Implementace GDPR v malé firmě

Bc. Radek Kudela

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 21.5.2018

podpis diplomanta

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

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

Jméno a příjmení:	**Bc. Radek Kudela**
Osobní číslo:	**A16161**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Implementace GDPR v malé firmě**
Téma anglicky:	**The Implementation of a GDPR in a Small Company**

Zásady pro vypracování:

1. **Definujte základní pojmy spojené s GDPR, které jsou spojeny s malými firmami.**
2. **Specifikujte možnosti implementace GDPR.**
3. **Vyhodnoťte zda současné podmínky ve firmě vyhovují pro provozování GDPR.**
4. **Navrhněte procesní opatření pro implementaci požadavků GDPR.**
5. **Zhodnoťte dopady implementace na chod firmy.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **GDPR Compliance and Its Impact on Security and Data Protection Programs. Actiance [online]. Washington: Osterman Research, 2017 [cit. 2017-11-27]. Dostupné z: https://www.actiance.com/wp-content/uploads/2017/03/WP-GDPR-Compliance-and-Its-Impact-on-Security-and-Data-Protection-Programs.pdf.**
2. **NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.**
3. **Nová pravidla ochrany osobních údajů [online]. Praha: Hospodářská komora České republiky Odbor legislativy, práva a analýz, 2017, , 19 [cit. 2017-11-27]. Dostupné z: https://www.komora.cz/wp-content/uploads/2017/06/PriruckaGDPR_final.pdf.**
4. **Preparing for Compliance with the General Data Protection Regulation (GDPR) A Technology Guide for Security Practitioners. SANS Institute [online]. London, 2017 [cit. 2017-11-27]. Dostupné z: https://www.sans.org/reading-room/whitepapers/analyst/preparing-compliance-general-data-protection-regulation-gdpr-technology-guide-security-practitioners-37667.**
5. **The GDPR and You. Dataprotection [online]. Ireland, 2017 [cit. 2017-11-27]. Dostupné z: https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf**
6. **Základní příručka k GDPR. Úřad pro ochranu osobních údajů [online]. Praha, 2017 [cit. 2017-11-27]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Práce se zabývá implementací GDPR v malé firmě. Je zde řešena problematika zhodnocení současných používaných systémů s přihlédnutím k zavedení GDPR. Stávající systémy jsou klasifikovány jako vyhovující, nebo nevyhovující a u nevyhovujících jsou navrženy podmínky, za jakých je službu možné provozovat. Zároveň je obsahem práce návrh procesních opatření pro implementaci požadavků GDPR.

Klíčová slova: GDPR, General Data Protection Regulation, Zákon o ochraně osobních údajů, Firemní procesy, Procesní analýza, Dopad GDPR, Procesní opatření

ABSTRACT

This thesis focuses on GDPR implementation in a small company. It deals with the issue of evaluation of the systems used today in regards to GDPR introduction. The existing systems are classified as either satisfactory or unsatisfactory. It it's the latter, there are conditions suggested, as to how it's possible to keep the service going. The thesis also contains suggestions of procedural measures for implementing GDPR's requirements.

Keywords: GDPR, General Data Protection Regulation, the Law on Personal Data Protection, Corporate processes, Process analysis, impact of GDPR, Procedural measures

Můj velký dík patří panu Ing. Davidovi Malaníkovi Ph.D. za předání zkušeností, cenné rady a za odborné vedení při vypracování diplomové práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

GDPR neboli General Data Protection Regulation je nařízení EU vstupující v platnost 25. května. Nastavuje rovné podmínky pro zpracování osobních údajů ve státech Evropské unie. Do této chvíle upravovali zpracování osobních údajů zákony vydané jednotlivými státy. V rámci České republiky se jednalo o nepovedený překlad současné směrnice upravující tuto problematiku, díky tomu docházelo k nejasným výkladům (doc. JUDr. Radim Polčák, Ph.D). GDPR dbá na větší práva občanů EU a jim samotným dává do ruky mocný nástroj pro zjištění svých osobních údajů, které jsou o nich zpracovávány. Nařízení je cíleno na velké nadnárodní firmy, aby došlo k jejich motivaci plnění podmínek, byly nastaveny pokuty až ve výši 4 % celosvětového obratu [5].

Práce je zaměřena na implementaci GDPR v malé rodinné firmě nesoucí název antikvarium s.r.o. Můžeme ji však rozdělit do pěti hlavních cílů, kterými jsou:

- definování základních pojmů spojených GDPR jako je správce, zpracovatel, osobní údaj atd.,
- specifikování možností implementace, kde jsou popsány jednotlivé metody pro dosažení cíle,
- vyhodnocení současných podmínek ve firmě, za tímto účelem je zpracována procesní analýza, která rozebírá jednotlivé části procesu a označuje místo procesu, kterého se GDPR dotýká,
- další část navrhuje procesní opatření, které jsou nutné pro splnění podmínek směrnice,
- a jako poslední jsou zhodnoceny dopady na firmu.

Obsahem práce je také právní vymezení směrnice bez, kterého by implementace nebyla možná, je třeba si uvědomit právní tituly zpracování osobních údajů. Drtivá většina osobních údajů zpracovávaných ve firmě je zpracovávána právními tituly za účelem plnění smlouvy, souhlasu a zákonné povinnosti.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY SPOJENÉ S GDPR V MALÉ FIRMĚ

Ochrana osobních údajů pro člověka je v době digitalizace velmi důležitá. Narozením člověk získá údaje, se kterými pracuje celý život, a postupem času si uvědomí, že bez těchto údajů nemůže existovat. Ztráta osobních údajů může člověku způsobit minimálně nepříjemné telefonáty, ale při ztrátě osobních dokladů tento problém může narůst a může se stát, že osoba, která se ztracenými doklady nakládá, může způsobit dotyčnému např. finanční problémy ve formě půjčky u nebankovní instituce, nebo zneužití dokladů v MHD, kdy nálezce jezdí tzv. na „černo“ a při kontrole předloží ztracené doklady [1] [3].

Pro pochopení terminologie v diplomové práci jsou popsané základní pojmy vyskytující se v celé práci.

1.1 Správce a zpracovatel

S pojmem správce a zpracovatel se v zákoně o ochraně osobních údajů setkáme velmi často, proto je zde uveden význam daných pojmů. Správcem je fyzická osoba, právnická osoba nebo orgán veřejné moci, který zpracovává osobní údaje, zatímco zpracovatel zpracovává osobní údaje právě pro správce. Dle zákona o ochraně osobních údajů zpracovatel a správce mezi sebou musí mít uzavřenou smlouvu, pokud zákon neuvádí jinak [4] [5].

Správcem osobních údajů se stává subjekt, v našem případě malá firma nebo e-shop, který sbírá osobní údaje pro své účely či činnost. Jedná se o údaje jako email, jméno, příjmení, adresa atd. Je důležité podotknout, že nařízení jako takové se nevztahuje na domácí uživatele. Správce údajů odpovídá jak za zpracování dat, tak i za ochranu údajů a má povinnost prokázat, že splňuje všechny podmínky pro plnění GDPR [4] [5].

Pokud se budeme zabývat zpracovatelem u malé firmy, zde se může jednat o účetní, která pracuje s nasbíranými daty za daný kalendářní rok, nebo také marketingová firma, ta může dále pracovat s daty správce za účelem cíleného marketingu v podobě rozesílání e-mailů apod. V praxi by to mělo vypadat tak, že správce by měl prověřit daný subjekt předtím, než mu poskytne údaje, a uzavřít s ním smlouvu, ve které by mělo být, že daný subjekt nebude data předávat dál, a přesně dané podmínky pro další nakládání s daty [4] [5].

Můžeme se setkat i se situací, kdy subjekt vykonává obě činnosti najednou, a to když subjekt provozuje e-shop, jenž je sdílený. Ten zpracovává údaje svých klientů, a zároveň se stará o údaje svého partnera, který provozuje činnost na jeho platformě [5].

1.2 Zpracování osobních údajů a jejich druhy

Jedná se o operace, při kterých správce nebo zpracovatel zpracovává osobní údaje, a to buď automatizovanými způsoby, nebo způsoby neautomatizovanými. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání dat na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace [6].

Osobní údaje musíme zpracovávat na základě konkrétního účelu a po dobu nezbytně nutnou. Ty je také doporučeno vhodně zabezpečit pomocí technických či organizačních opatření před možnou ztrátou, zničením nebo zneužitím. GDPR stanovuje zpracování osobních údajů na základě několika právních titulů. těmi jsou:

- právní titul plnění smlouvy,
- zákonná povinnost,
- oprávněný zájem,
- sběr dat pro výkon úřední moci,
- životně důležitý zájem,
- souhlas [7].

Často se v minulosti stávalo, že databáze byly prodávány nebo sdíleny několika subjekty a ty ani nevěděly, jaký právní titul při nakládání s daty používali. Proto jsou v kapitole popsány jednotlivé právní tituly a jejich využití [8].

Mezi právní titul plnění smlouvy můžeme zařadit získávání údajů z e-shopu, kdy požadujeme od zákazníka údaje nutné k doručení zakoupeného předmětu. U zákonné povinnosti, jak nám již pojem napovídá, lze získat údaje pouze tehdy, když jsme povinni takto činit ze zákona. Ve firmě je ze zákona povinnost vést evidenci zaměstnanců a uchovávat smlouvy o výkupu. U oprávněného zájmu se jedná o situaci, kdy osobní zájem převažuje nad případnou újmou někoho, o němž tyto údaje evidujeme. Příkladem může být kamerový systém v objektu, kde máme cenné věci a pohybují se zde zákazníci nebo zaměstnanci. Oprávněný zájem je v tomto případě opodstatněný. Jedná se o zpracování osobních dat za účelem ochránění cenných věcí před ztrátou. Sběr dat pro výkon úřední moci se firmy jako takové netýká, tato možnost získávání údajů se týká jen státních institucí, určenými na základě skutečností definovaných v zákoně. U životně důležitého zájmu je výklad poněkud sporný. Největší shoda panuje nad výkladem, který říká, že údaje

pomocí tohoto právního titulu je možné získat pouze tehdy, když je ohrožen život dané osoby za účelem poskytnutí pomoci [7] [8].

Získávání údajů na základě souhlasu představuje největší problém pro firmu, pokud máme uzavřenou smlouvu se subjektem a nezískáme jeho rodné číslo pomocí zákonné povinnosti a získáme ho souhlasem. může se stát, že zákazník požádá o výmaz rodného čísla a my tak nebudeme schopni identifikovat daný subjekt, který firmě dluží. proto je tento způsob získávání údajů nejméně doporučovaný, jelikož subjekt může tento souhlas kdykoliv odvolat. Souhlas jako takový musí být jednoznačný, konkrétní, projevem svobodné vůle a subjekt musí být informovaný dostatečně o účelu zpracování [8].

Pro naši firmu nás budou zajímat 3 tituly. Souhlas, zákonná povinnost a plnění smlouvy. V případě, že zákazník zakoupí zboží na našem e-shopu, vyplní jméno, příjmení, telefon a doručovací adresu. Jedná se o titul plnění smlouvy. Pokud má zájem o newsletter, zaškrtne pole za účelem zasílání reklamních sdělení. V tomto případě se jedná o titul souhlas. Poslední zmiňovaným titulem je zákonná povinnost. Firma musí ze zákona uchovávat smlouvy o výkupu [7][8].

1.2.1 Citlivý údaj

Citlivý údaj je spojován s osobním údajem, jedná se o kategorii osobního údaje, přičemž diference mezi těmito pojmy je, že citlivý údaj podléhá větší ochraně než osobní. Můžeme zde zařadit rasu nebo etnický původ, náboženství, sexuální orientaci atd. Dle zákona o ochraně osobních údajů správce nebo zpracovatel nemůžou tyto údaje od osoby požadovat [2] [9].

1.2.2 Anonymní údaj

Anonymní údaj můžeme specifikovat jako údaj, podle kterého nemůžeme jasně určit, o jakou osobu se jedná. Údaj jako takový popisuje zákon č. 101/2000 sb., ten ho definuje jako údaj, jenž v původním tvaru, nebo po jeho zpracování nemůže identifikovat danou osobu. V zákoně můžeme najít taky pojem anonymizovat údaj, tzn. z osobních údajů uděláme údaj anonymní, a to buď úplně, abychom nemohli osobu identifikovat, nebo částečně, kde smažeme nebo začerníme údaje identifikující osobu. Právě u částečné anonymizace existuje v zákoně výjimka, a to pro účely statistické nebo vědecké [3] [9].

1.2.3 Identifikační údaj

Jedná se o nejpoužívanější typ osobních údajů. O jaké údaje se jedná, záleží na jistých konvencích nebo na jejich zakotvení v právních předpisech dané země. Můžeme obecně říci, že definují vlastnost nebo charakteristiku, která se rozlišuje u všech lidí patřících do jisté komunity a jejich užívání je formálně podporované. Často právníci říkají, že právě identifikační údaje jsou jediné, které je možné vztahovat k dané osobě [2] [3].

Mezi identifikační údaje řadíme jméno a příjmení, které mohou být do jisté míry ovlivněny samotnou osobou, resp. je ovlivněná rodiči dítěte. Mít a využívat své jméno a příjmení není jen právem, ale i povinností každého subjektu při jakémkoliv jednání s úřady a orgány veřejné moci. Můžeme se také setkat s používáním pseudonymů, které se vztahují na zákon 121/2000 sb. Pseudonym se specifikuje jako projev svobodné vůle jeho nositele [6].

Dalšími důležitými identifikačními údaji jsou datum a místo narození. Vzhledem k tomu, že rodiče často pojmenovávají děti podle sebe, nemůžeme při zpracování údajů jasně určit identitu osoby, proto jsou důležité dodatečné identifikační údaje.

Mezi více chráněné identifikační údaje můžeme zařadit rodné číslo. To je přiřazeno každému občanu při narození a je jedinečné. Jelikož přímo identifikuje danou osobu, je toto číslo chráněné více než ostatní osobní údaje. Zpracování rodného čísla je striktně vymezeno v zákoně 101/2000 sb. To je možno pouze po souhlase občana za podmínky, že je o tom dostatečně informován. Souhlas musí správce předložit při jakékoliv kontrole po celý čas zpracování. Potencionálním problém jsou veřejné registry, kde jsou uvedena data narození jako např. obchodní rejstřík nebo katastr nemovitostí. Jelikož k datům může přistupovat každý, jsou tyto registry hrozbou [1] [6].

Za zmínku stojí i další identifikační údaje, které jasně definují občana. Jsou jimi číslo občanského průkazu, číslo pasu, IČO a ID zaměstnance. Všechny tyto údaje jsou upravené zvláštními zákony [1].

1.2.4 Adresní údaj

Osobní údaje, které nám určují, kde můžeme zastihnout osobu, se nazývají adresní. Mezi ně můžeme zařadit místo trvalého pobytu, který upravuje zákon č. 133/2000 sb. Podobnou funkci plní i údaje o přechodném bydlišti nebo adresa zaměstnavatele. Pod adresní údaje můžeme zařadit i telefonní číslo, fax nebo adresu elektronické pošty, to nám nezaručí, že danou osobu zastihneme kdykoliv potřebujeme, je běžné, že osoba využívá několika adres

elektronické pošty a telefonních čísel. Podstatné je, že tyto údaje identifikují danou osobu a mohou být zneužity [1] [10].

1.2.5 Popisné údaj

Popisné údaje obsahují poměrně široké rozmezí, které se dostává k hranici toho, co je ještě možné považovat za osobní údaje a co mezi ně už nepatří. Dá se zjednodušeně říct, že za osobní údaj lze považovat údaje, které ve spojení s dalšími údaji identifikují danou osobu. Abychom uvedli příklad popisného údaje, můžeme zmínit např. vysokoškolský titul, který při spojení s dalšími údaji může jasně identifikovat osobu, nebo alespoň zmenšit okruh. Jelikož ho chrání zákon 200/1990 sb., který nedovoluje neoprávněně využívat jakýkoliv titul, jež mu nepřísluší. Dalšími popisnými údaji jsou ID zákazníka nebo číslo smlouvy [10].

1.3 Shromažďování

Můžeme obecně říct, že shromažďování, je prvním úkonem, který správce při styku s osobními udělá. Definice shromažďování dle zákona je systematický postup nebo soubor postupů, jehož cílem je získat osobní údaje, za účelem jejich následného uložení na úložiště a připravením pro další krok, kterým je zpracování. Rozdělujeme náhodné a cílené shromažďování údajů, za cílené můžeme považovat databázi zákazníků na e-shopu a za náhodné můžeme považovat, když najdeme ve veřejném prostoru vizitku nebo jakýkoliv jiný osobní údaj [1] [6].

1.4 Časté omyly

Prvním častým omylem, je výmaz údajů na základě všech právních titulů, požadavek na výmaz musí správce nebo zpracovatel provést jen tehdy, pokud zpracovává data nelegálně nebo za základě jediného právního titulu a tím je souhlas, proto je doporučeno získávat údaje jakýkoliv jiným právním titulem, než je souhlas.

Povinnost šifrování u každé organizace je dalším omylem. Organizace, u kterých se data musí šifrovat jsou takové, které systematicky shromažďují velké objemy dat a hrozí u nich potenciální riziko odcizení [10].

Převedení zodpovědnosti na třetí subjekt je dalším omylem. Firmy si myslí, že pokud si nechají implementovat GDPR od někoho zbavují se veškeré odpovědnosti. V zákoně je řečeno, že za GDPR odpovídá správce údajů [10].

Další častou mýlkou je, že každá organizace musí mít svého pověřence. Ten musí být v organizaci, který má více jak 250 zaměstnanců nebo hromadně a systematicky zpracovává údaje svých klientů, zde si můžeme představit organizace jako Google, Facebook, Twitter. Pověřenec může být například ze současných struktur, který projde školením a nemá střet zájmu [10].

2 PRÁVNÍ VYMEZENÍ

Kapitola se zabývá zákonem jako takovým. Abychom pochopili tento zákon je nutné vymezit pojem práva na soukromí. Zde jsou popsány základní pilíře zákona o ochraně osobních údajů.

2.1 Právo na soukromí

Soukromí je vylíčeno v jednotlivých pramenech rozličně. Můžeme ho definovat jako oblast intimního, potažmo osobního života jedince, kde bez jeho odsouhlasení nikdo nemůže vstupovat. Literatury se shodují, že mezi tuto oblast patří jak myšlenkový směr, tak i ten fyzický. Pro představu jde o oblasti jako např. obydlí nebo rodinný život. Co se týče českého právního řádu, je tento pojem vymezen neurčitě a je zvažován u každého případu dle okolností [11].

Pokud mluvíme o soukromí, musíme vzpomenout nejvíce skloňovaný soud s tímto pojmem. Tím je Evropský soud pro lidská práva. Ten jako první rozhodoval o případu týkajícího se práva na soukromí. Konečný verdikt zněl, že „není možné uvést definici soukromí ani taxativní výčet jeho složek“. V dalších případech se zaobíral vymezím obsahu soukromí a verdikt byl, že podstatnou součástí soukromí jsou údaje spojené s osobností jedince jako je pohlaví, sexuální orientace, jméno a příjmení. V dalším případě se zaobíral záležitostí narušení soukromí, kde obžalovaný zveřejnil fotografii bez souhlasu, kterou publikoval v tisku. Této stížnosti bylo vyhověno a bylo to poprvé, co soud uznal podobnou stížnost [11].

První případ, který se řešil u soudu ohledně zveřejnění osobních údajů na Internetu byla kauza Lindqvist, kde Švédka zveřejnila bez souhlasu na webové stránce údaje o osobách, kteří vykonávali dobrovolnickou činnost v její farnosti. Švédský soud uznal její vinu a uložil ji peněžitou pokutu [11].

2.2 Osobní údaje a jejich zpracování

Soukromí je velmi těžké definovat, jak jsme v předchozí kapitole zmínili. Je ale možné říci, že k jeho narušení dochází při každém kontaktu s danou osobou. Informace, které poskytneme osobě, která zpracovává informace o nás jak o naši osobnosti, tak holá data a předává je bez našeho vědomí dál, tak v tomto případě dojde k narušení soukromí. Zde můžeme uplatnit zákon o ochraně osobních údajů jako takový. Ochranu osobních údajů

můžeme tedy specifikovat jako poskytnutí ochrany před zásahy do soukromí jedince, které jsou zapříčiněny shromážděním a později zpracováním dat o dané osobě [12].

Rozlišujeme vztah mezi osobnostními právy a osobními údaji. tímto problémem se zabývá ve své práci Radim Polčák, kde poukazuje na jejich odlišnosti. Říká, že ochrana osobních údajů na rozdíl od osobnostních práv musí být jednoznačně objektivní. Ochranu soukromí jako takovou musíme posuzovat dle osoby. Záleží hlavně na povaze a povolání člověka. Ale v ochraně osobních údajů nemůžeme zohledňovat tyto okolnosti, zde je nezáleží, jaké osobě se zasahovalo do soukromí, vždy to musí být posouzeno dle daného práva [12].

Osobní názor je takový, že při žalobách do zásahu soukromí, bychom měli rozlišovat osobnosti a jejich pracovní pozice. Např. politik musí být smířený s tím předtím, než nastoupí do funkce, jelikož je volený lidmi, kteří mají právo vědět s kým se daná osoba stýká a na koho má kontakty.

Dalším rozdílem mezi osobními právy a osobními údaji je ten, že osobní práva jsou chráněna soukromoprávně, což znamená, že každá osoba si tento zásah do soukromí posuzuje sama a podává žalobu, zatímco osobní údaje jsou chráněny zákonem, a tak můžeme říci, že ochranu těchto údajů necháváme na moci výkonné [12].

2.2.1 Zákon o ochraně osobních údajů

V médiích se můžeme setkat se články vyvolávající strach v lidech mající na starost implementaci GPDR, aby využívali služby advokátních kanceláří a IT firem. Nová práva, o kterých se tak často mluví, jako je právo na výmaz, byla zakotvena i v dosavadním zákoně (Petra Dolejšová).

Doposud platný zákon se opírá o směrnici 95/46/ES. Pro potvrzení výroku Petry Dolejšové můžeme citovat současnou legislativu. Zní následovně: *„Každé osobě musí být umožněno docílit, podle povahy případu, opravu těchto údajů nebo jejich vymazání, jestliže byly zpracovány v rozporu s vnitrostátním právním řádem uplatňujícím základní zásady stanovené v této Úmluvě.“* Tato směrnice umožňuje také člověku získat jeho osobní údaje od subjektu, který ho vede v jeho databázi. Toto se vztahuje na evropskou směrnici. V české úpravě tohoto zákona se píše, že subjekt při zjištění, že správce jakkoliv nakládá s osobními údaji v rozporu se zákonem, může urgovat správce, aby jeho osobní údaje odstranil. Momentální situace je poněkud nepříznivá, i když se může zdát, že je tomu dle zákona jinak. Dnes je tomu tak, že právě správce shledává, jestli jsou údaje zpracovávány dle zákona, či nikoliv. Správce má totiž jednu hlavní povinnost a tou je zpracovat data

s parametry uvedenými v zákoně. Jelikož výklad umožňuje správci dělat právní kličky, je tento zákon nedostatečnou ochranou pro občany [6] [13].

2.2.2 Nový zákon o ochraně osobních údajů

Jedná se o reformu již zmiňované směrnice 95/46/ES. Tato reforma se bude dotýkat všech členů Evropské unie.

Nynější zákon o ochraně osobních údajů nebyl připraven pro tak obrovský rozvoj informačních a vývoje stále nových technologií. Z tohoto důvodu tento zákon ztrácel význam. Následky zastaralého zákona byly např., že data nebyla dostatečně chráněna nebo stále zvyšující se objemy databází s osobními daty, která byla často zneužívaná. Problémem v členských státech EU se stalo to, že každá země si zákon pro ochranu osobních údajů upravovala nejednotně, což zapříčinilo diference ve výkladu, a proto osobní údaje nebyly chráněny v každé zemi EU stejně, což pro firmy působící napříč celoevropským trhem mělo nepříznivý vliv [14].

Nový zákon o ochraně osobních údajů je platný v celém svém znění ve všech státech EU a má za účel sjednotit ochranu osobních údajů. Zde panuje rozpor mezi odborníky, jestli stávající zákon má být přizpůsobený této směrnici nebo nahrazen úplně novým [14].

Hlavním úkolem je, aby správce a zpracovatel nakládali s osobními údaji tak, aby nedocházelo k narušení bezpečnosti nebo zásahu do soukromí občana. Vychází tak ze základního práva EU a také aktů mezinárodního práva týkající se ochrany soukromí [14].

Nařízení jako takové dává větší práva občanům při zpracování a pohybu osobních údajů, a dále také stanovuje nová práva např. právo na výmaz nebo také právo na přenositelnost. Pokud se podíváme z opačného pohledu, tak správcům a zpracovatelům osobních údajů to přinese nepříjemnou zátěž, kde mají povinnost zajistit nejvyšší míru ochrany osobních dat při zpracování. Efektivnost dozoru dle směrnice je zajištěna tak, že úřady k tomuto určené budou muset mít práva pro vykonání této činnosti. Tyto úřady pak budou dohlížet na dodržování povinností, a pokud zjistí pochybení, budou oprávněny pokutovat správce nebo zpracovatele [14].

Nařízení bude mít dopad na všechny osoby, které jakkoliv zpracovávají osobní údaje. Ty můžeme členit na:

- podnikatele, kteří nakládají s osobními údaji zaměstnanců, klientů nebo dodavatelů,
- provozovatele online aplikací,

- orgány veřejné moci,
- neziskové organizace apod.

Důležité podotknout, že nařízení má několik výjimek. Jmenovitě to jsou:

- oblasti působnosti práva EU, kde můžeme zařadit např. národní bezpečnost,
- oblast do jejichž působnosti spadá Hlava V, jedná se o společnou politiku jak zahraniční, tak bezpečnostní,
- oblast zpracování osobních dat pro osobní využití [14].

Hlavní posun oproti staré směrnici je ten, že správce nebo zpracovatel, je povinen dodržovat nařízení i když nemá sídlo v EU. Jedná se o situaci, kdy subjekt nabízí jakékoliv služby nebo jiné věci na unijním trhu, ale spravuje je z jiné části světa. Zde panuje shoda odborníků, že tento článek je napsán nešťastně a bude působit velké problémy. Hlavní kritizovanou chybou je špatně zformulované a velmi široké vymezení působnosti. Proto výklad není jasný a dosti se liší. Zde je velmi diskutovanou otázkou, zda tento článek bude akceptován mimounijními zeměmi bez jakékoliv zahraniční úmluvy [14].

Můžeme obecně říci, že nařízení jako takové dává větší kontrolu a ochranu na stranu občana. Ten je díky tomu více informován, jak je z jeho osobními údaji nakládáno. To je uvedeno v článku 7, kde najdeme „podmínky vyjádření souhlasu“ [14].

Správce nebo zpracovatel jsou povinni umístit podmínky pro zpracování na viditelné místo, kde musí být napsány srozumitelně, a také musí být čitelné, což znamená naformátovaný text a dostatečně velké písmo. Takže se již nemůže stát, že správce umístí tento souhlas mezi obecné ustanovení nebo obchodní podmínky, kde je navíc text psán v jednom odstavci a ještě zmenšeným písmem. Stejně jednoduché jako odsouhlasení zpracování osobních údajů musí být i jejich vymazání z webu. Často kladená otázka je, jestli data budou vymazána ze všech úložišť, které správce vlastní. Dnes již v každé instituci existuje zálohování dat - tzn. když občan požádá o výmaz z vyhledávání, dojde tak pouze v části jejich domén. Z toho vyplývá, že pokud budeme vyhledávat tento obsah v ČR, bude blokovaný, ale v případě přístupu k těmto datům mimo EU, data budou dohledatelná [14] [15].

Pokud se podíváme na web transparecnyreport.google.com, můžeme zde vidět žádosti o zveřejnění osobních údajů a také jejich vyhovění v čase. Statistika je vedena od roku 2011. Také se zde můžeme setkat s odstraněním z vyhledávání na základě evropských předpisů na ochranu soukromí, kde vidíme počet žádostí a jejich členění. Převážné se jedná o výmaz z adresářů, zpravodajských webů nebo sociálních médií [15].

Článek 33 pojednává o oblasti ohlašování narušení bezpečnosti osobních údajů. Tento článek klade nemalé nároky právě na správce a zpracovatele osobních údajů a výslovně počítá s tím, že úložiště, kde jsou údaje uloženy, může být narušeno, a to jak z vnějšku ve formě hackerského útoku, tak i zevnitř ve formě vynesení dat zaměstnancem. proto je správce a zpracovatel nucen vést záznamy o narušení systému kvůli možné kontrole od oprávněného úřadu, který následně zkontroluje, zda je systém dostatečně zabezpečen či nikoliv. Pokud daný úřad zjistí pochybení, správce nebo zpracovatel je povinen tuto chybu do 72 hodin odstranit [14].

V nařízením jsou popsané také částky pro pokuty, které může úřad při pochybení uložit. Rozlišujeme 3 typy porušení:

- správce nebo zpracovatel při porušení této směrnice může dostat pokutu ve výši od 10 mil. € až do 20 mil. €,
- firma při porušení může obdržet pokutu až do výše od 2 % do 4 % celkového ročního obratu,
- nedodržení úkonů od pověřeného úřadu dle článku 58 může organizace obdržet pokutu až 20 mil. € nebo až 4 % celosvětového obratu [14].

3 IMPLEMENTACE GDPR

Implementace GDPR pro malou firmu nemusí být až tak složitým úkonem, jak se může zdát. Je třeba dbát na několik zásadních věcí, jako je splnění informativní povinnosti a ochrany osobních dat. Jedním z mála způsobů ochran dat je jejich zálohování. Zde se již předpokládá, že firmy si cení dat natolik, že svá data v nějaké formě již zálohují. Dalším opatřením, i když ne povinným, na které by se měla firma zaměřit, je šifrování. Dva nejpoužívanější operační systémy v EU, jimiž jsou Windows a Mac OS X, mají v základu nástroje, které tuto funkci podporují. Ztíží se tak nebo úplně zamezí neoprávněnému přístupu k úložišti údajů [10].

Důležitou část zastávají práva pro přístup k údajům. hned před implementací GDPR by měla být vymezena práva pro jednotlivé zaměstnance, k jakým údajům budou mít přístup. Zamezí se tak možnému zneužití údajů, které mohou zaměstnanci z jakéhokoliv důvodu vynést z firmy [10].

Dalším důležitým krokem, který by měla firma podniknout, je stanovit si striktní pravidla pro zpracování dat v případě, že data budeme dále předávat nějakému zpracovateli. Musíme si nastavit, jaká data mu předáme a za jakým účelem. Tyto kroky by měly být uvedeny ve smlouvě mezi správcem a zpracovatelem. Vhodné je taky si vymezit zpracování dat firmou, pro jaký účel data zpracovává, počet osobních údajů, které po uživateli požadujeme, vymezení právního titulu na určitá data a v neposlední řadě dobu zpracování. Pro všechny tyto kroky je vhodné vytvořit směrnici, ve které budou sepsány jednotlivé procesy a přístupy k jednotlivým datům. Usnadní nám to vysvětlování při kontrole oprávněným úřadem [10].

Vhodnou úpravou při zpracování dat je minimalizace požadovaných údajů. Můžeme se tak vyhnout nezákonnému zpracování dat. Platí, že by měla být zpracovávána jen ta data, která jsou relevantní. Předpokládá se, že správce bude zpracovávat jen aktuální data. Směrnice předpokládá, že správce bude aktualizovat data při každém dalším setkání s uživatelem, kterého vede v databázi. Firma by měla mít stanovenou dobu, na jakou bude data zpracovávat. V situaci, kdy si zákazník objedná zboží z e-shopu, je vhodné zpracovávat data na stejnou dobu, jako je např. doba pro reklamaci výrobku [10].

Informativní povinnost je další částí nařízení o GDPR. Říká, co musíme splnit v případě, že nás někdo žádá o informace, které osobní údaje o něm evidujeme. Nejpozději v okamžiku získávání údajů musíme subjekt údajů informovat o tom, jaké data

zpracováváme, v jakém rozsahu, na základě jakého právního titulu a po jakou dobu. Dále musíme informovat osobu o tom, zda data budou dále zpracována a jakým zpracovatelům budou poskytována. Nařízení také hovoří o povinnosti informovat osobu, jaké úkony je oprávněná s údaji provádět. Jedná se o právo na výmaz, pokud jsou data získávána na základě souhlasu. V další řadě je to právo na opravu svých dat a také informování o tom, že subjekt má právo podat námitku, případně stížnost dozorovému orgánu. Informativní povinnost je nutná při jakémkoliv získávání dat jak fyzicky, tak i online [10].

3.1 Možné kroky při implementaci GDPR

V této části budou popsány doporučené kroky pro implementaci GDPR. Jedná se o analýzy, o audity a o obecné postupy pro splnění vymezeného projektu. Samotné kroky je možno využít v malých, středních i velkých firmách.

3.1.1 Vytyčení týmu

Pro implementaci je nutné si stanovit tým, který bude tento úkon provádět, aby byl celý proces efektivní. Tým by se měl skládat ze členů top managementu, kteří jsou hlavní rozhodovací složkou týmu a také z IT specialistů, právníků a důležitých osob ve firmě. Pokud si firma stanoví svého pověřence, měl by být ve složení týmu přítomen taktéž. Při vytyčování týmu by měly být představeny cíle, jednotlivé kroky a stanovit časový harmonogram pro implementaci [16].

3.1.2 Stanovení cílů

Hlavním cílem je splnění jednotlivých kroků, které splňují nařízení 2016/679. Je třeba stanovit jednotlivé procesy tak, aby ve výsledku splňovali požadavky GDPR. Můžeme zde zařadit kroky jako analýzu současného stavu, korekci smluv se zpracovateli osobních údajů, proces implementace GDPR atd. [16].

3.1.3 Rozpočet

Dle současného stavu bychom měli stanovit rozpočet, který je pro implementaci nezbytný. Musíme zde započítat jak přípravu a implementaci, tak i náklady na její následný provoz. V rozpočtu bychom neměli opomenout jednotlivé položky:

- analýzy,
- náklady na implantaci změn,
- školení zaměstnanců,

- konzultace,
- hardware a software,
- náklady spojené s provozem [16].

3.1.4 Časový plán

Konečný termín tohoto časového plánu je poměrně jasný. Jedná se o datum 25. května 2018, kdy vstupuje v planost nařízení. Sestavení časového plánu má obrovskou výhodu, a to takovou, že lidi rádi odkládají nutné věci, které se netýkají jejich výrobního procesu nebo činností firmy na poslední chvíli.

3.1.5 Analýza současného stavu

Analýza současného stavu je důležitá pro zavedení pravidel GDPR. Zjistíme, s jakými údaji vlastně pracujeme, jaký objem dat zpracováváme a jaké právní tituly používáme, jaké dotazníky a údaje v nich požadujeme atd. Analýza nám poskytne nedokonalosti v systému a pomůže nám zjistit, jaké změny musíme zavést, aby bylo v souladu s nařízením.

3.1.6 Audit údajů

Účelem auditu osobních údajů je najít všechny parametry, které jsou jakkoliv spojeny se zpracováním. Zjistíme celý proces nakládání s osobními údaji od jejich shromažďování až po zaměstnance, kteří k nim mají přístup, popř. práva zaměstnanců přístupu k jednotlivým databázím až po zpracovatele. Pokud chceme zjistit celý proces údajů, musíme se ptát na základní otázky:

- **Proč?** U této otázky se ptáme na účel, pro který data od subjektů zpracováváme. U naší firmy je zpracování údajů za účelem doručení objednávky, propagace firmy, uzavření smluv.
- **O kom?** Cílem je zjistit, o kom údaje získáváme. Jasně určíme subjekt, který je oprávněn požádat o výmaz a úpravu údajů.
- **Co?** Zjistíme, jaký typ osobních údajů zpracováváme, jejich zdroj a právní titul, který využíváme pro jejich získávání.
- **Kdy?** Jedná se o určení času, kdy byla data získána, kdy byla provedena jejich aktualizace a dobu uchování.
- **Jak?** Nutno je také zjistit, jak se údaje ukládají, zpracovávají a shromažďují. Zjistíme, jaký SW a HW se pro zpracování používá a postup.

- **Kdo?** Zde vymezíme, kdo je odpovědný za zpracování údajů a kdo odpovídá za jejich aktuálnost a kvalitu, a dále kdo bude mít přístup k údajům.
- **Kde?** Jedná se o všechny aplikace, služby, software zpracovávající osobní údaje [16].

3.2 Procesní analýza

V procesní analýze se věnujeme jednotlivým procesům, v jejichž rámci se osobní údaje zpracovávají. Hlavním úkolem je vyznačit jednotlivé činnosti a vyobrazit současný stav zpracování údajů. Můžeme zde zmínit předávání údajů od správce ke zpracovateli.

3.3 Revize dotazníků, smluv, formulářů

Důležité je minimalizovat údaje v dotaznících, smlouvách a formulářích a také upravit právní tituly tak, aby byl souhlas co nejméně obsažen. Údaje v databázi zpracované před implementací GDPR, je nutné prověřit, zda splňují toto nařízení. Pro ujištění se, že právní tituly jsou oprávněné, je třeba využít právní konzultace [10].

3.4 Analýza rizik

Jedná se o jednu z nejdůležitějších částí, kde zjistíme případné chyby a zranitelnosti v systému. Zde je důležité, abychom se vyhnuli případným:

- ztrátám osobních údajů,
- pokutám,
- rizikům, která plynou z občansko – právních sporů,
- ztráty důvěry zákazníků při úniku údajů,
- pracovně – právním sporům.

Výstup z analýzy použijeme pro posouzení jednotlivých činností pro zabezpečení údajů a také je lze využít i pro diskuzi, jestli opatření nejsou moc drahá na to, jaká je pravděpodobnost těchto rizik [10].

3.5 Analýza bezpečnosti informací a zabezpečení údajů

V analýze je nutné se zaměřit na systémy, které jsou ve firmě již použity, a zda je jejich dosavadní zabezpečení dostačující nebo je nutné provést změny pro to, aby splňovaly všechny kritéria pro GDPR.

3.6 Audit dopadů na firmu

Nařízení jako takové mění podmínky pro zpracování údajů. Z toho důvodu se změní procesy a přibude více úkonů, a také další náklady spojené s GDPR. Pro změny v GDPR je bezpochybně potřeba právní konzultace nebo náklady spojené s údržbou systému [16].

3.7 Právní audit

Audit má zjistit, do jaké míry splňuje daná firma požadavky na směrnici. To znamená, že je třeba spolupráce jak IT specialistů, tak i právníků, kteří provedou analýzu nynějšího stavu a porovnají je s požadavky na směrnici. V našem případě se jedná např. o firemní postupy, nakládání s dokumenty, požadavky od klientů na výmaz, na úpravu a aktualizaci údajů. Ve směrnici je popsáno, že texty, které zákazník čte předtím, než odsouhlasí zpracování, musí být srozumitelné a naformátované tak, aby byly jasně čitelné a neschovávali důležité stanovení v podobě malého písma nebo písma na nečitelném pozadí [16].

Je třeba prověřit, zda jsou všechny již zpracované údaje v souladu se směrnicí a pokud se zjistí pochybení, musí být souhlas o zpracování zaslán subjektu co nejdříve. Např. když jakákoliv smlouva mezi subjektem a správcem údajů bude znovu obnovena a byl ve smlouvě včleněn souhlas, který je v rozporu s GDPR, musí být takové smlouvy předělány a znovu uzavřeny [16].

V případě dalšího předávání dat jiné instituci je třeba dbát na smlouvy mezi správcem a zpracovatelem. Ty by měly jasně definovat, za jakých podmínek může zpracovatel s daty nakládat a s jakými daty může operovat [16].

3.8 Návrh možných řešení

V předchozích krocích bylo zpracováno všechno, co potřebujeme pro návrh na implementaci. Z analýz a auditů musíme vyčlenit nedostatky a využít je pro zpracování výsledného návrhu. Je nutno spojit nedostatky z právního auditu, tak i z toho bezpečnostního [16].

3.9 Vliv požadavků směrnice na jednotlivé procesy

Zpracované podněty a data o současném stavu nám pomohou posoudit vliv nařízení na jednotlivé procesy. Pro zjištění vlivu na jednotlivé procesy budeme postupovat následovně:

Monitorování systému – vyhodnocení stávajícího systému, kde musíme chápat jak jednotlivé cykly, vlastnosti a činnosti fungují.

Zpracování nároků – určení důležitých cílů potřebných pro zavedení nových či pokrokových systémů.

Komparace – obsahuje komparaci vlastností a atributů současných a budoucích procesů.

Dopady – tady jsou popsána rizika, která jsou v souvislosti s vývojem nového procesu.

Rekomendace – feedback je důležitý pro neustálé zlepšování systému [16].

3.10 Vliv požadavků směrnice na informační technologické systémy

Hlavní předpokladem zpracování této analýzy je zjistit, jak jsou současné systémy připraveny splnit požadavky směrnice. Důležitým bodem, na který bychom se měli zaměřit v této analýze, je bezpečnost údajů a nakládání s nimi. K údajům by měli mít přístup jen osoby, které pro vykonávání své práce nutně tyto údaje potřebují, a také by měly být zaznamenány veškeré operace. Zaměřit bychom se měli také na procesy, které jsou nutné pro splnění podmínek GDPR jako smazaní, aktualizaci a optimalizaci údajů [16].

3.11 Procesy nutné pro zavedení nařízení

Nařízení staví správce před relativně složitou úlohu. Je třeba splnit několik úkonů proto, aby byl systém v souladu s GDPR. Jednotlivé kroky, které musí správce splnit, jsou podrobně rozebrány níže.

Logy o zpracování – Při manipulaci s údaji musí být všechny kroky zaznamenány a řádně uloženy. Tyto logy se musí zpracovávat za dvou podmínek. Jedna z nich je, že firma musí mít minimálně 250 zaměstnanců nebo s údaji pracuje jen příležitostně.

Právo občana na informace – Každý občan má právo na informace, které o něm kdokoliv zpracovává. Tyto informace musí být poskytnuty každému na požádání. občan má právo vědět, jaké informace jsou o něm zpracovávány, dle jakého právního titulu a pro jaký účel.

Smazaní údajů – V případě, že zpracováváme data, kde vyžadujeme souhlas, musíme počítat s tím, že subjekt může kdykoliv požádat o jeho výmaz. proto musíme zakompono-

vat do systému proces, který nám umožní tato data smazat. Povinností je také sdělit subjektu délku zpracování dat a v případě, že tuto dobu nemáme stanovenou, měli bychom mít stavena pravidla pro určení doby zpracování. Za předpokladu, že jsou údaje uloženy na více místech, je povinností správce oznámit, v jakých databázích se data nacházejí.

Optimalizace při zpracování – Správce musí zpracovávat jen data, která využije. pokud tak neučiní a dostatečně neobhájí jejich využití, může být pokutován. Subjekt jako takový má právo na částečný výmaz údajů. Týká se to jen těch údajů, o kterých si myslí, že jsou správci nadbytečná nebo nechce, aby je někdo zpracovával.

Právo na námitku – Každý občan má právo na to vznést námitku. Správce je potom povinen ověřit, jestli data zpracovává v souladu se všemi zákony a toto ověření je povinen předat subjektu nebo úřadu. Tato činnost je spíše vzácná, ale je třeba s ní počítat. Nejvíce udání na nesprávnost při zpracování osobních údajů podávají bývalý zaměstnanci firmy.

Právo na aktualizaci – Právo na aktualizaci nebo také na opravení musí správce osobních údajů na požádání provést. Každá firma by měla mít nástroje pro ověření těchto aktualizovaných údajů. Ideálně by tyto postupy měly být popsány v procesech nakládání s daty.

Právo na přemístitelnost – Správce musí být schopen předat údaje jinému správci a také musí mít takový systém, který umí předat údaje v čitelné podobě. Zde můžeme převádět např. údaje o zaměstnancích [18].

3.12 Výběr DPO

DPO neboli pověřenec není nutný pro každou firmu, jen pro ty, kteří mají více jak 250 zaměstnanců. DPO musí splňovat několik podmínek pro vykonávání této činnosti, jsou to např. vzdělání oblasti právní, IT bezpečnosti a také tato osoba nemůže být ve střetu zájmů. Jeho hlavní činností je poskytnout podporu a odpovědnost při zpracování údajů, také by měl být jakýmsi spojením mezi IT specialisti a nejvyšším vedením. Měl by být také přítomen od začátku implantace GDPR nebo mu poskytnout takové materiály, aby měl přehled o všech procesech spojených s tímto nařízením. Předpokládá se, že počet odborníků bude nedostatečný, proto je vhodné zvolit služby v rámci externí firmy [17].

3.13 Implementace a následné udržování

Předešlé zpracované analýzy nám pomohou při implementaci GDPR. Ta bude zahrnovat změnu procesů, jejich možné doplnění, možnou modernizaci hardwaru, nebo implementaci nového softwaru, korekci stávajících procesů a zabezpečení dat.

Pokud si firma neudělá implementaci sama a nechá celý proces implementace na externí firmě, je důležité, aby měla všechny smlouvy spojené s poskytováním této služby v pořádku, (hlavně mezi správcem a zpracovatelem) a aby tyto smlouvy mohla kdykoliv předložit při případné kontrole [18].

Vize tvůrců nařízení je taková, že data budou zabezpečena již při prvním shromažďování a co nejdříve minimalizována a anonymizována tak, aby při dalším sběru dat nebylo nutné identifikovat danou osobu [18].

Po úspěšné plnění GDPR je nutné udržovat kroky jako vyřizování stížností a žádostí od subjektů, je možné zavést buď automatizované řešení, nebo vytyčit si osobu, která bude tuto činnost vykonávat.

Každé přidaní funkce, která zpracovává osobní data, musí být vyhodnoceno a pokud bude využívat souhlasu, musí zde být doplněn odkaz nebo text na podmínky. Při zasílání reklamních sdělení bychom měli dodržovat podmínky, které nám GDPR stanovuje, a to posílat jenom lidem, kteří dají souhlas pro tuto činnost nebo firma má uzavřenou smlouvu s příjemcem tohoto obsahu [18].

GDPR předpokládá, že každý, kdo jakkoliv pracuje s osobními údaji ve firmě, bude řádné vyškolen a také, že se bude v této oblasti neustále vzdělávat. Na paměti bychom měli mít, že firma při jakémkoliv úniku údajů musí tuto skutečnost oznámit příslušenému úřadu nebo dotčené osobě, a to do 3 dní [18].

3.14 Pojištění

Z toho důvodu, že pokuty spojené s nedodržováním GDPR mohou být pro firmu likvidační, je vhodné se proti tomuto riziku pojistit. Jak obecně platí, tak i pro toto pojištění musí splňovat firma podmínky dané pojišťovnou. Firma nebude pojištěna nebo odškodněna, pokud nebude dodržovat základní podmínky. Proto se zde nedoporučuje balancovat na hraně zákona. V tomto případě se pojišťujeme proti kybernetickým hrozbám a proti chybě lidského faktoru [19].

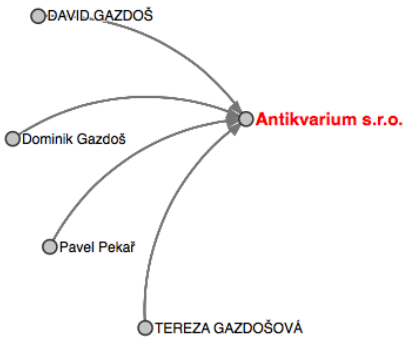
3.15 Závěrečné shrnutí

Ze zpracovaných dokumentů si ověříme, zda je systém funkční i v praxi. Testování je vhodné provádět několikrát, abychom se ujistili, že všechny procesy správně fungují. Hlavním úkolem je srovnat, co bylo splněno a co ještě musí být doladěno nebo přidáno.

II. PRAKTICKÁ ČÁST

4 ANALÝZA SOUČASNÉHO STAVU FIRMY

Pro diplomovou práci byla vybrána firma zabývající se výkupem a prodejem knih a starožitných předmětů. Jedná se o rychle rozrůstající rodinnou firmu založenou v roce 2016. Firmu tvoří 4 spoluvlastníci, a také několik brigádníků, kteří jsou povolávání dle potřeby.



Obr. 1. Struktura firmy [20]

Disponují celkově 5 webovými stránkami, jednotlivě to jsou:

- antikvarium.cz,
- antikvariat-palmovka.cz,
- ptolemaia.cz,
- ptolemaia.sk,
- ptolemaia.pl.

Hlavní kostru tvoří web antikvarium.cz, který slouží jako e-shop, antivariat-palmovka.cz je informačním webem pro zákazníky. Jedná se o značku, jenž je vlastněna firmou Antikvarium s.r.o. od jejího zakoupení v roce 2017. Weby Ptolemaia.cz/sk/pl slouží jako vyhledávače starých předmětů. Prozatím se jedná o demo verzi.

Firma původem ze Zlína disponuje 3 výdejními místy, a to v Praze 8, Brně a Zlíně, které slouží mimo výdej také pro osobní prohlídku předmětů. Za dva roky se firma rozrostla o 2 výdejní místa a sklad v Praze 8. Zásadní filozofií je dělat věci jinak než ostatní konkurenti v oboru, proto firma vyvíjí svůj vlastní algoritmus pro oceňování starožitných věcí a cílí s ním na zahraniční trh.

4.1 Identifikace a analýza základních procesů

Abychom zjistili místa implementace GDPR, je nutné vytvořit analýzu procesů a zjistit, v jaké části procesu je potřeba osobní údaje zpracovávat a jestli firma takové údaje skutečně potřebuje pro své fungování, a jako poslední jasně určit právní tituly, podle kterých údaje budou zpracovávány.

Nejprve před samotnou analýzou definujeme vnější reakce a události. Tyto reakce nám určí, jak se firma chová mimo firemní zázemí.

Události samotné se tvoří mimo firemní zázemí a mají dopad na vnitřní procesy ve firmě. Taková je definice základních procesů ve firmě, bez kterých firma nemůže existovat. Ta byla popsána panem prof. Ing. Václavem Řepou, CSc., který mimo jiné vytvořil novou metodiku modelování a analýzu podnikových procesů. Metodika má určit procesy ve firmě a následně z nich udělat komplexní model. Ten pak usnadní představu o tom, jak firma funguje a potom lze jednodušeji optimalizovat procesy ve firmě [24].

Tab. 1. Události a reakce

Události	Reakce
Objednání knihy nebo starožitných předmetů	předání zásilky přeprvaci a následné doručení
Nabídka knih nebo starožitných předmetů	výkup od zákazníků
Vykoupení zboží od zákazníků	Nabídka vykoupeného zboží konečním zákazníkům
Zákazníci požaduící osobní prohlídku předmětů	Osobní schůzka v jedné z výdejen

Tabulka 1 zobrazuje události a následné reakce na ně. Za hlavní proces ve firmě je jednoznačně považována poptávka po předmětech a jejich následné objednání. Ta vyvolá reakci v podobě předání zásilky přepravci, který doručí zásilku na požadované místo. Celý proces způsobí uspokojení zákaznické potřeby. Pokud má zákazník zájem o osobní prohlídku, může si po domluvě zboží prohlédnout a rozhodnout se, zda si předmět zakoupí. V případě neuspokojení potřeby, může zákazník zboží do 14 dnů vrátit. Celý proces by nemohl proběhnout, pokud by firma nezískala knihy, které byly vykoupeny od zákazníků. Ty jsou následně uloženy na sklad ve městě, kde výkup probíhal.

V následující části je provedena analýza základních procesů, ve kterých jsou definovány základní řetězce činností ve firmě. Je důležité připomenout, že identifikace a analýza základních procesů neslouží pouze pro identifikování chyb, ale při analyzování si firma může uvědomit zásadní nedostatky v procesech a tím pádem mohou vzniknout procesy nové. Tento poznatek je důležitý pro samotnou implementaci GDPR [24].

Analyzováním procesů na základě událostí a reakcí popsaných v tabulce 1, určíme následné základní řetězce činností:

- výkup knih a starožitných předmětů,
- skladování předmětů,
- prodej předmětů,
- péče o koncového zákazníka.

4.1.1 Analýza procesu: Výkup knih a starožitných předmětů

Charakteristika: Proces při, kterém firma získává předměty k prodeji na trhu. Z drtivé části se jedná o zákazníky, kteří kontaktují firmu na základě vyhledání antikvariátu přes vyhledávače nebo již s firmou do styku přišli. Dalším krokem je smlouvání o ceně a uzavření smlouvy se zákazníkem.

Událost: Nabídka předmětů od zákazníků.

Reakce: Výkup předmětů.

Akce: Vyjednávání o ceně, určení cenných předmětů, ohodnocení předmětů, poptávka po předmětech, průzkum trhu, uzavření smlouvy.

Zúčastněné osoby: Zákazník, znalec.

Vstupy: Získání zákazníků.

Výstupy: Vykoupené předměty.

Rozhodující vliv: Nedostatek zákazníků.

Zpracování údajů: Zpracování údajů probíhá při uzavření výkupní smlouvy.

4.1.2 Analýza procesu: Skladování předmětů

Charakteristika: Proces začíná v okamžiku odkoupení předmětů od zákazníka. Předměty se označí, ocení, založí se do regálů a roztřídí se dle předem daných podmínek. Následně jsou vystaveny na e-shopu.

Událost: Naskladnění předmětů po výkupu.

Reakce: Vystavení předmětů na e-shopu => nabídnutí zákazníkům.

Akce: Roztřídění předmětů do regálů, přijmutí předmětů z výkupu, nafocení, popsání předmětů pro e-shop, předání zboží přepravci, ocenění předmětu.

Zúčastněné osoby: Znalec, copywrighter, zákazník od, kterého vykupujeme, sklad (výdejní místo) – brigádníci, systém pro focení předmětů – brigádnici, e-shop – brigádníci/jednatelé.

Vstupy: Vykoupené předměty.

Výstupy: Naskladněné předměty, vystavené předměty na e-shopu.

Rozhodující vliv: Kvalita nafocení předmětu, rychlost předání přepravci, kvalita předmětů.

Zpracování údajů: Brigádníci potažmo jednatelé na skladě mají přístup k osobním údajům skrze interní systém.

4.1.3 Analýza procesu: Prodej předmětů

Charakteristika: Proces začíná, když zákazník navštíví e-shop, vloží do košíku vybrané předměty a potvrdí objednávku. Následně probíhá zpracování objednávky ve skladu, kde se zboží nejprve vyhledá, a pak je zabaleno. Po zabalení se zboží předá přepravci. Pokud si zákazník vyžádá osobní prohlídku předmětu, je zaslán na jednu z výdejen, kde se zákazník rozhodne, jestli předmět zakoupí či nikoliv.

Událost: Objednávka předmětu.

Reakce: Předání zboží přepravci a následné doručení zákazníkovi.

Akce: Nalezení předmětu ve skladu, zabalení předmětu, předání přepravci, prohlídka předmětu na výdejním místě.

Zúčastněné osoby: Sklad – brigádníci, zákazník, dopravci, zaměstnanci na výdejně.

Vstupy: Vytvoření objednávky zákazníkem.

Výstupy: Doručení předmětu objednávajícímu.

Rozhodující vliv: Označení předmětu pro jeho rychlé nalezení, vhodné zabalení předmětu, spolehlivost/cena dopravce, přítomnost zboží na výdejně.

Zpracování údajů: Firma zpracovává osobní údaje zákazníků při převzetí objednávky, následně s nimi pracují brigádníci při balení a předání dopravci.

4.1.4 Analýza procesu: Inovace

Charakteristika: Trh jako takový se neustále mění a firma musí hledat inovativní řešení tak, aby byla vždy o krok před konkurencí. Proto vyvíjí srovnávač a vyhledávač se starožitnými předměty. Dále pracuje s nástroji analyzujícími chování uživatelů na webu

a s těmito daty dále nakládá.

Událost: Zákazník vyhledává snadnější a příjemnější místo pro nákup.

Reakce: Inovativní prodej.

Akce: Nalezení potřeb, testování a následné zavedení inovací.

Zúčastněné osoby: Zákazník, programátor a vedení firmy.

Vstupy: Rozpoznaná potřeba, sběr dat pro podrobnou analýzu, inspirování se u konkurence nebo jiných odvětvích.

Výstupy: Myšlenky, inovace, satisfakce zákazníků.

Rozhodující vliv: Nevyhovující inovace pro zákazníka, reakce na konkurenci.

Zpracování údajů: Při hledání inovací se pracuje s daty, které poskytují nástroje třetích stran (jedná se pouze o data sledující chování zákazníků na e-shopu, pro vylepšení struktury).

4.2 Identifikace procesů

V celé firmě bylo identifikováno 11 procesů, z toho na 9 z nich bude mít GDPR dopad. V procesech identifikovaných v rámci e-shopu a webových stránek se pracuje s osobními daty jako jméno, příjmení, doručovací adresa, email, telefonní číslo a cookies, které jsou podstatné pro propagaci dané firmy. Dále budeme pracovat jen s procesy, kterých se nařízení týká.

Tab. 2. Identifikované procesy

Název	Popis	Dopad GDPR
Prodej předmětů	Hlavní proces je reakcí na zákazníkovu potřebu, proces začíná za ujmutím zákazníka a končí předáním předmětu přepravci, který ho doručí.	ANO
Inovace	Vyhodnocování dat, které jsou zpracovávány třetími stranami, jedná se o zpracování za účelem vylepšení funkčnosti e-shopu.	ANO

Propagace	Zpracování dat na základě propagace firmy, jedná se o newslettery, reklamní služby adwords a sklik.	ANO
Informační technologie	Proces zahrnující komplexní správu software a hardware ve firmě.	ANO
Nabídka předmětů	Proces zahrnuje péči o e-shop, nabídku samotného zboží až po samotnou tvorbu objednávky.	ANO
Customer care	Proces, který zahrnuje zodpovídání dotazů zákazníka až po vrácení zboží.	ANO
Výdejna	Proces předávání předmětů zákazníkovi nebo vrácení zboží.	ANO
Finance (účetnictví)	Proces, při kterém spravujeme finanční prostředky společnosti.	NE
Výkup předmětů	Proces získávání předmětů pro další prodej.	ANO
Skladování	Naskladňování vykoupených předmětů.	NE
Lidské zdroje	Hledání nových zaměstnanců.	ANO

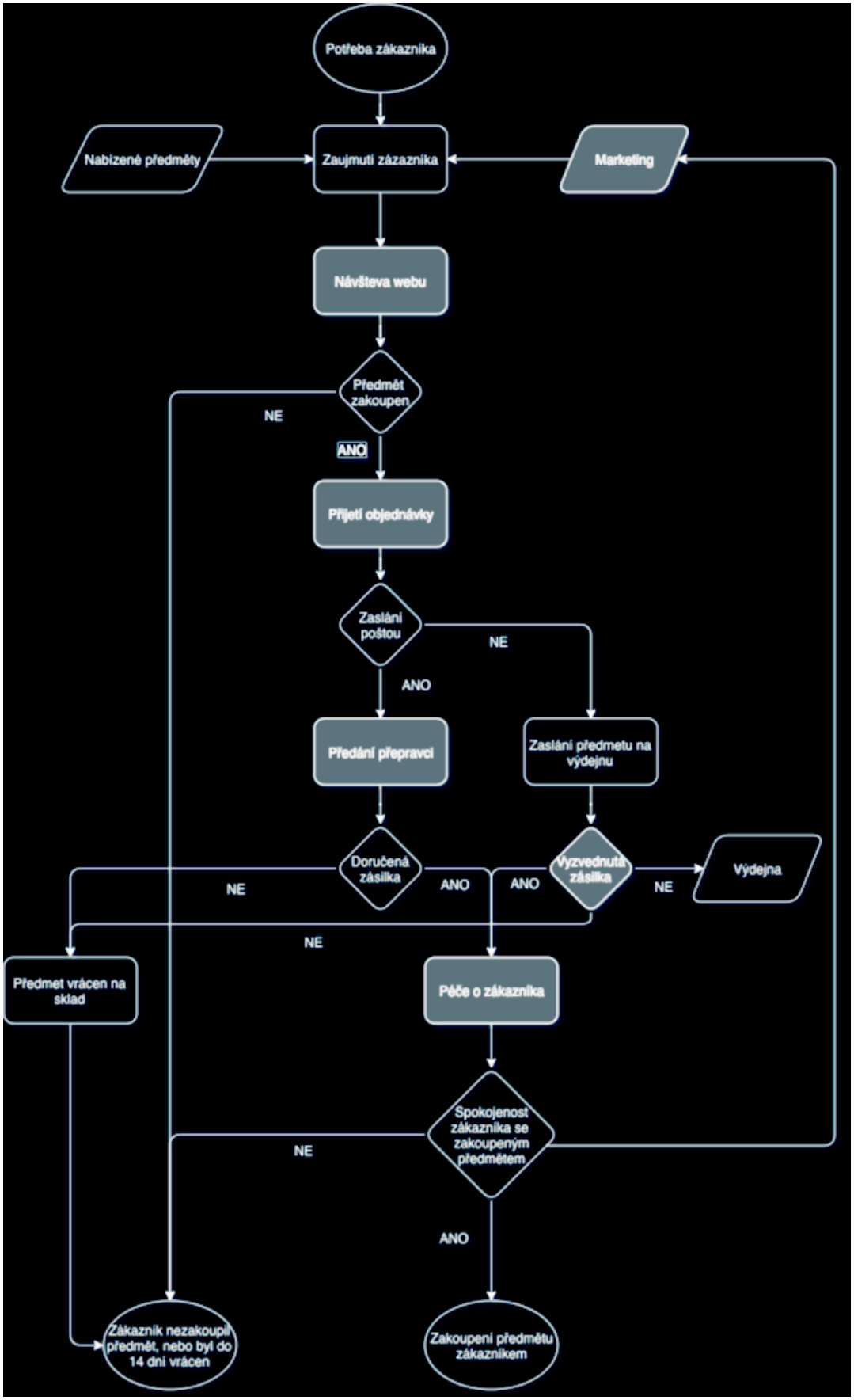
5 PROCESNÍ ANALÝZA

V kapitole jsou podrobně popsány procesy identifikované v předchozí části. Pro lepší identifikaci části procesů, jež se GDPR dotkne, jsou procesy zobrazeny vývojovými diagramy. Tento krok je potřebný kvůli tomu, aby bylo zjištěno, kde je potřeba implementovat GDPR. Zobrazení procesů vývojovými diagramy pomůže vytvořit lepší představu o fungování procesů a díky tomu mohou být odstraněny nedostatky, které mohou přispět k lepšímu fungování firmy.

5.1 Prodej předmětu

Celý proces začíná zákazníkovou potřebou, který si vybral e-shop na základě nabízeného zboží. Jelikož se firma soustředí na předměty exklusivní, vyskytující se v konkurenčních antikvariátech jen zřídka, má firma před konkurencí díky tomuto kroku výhodu. Z toho vyplývá, že při hledání vzácnějších předmětů zákazníkem je velká pravděpodobnost, že navštíví právě e-shop antikvarium.cz. Další možností, jak zaujmout zákazníka, je marketing firmy, který je soustředěný z drtivé části na online prostřední.

Poté, co se zákazník rozhodne předmět zakoupit, vytvoří tím viditelný impuls pro firmu. Vytvořením objednávky se v systému objeví upozornění v podobě nevyřízené objednávky. V tomto momentě přebírají iniciativu zaměstnanci na skladě, kteří předmět nejprve vyhledají v označených krabicích, následně ho zabalí, označí a předají dopravci, nebo je zaslán za poplatek na výdejnu. Pokud přepravce úspěšně doručí předmět, nastane proces péče o zákazníka, který následně řeší spokojenost zákazníka s předměty. V případě, že se zákazník rozhodne zboží vrátit do 14 dní, zboží putuje na sklad. V momentě, kdy se zákazník rozhodne předmět ponechat a nemá důvod pro odstoupení z kupní smlouvy, může firma zpracovat osobní údaje určené pro marketing firmy. Zpracováván je pouze e-mail pro emailing. Na e-mailové adresy mohou být zasílány jen reklamní sdělení týkající se zakoupených předmětů. Obsahem e-mailu nemůže být reklama na starožitná křesla, když zákazník zakoupil knihu (Mgr. Petra Dolejšová).



Obr. 2. Procesní analýza - prodej předmětu [Vlastní zdroj]

5.1.1 Procesy dotčené GDPR

Procesy dotčené GDPR jsou procesy vyznačené v diagramu šedou barvou. Na začátku zákazník předá osobní údaje v podobě objednávky, jím vybraným předmětem. S těmito údaji se pak dále pracuje. Jako první, kdo s údaji pracuje, jsou pracovníci ve skladě, kteří předmět zabalí a označí. Potom ho předají na expedici k přepravci. V tomto okamžiku vstupuje do procesu zpracovatel dat, se kterým musí být uzavřena zpracovatelská smlouva. Zabalený a předaný předmět putuje přímo k zákazníkovi nebo na výdejnu, kde je pracováno s osobními daty při výdeji objednávky. Péče o zákazníka je spojena s komunikací se zákazníkem, kde jsou využity jeho údaje, které vstoupily do procesu na začátku, kdy zákazník objednal předmět. S těmito daty je nakládáno v oblasti marketingu firmy, kde jsou data využita pro vytvoření potřeby zákazníka.

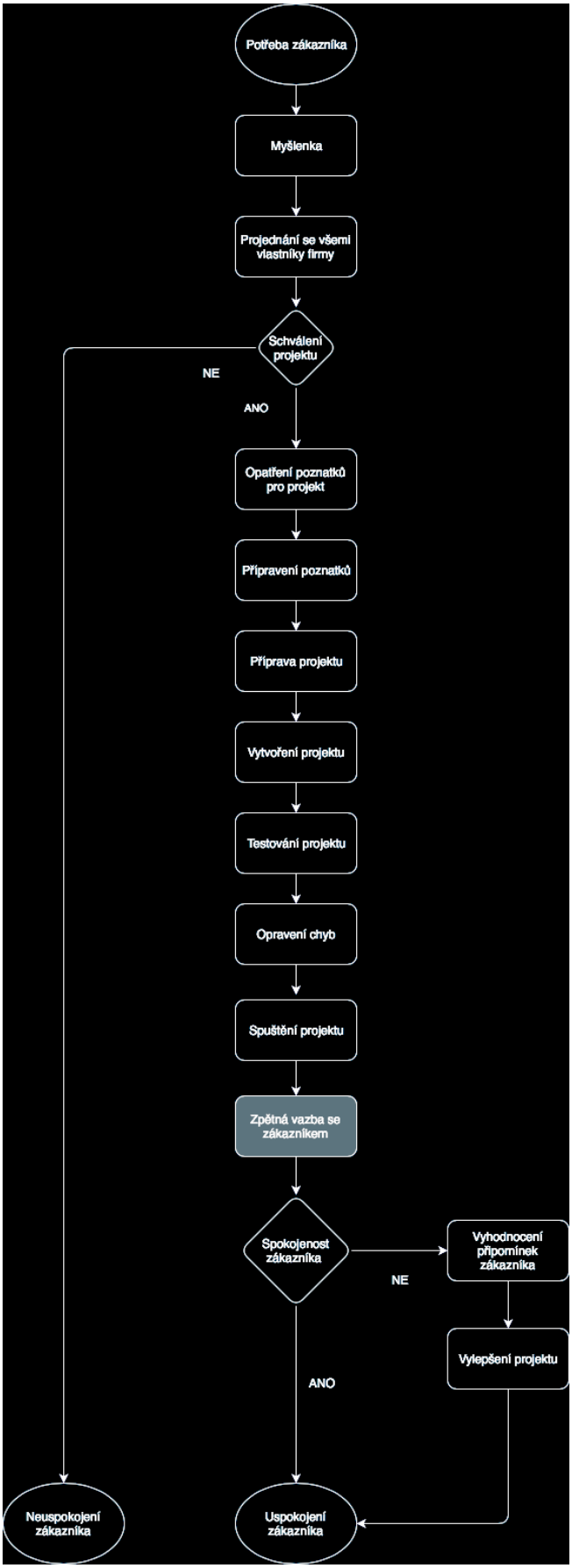
Všechny tyto procesy budou rozebrány a diskutovány v další části této práce.

5.2 Inovace

Proces inovace uspokojuje potřebu zákazníka. Jedná se především o zlepšování prostředí pro nákup. Zde můžeme zahrnout např. změnu uživatelského prostředí, přidání možností pro platbu, vytvoření objednávky co nejrychleji a na co nejmenší množství kliků, zrychlení vystavování předmětů atd. Firma samotná se snaží co nejvíce jít inovaci naproti. Důkazem toho je jejich projekt Ptolemaia.cz, který pro nich slouží jako ohodnocovač předmětů a pro zákazníky slouží jako vyhledávací nástroj pro hledání starožitných předmětů nebo knih. Další inovací z jejich dílny je fotokabina, která umožňuje co nejrychlejší přidání předmětů na e-shop. Firma se snaží proces co nejvíce zautomatizovat tak, aby mohla omezit lidské zdroje a čas a ušetřené prostředky vynaložit na další rozvoj.

Proces je popsán obecně, jelikož každá inovace je specifická, a proto není proces zformulován do úplného detailu.

V případě, že se jedná o vylepšení struktury webu, jsou zákazníci dotazováni anketou umístěnou na webu a analyzují se data zpracovávané službou smartlook.cz pro vyhodnocení zavedené funkce. Služba monitoruje pouze chování návštěvníka webu a nezpracovává žádná osobní data.



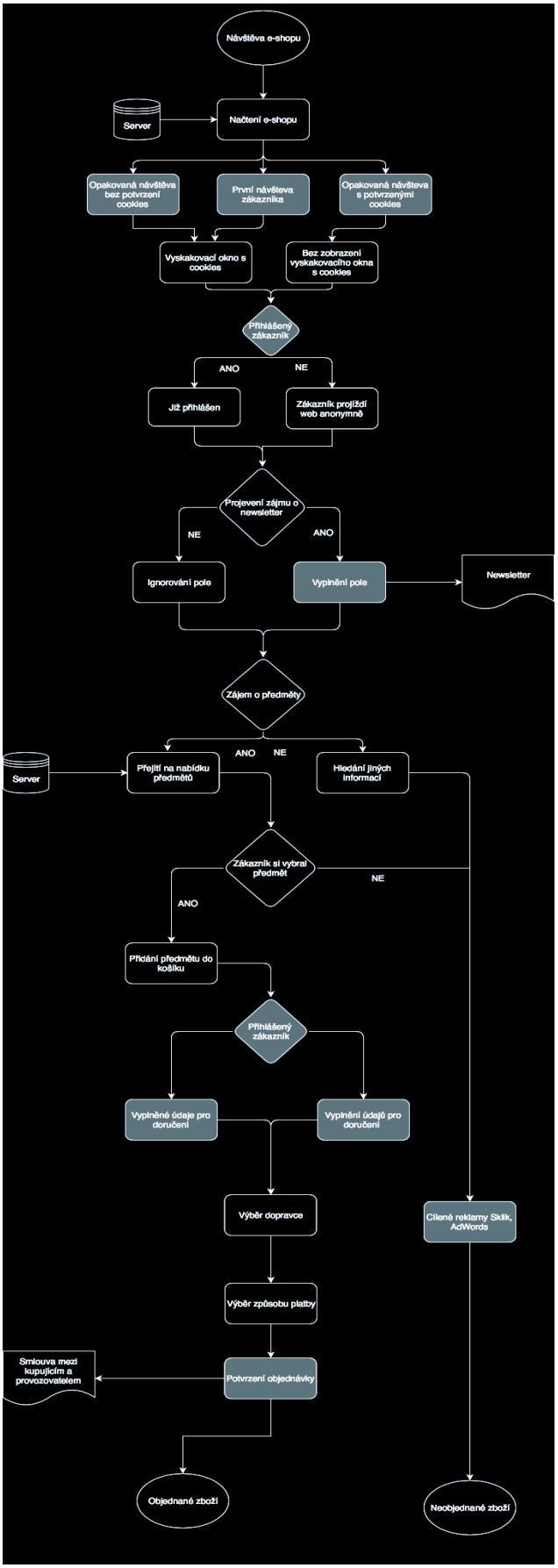
Obr. 3. Procesní analýza - inovace [Vlastní zdroj]

Samotný proces začíná tím, že zjistíme potřebu zákazníka. Reakcí na to je myšlenka, která by mohla daný problém vyřešit. Ta je prodiskutována s ostatními vlastníky firmy, a pokud je úspěšné schválená, přejde do procesu příprav, kde se nejprve zjistíme, jak daný problém řešit, a na základě těchto poznatků si připravíme věci potřebné pro samotnou realizaci. Po realizaci je projekt testován a na základě zjištěných chyb je postupně zlepšován. Po úspěšném testování je projekt spuštěn a zákazník je dotazován ve formě anket na případné nedostatky. Pokud jsou nějaké zjištěny, jsou přehodnoceny, jsou-li relevantní a následně je projekt vylepšován do stavu, kdy uspokojí zákazníka.

5.3 Nabídka předmětů

Proces nabídka předmětů je svázaný s procesem prodej předmětů. Je zahájen tím, že zákazník navštíví e-shop. V této chvíli se začíná pracovat s osobními daty zákazníka. Po načtení stránky ze serveru, na zákazníka, který nikdy nepotvrdil cookies nebo je na stránce poprvé, vyskočí vrchní lišta s informacemi o cookies. Dle nařízení by měl zákazník pokračovat v prohlížení e-shopu bez toho, aniž by o něm byla sbírána jakékoliv data, i když by s cookies nesouhlasil. Tento krok je ovšem technicky náročný, proto Evropská komise připravila návrh, který tuto odpovědnost přenáší na prohlížeče. V jejich nastavení by pak mělo být, na kterých stránkách budou cookies povoleny a na kterých budou striktně zakázány [5].

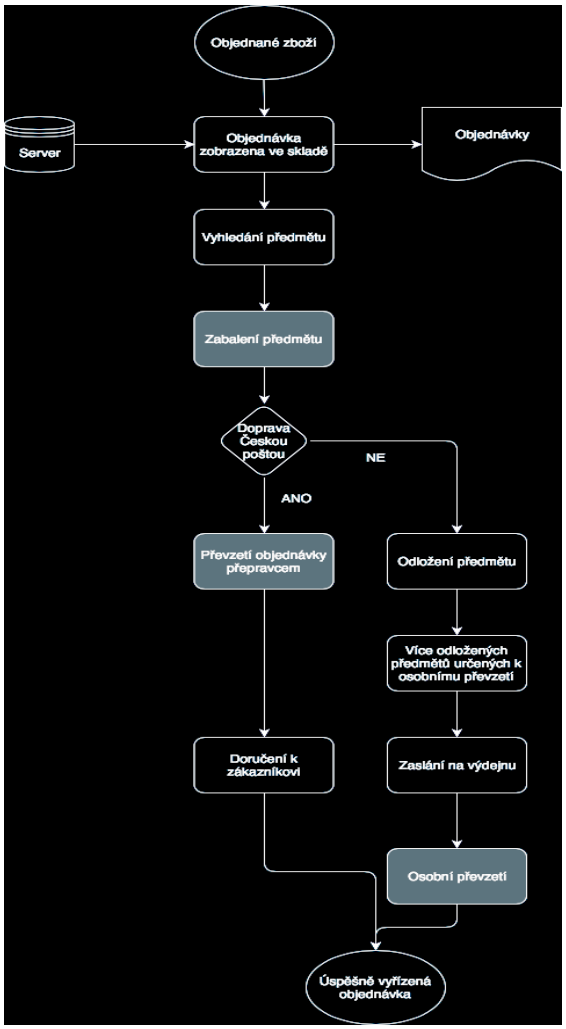
Po potvrzení cookies se tato lišta již nezobrazuje. Pokud je zákazník přihlášen, jsou o něm zpracovávána data a ta jsou pak přiřazována právě k jeho přihlašovacím údajům. V případě, že zákazník není přihlášen, prohlíží web „anonymně“. Stále jsou o něm zpracovávána data o jeho chování na webu. Dalším krokem je upozornění zákazníka na možnost odběru newsletteru. Má-li zákazník zájem, vyplní pole s emailem, pokud ne pokračuje dále v prohlížení e-shopu. Zde má zákazník dvě možnosti: Buď hledá informace o dané firmě, která ho provozuje, nebo má zájem o nabízené předměty. Za těchto okolností se ptáme, jestli má zákazník zájem o zboží, nebo si ho jen prohlíží bez myšlenky jeho zakoupení. Když si chce zákazník zboží zakoupit, vloží ho do košíku, kde v dalším kroku vyplní doručovací údaje, vybere dopravce, způsob platby a posledním krokem je potvrzení objednávky. V tomto momentě se uzavírá smlouva mezi kupujícím a prodávajícím. Na zákazníky, kteří opustí e-shop bez nákupu a potvrdí souhlas se pracováním osobních údajů, je cílena reklama.



Obr. 4. Procesní analýza - nabídka předmětu [Vlastní zdroj]

5.4 Vyřízení objednávky

Proces začíná zákazníkovým dokončením objednávky. Tímto krokem firma dostává viditelný podnět od zákazníka. Podnět je zobrazen ve formě upozornění na zařízeních na skladě. Jakmile je předmět objednán na e-shopu, automaticky se vymaže ze stávající nabídky. V momentě kdy upozornění o objednávce dorazí na sklad, začíná se předmět nejprve hledat. Systém uspořádání předmětů je takový, že předměty jsou uloženy v označených krabicích, ve kterých se nachází několik desítek kusů předmětů. Při přijmutí objednávky zaměstnanec ví, jak předmět vypadá, proto je jednodušší ho najít. Po vyhledání jsou předměty zabaleny a rozstříženy dle toho, jestli si zákazník zvolil přepravu poštou nebo osobní převzetí. Objednávky pro osobní převzetí jsou shromažďovány a jednou týdně odesílány na výdejnu. Na konci pracovního dne jsou objednávky doručovány poštou, odevzdány přepravci.

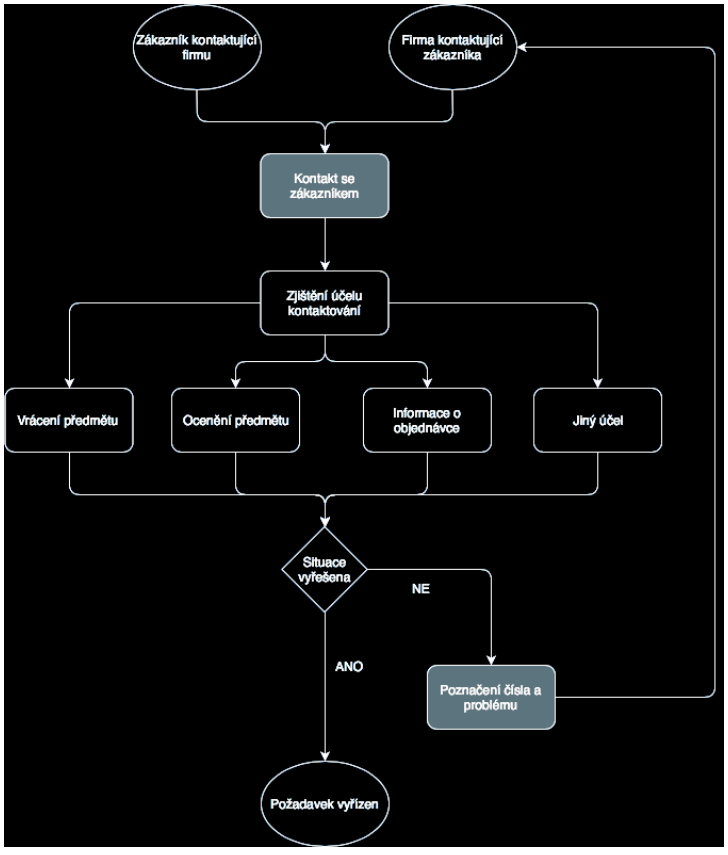


Obr. 5. Procesní analýza – vyřízení objednávky [Vlastní zdroj]

V samotném procesu se pracuje s osobními daty až při balení objednávky, protože každá objednávka má své pořadové číslo. To znamená, že s osobními daty se nemusí pracovat při jejím vyhledávání. Také při předání balíků dopravci se pracuje s osobními údaji – správce osobních údajů předává osobní data zpracovateli osobních údajů. Zpracování údajů za účelem dopravení objednávky na místo určení je dle nařízení zpracování nezbytné pro plnění smlouvy. Bylo by totiž nemožné bez údajů, které zákazník vyplňuje při objednávce, doručit balíček [5]

5.5 Customer care

Proces customer care je proces, který je vyvolaný potřebou kontaktovat zákazníka nebo potřebou zákazníka kontaktovat firmu. Nejčastějším důvodem kontaktování firmy zákazníkem je ocenění předmětů. Tuto činnost provádí jeden z jednatelů firmy nebo je provedena pomocí dat nasbíraných z databází ostatních antikvariátů. Dalším častým dotazem od zákazníka je stav jejich objednávky. Jelikož jsou sklady na 3 místech po České republice, stává se, že objednávka může nabrat zpoždění cestou na výdejnu.



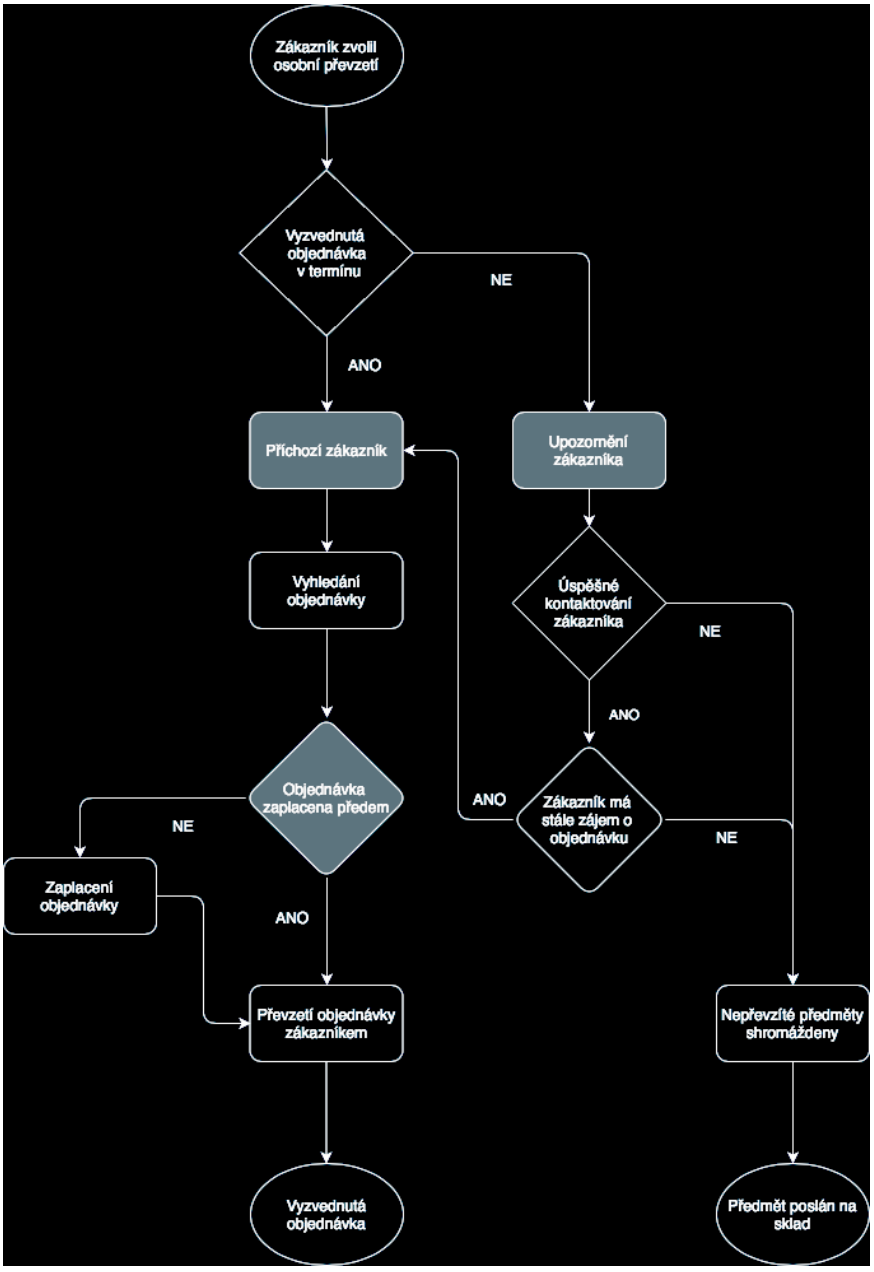
Obr. 6. Procesní analýza – customer care [Vlastní zdroj]

V celém procesu pracujeme s osobními daty volajícího. Hned na začátku potřebujeme identifikovat osobu a účel kontaktování. V případě, že zákazník chce ocenit předmět, je po něm požadováno, aby zanechal své kontaktní údaje, které jsou následně zaznamenány. Při zpracování údajů takovou formou je předpokládáno, že zákazník sděluje své údaje dobrovolně, za účelem obohacení, protože předměty jsou ohodnocovány zdarma.

5.6 Výdejna

Podnět pro začátek procesu přichází od zákazníka, který zvolil osobní předání předmětu. V momentě, kdy je objednávka doručena, je zákazníkovi posláno upozornění o naskladnění objednávky na výdejnu. Stává se poměrně často, že zákazník si předmět objedná na výdejnu a nevyzvedne si ho. V takovém případě je zákazník kontaktován opakovaně. Pokud si ani po opakovaném upozornění zákazník předmět nevyzvedne, jsou předměty odloženy a při větším množství přemístěny na sklad. Ve výjimečných případech se stává, že zákazník si objedná na výdejnu předmět, aby se ujistil, jestli odpovídá popis stavu realitě. Při vyzvednutí na výdejně platí zákazník poplatek za osobní převzetí. Platí tím náklady spojené s dopravou předmětu na výdejnu. Poplatek může zaplatit buďto předem, nebo dohromady spolu s cenou předmětu.

Zaměstnanci pracují na prodejně s osobními daty tehdy, když kontaktují zákazníka o přítomnosti objednávky na výdejně, nebo v momentě, kdy zákazník dojde na výdejnu pro samotný předmět. V této chvíli je nutné identifikovat příchozího pro vydání objednávky. Stejně jako doprava, tak i výdej objednávek by se bez těchto údajů neobešel, takže zpracování těchto údajů je nutné pro plnění smlouvy.



Obr. 7. Procesní analýza - výdejna [Vlastní zdroj]

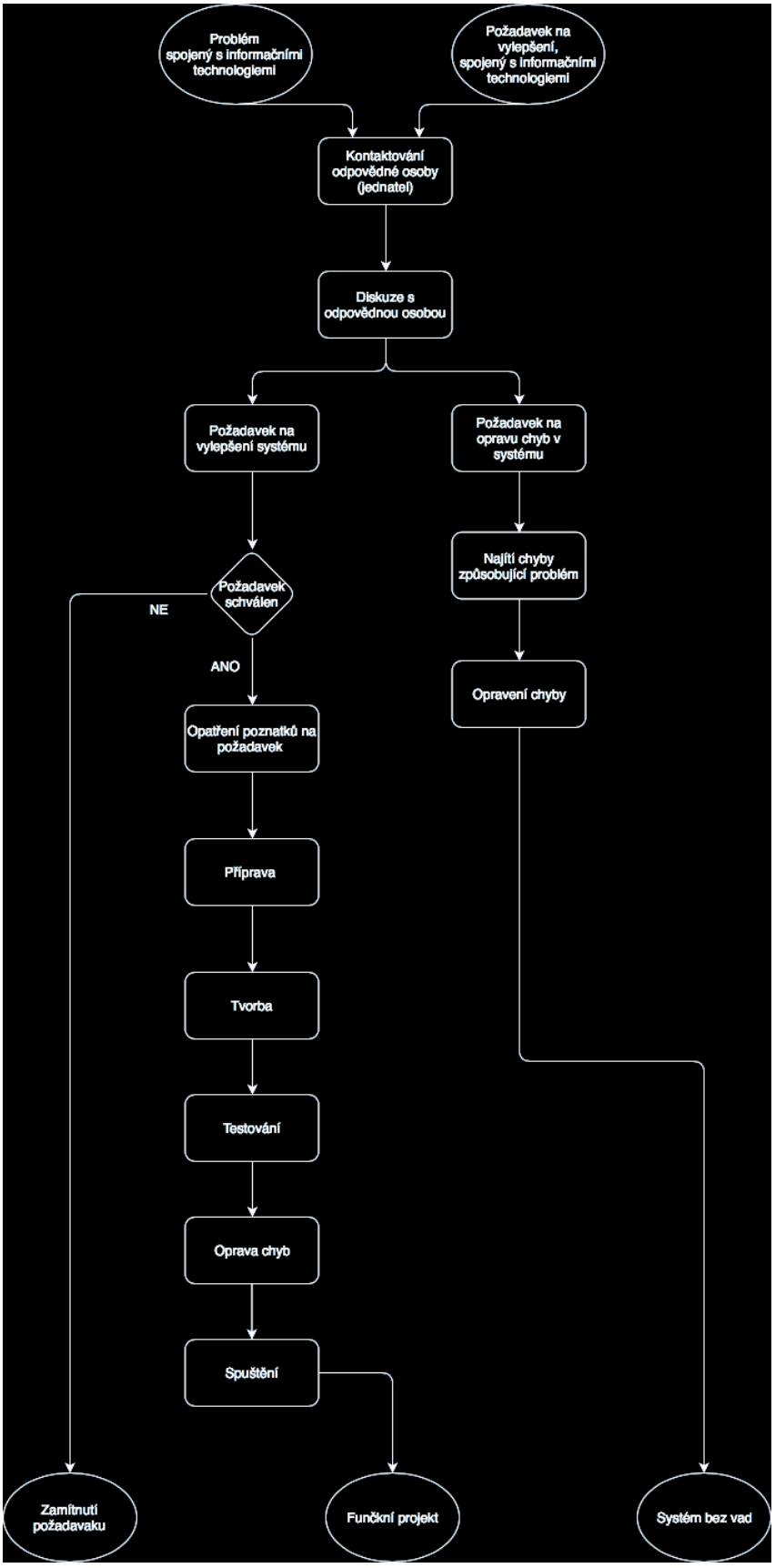
5.7 Informační technologie

Nejdůležitější proces pro fungování konceptu firmy. Základní myšlenka je dělat věci jinak než ostatní, proto firma samotná se snaží plně automatizovat všechny procesy v antikvariátu. Bohužel nemá dostatek lidských zdrojů pro to, aby firma vyvinula a realizovala všechny potřebné systémy a zařízení, které potřebuje, pro co největší automatizaci procesů. Firma má v plánu dodávat svá řešení ke své konkurenci, a tím rozšířit firmu o další odvětví. Zatím jsou projekty ve fázi testovací. Projekt ptolemaia.cz slouží pro lidi jako vyhledávač starých knih a předmětů, ale pro firmu slouží jako databáze pro oceňování

předmětů. tímto krokem ušetří za znalce. Dalším projektem je fotobuňka, která umožňuje co nejrychlejší přidání knih na e-shop. Ta umí knihu nafotit a podle fotografie přenést text do digitální podoby a vyplnit základní informace o knize.

Proces samotný je na obrázku 7 stavěn obecně, jelikož pokaždé je řešen jiný problém. Ten je vyvolán potřebou modernizace současného systému nebo potřebou opravit chybu v systému. Firma má pouze jedinou osobu, která řeší všechny tyto požadavky, proto jsou všechny operace s touto osobou diskutovány. Jelikož zajišťuje všechny funkce v systému, je třeba vybrat nejdůležitější požadavky a provést je jako prioritní. Prioritu mají chyby, které ohrožují funkčnost celého systému. poté jsou řešeny rozdělané současné projekty. Každý projekt vzniká tím, že je odsouhlasen většinou vlastníků a poté vše přejde na odpovědnou osobu, která provádí vývoj samotného projektu. Nejprve jsou opatřeny poznatky pro samotný projekt, a potom se začíná s přípravou, kde je potřeba zajistit všechny zdroje. Poté je projekt vytvářen. v momentě, kdy je systém funkční, přichází fáze testování a opravování chyb. Pokud je projekt dostatečně dlouho testován, přejde do plného provozu.

Celý proces je nedotčený GDPR, jelikož se zde nepracuje s osobními daty. V případě, že projekt slouží pro veřejnost, jsou data zpracovávána až v momentě, kdy je systém plně funkční.

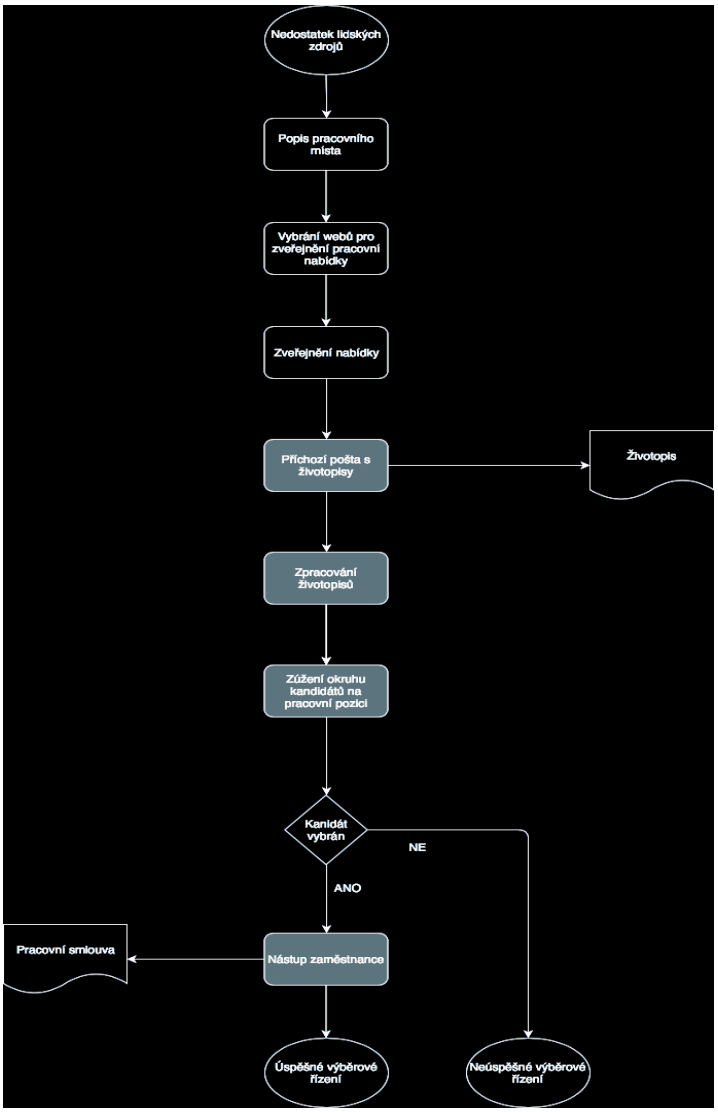


Obr. 8. Procesní analýza – informační technologie [Vlastní zdroj]

5.8 Lidské zdroje

Podnět pro začátek procesu je nedostatek lidských zdrojů ve firmě. Ta vyvolá reakci, která je ve firmě zakořeněná od založení. Nejprve je sepsán text na pracovní pozici, potom je zveřejněn na sociálních sítích. Výjimečně jsou použity jiné portály nebo webové stránky. Po zájemcích je vždy požadován životopis, který je zaslán na firemní e-mail, kde jsou pak životopisy shromážděny a procházeny do té doby, než je vybrán úzký okruh zájemců, kteří jsou pozváni na pohovor. Pokud je uchazeč přijat je s ním sepsána pracovní smlouva.

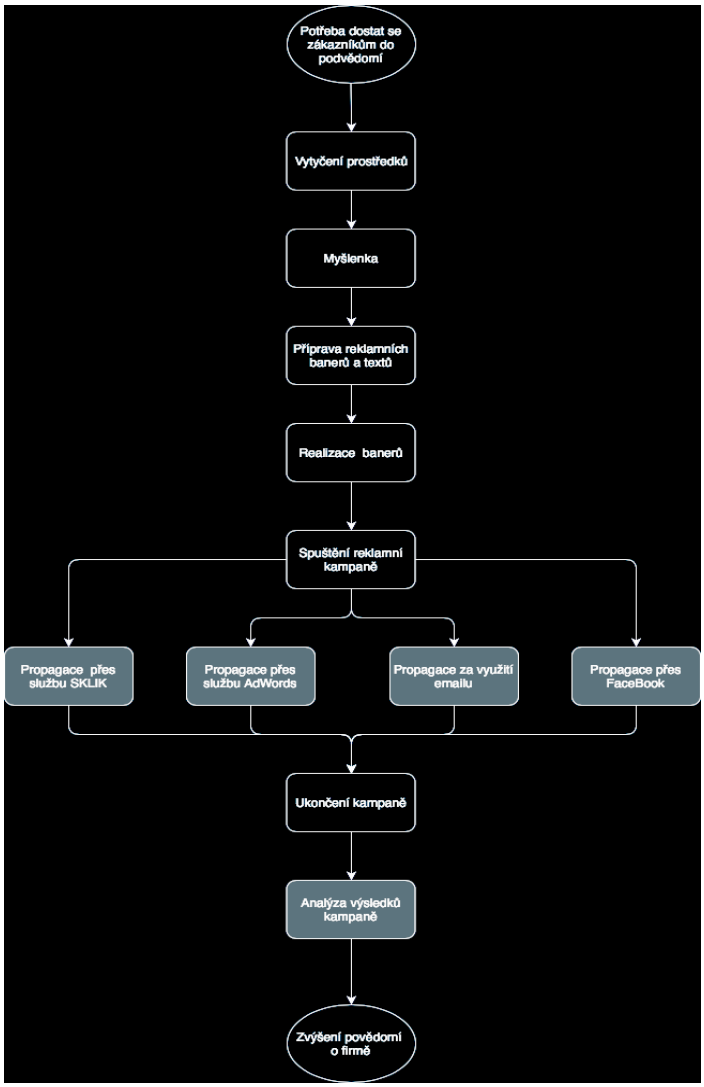
V samotném procesu se pracuje s osobními daty od té doby, co uchazeč pošle jeho životopis na firemní e-mail. Je nutné upozornit na to, že po úspěšném výběrovém řízení jsou tyto emaily s životopisy mazány. K firemnímu emailu pak mají přístup všichni zakladatelé.



Obr. 9. Procesní analýza – lidské zdroje [Vlastní zdroj]

5.9 Propagace

Proces propagace začíná potřebou dostat se zákazníkům do podvědomí. Jelikož je firma závislá na předmětech, které jsou vykupovány od běžných lidí nabízejících starožitné předměty, je tento krok životně důležitý pro fungování firmy. Na každou akci jsou nejprve vytyčeny prostředky, a potom se začíná s pracemi na bannerech. Nejdůležitější částí je myšlenka, jak zaujmout co nejvíce potencionálních zákazníků. V okamžiku, kdy jsou bannery hotové, jsou využity pro propagaci aplikace Sklik, AdWords a Facebook. Součástí propagace je tzv. emailing, kdy jsou posílány reklamní sdělení cílící na zákazníky, kteří již v e-shopu nakoupili. Firma zkoušela propagaci ve formě letáků do schránek, ale taková forma reklamy se neosvědčila. proto již není využívána. Po dokončení reklamní kampaně jsou analyzovány výsledky pomocí nástrojů Google Analytics. Data jsou pak využita pro další reklamní kampaň.



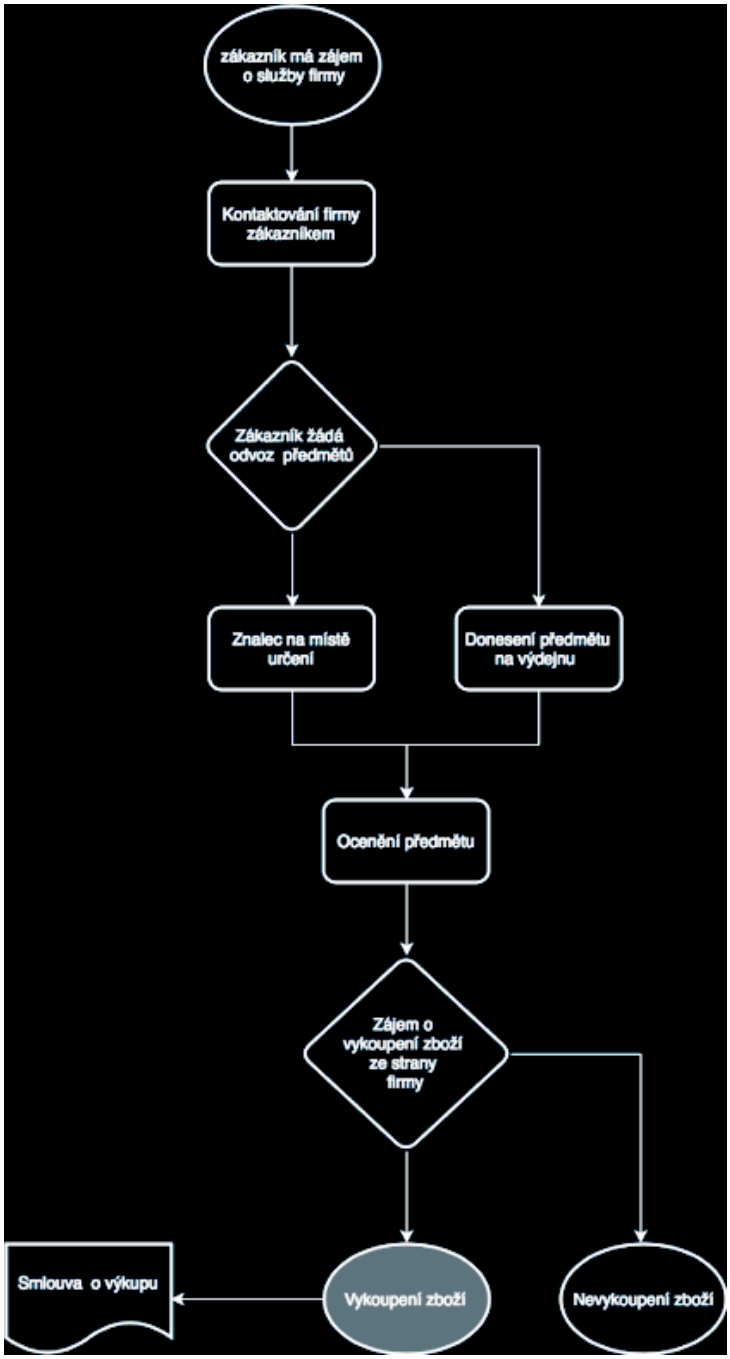
Obr. 10. Procesní analýza - propagace [Vlastní zdroj]

S osobními údaji firma pracuje tehdy, když posílá cílené emaily zákazníkům, kteří jsou uloženi v databázi. Jedná se o emaily, které byly poskytnuty buď vyplněním newsletteru, nebo vyplněním kontaktních údajů při objednání zboží z e-shopu. Další osobní data jsou zpracovávána společnostmi Google a Seznam kvůli cílené reklamě. Toto zpracování podléhá ePrivacy nařízení, které si podrobněji rozebereme v další části práce.

5.10 Výkup předmětů

Výkup předmětů je jeden z hlavních procesů ve firmě, bez něhož by nebyl koncept firmy možný. Jedná se o proces, při kterém získáváme předměty pro další prodej. Propagace předchází samotnému procesu výkupu předmětů. Bez zaujetí zákazníka zajímajícího se o služby firmy by nikdy k procesu nedošlo. Výkup předmětů začíná právě zájmem zákazníka o služby Antikvarium s.r.o., který naváže komunikaci s firmou. V případě zájmu o kompletní servis v podobě odvozu a ocenění předmětů přichází nejprve na řadu znalec, který provede ocenění na místě a podle toho rozhodne, zda má zájem o předměty. Dohodnou-li se obě strany, dojde k výkupu samotnému. Pro všechny antikvariáty plyne ze zákona povinnost uzavřít smlouvu o výkupu.

V procese jsou zpracovávány osobní údaje při uzavření smlouvy o výkupu mezi zákazníkem a firmou Antikvárium s.r.o. Smlouva je uzavřena z důvodu zákonné povinnosti. GDPR v tomto případě stanovuje informativní povinnost, která musí být součástí smlouvy nebo dodatku ke smlouvě [5].



Obr. 11. Procesní analýza - výkupj předmětu [Vlastní zdroj]

5.11 Shrnutí

Pomocí procesní analýzy jsme identifikovali všechny procesy ve firmě. Bylo zjištěno, že všechny hlavní procesy jsou nějak dotčeny GDPR. Před procesní analýzou jsme v tabulce 2 identifikovali veškeré procesy, kde bylo poznačeno, jestli se daného procesu GDPR týká či nikoliv. Procesy byly v procesní analýze rozebrány a bylo zjištěno, v jakém bodě se začíná pracovat s osobními daty. V některých případech pracujeme s osobními daty v celém procesu a někdy jenom v jeho části Tento krok nám pomůže pro samotnou

implementaci GDPR ve firmě. Jelikož se jedná o e-shop, valná většina osobních údajů je uložena na serveru nebo v zařízeních vlastněných firmou. V tištěné podobě jsou pouze smlouvy se zákazníky nebo se zaměstnanci. Bylo také zjištěno, že bude potřeba uzavřít několik smluv se zpracovateli osobních údajů, protože firma využívá nástroje a služby třetích stran. Společnosti jako Seznam a Google již nabízí pro své zákazníky řešení.

Z procesní analýzy vyplývá, jaké právní tituly pro zpracování osobních údajů bude potřeba. Největší zastoupení má zpracování za účelem plnění smlouvy. Právní titul souhlas je využit pro zpracování údajů, které slouží k propagaci firmy, ve výjimečných případech je tento titul využit v procese inovace. Poslední právní titul zpracování údajů za účelem plnění zákonné povinnosti se týká procesu výkup předmětů.

Firma před účinností GDPR zpracovávala všechny osobní údaje dle platného zákona. V obchodních podmínkách má jasně stanoveno, že data jsou zpracována na dobu neurčitou, tímto krokem splňuje rámce zákona. Tento krok je však pro GDPR nedostatečný, je nutné stanovit, na jakou dobu budou data zpracovávána. Procesní analýza nám pomůže si uvědomit, na jakou dobu jsou tyto údaje ve firmě potřebné, a tím jednodušeji stanovíme dobu pro zpracování.

V další kapitole jsou modelovány procesy, které ve firmě chybí a budou nutné pro splnění všech bodů směrnice.

6 PROCESNÍ OPATŘENÍ

V předchozí kapitole byla identifikována všechna místa, kde je nutno počítat se změnami v procese. Do 25.5 2018 bude vyžadováno udělat několik změn jak technického, tak i procesního charakteru. V následující časti práce, jsou popsány nově vzniklé procesy, které jsou nutné pro splnění všech podmínek GDPR.

Je již jasné, že právní titul pro zpracování osobních údajů za pomocí souhlasu bude mít dopad na celou e-commerce a marketingovou sféru. Firma zpracovává osobní údaje za účelem souhlasu pouze v cookies, newsletterech a hlídači předmětů. Cookies jsou specifické, proto jsou rozebrány v samostatné podkapitole.

V momentě, kdy zákazník zakoupí předmět v e-shopu, vzniká mezi kupujícím a prodejcem smlouva o koupi, kde podle GDPR není nutná potřeba souhlasu. Jedná se o zpracování za účelem plnění smlouvy. Je nutné, aby prodávající měl k dispozici doručovací údaje pro doručení objednávky zákazníkovi. Není jasné, jaké údaje je po zákazníkovi možné vyžadovat a co je již v rozporu s nařízením. Vybere-li si zákazník osobní předání na prodejně, jsou adresní údaje prodávajícímu zbytečné, ale na druhou stranu musíme brát v potaz nutnou identifikaci při osobním převzetí. Podle jména a příjmení bychom nemohli jasně určit, komu by měl být balíček vydán [5].

Pro právní titul za účelem plnění smlouvy není vyžadován souhlas, ale dle GDPR je nutné upozornit subjekt, že jsou zpracovávány osobní údaje. Upozornění musí obsahovat dobu zpracování, správce a zpracovatele osobních údajů. Osobní údaje použity při přijetí objednávky jsou předávány přepravci kvůli doručení na místo určení a doba pro zpracování je 10 let kvůli zákonné povinnosti o archivaci účetních dokladů [5].

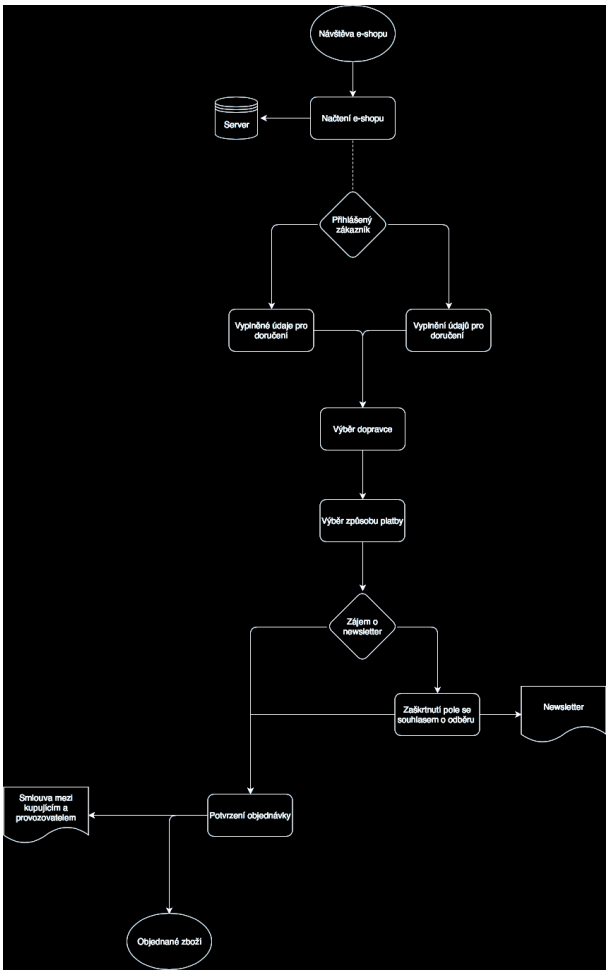
Drtivá většina e-shopů využívá k zasílání newsletterů souhlas, který je udělen zákazníkem při zakoupení zboží. Samotný kupující si není toho vědom, jelikož souhlas je součástí obchodních podmínek a většinou zde není možnost, zdali chce zákazník obchodní sdělení přijímat či nikoli. GDPR říká, že takto specifikovaný souhlas nelze dále využívat, musí být jasně viditelný a udělován zvlášť při odeslání objednávky. Je-li při odesílání objednávky souhlas reprezentován zaškrtávacím polem, musí být pole nevyplněné nebo nepodmíněné pro odeslání objednávky. Stává se, že e-shopy tato pole mají již předvyplněná nebo dokonce bez jejich odsouhlasení nelze objednávku odeslat [5].

Na e-shopu antikvarium.cz se nachází pole, které může zákazník vyplnit a udělit tím souhlas o zaslání sdělení. Jedná se o hlídacího psa, kdy zákazník požaduje po provozovate-

li, aby při dostupnosti předmětu zaslal upozornění. Dalším polem pro vyplnění je pole pro souhlas se zasíláním newsletterů. V takovém případě jedná subjekt dle vlastního uvážení a je si vědom zpracování osobních dat. Zde je ale také nutno sdělit informaci o zpracování osobních dat.

6.1 Newsletter

Současná podoba při odesílání objednávky nevyhovovala požadavkům – nebylo zde žádné pole pro souhlas se zasíláním newsletterů. Je ale nutno podotknout, že doposud byly splněny všechny rámce současného zákona, neboť informace o souhlasu byly obsaženy v obchodních podmínkách. Automaticky se počítalo po úspěšné objednávce, že zákazník tímto krokem udělil souhlas. Nově se zde musí nacházet pole se souhlasem, kde si zákazník může svobodně vybrat, jestli mu budou zasílány reklamní sdělení či nikoliv [5].



Obr. 12. Procesní opatření – newsletter [Vlastní zdroj]

Pole nesmí být předvyplněné nebo nemůže být podmínkou pro další pokračování v objednávce. Povinností je uvést informativní větu vedle daného pole. Těmito kroky zajistíme, že zákazník nebude přihlašován k newsletteru automaticky, ale bude mít možnost výběru. Souhlas se bude nacházet pod formulářem pro vytvoření objednávky. Výstupem souhlasu jsou data, která jsou uložena v databázi. Nově budou muset být v databázi zpřesněny informace o udělení souhlasu, jedná se hlavně o položku času jeho udělení.

6.2 Cookies

Cookies mohou být dle GDPR využívány pouze za účelem souhlasu, ale dle mnoha expertů se pohled na tuto problematiku různí. Faktem je, pokud cookies jakýkoliv způsobem spojí subjekt s daty, jedná se o zpracování osobních údajů. Samotné cookies jsou ukládány na disk uživatelova zařízení, což je jedna z mála výhod pro správce a zpracovatele – nemusí se starat o zabezpečení těchto dat na svém úložišti. Správce dat je povinen informovat zákazníka o zpracování osobní dat, může tak učinit podstránkou obsahující oznámení o zpracování osobních údajů za pomocí cookies [5].

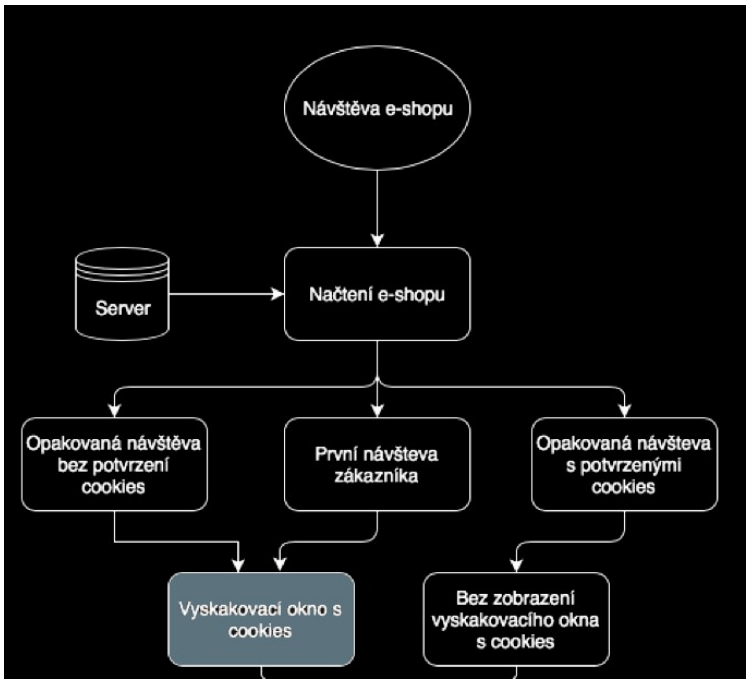
Rozlišujeme několik druhů cookies, proto bychom se měli před implementací GDPR zeptat na to, jaké typy cookies využíváme. Dle GDPR je možné využívat režim opt-out bez informování zákazníka. Jedná se o typy session cookies, které jsou smazány v momentě, kdy uživatel zařízení opustí. Další typy cookies jsou např. ty, které jsou využívány k retargetingu. Takové cookies v režimu opt-in vyžadují dle většiny expertů souhlas, tzn. takový, který je nutný před samotným zpracováním [5].

Kdy získávat souhlas od uživatelů a kdy ne, bylo v České republice diskutováno po mnoho let, jelikož zákon o ochraně osobních údajů vycházející ze směrnice 95/46/ES, byl špatně přeložen a tím se rozcházel s originální verzí. Výklad nebyl jasný a správci osobních údajů si nebyly, jistí, v jakých situacích souhlas použít. Současná situace s GDPR je podobná jako před lety.

Výklad současného nařízení není zcela jasný a liší se ve většině výkladů. Podle nejhoršího scénáře by před přístupem na samotný web mělo být okno, kde uživatel musí vyplnit rok narození a stát. Následně dle legislativy jednotlivého státu by mělo být rozhodnuto, zda je uživatel oprávněn udělit souhlas či nikoliv. V případě, že by byl uživatel dostatečně starý a udělil tento souhlas, měl by správce povinnost takový souhlas uložit do své databáze a zarchivovat ho. Provozovatel webových stránek by měl počítat s tím, že uživatel souhlas

neudělí a bude chtít pokračovat v prohlížení. Dle GDPR by to mělo být možné, bohužel technicky je tento proces velmi těžce proveditelný [5].

Díky nejasnému výkladu a technicky takřka neproveditelným řešením předložila Evropská komise ke schválení návrh ePrivacy. Ten přesouvá povinnost od provozovatelů webů na prohlížeče. Není zcela jasné, kdy ePrivacy vejde v platnost. Mluvilo se o začátku roku 2018, později byl tento krok přesunut na konec roku 2018. Uživatel bude moci vybrat v nastavení prohlížeče, na jakých stránkách povolí zpracování cookies a v jakém rozsahu. Provozovateli webu zbyde pak pouze povinnost informovat, jaké typy cookies jsou na webu zpracovávány.



Obr. 13. Procesní opatření – cookies [Vlastní zdroj]

Proces jako takový zůstane beze změny, ale vyskakovací okno projde značnou změnou. Musí zobrazovat minimálně informativní větu o zpracování cookies na e-shopu a odkaz s proklikem. Další možností je roztahovací okno, kde se při najetí na symbol okno roztáhne a návštěvník webu uvidí všechny povinné informace v jednom okně. Obsah vyskakovacího okna je popsán v tabulce č. 3 a 4. Směrnice říká, že informativní text musí být srozumitelný pro každého. V tabulce č. 4 jsou cookies rozděleny podle kategorií, a to podle nutných, preferenčních, statistických a marketingových. Popisky byly zvoleny tak, aby i laik byl schopen pochopit význam těchto pojmů. Každá kategorie cookies je popsaná a v tabulkách jsou uvedeny všechny důležité náležitosti jako účel, doba zpracování a typ cookie.

Tab. 3. Obsah souhlasu cookies lišty – 1. část

Tato webová stránka používá cookies
K personalizaci obsahu a reklam, poskytování funkcí sociálních médií a analýze naší návštěvnosti využíváme soubory cookie. Informace o tom, jak náš web používáte, sdílíme se svými partnery pro sociální média, inzerci a analýzy. Partneři tyto údaje mohou zkombinovat s dalšími informacemi, které jste jim poskytli nebo které získali v důsledku toho, že používáte jejich služby.
O cookies
Cookies jsou malé textové soubory, které mohou být používány webovými stránkami, aby učinily uživatelský zážitek více efektivní. Zákon uvádí, že můžeme ukládat cookies na vašem zařízení, pokud jsou nezbytně nutné pro provoz této stránky. Pro všechny ostatní typy cookies potřebujeme vaše povolení. Tato stránka používá různé typy cookies. Některé cookies jsou umístěny službami třetích stran, které se objevují na našich stránkách.

Tab. 4. Obsah souhlasu cookies lišty – 2. část

Nutné			
Nutné cookies pomáhají, aby byla webová stránka použitelná tak, že umožní základní funkce jako navigace stránky a přístup k zabezpečeným sekcím webové stránky. Webová stránka nemůže správně fungovat bez těchto cookies.			
Jméno	**Účel**	**Vypršení**	**Typ**
itfpctmp	Neklasifikované	Session	HTTP
threeInitialOptionsShown	Neklasifikované	6 dní	HTTP
com.sap.engine.security.authentication.original_application_url	Neklasifikované	Session	HTTP
saplb_*	Neklasifikované	Session	HTTP
Preferenční			
Preferenční cookies umožňují, aby si webová stránka zapamatovala informace, které mění, jak se webová stránka chová nebo jak vypadá. Je to například preferovaný jazyk nebo region, kde se nacházíte.			
Jméno	**Účel**	**Vypršení**	**Typ**
jStorage	Slouží k zapamatování údajů	Persistent	HTML
jStorage_update	Slouží k zapamatování údajů	Persistent	HTML
Statistické			
Statistické cookies pomáhají majitelům webových stránek, aby porozuměli, jak návštěvníci používají webové stránky. Anonymně sbírají a sdělují informace.			
Jméno	**Účel**	**Vypršení**	**Typ**
__utma	Shromažďuje data, odkud uživatel pochází, jaké vyhledávací zařízení bylo použito, na jaký odkaz bylo kliknuto a jaký termín byl použit pro vyhledávání. Tato data využívá analytický systém Google Analytics.	2 roky	HTTP
__utmb	Registruje časové razítko s přesnou dobou, kdy uživatel vstoupil na stránku. Využívá se analytickým systémem Google Analytics pro výpočet doby trvání návštěvy na stránce.	Session	HTTP
__utmv	Ukládá uživatelem definované parametry sledování pro používání v analytickém systému Google Analytics.	Session	HTTP
_gat	Používá se systémem Google Analytics pro regulaci rychlosti zadávání požadavků.	Session	HTTP
Marketingové			
Marketingové cookies jsou používány pro sledování návštěvníků na webových stránkách. Záměrem je zobrazit reklamu, která je relevantní a zajímavá pro jednotlivého uživatele a tímto hodnotnější pro vydavatele a inzerenty třetích stran.			
Jméno	**Účel**	**Vypršení**	**Typ**
ads/ga-audiences	Používá se službou Google AdWords pro cílenou reklamu.	Session	Pixel
collect	Používá se systémem Google Analytics pro posílání dat o zařízení a chování návštevníka webu.	Session	Pixel
khaos	Sbírá data o zemi a o reklamách na které rohlížející kliknul.	1 rok	HTTP

6.3 Vyřízení objednávky

Při prvotním přijetí objednávky je pracováno pouze s ID a s osobními daty se pracuje až při balení. Podle směrnice by mělo pod rukami zaměstnanců projít co nejmenší množství osobních údajů. Při balení objednávky jsou tisknuty štítky, které jsou lepeny na balíky spolu s ID objednávky, je tento proces vyhovující. Zaměstnanci prochází pod rukami minimum osobních údajů, a navíc proces je efektivní. Proces vyřízení objednávky se měnit nebude a zůstane beze změny.

Místu, kterému bychom se měli více věnovat je předání objednávky České poště. Zde je potřeba se soustředit na současné smlouvy a ujasnit si základní podmínky se zpracovatelem osobních údajů. Doporučuje se nastavit dobu zpracování osobních údajů s přepravcem a ošetřit úniky osobních dat z jeho strany. Česká pošta disponuje certifikátem ČSN ISO/IEC 27001:2014, který dle jejich webu deklaruje, že přijali všechna opatření pro ochranu citlivých informací, čemuž se rozumí osobní údaje a zákaznické informace jako celek, avšak by se smlouva o zpracování osobních údajů neměla opomíjet. Jelikož se jedná o nejčastější přestupek, drtivá většina podniků tímto dokumentem nedisponuje [23].

Dalším místem kde zaměstnanci přicházejí do kontaktu s osobními údaji je výdejna. Zde mají přístup k systému, kde jsou zobrazeny osobní údaje, jelikož bez nich by nemohli identifikovat osobu a jasně určit, komu mají objednávku vydat. Jedná se o zpracování osobních údajů za účelem plnění smlouvy. V tomto případě jsou všechny postupy obhajitelné. Jediným vylepšením by mohlo být upravení systému způsobem, že zaměstnanci na výdejně budou oprávněni přistupovat pouze k objednávkám, které jsou vydávány na výdejně. Současný systém nedisponuje možností řízení přístupů ani není stavěný na takové operace.

6.4 Lidské zdroje

Jedná se o proces, ve kterém se bez pochyb osobní data zpracovávají, a to nejprve při hledání zaměstnance a později při uzavření smlouvy. Tyto údaje jsou dále zpracovávány pro výplaty, výpovědi apod. Hledání zaměstnanců probíhá přes portály nebo sociální sítě. Zde je uvedena e-mailová adresa, na kterou jsou zasílány životopisy, které jsou dále zpracovávány. Zájemce zasláním e-mailu s životopisem činí dobrovolně, avšak dle GDPR by měl být informován o rozsahu zpracování osobních dat. Při prvotním zaslání e-mailu je tento problém velmi těžko řešitelný, informativní povinnost by musela být splněna přímo v inzerátu nebo potom je jedinou možností umístit informace o zpracování do obsahu

emailu. Inzertní servery určené pro nabídku pracovních pozic mají tento problém již vyřešen – mají zde pole, kde je zákazník informován o zpracování údajů. Důležité je vymezit dobu pro zpracování osobních údajů. Zaměstnavateli se mohou tyto životopisy hodit minimálně po zkušební dobu zaměstnance [5].

Zpracování údajů probíhá v momentě, kdy zájemce podepíše pracovní smlouvu. Informace o zpracování by měli být v samotné smlouvě nebo v jejím dodatku. Jsou-li údaje poskytovány třetím osobám. Měl by být tento fakt uveden také. Současní zaměstnanci musí podepsat tento dodatek mimo pracovní smlouvu, jelikož předešlá smlouva je platná dle znění Zákona o ochraně osobních údajů z roku 2000. Rozdíly mezi GDPR a zákonem z roku 2000 jsou minimální. Důležité je poznamenat, že zaměstnanec má vždy právo vědět, kdo jeho osobní údaje zpracovává, v jakém rozsahu, po jakou dobu a za jakým účelem. Odmítnutí poskytnutí takových informací je v rozporu s nařízením [5] [6].

6.5 Privacy by Design

Jedna z nových věcí týkající se ochrany osobních údajů je Privacy by Design. Hlavní myšlenkou je vybudovat systém, který již od prvotních idejí dbá na ochranu a bezpečnost osobních údajů. Fungující systém pak nepotřebuje žádné opatření k ochránění soukromí a úniku dat. Privacy by Design je spojeno s GDPR tím, že je důležité zpracovávat pouze data, která jsou pro správce nutná. Dále je spojován s nařízením díky pseudonimizaci a anonymizaci dat, které eliminují pravděpodobnost zneužití při úniku dat [22].

Ve firmě se týká Privacy by Design procesů informační technologie a inovace. Nejedná se však o platné nařízení, je to pouze doporučení a při kontrole nemůže být počínání mimo rámec tohoto doporučení nijak penalizováno. Doporučením pro firmu je, že pokud bude vyvíjet nový systém, měla by se držet Privacy by Design, a tím předcházet následkům, které by mohli nastat při možném úniku dat. Je důležité, aby se s tímto konceptem pracovalo již od samotných plánů [22].

V případě, že firma zvolí tuto metodiku, neexistuje žádný institut, který by posuzoval, jestli je chystaný projekt v souladu s Privacy by Design. Jde spíše o to, že firma by měla mít odpovědnost vůči veřejnosti a citlivé údaje chránit bez jakýkoliv nařízení nebo doporučení. V dnešní digitalizované době mají osobní údaje obrovskou cenu. Může se zdát, že aplikace FaceBook je zdarma, ale realitou je, že každý krok v této aplikaci je monitorován a data jsou pak analyzována a prodávána za obrovské finanční prostředky, proto by si měl být uživatel vědom, kolik dat o sobě předává provozovatelům webů [22].

Procesy ve firmě se díky Privacy by Design, nebudou nijak měnit, je třeba dbát více na přípravnou část, navrhovat systémy, kde budou minimalizovány bezpečnostní chyby využívající důmyslně propracované bezpečnostní řešení. Při tvorbě systému, který jakkoliv sbírá osobní údaje, je třeba dbát na psedonimizaci a anonimizaci údajů. Tím se vyhneme problémům při odcizení databáze [22].

6.6 Dokumentace

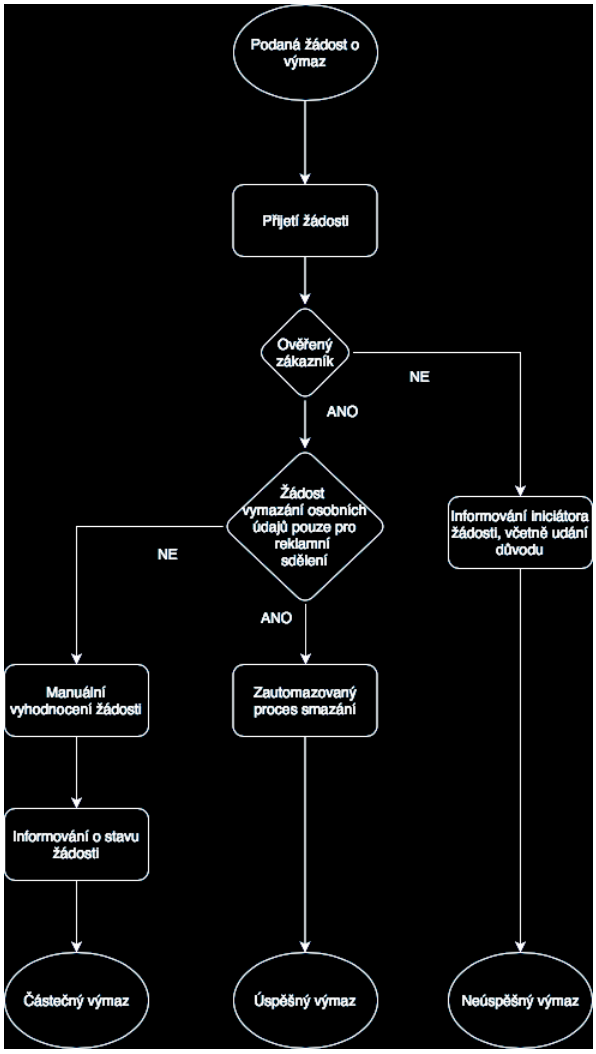
Dokumentace ve firmě není potřeba. Je nutná až od 250 zaměstnanců. Pro případ rozmachu firmy si alespoň definujeme základy dokumentace. Ta není povinná pro firmu, která je předmětem diplomové práce, ale má své důvody. Firmy si většinou až po jejím zpracování uvědomí rozsah zpracování a vhodnost omezení zpracování osobních údajů. V případě, že má firma povinnost tuto dokumentaci zpracovat, je nutné ji držet aktualizovanou. To znamená aktualizovat nové způsoby zpracování osobních údajů, úpravu těch stávajících a spolupráci s novými zpracovateli osobních údajů. Pokud firma bude expandovat na další trhy, je nutná aktualizace i této události, jelikož firma předává tímto údaje do dalšího státu [5].

6.7 Proces vymazání údajů na základě žádosti

Žádost o vymazání osobních údajů není novinkou GDPR. Mohli jsme se setkat s tímto krokem již v minulosti. Sama organizace pak posuzovala, jestli je zpracování v rozporu se zákonem či nikoliv. Dle toho byla data mazána. Neznamená to, že uživatel dojde na web a požádá instituci o vymazání osobních údajů a ta mu hned vyhoví. Je důležité rozeznávat údaje, které byly získány pomocí souhlasu a ty, které byly získány na základě plnění smlouvy. Pokud má firma povinnost skladovat účetní doklad po dobu 10 let od finančního úřadu, nemůže je bez rozmyslu vymazat [6].

V GDPR jsou stanoveny důvody, při jakých subjekt může o výmaz požádat. Jak již bylo řečeno, pokud správce nebo zpracovatel nesouhlasí s touto žádostí, může ji odmítnout.

Může nastat situace, kdy si zákazník zakoupí předmět, souhlasil se zasíláním reklamních sdělení a po 14 dnech se rozhodne, že požádá o výmaz všech údajů, které o něm firma vede. Ta rozhodne, že smaže pouze údaje pro reklamní sdělení, ale údaje obsaženy v účetním systému si ponechá.



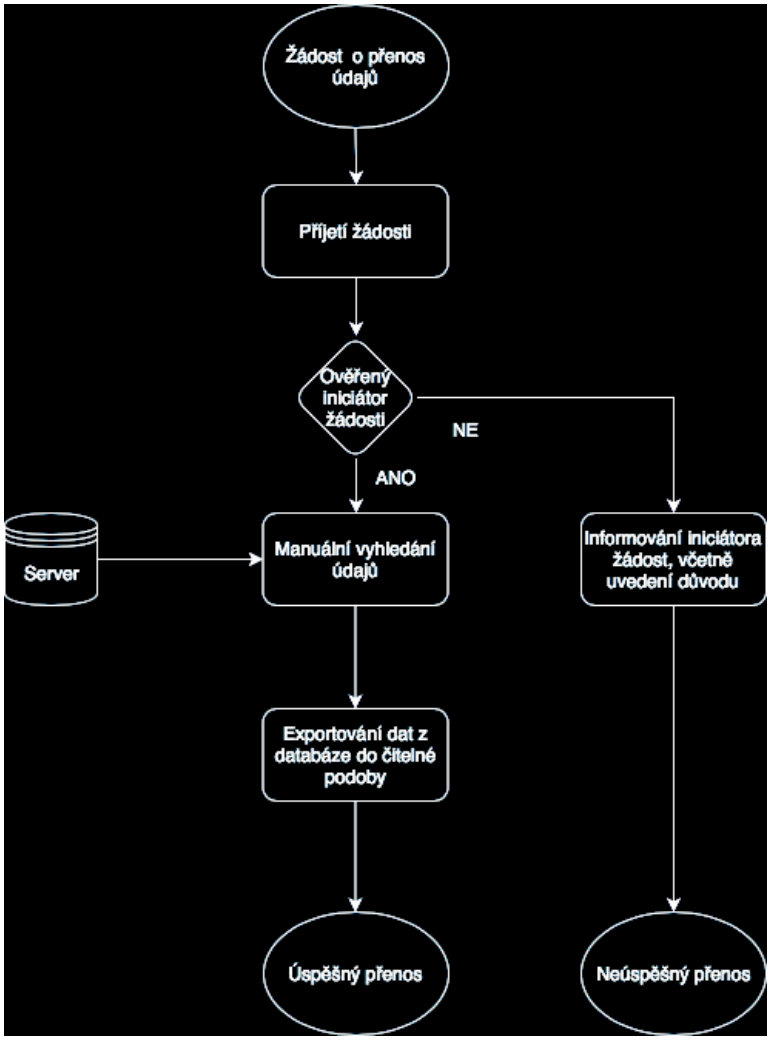
Obr. 14. Procesní opatření - žádost o výmaz [Vlastní zdroj]

Díky právu na výmaz vznikne ve firmě nový proces, který začíná požadavkem zákazníka na výmaz osobních údajů. Nutností je ověřit identitu osoby, jež žádost zaslala. Nejjednodušší cesta je umístit registrovanému zákazníku do profilu tlačítko na výmaz osobních údajů. Vyhneme se tím nutnosti ověřování. Neregistrovaný zákazník pak musí dokázat jeho totožnost. Odpovědná osoba rozhodne, jestli se subjekt prokázal dostatečně či nikoliv. V případě, že iniciátor žádosti požádá pouze o výmaz údajů pro reklamní sdělení, bude tento proces proveden automaticky. V případě, že žádost bude obsahovat výmaz všech údajů, bude automaticky přehodnocena a verdikt bude zaslán iniciátorovi žádosti.

6.8 Proces přenos údajů na základě žádosti

Právo na přenositelnost údajů je dalším právem, které opravňuje uživatele nakládat se svými osobními údaji. Právo jako takové není žádným novým pojmem, jedná se pouze o úpravu stávajícího práva na přístup ke zpracovaným informacím o uživateli. Na žádost je

povinen správce nebo zpracovatel osobních údajů předat v čitelné podobě všechny údaje, které jsou o něm zpracovávány. Týká se to jak údajů, které jsou zpracovávány na základě plnění smlouvy, tak i těch, které jsou zpracovávány na základě souhlasu. Je důležité, aby firma při tomto kroku nevynakládala nepřiměřené prostředky. GDPR neukládá žádný formát pro předání ani samotný způsob doručení. Prvotní zamýšlení bylo takové, že tímto krokem se zaručí rychlost a jednoduchost předání osobních údajů mezi institucemi poskytující stejnou službu. Ve skutečnosti, má každá instituce vlastní formáty pro zpracování a není jasné, jestli bude tato myšlenka úspěšná [5].



Obr. 15. Procesní opatření - žádost o přenos [Vlastní zdroj]

Celý proces začíná podáním žádosti o přenos údajů. Jelikož se nepočítá s ojedinělým jevem, celý proces bude dělán manuálně. Po přijetí žádosti bude ověřena identita uživatele, po jejím úspěšném ověření budou údaje vyhledány a exportovány do textového dokumentu, jenž se předá iniciátorovi žádosti. Pokud žadatel dostatečně neprokáže svoji totožnost, bude žádost automaticky zamítnuta.

7 DOPADY IMPLEMENTACE

GDPR představuje pro firmu další finanční náklady a pro malé živnostníky další zbytečně vynaložený čas věnovaný tomuto problému. Mediální bublina udělala z GDPR likvidátora firem, ve skutečnosti je toto nařízení cílené proti velkým korporacím, aby nezpracovávaly obrovské množství dat a neprodávali je za velké finanční obnosy analytickým firmám. Procesy ve firmě se budou měnit jen minimálně. Malé firmy, které nemají zaměstnance na tuto problematiku, vynaloží náklady na implementaci v jednotkách desítek tisíc korun. Přitom samotnou implementaci zvládne zkušený uživatel bez problémů.

7.1 Finanční dopad

Firma samotná byla nucena zaplatit peněžní prostředky za služby advokátní kanceláře, která pomáhala s oznamovací povinností uživatele na webu. Další finanční prostředky vynaloženy nebyly, jelikož všechny technické věci byly provedeny odpovědnou osobou. Musíme ale započítat čas vynaložený zaobíráním se tohoto problému. Ten mohl být vynaložen k účelům zajištění větší konkurenceschopnosti firmy, jelikož osoba provádějící tyto úkony má na starosti všechny inovativní projekty. Dalším možným nákladem může být zvýšená cena na reklamu. Z důvodu menšího objemu zpracovaných dat bude firma cílit na více potencionálních zákazníků a tím bude muset vynaložit větší prostředky na propagaci.

7.2 Dopad na PPC

Dopad na reklamní kampaně GDPR bude mít, avšak ne takový, jak by se na první pohled mohlo zdát - podle mnoha expertů může dojít ke zdražení reklamy, která díky GDPR nebude moci být cílená jako doposud, pokud bude spojováno mnoho údajů, které identifikují daný subjekt, bude muset přistoupit správce na opatření plynoucích z GDPR.

7.2.1 SKLIK

Pro reklamní kampaň využívá firma služeb společnosti Seznam.cz, zde jsou změny pouze minimální – bude zde nadále využíváno retargetingu, ale pouze v případě, že budeme cílit na skupinu o více než 30 potencionálních klientech. To zajistí jasnou neidentifikovatelnost zákazníka.

Behaviorální cílení se bude provozovat i nadále. Informací jako muž 25 let mající rád mobilní zařízení se GDPR netýká.

Jedinou povinností provozovatele webu je informativní sdělení o zpracování osobních dat za tímto účelem.

7.2.2 Google AdWords a Analytics

Dopad GDPR na službu AdWords je poměrně znatelnější než na jeho konkurenta. Bez souhlasu o sběru dat pro cílené reklamy nebude možné jasně identifikovat přání zákazníka a tím se může reklama pro firmu prodražit. Jedná se o reklamu, kdy inzerent cílí reklamu na potencionálního zákazníka za použití údajů jako jsou e-mailová adresa a telefonní číslo. Dále je nutné se společností Google uzavřít smlouvu. Ta je každému uživateli přístupná po přihlášení do administrace pod ikonou klíče. Po rozkliknutí zde najdeme tlačítko Pravidla a podmínky.

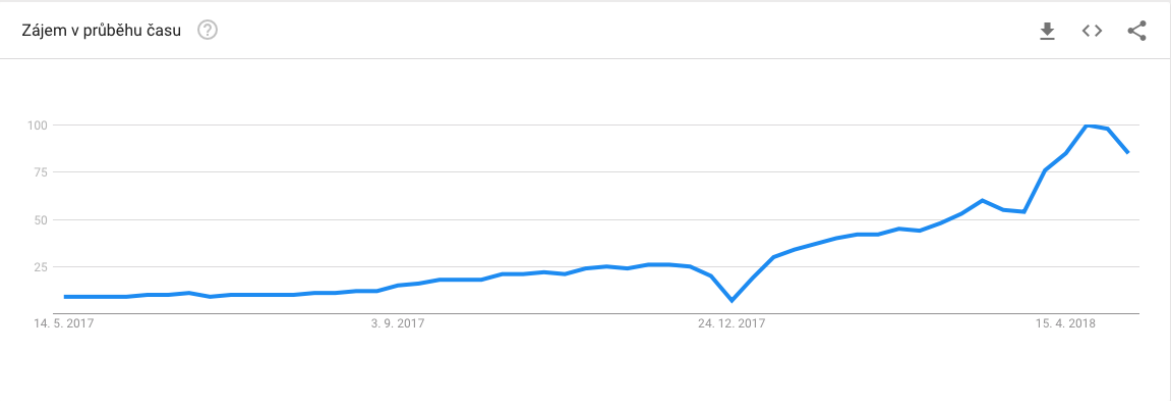
Google Analytics identifikuje zákazníka pomocí IP adresy a po opuštění webu je mazána. Tímto krokem nedochází ke zpracování osobních údajů. Jsou zde pak sbírána data, která nejsou přiřazena k jednotlivé IP adrese. Google uvádí, že na webu bude možnost zvolit, po jakou dobu bude mít uživatel k těmto údajům přístup. Bude se jednat o rozmezí mezi 14-50 měsíci. Stejně jako v administraci AdWords, tak i v administraci Google Analytics je nutno odsouhlasit smluvní podmínky. Tímto krokem vznikne mezi uživatelem služby a společnostní Google smlouva.

7.3 Dopad na e-mailing

Firma disponuje poměrně velkou databází kontaktů na své zákazníky. Problémem je, že je potřeba jasně stanovit dobu, po kterou bude e-mail skladován, a požádat všechny v databázi kontaktů o nový souhlas. Tímto krokem přijde firma o značnou část kontaktů, a jelikož se jedná o součást úspěšné reklamní strategie, může tento problém v budoucnu způsobit nedostatek předmětů k prodeji. Jedná se o to, že reklamní sdělení je cíleno spíše na starší lidi, kteří hojně využívají e-maily a jsou hlavními zásobovateli předměty.

ZÁVĚR

Diplomová práce se zabývá implementací GDPR a jeho dopady na procesy ve firmě antikvarium s.r.o. Nařízení jako takové se týká všech institucí zpracovávajících osobní údaje, proto je toto téma velmi často skloňované v médiích. Ta vytvořila mediální bublinu kolem GDPR, jak můžeme vidět z grafu. Informace publikované o problematice byly často zkreslené a přehnané.



Obr. 16. Vyhledávání pojmu GDPR [21]

V práci jsou využity myšlenky a poznatky z konferencí o GDPR. Hlavní inspirací byly výklady nařízení od advokátní kanceláře Elegal, která se problematikou ochrany osobních údajů zabývá již od začátku. Pro splnění všech cílů práce bylo nastudováno Obecné nařízení o ochraně osobních údajů, avšak omezením této práce jsou autorovy výklady. Ty se liší i mezi právníky samotnými, proto bylo vždy přikloněno k výkladům, které měli nejvyšší shodu. Procesy jsou zpracovány ve firmě, v níž má autor práce praxi a výhodou je znalost většiny procesů, a také samotných majitelů, se kterými byly všechny procesy ve firmě diskutovány.

Nové nařízení Obecné nařízení o ochraně osobních údajů oproti starému zákonu č. 101/2000 Sb. v mnoha ohledech zpřísňuje samotné zpracování. Toto tvrzení bylo potvrzeno v procesní analýze, kde současné opatření, nutno poznamenat v souladu se zákonem č. 101/2000 Sb., je v mnoha ohledech nedostačující. Jedná se o zpřísnění informativní povinnosti nebo přidání nových procesů v podobě výmazu osobních údajů na žádost a přenos osobních údajů na žádost zákazníka.

Hlavním cílem práce je navrhnout procesní opatření pro implementaci GPDR. Pro splnění cíle byla provedena procesní analýza. Výstupem analýzy je zjištění míst v procesu, kde jsou nutné změny pro splnění všech bodů legislativy. Byl zjištěn dopad směrnice na

většinu procesů ve firmě. Jmenovitě se jedná o prodej předmětů, inovace, propagace, informační technologie, nabídka předmětů, customer care, výdejna, výkup předmětů a lidské zdroje. Změny se dotknou hlavně zpracování dat právním titulem souhlas, ta jsou potřeba pro propagaci firmy. Otazníkem je pořád nařízení ePrivacy, které by mělo ke konci letošního roku vejít v platnost. To upravuje zásady používání cookies. Jak s cookies nakládat definuje i GDPR, ale bylo zjištěno, že požadavky jsou technicky těžko proveditelné a ne všechny instituce by byly schopny tento problém vyřešit. Proto postačí detailnější popis umístěný na vyskakovací liště při vstupu na e-shop.

Směrnice dává subjektům nová práva. S tím jsou spojeny i nově vzniklé procesy, kdy subjekt požádá o výmaz nebo o přenos osobních údajů. Smazání osobních údajů značně závisí na právním titulu zpracování. Firma je ze zákona povinna skladovat účetní doklady 10 let, takže osobní údaje, které firma musí skladovat ze zákonné povinnosti, nemůže vymazat. V takovém případě jsou jasně oznámeny důvody nevyhovění žádosti o výmaz všech dat. Další se vzniklých procesů je ohlášení o úniku dat do 72 hodin příslušnému úřadu. V minulosti se stalo, že firmy své úniky osobních údajů nezveřejňovali a jejich zákazníci se dozvěděli o úniků až z médií. Ohlášení do 72 hodin má zamezit takovému scénáři.

Součástí práce je pět hlavních cílů, jimiž jsou:

- definování základních pojmů spojených GDPR,
- specifikování možností implementace,
- vyhodnocení současných podmínek ve firmě,
- procesní opatření,
- a jako poslední jsou zhodnoceny dopady na firmu.

První cíl byl splněn pomocí analýzy dokumentu GDPR platného od 25. 5. 2018. V první části jsou rozebrány zásadní pojmy pro porozumění problematiky, jako jsou osobní údaje a jejich druhy, právní tituly pro zpracování osobních údajů, správce a zpracovatel. Poslední jmenované pojmy jsou porovnány, aby bylo jasné, za jakých podmínek je firma zpracovatelem a správcem. Část právní vymezení definuje příčiny, jež vedly k vytvoření nové směrnice o GDPR.

Specifikování možností implementace je cíl druhý. V části jsou popsány možné postupy, jimiž lze implementace docílit. Pro praktickou část implementace byly zvoleny metody analýzy současné situace a procesní analýzy.

Cíl analyzování současné situace je splněn pomocí analýzy současného stavu identifikující všechny procesy ve firmě. Na tyto procesy je provedena procesní analýza ukazující na místa, kde je nutno nasadit opatření pro splnění podmínek směrnice.

Předposledním cílem jsou procesní opatření pro implementaci GDPR. Zde jsou formovány a popsány procesy, které nově vzniknou nebo které je nutné upravit. Bylo zjištěno, že nově vzniklých procesů nebude tolik, kolik se předpokládalo na počátku. Spíše se jedná o úpravy stávajících procesů, které nevyhovují současnému nařízení. Nejčastějším úkonem pro úspěšnou implementaci je úprava nebo přidání informativní povinnosti na místa, kde jsou zpracovávány osobní údaje.

Poslední cíl hodnotí dopady GDPR na firmu. Kapitola upozorňuje na možné zvýšené náklady týkající se marketingu. Po 25. 5. 2018 nebudou moci být zpracovávány údaje v takovém množství jako doposud bez souhlasu návštěvníka webu. To povede k vyšším nákladům na propagaci. Firma bude cílit na větší skupinu lidí a tím budou reklamní kampaně méně účinné. Dalším problémem je e-mailing. Ten tvoří spolu s PPC úspěšnou osvědčenou strategii propagace. Současná databáze kontaktů bude muset být promazána, jelikož ti, kteří neobnoví souhlas se zasíláním reklamního sdělení, budou muset být z databáze odstraněni. Další mazání kontaktů bude muset být provedeno po uplynutí doby zpracování. Ukáže se až v budoucnu, jestli firma tímto krokem přijde o své zákazníky či nikoliv.

Autor práce se snažil zahrnout celou problematiku GDPR v co největším rámci. Nachází se zde několik částí, jež budou muset být prodiskutovány v budoucnu. Problematika cookies bude vyřešena s příchodem nové směrnice ePrivacy ke konci roku 2018 a ovlivní tím i fungování Úřadu pro ochranu osobních údajů.

SEZNAM POUŽITÉ LITERATURY

[1] *Mezinárodní pakt o občanských a politických právech*[online]. Praha: United Nations, 2016 [cit. 2018-05-11]. Dostupné z: http://www.osn.cz/knihovna/dokumenty/osn/

[2] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů* [online]. Praha: EU, 2016 [cit. 2018-05-11]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp ?id_org=200144&id=1751&n=pojem%2Dosobni%2Dudaj

[3] SLÁDEČEK, Vladimír. *Obecné správní právo.* 3., aktualizované a upravené vydání. Praha: Wolters Kluwer ČR, 2013

[4] *Správce, zpracovatel* [online]. Praha: Úřad pro ochranu osobních údajů., 2017 [cit. 2018-05-11]. Dostupné z: https://www.uoou.cz/7-spravce-zpracovatel/d-27278

[5] *Kompletní znění GDPR v českém překladu jako Obecné nařízení o ochraně osobních údajů* [online]. Praha: EU, 2017 [cit. 2018-05-11]. Dostupné z: https://www.gdpr.cz/gdpr/kompletni-zneni-gdpr/

[6] *Zákon č. 101/2000 Sb., o ochraně osobních údajů* [online]. Praha: ÚOOÚ, 2000 [cit. 2018-05-11]. Dostupné z: https://www.uoou.cz/files/101_cz.pdf

[7] PRÁVNÍ TITULY. *Novinky GDPR* [online]. Praha: Odborný deník, 2017 [cit. 2018-05-13]. Dostupné z: https://www.novinkygdpr.cz/pravni-tituly/

[8] Právní tituly zpracování osobních údajů a nejčastější chyba při implementaci GDPR. *Advokátní kancelář JURÁŇ* [online]. Praha: Advokátní kancelář JURÁŇ, 2017 [cit. 2018-05-13]. Dostupné z: http://www.advokat-juran.cz/blog/86-gdpr-prehledne-2-dil-pravni-tituly-zpracovani-osobnich-udaju-a-nejcastejsi-chyba-pri-implementaci-gdpr

[9] Slovníček nejdůležitějších pojmů. *ÚOOÚ* [online]. Praha: ÚOOÚ, 2017 [cit. 2018-05-13]. Dostupné z: https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617/p1=2617

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

[11] VOJTĚCH ŠIMÍČEK (ED.). *Právo na soukromí* [online]. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011 [cit. 2018-05-13]. ISBN 80-210-5449-2.

[12] POLČÁK, Radim. *Právo na internetu* [online]. Brno: Computer Press, 2007 [cit. 2018-05-13]. ISBN 80-251-1777-4.

[13] 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. *Eurlex* [online]. Brusel: EU, 1994 [cit. 2018-05-13]. Dostupné z: http://www.eurlex.cz/dokument.aspx?celex=31995L0046

[14] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů* [online]. Praha: Wolters Kluwer, 2017 [cit. 2018-05-13]. Praktický komentář. ISBN 978-807-5527-653.

[15] Transparency report. *Transparency report* [online]. San Francisco: Google, 2017 [cit. 2018-05-13]. Dostupné z: https://transparencyreport.google.com

[16] Implementace GDPR. *SPMO* [online]. Praha: CATANIA GROUP, 2017 [cit. 2018-05-13]. Dostupné z: https://spmo.cz/wp-content/uploads/2017/07/Implementace-GDPR-e-kniha.pdf

[17] Pověřenec pro ochranu osobních údajů dle nařízení GDPR. *Epravo* [online]. Praha: epravo, 2017 [cit. 2018-05-13]. Dostupné z: https://www.epravo.cz/top/clanky/poverenec-pro-ochranu-osobnich-udaju-dle-narizeni-gdpr-nove-pokyny-wp29-k-vykonu-funkce-104829.html

[18] VESELÁ, Lucie. *Determinanty adopce elektronické výměny dat*. Brno, 2017. Disertační. Mendelova univerzita. Vedoucí práce Doc. Ing. Lea Kubíčková, Ph.D.

[19] GDPR a pojištění kybernetických rizik. *Modul Servis* [online]. Praha, 2018 [cit. 2018-05-13]. Dostupné z: http://www.modulservis.cz/2018/02/15/gdpr-a-pojisteni-kybernetickych-rizik/

[20] Obchodní rejstřík. *Ministerstvo spravedlnosti České republiky* [online]. Praha, 2018 [cit. 2018-05-13]. Dostupné z: https://or.justice.cz/ias/ui/rejstrik

[21] Google Trends. *Google Trends* [online]. San Francisco, 2018 [cit. 2018-05-13]. Dostupné z: https://trends.google.com/trends/explore?q=GDPR

[22] Privacy by Design. *IPC* [online]. Toronto, 2018 [cit. 2018-05-13]. Dostupné z: https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

[23] Ochrana osobních údajů. *Česká pošta* [online]. Praha, 2018 [cit. 2018-05-13]. Dostupné z: https://www.ceskaposta.cz/o-ceske-poste/kontakty/ochrana-osobnich-udaju

[24] ŘEPA, Václav. *Podnikové procesy: Procesní řízení a modelování, 2., aktualizované a rozšířené vydání*. Praha: Grada Publishing, 2007. ISBN 8024767228.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EU	Evropská unie.
GDPR	General Data Protection Regulation.
IČO	Identifikační číslo organizace.
ID	IDentification.
IT	Informační Technologie
DPO	Data Protection Officer
PPC	Pay Per Click
MHD	Městská hromadná doprava.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK