní této diplomové práce.

5.2.1 Časová náročnost

Identifikaci získávaných osobních údajů, jejich sběrných uzlů, účelů a důvodů zpracování provedla asistentka jednatele. Tato činnost zabrala asi půl pracovního dne.

Asistentka po konzultaci s právníkem, se kterým společnost dlouhodobě spolupracuje, připravila zpracovatelskou smlouvu s účetní a upravila vzory smluv, které budou uzavřeny s budoucími klienty.

Při psaní této diplomové práce byly zpracovány záznamy o činnostech zpracování pro kamerový systém, systém GPS, evidenci zákazníků. Tyto činnosti trvaly asi jednu hodinu. Dále byl upraven souhlas se zpracováním osobních údajů prostřednictvím kamerového systému a systému GPS pro případ přijmutí nových zaměstnanců v budoucnosti. Na webové stránky bylo jednatelem přidáno zaškrtávací políčko ke kontaktnímu formuláři

Celkově byl implementaci Nařízení GDPR věnován asi jeden den.

5.2.2 Personální náročnost

Osobní údaje zpracovává pouze jednatel a asistentka jednatele. Implementaci GDPR se věnovala především asistentka. Zapojil se i jednatel a autor této diplomové práce.

5.2.3 Organizační náročnost

Personální evidence a evidence smluv a faktur s klienty byla přesunuta z provozovny do sídla společnosti. Přemístění dokumentů nebude pro společnost problémem, protože jednatel i asistentka pracují v sídle i provozovně společnosti.

5.2.4 Ekonomická náročnost

Společnost využila služeb svého právníka. Cena konzultace byla asi 1000 Kč. Dále je potřeba započítat jeden pracovní den asistentky věnovaný implementaci.

5.3 Vzor smlouvy o zpracování osobních údajů

Pro potřeby živnostníka byla vypracována smlouva o zpracování osobních údajů jako dodatek, k již uzavřeným obchodním smlouvám pro poskytování služeb v oblasti BOZP a PO. Vzor smlouvy je Přílohou 1 této diplomové práce.

5.4 Vzor záznamů o činnostech zpracování osobních údajů

Pro potřeby společnosti byl zpracován záznam o činnostech zpracování osobních údajů pro provoz kamerového systému. Záznam je v tabulce Tabulka 9.

Tabulka 9 Záznam o činnostech zpracování – kamerový systém

Záznam o činnostech zpracování - kamerový systém

Správce:	Název společnosti Adresa společnosti IČ společnosti Kontaktní osoba
Účel zpracování:	Ochrana majetku společnosti Ochrana zaměstnanců a ostatních osob v prodejním skladu
Právní důvod:	Oprávněný zájem správce Oprávněný zájem třetích osob (GDPR čl. 6, odst. 1 f)
Subjekty údajů:	Zaměstnanci společnosti ve skladu společnosti Jiné osoby (zákazníci, dodavatelé, servis)
Kategorie osobních údajů:	Obrazový záznam osob - bez zpracování biometrických údajů
Informování subjektů údajů:	Piktogram na vstupních dveřích Podepsaný souhlas se zpracováním osobních údajů zaměstnanci
Další zpracování:	V případech incidentů orgány činné v trestním řízení a pojišťovna
Počet a umístění kamer	4 kamery Hlavní vchod, venkovní prostor před vchodem, hlavní sklad, zadní sklad
Doba uchování:	Běžně maximálně 1 týden. Incidenty po dobu nezbytně nutnou
Zabezpečení:	Omezený přístup k záznamu (pouze jednatel) V případě předání třetí straně je vyhotoven předávací protokol Kamery jsou chráněny krytem

Zdroj: vlastní zpracování

5.5 Doporučený postup implementace Nařízení GDPR

Doporučený postup implementace Nařízení GDPR pro malé správce a zpracovatele vychází především z dokumentů vydaných přímo úřadem pro ochranu osobních údajů. Vzhledem k tomu, že ÚOOÚ je kontrolním orgánem, by úřadem vypracované vzory dokumentů a dokumenty vypracované podle jejich metodiky měly splňovat veškeré požadavky úřadu během kontrol. Pro běžného drobného podnikatele jsou informace na webových stránkách ÚOOÚ dostupnější, než v odborné literatuře a důvěryhodnější než na jiných webech, které se často snaží hlavně prodat své produkty nebo služby.

Z prohlášení v úvodech dokumentů vydaných ÚOOÚ je vidět, že si úřad uvědomuje administrativní dopad Nařízení GDPR na malé firmy, a proto vydal materiály zmíněné během postupu implementace. Tyto dokumenty jsou snadno srozumitelné a využitelné právě především malými firmami. Tyto dokumenty srozumitelně vysvětlují některé kroky implementace Nařízení GDPR, ale chybí zde doporučení postupu, jak přesně by měla firma v implementaci postupovat.

Nařízení GDPR ukládá základní čtyři nové povinnosti pro správce. Těmi jsou záznamy o činnostech zpracování, jmenování pověřence pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů a předchozí konzultace s dozorovým úřadem. Pokud správce využívá zpracovatele osobních údajů, musí s ním mít uzavřenou smlouvu o zpracování osobních údajů.

Jmenování pověřence pro ochranu osobních údajů nebude pro většinu malých firem povinné. Pověřenec je nutný pro veřejné subjekty, systematické monitorování osob a rozsáhlé zpracování zvláštních kategorií osobních údajů a údajů o rozsudcích v trestních věcech.

Malé množství firem bude muset zpracovat posouzení vlivu na ochranu osobních údajů a konzultovat s ÚOOÚ.

Naopak vypracování záznamů o činnostech zpracování osobních údajů se doporučuje téměř všem podnikatelům. Povinně je musí zpracovávat všechny firmy s alespoň 250 zaměstnanci, nebo když zpracování pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech. Záznamy o činnostech jsou doporučené aspoň pro vedení personální evidence zaměstnanců.

Navržený postup implementace by měl zajistit splnění veškerých povinností.

1. **Identifikace zpracování osobních údajů**

Prvním krokem by měla být identifikace činností při kterých dochází ke zpracování osobních údajů. Provádí-li firma pouze činnosti na seznamu vydaným ÚOOÚ *(Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů)*, je už po prvním kroku jasné, že firma nemusí zpracovat DPIA.

2. **GAP analýza současného stavu**

Pro každou činnost by se měla zpracovat analýza. Výstupem analýzy je tabulka, která identifikuje místa kde ve firmě dochází ke sběru osobních údajů a jaké údaje jsou shromažďovány, jaký je právní důvod a účel zpracování, kde jsou osobní údaje uloženy, kdo k nim má přístup a jak jsou zabezpečeny.

3. **Vyhodnocení GAP analýzy (účel a právní důvod zpracování)**

Po analýze současného stavu je potřeba zjistit, zda jsou veškeré zpracovávané osobní údaje nutné. Pokud nejsou nesmí je firma získávat a zpracovávat.

Pokud není žádný z právních důvodů pro zpracování uvedených v závorce (nezbytnost zpracování pro splnění smlouvy se subjektem údajů; nezbytnost pro splnění právních povinností správce; nezbytnost pro ochranu životně důležitých zájmů subjektu nebo jiné fyzické osoby; nezbytnost pro výkon veřejné moci nebo úkolu ve veřejném zájmu; nezbytnost zpracování pro účely oprávněných zájmů správce nebo třetí strany) je třeba získat souhlas se zpracováním osobních údajů.

4. **Souhlas se zpracováním osobních údajů, informovanost**

Pro zpracování osobních údajů z jiných právních důvodů je nutné vytvořit systém pro získání jednoznačného souhlasu.

5. **Vyhodnocení rizika**

Rizika by měla být vyhodnocena např. podle metodiky ÚOOÚ (*K povinnosti správců provádět DPIA*). Jde o jednoduchý systém, kdy je deseti kritériím zpracování přiřazena nízká, významná nebo kritická hodnota. Vyhodnocení rizik firmu navede, kterým oblastem by měla věnovat zvýšenou pozornost.

Z vyhodnocení rizik také vyplývá povinnost zpracovat DPIA, pokud má firma dvě kritické hodnoty kritérií nebo jednu kritickou a alespoň pět významných hodnot.

6. Zpracování DPIA a konzultace s ÚOOÚ

Pokud má firma povinnost zpracovat DPIA, může k tomuto účelu využít metodiku ÚOOÚ v pracovní verzi „*Metodika obecného posouzení vlivu na ochranu osobních údajů*“. Dá se předpokládat, že ÚOOÚ v blízké době vydá i oficiální verzi této metodiky.

Pokud po zpracování DPIA zbyde stále vysoké riziko, má firma povinnost konzultovat situaci s ÚOOÚ. Zpracování DPIA a konzultace s ÚOOÚ se bude týkat pouze menšího počtu malých firem.

7. Zabezpečení

Podmínky zabezpečení osobních údajů je nutné řešit z hlediska technického (umístění listinné evidence, zabezpečení elektronické evidence, zajištění při předávání osobních údajů k dalšímu zpracování), organizačního (doba uchovávání, možnost zapomenutí, předávání třetím osobám) a personálního (omezení přístupu k osobním údajům, proškolení zaměstnanců zpracovávajících osobní údaje, případné jmenování pověřence).

8. Vytvoření pravidel

Pro vytvoření interních pravidel se firma může inspirovat textem ÚOOÚ *(Desatero zpracování pro správce)*. Kromě výše zmíněných bodů by mělo být v pravidlech zmíněno informování subjektu údajů o zpracování (zaměstnanci, návštěvníci objektu sledovaného kamerovým systémem) a likvidace nepotřebných osobních údajů.

9. Vypracování záznamu o činnostech zpracování

Vzor záznamu o činnostech je možné najít na webu ÚOOÚ a je i součástí této diplomové práce (Tabulka 2). Jeho součástí musí být kontaktní údaje správce, účely zpracování, popis subjektu údajů, popis kategorií zpracovávaných osobních údajů, případní další zpracovatelé, kterým budou osobní údaje poskytnuty, doba, po kterou jsou osobní údaje uchovávány a popis technického a organizačního zabezpečení.

10. Uzavření zpracovatelské smlouvy

Pokud je firma zpracovatelem osobních údajů pro jiné správce, nebo jako správce nechává zpracovávat spravované osobní údaje jinými zpracovateli, musí být mezi správcem a zpracovatelem uzavřena smlouva o zpracovávání osobních údajů.

5.5.1 Ověření ochrany osobních údajů ve firmě

Pro podnikatele, kteří se oblasti ochrany osobních údajů věnují, nebo přijaly některá opatření v době kolem přijetí Nařízení GDPR a chtějí zjistit co mají v pořádku a co by měli doplnit, je možné ověřit soulad s Nařízením GDPR prostřednictvím odpovědí na otázky, ze kterých plynou doporučení. Otázky se týkají plnění základních principů a povinností v oblasti ochrany osobních údajů.

Zákonnost:

Zpracovávám osobní údaje pro jiné účely než plnění smlouvy, právních povinností, životně důležitých zájmů, výkonů veřejné moci nebo pro veřejné nebo oprávněné zájmy?

ANO *je-li účel zákonný, potřebuji získat souhlas se zpracováním, jinak nemohu pro tento účel osobní údaje zpracovávat*

NE *splňuji zásadu zákonnosti*

Transparentnost:

Informuji subjekt údajů o důvodech zpracování osobních údajů a o tom, kdo má k nim přístup?

ANO *splňuji zásadu transparentnosti*

NE *je třeba vhodným způsobem informovat (např. podepsání seznámení, informování veřejnosti pomocí piktogramů)*

Korektnost:

Zpracovávám osobní údaje jen pro účely, pro který mám právní důvod?

ANO *splňuji zásadu korektnosti*

NE *potřebuji získat souhlas s tímto zpracováním*

Účelové omezení:

Sdělil(a) jsem účel zpracování subjektu údajů?

ANO *splňuji zásadu účelového omezení*

NE *nemohu osobní údaje shromažďovat a zpracovávat*

Minimalizace údajů:

Zpracovávám pouze osobní údaje, které potřebuji pro daný účel?

ANO splňuji zásadu minimalizace údajů

NE údaje, které nepotřebuji, nemůžu zpracovávat ani shromažďovat

Přesnost:

Jsou zpracovávané osobní údaje přesné?

ANO je potřeba osobní údaje v budoucnu kontrolovat a aktualizovat

NE je nutné bez zbytečných odkladů opravit chyby, zabývat se žádostmi o opravení nebo doplnění a udržovat evidenci aktuální

Omezení uložení:

Shromažďuji osobní údaje, které jsem v minulosti potřeboval(a) pro účel který už pominul?

ANO je nutné tyto osobní údaje zlikvidovat (nebo anonymizovat) a přestat shromažďovat

NE splňuji zásadu omezení uložení

Integrita a důvěrnost:

Mám vhodně zabezpečeny osobní údaje v elektronické i písemné podobě? (omezení přístupnosti – zamčená místnost, zamčená skříň, heslo v PC a telefonu; proškolení zaměstnanců pracujících s osobními údaji apod.)

ANO pokud k osobním údajům nemá přístup nikdo, kdo je nemá právo zpracovávat, splňuji zásadu integrity a důvěrnosti

NE musím lépe zabezpečit osobní údaje

Další zpracování:

Dochází k dalšímu zpracování mimo firmu nebo jsem zpracovatelem osobních údajů pro jiné správce? (např. externí zajištění účetnictví a BOZP a PO)

ANO je nutné uzavřít smlouvu o zpracování osobních údajů a postupovat podle ní

NE nedochází k dalšímu zpracování

Záznam o činnostech zpracování:

Zaměstnávám více než 250 zaměstnanců?

Provádím zpracování osobních údajů rizikové pro subjekt?

Provádím zpracování, které není příležitostné?

Zpracovávám zvláštní kategorie údajů nebo údaje o rozsudcích v trestních věcech?

Aspoň 1x ANO musím zpracovat záznamy o činnostech

4x NE nemusím zpracovat záznamy o činnostech

Jmenování pověřence:

Provádím pravidelné a systematické monitorování subjektů osobních údajů nebo zpracovávám zvláštní kategorie údajů a údaje o rozsudcích v trestních věcech v rámci své hlavní činnosti?

ANO je nutné jmenovat pověřence

NE pověřenec není nutný

Posouzení vlivu na ochranu osobních údajů:

Provádím operace, které nejsou na seznamu operací zpracování osobních údajů, které nepodléhají posouzení vlivu na ochranu osobních údajů?

ANO je nutné vyhodnotit rizika a případně zpracovat DPIA

NE není nutné zpracovat DPIA

6 Závěr

Hlavním cílem této diplomové práce bylo navržení postupu implementace Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES do podnikatelské činnosti malých firem a osob samostatně výdělečně činných. Ke splnění tohoto cíle bylo nutné využít odbornou literaturu a metodické postupy. Většina kroků navrženého postupu byla využita při kontrole souladu činnosti dvou firem s požadavky Nařízení GDPR. U těchto podnikatelských subjektů byla vyhodnocena časová, finanční, organizační a personální náročnost implementace Nařízení GDPR a byla jim navržena opatření k zajištění souladu s Nařízením GDPR.

Dílčím cílem této diplomové práce bylo zpracování vzorového záznamu o činnostech pro jednu konkrétní činnost správce osobních údajů a návrhu smlouvy o zpracování osobních údajů jako dodatku k již uzavřeným obchodním smlouvám. Tyto cíle byly naplněny zpracováním záznamu pro provoz kamerového systému společnosti a návrhem smlouvy o zpracování osobních údajů pro služby BOZP a PO.

Pro zjištěné nedostatky v zavádění Nařízení GDPR do činnosti vybraných podnikatelských subjektů byla navržena nápravná opatření. Většina těchto opatření byla implementována v průběhu psaní této diplomové práce.

Hlavním výstupem diplomové práce je navržený postup implementace Nařízení GDPR pro malé firmy. Tento postup je jednou formulován krok za krokem a je určen především pro firmy, které se ochranou osobních údajů dosud blíže nezabývají a chtějí implementaci Nařízení GDPR věnovat více času.

Naopak pro firmy, které se ochraně osobních údajů věnují, v minulosti přijaly některá opatření nebo na implementaci nemají dostatek času a chtějí v rychlosti zjistit, co ještě musí udělat je postup formulován prostřednictvím odpovědí na otázky a z nich vyplývajících doporučení.

7 Seznam použitých zdrojů

FOULSHAM, Mark, Brian HITCHEN a Andrew DENLEY. GDPR: how to achieve and maintain compliance. New York, 2019. ISBN 978-1-138-32617-0.

MINISTERSTVO PRŮMYSLU A OBCHODU. Příručka pro přípravu malých a středních firem na GDPR. I. vydání. 2018. ISBN 978-80-906942-3-1. Dostupné také z: https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/Podpurna-opatreni-mpo/2018/4/Prirucka-pro-pripravu-malych-a-strednich-firem-na-GDPR.pdf

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

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

Ochrana osobních údajů: vybrané otázky : příručka pro podnikatele. Brno: Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011. ISBN 978-80-210-5572-8.

ŠKORNIČKOVÁ, Eva. Je nejlepším řešením GDPR přechod na cloud? | GDPR.cz. GDPR | Obecné nařízení o ochraně osobních údajů — prakticky [online]. 17. 9. 2017 Dostupné z: https://www.gdpr.cz/blog/je-nejlepsim-resenim-gdpr-prechod-na-cloud/

The Data Protection Officer: Profession, Rules, and Role, Paul Lambert, CRC Press, 2017

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 11. Sankce, pokuty: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25.4.2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 2. Nové přístupy a povinnosti: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25.4.2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/2-nove-p-istupy-a-povinnosti/d-27268

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 4. Zásady a právní důvody zpracování: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25.4.2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 5. Zvláštní kategorie osobních údajů (citlivé údaje): *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 5.3.2018 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 6. Práva subjektu údajů: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25.4.2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaj/d-27276

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. 8. Zabezpečení osobních údajů: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25.4.2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/8-zabezpe-eni-osobnich-udaj/d-27282

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Adaptační legislativa k GDPR vstoupila v účinnost: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 25. 4. 2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/adaptacni-legislativa-k-nbsp-gdpr-vstoupila-v-nbsp-ucinnost/d-33656

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Desatero zpracování pro správce: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/desatero-zpracovani-pro-spravce/ds-4821/p1=4821

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA). Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33193

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Metodika obecného posouzení vlivu na ochranu osobních údajů. Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=37330

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů. Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30738

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Role ÚOOÚ: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/role-uoou/ds-4726/p1=4726

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Úřad předkládá k veřejné diskuzi metodiku DPIA: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 23. 10. 2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/urad-predklada-k-nbsp-verejne-diskuzi-metodiku-dpia/d-37262

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k GDPR: Zaměstnavatelé a zaměstnanci : *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 24. 4. 2019 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=2075

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Zaměstnavatel jako správce osobních údajů: *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 13. 12. 2013 [cit. 24.11.2019]. Dostupné z: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Zpracovatel: GDPR (obecné nařízení): *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. 15.10.2018 [cit. 22.11.2019]. Dostupné z: https://www.uoou.cz/zpracovatel/d-29316/p1=3938

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2018 : Brno, 2019. Dostupné také z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33526

ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, [2017]. Právo (ANAG). ISBN 978-80-7554-097-3.

8 Přílohy

Smlouva o zpracování osobních údajů

uzavřená mezi:

Správce

se sídlem: _____
IČ: _____
(dále jen „**Správce**“)

a

Zpracovatel

Živnostník
se sídlem: _____
IČ: _____

Spolupracující OSVČ

se sídlem: _____
IČ: _____
(dále jen „**Zpracovatel**“)

(dále společně jen „**Smluvní strany**”)

Preambule

(A) Smluvní strany uzavřely dne _____ smlouvu, na základě které se Zpracovatel zavázal poskytovat Správci služby v oblasti BOZP a PO (dále jen „**Služby**”).

(B) Řádné poskytování Služeb vyžaduje mimo jiné i zpracování osobních údajů zákazníků a zaměstnanců Správce (dále jen „**Osobní údaje**“), které bude pro Správce provádět Zpracovatel.

S ohledem na výše uvedené Smluvní strany uzavírají v režimu Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „**Nařízení**”) a ve spojení se zákonem o zpracování osobních údajů následující smlouvu o zpracování
osobních údajů (dále jen „**Smlouva**“).

I.
Předmět Smlouvy

1.1 Předmětem této Smlouvy je úprava vzájemných práv a povinností Smluvních stran při zpracování Osobních údajů, které Zpracovatel získá v souvislosti s poskytováním svých Služeb.

II.
Podmínky zpracování Osobních údajů

2.1 Účelem zpracování Osobních údajů je plnění povinností vyplývajících ze zákona 262/2006 Sb., ve znění pozdějších předpisů a zákona 133/1985 Sb., ve znění pozdějších předpisů a v souladu se smlouvou o poskytování Služeb a s obecně závaznými právními předpisy.
2.2 Osobní údaje zaměstnanců Správce budou zpracovány v rozsahu:

- jméno, příjmení a titul,
- datum narození,
- e-mailová adresa,
- telefonní číslo,
- data školení nutných pro výkon práce,
- adresa bydliště
- data lékařských prohlídek nutných pro výkon práce.

2.3 Předmětem zpracování Osobních údajů na základě této Smlouvy nejsou citlivé údaje ve smyslu Nařízení.

2.4 Zpracováním Osobních údajů ve smyslu této Smlouvy se rozumí zejména jejich shromažďování, ukládání na nosiče informací v rozsahu nezbytném pro zajištění řádného poskytování Služeb.

2.5 Osobní údaje budou zpracovány po dobu poskytování Služeb s tím, že ukončením smlouvy o poskytování Služeb bez dalšího zaniká i tato Smlouva. Ukončením této Smlouvy nezanikají povinnosti Zpracovatele týkající se bezpečnosti a ochrany Osobních údajů až do okamžiku jejich protokolární úplné likvidace či protokolárnímu předání jinému zpracovateli.

2.6 Smluvní strany se dohodly, že zpracování Osobních údajů na základě této Smlouvy bude bezplatné, přičemž Zpracovatel nemá nárok na náhradu nákladů spojených s plněním této Smlouvy. Tím není dotčen nárok Zpracovatele na odměnu za poskytování Služeb.

III.
Povinnosti Smluvních stran

3.1 Správce je při plnění této Smlouvy povinen:

a) zajistit, že Osobní údaje budou zpracovány vždy v souladu s Nařízením a zákonem o zpracování osobních údajů, že tyto údaje budou aktuální, přesné a pravdivé, jakož i to, že tyto údaje budou odpovídat stanovenému účelu zpracování;

b) přijmout vhodná opatření, aby poskytl subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace a učinil veškerá sdělení požadovaná Nařízením a zákonem o zpracování osobních údajů.

3.2 Zpracovatel je při plnění této Smlouvy povinen:

a) nezapojit do zpracování Osobních údajů žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Správce;

b) zpracovávat Osobní údaje pouze na základě doložených pokynů Správce, včetně v otázkách předání Osobních údajů do třetí země nebo mezinárodní organizaci;

c) zohledňovat povahu zpracování Osobních údajů a být Správci nápomocen pro splnění Správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů, jakož i pro splnění dalších povinností ve smyslu Nařízení;
d) po skončení této Smlouvy protokolárně odevzdat Správci nebo nově pověřenému zpracovateli všechny Osobní údaje zpracované po dobu poskytování Služeb.

3.3 Smluvní strany jsou při plnění této Smlouvy povinny:

a) zavést technická, organizační, personální a jiná vhodná opatření ve smyslu Nařízení, aby zajistily a byly schopny kdykoliv doložit, že zpracování Osobních údajů je prováděno v souladu s Nařízením a zákonem o zpracování osobních údajů tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k Osobním údajům a k datovým nosičům, které tyto údaje obsahují, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití, a tato opatření podle potřeby průběžné revidovat a aktualizovat;

b) vést a průběžně revidovat a aktualizovat záznamy o zpracování Osobních údajů ve smyslu Nařízení;

c) řádně a včas ohlašovat případná porušení zabezpečení Osobních údajů Úřadu pro ochranu osobních údajů a spolupracovat s tímto úřadem v nezbytném rozsahu;

d) navzájem se informovat o všech okolnostech významných pro plnění předmětu této Smlouvy;

e) zachovávat mlčenlivost o Osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení Osobních údajů, a to i po skončení této Smlouvy;

f) postupovat v souladu s dalšími požadavky Nařízení a zákona o zpracování osobních údajů, zejména dodržovat obecné zásady zpracování osobních údajů, plnit své informační povinnosti, nepředávat Osobní údaje třetím osobám bez potřebného oprávnění, respektovat práva subjektů údajů a poskytovat v této souvislosti nezbytnou součinnost.

IV.
Závěrečná ustanovení

4.1 Tato Smlouva a právní poměry z ní vzešlé a s ní související se řídí Nařízením a právními předpisy České republiky, zejména pak ustanoveními zákona o zpracování osobních údajů.

4.2 Tato Smlouva nabývá platnosti a účinnosti okamžikem podpisu poslední ze Smluvních stran.

4.3 Tuto Smlouvu lze měnit, doplňovat nebo zrušit pouze písemně, nikoliv ovšem prostřednictvím elektronických zpráv bez kvalifikovaného elektronického podpisu ve smyslu Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS).

4.4 Tato Smlouva se vyhotovuje ve dvou (2) originálech, přičemž jedno (1) vyhotovení je určeno pro Správce a jedno (1) pro Zpracovatele.

4.5 Smluvní strany prohlašují, že si návrh této Smlouvy pozorně a pečlivě přečetly, že dobře rozumí jeho obsahu a že ten odpovídá jejich skutečné vůli, na důkaz čehož připojují své podpisy a uzavírají tuto Smlouvu.

Ve _____ dne _____

……..

Správce:

……..

Zpracovatel 1:

……..

Zpracovatel 2: