Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Ochrana osobních údajů a aplikace GDPR

Martin Bartošek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Bartošek

Systémové inženýrství a informatika
Informatika

Název práce

Ochrana osobních údajů a aplikace GDPR

Název anglicky

Personal data protection and implementation of GDPR

Cíle práce

Cílem této diplomové práce je analyzovat aktuální postupy používané při zpracování osobních údajů a provést jejich porovnání s aktuálními legislativními nařízeními, především pak s GDPR. Práce bude zaměřena hlavně na používané systémy ve vybraných firmách a bude se zabývat uchováváním dat, jejich zpracováváním, jejich dostupností a povinnostmi firem s nimi nakládajícími. Dílčí části práce se budou zabývat analýzou používaných technologií a právních náležitostí s nimi spojenými, právně konzultačními službami poskytovanými třetími stranami a nově zavedenou funkcí pověřence pro ochranu osobních údajů. Jedním z výstupů práce bude tvorba pomůcky pro kontrolu správnosti používaných systémů z hlediska platné legislativy a pro případné nalezení validních alternativ.

Metodika

Teoretická část práce se bude zabývat tématikou osobních údajů, jejich ochrany a možnými následky jejich ztráty, poškození, či odcizení. V dílčí části budou řešeny zákony vztahující se na osobní údaje a jejich zpracování a bude obsahovat souhrn důležitých pojmů. Při tvorbě práce bude využito odborné a vědecké literatury a zdrojů dostupných online. Práci bude dále tvořit analýza hrozeb, kterým mohou být osobní údaje vystaveny a postupů používaných při prevenci těchto rizik.

Praktická část diplomové práce se bude zabývat používanými postupy ve vybrané skupině firem a jejich komparací s postupy předepsanými právními nařízeními (např.způsoby anonymizace). Dále se tato část bude zabývat rozborem nákladů vynaložených na zavedení validních postupů a jejich možnými alternativami a zefektivněním.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

osobní údaje, GDPR, internet, ochrana dat

Doporučené zdroje informací

NEZMAR, L. GDPR. praktický průvodce implementací. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.

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

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

ŽŮREK, J. Praktický průvodce GDPR. Včetně úplného znění GDPR. Olomouc: ANAG 2018. ISBN 978-80-7554-152-9.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 20. 03. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Ochrana osobních údajů a aplikace GDPR" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 20.3.2020 _____

Poděkování

Rád(a) bych touto cestou poděkoval Václavu Lohrovi, Ph.D. za konzultace a pomoc při výběru podkladů důležitých pro vypracování bakalářské práce

Ochrana osobních údajů a aplikace GDPR

Abstrakt: Tato diplomová práce analyzuje aktuálně používané postupy zpracování osobních údajů a porovnává je s platnými legislativními nařízeními jako je GDPR. Hlavní část práce se soustředí na systémy používané ve vybraných firmách a zabývá se sbíráním a uchováváním dat a jejich následným zpracováváním jakožto i povinnostmi firem s nimi nakládajícími. Dílčí cíle práce se zabývají například používanými technologiemi, konkrétními zásadami, které je třeba dodržovat nebo nově zavedenou funkcí pověřence pro ochranu osobních údajů.

Rešeršní část práce se zabývá tématikou osobních údajů a jejich ochrany a podrobněji probírá zákony, které se na zpracování dat vztahují. Ústřední pozici mezi těmito nařízeními pak zaujímá GDPR. Při tvorbě práce bylo využito odborné, vědecké a právnické literatury jakožto i zdrojů dostupných online. Práci se dále zmiňuje o některých hrozbách, kterým mohou být osobní údaje vystaveny, příkladech dřívějších úniků jakožto i o postupech používaných při prevenci těchto rizik.

Praktická část diplomové práce se zabývá používanými postupy ve vybraných odvětvích (primárně bankovnictví a hostingové firmy) a jejich porovnáním s těmi předepsanými právními nařízeními. Tato část používá metody jako dotazníkové šetření, polostrukturované rozhovory a přímé pozorování.

Klíčová slova: osobní údaje, GDPR, internet, ochrana dat, Implementace GDPR, hodnota osobních údajů

Personal data protection and application of GDPR

Abstract: This thesis analyzes currently used procedures of personal data processing and compares them with valid legislative regulations such as GDPR. The main part of the thesis is focused on systems used in selected companies and deals with the collection and storage of data and their subsequent processing as well as the obligations of companies dealing with them. Partial objectives of the thesis deal with, for example, the technologies used, the specific guiding principles or the newly introduced function of the Data Protection Officer.

The research part of the thesis deals with the topic of personal data and their protection and discusses in more detail the laws that apply to data processing. GDPR occupies the key position among these regulations. The work was made using scientific and legal literature as well as resources available online. The work also mentions some of the threats to which personal data may be exposed, examples of past leaks, as well as procedures used to prevent these risks.

The practical part of the thesis deals with the procedures used in selected sectors (primarily banking and hosting companies) and their comparison with those prescribed by legal regulations. This part uses methods like questionnaire survey, semi-structured interviews and direct observation.

Keywords: personal data, GDPR, internet, data protection, GDPR implementation, value of personal data

Obsah

1 Úvod **13**

2 Cíl práce a metodika **14**

2.1 Cíl práce 14

2.2 Metodika 14

3 Teoretická východiska **15**

3.1 Hodnota osobních údajů 15

3.1.1 Hodnota pro online platformy 15

3.1.2 Hodnota pro firmy 15

3.1.3 Benefity pro spotřebitele 16

3.2 Obecné nařízení o ochraně osobních údajů 16

3.3 Vymezení pojmů 17

3.3.1 Osobní údaj 17

3.3.2 Zpracování 19

3.3.3 Profilování 20

3.3.4 Pseudonymizace 20

3.3.5 Správce 21

3.3.6 Zpracovatel 21

3.3.7 Souhlas 22

3.3.8 Porušení zabezpečení 22

3.3.9 Genetický údaj, biometrický údaj, zdravotní stav 23

3.4 Zásady zpracování 24

3.4.1 Zásada zákonnosti 24

3.4.2 O korektnosti a transparentnosti 25

3.4.3 Účelového omezení 26

3.4.4 Minimalizace 27

3.4.5 Přesnosti 28

3.4.6 Omezení uložení 28

3.4.7 Anonymizace 29

3.4.8 Integrity a důvěrnosti 30

3.4.9 Odpovědnosti 30

3.5 Zvláštní podkategorie osobních údajů 30

3.5.1 Citlivé údaje 30

3.5.2 Údaje o trestní činnosti 32

3.5.3 Zpracování nevyžadující identifikaci 32

3.6 Práva subjektu údajů 33

3.6.1 Postupy pro komunikaci se subjektem ... 33
3.6.2 Informace a přístup k údajům ... 34
3.6.3 Práva na opravu a výmaz ... 35
3.6.4 Práva týkající se se automatizovaných systémů a právo vznést námitku ... 36
3.7 Správce a zpracovatel ... 37
3.7.1 Obecné povinnosti ... 37
3.7.2 Zabezpečení údajů ... 38
3.7.3 Posouzení vlivu zpracování ... 39
3.7.4 Pověřenec pro ochranu osobních údajů ... 41
3.7.5 Kodexy chování ... 43
3.8 Předávání údajů do zahraničí ... 43
3.8.1 Předání na základě rozhodnutí o odpovídající ochraně ... 44
3.8.2 Předání na základě poskytnutých záruk ... 44
3.8.3 Výjimky pro specifické situace ... 45
3.9 Právní ochrana, odpovědnost a sankce ... 45
3.10 Implementace GDPR ... 47
3.10.1 GAP analýza ... 47
3.11 Rizika a jejich hodnocení ... 48
3.12 IT technologie ... 50
3.12.1 Reprografická zařízení ... 50
3.12.2 Další koncová zařízení ... 50
3.12.3 Mazání dat ... 52
3.13 Kybernetická bezpečnost ... 52
3.14 Document Management System ... 53
3.15 Zabezpečení Wi-Fi ... 54
3.16 Hesla a práce s nimi ... 54
3.16.1 Heslová politika ... 54
3.16.2 Hashování ... 55
3.17 Nebezpečí virů ... 56
3.18 Online aspekty ... 57
3.19 Příklady dřívějších prohřešků ... 58

4 Vlastní práce ... 60
4.1 Posuzování ... 60
4.1.1 Sběr informací ... 60
4.1.2 Hodnocení jednotlivých kritérií ... 63
4.1.3 Úprava použitých postupů po absolvování diplomantského semináře ... 65
4.2 Zkoumané firmy ... 65
4.2.1 Výzkumná agentura STEM/MARK ... 65

4.2.2 Alza ... 66
4.2.3 Českomoravská stavební spořitelna – centrála ... 69
4.2.3.1 Právní stránka ... 69
4.2.3.2 Bezpečnostní politika firmy ... 71
4.2.4 ČSOB ... 72
4.2.5 Air/Bank ... 74
4.2.6 Komerční banka ... 76
4.2.7 Ignum ... 77
4.2.7.1 Úvodem ... 77
4.2.7.2 Veřejně dostupné informace ... 78
4.2.7.3 Další právní a organizační charakteristiky ... 79
4.2.7.4 Uchovávané údaje ... 79
4.2.7.5 Zabezpečení ... 80
4.2.7.6 Sdělování informací a změna dat ... 81
4.2.7.7 Zaměstnanci ... 81
4.2.7.8 Kamerový systém ... 82
4.2.7.9 Řešení bezpečnostních incidentů a používané technologie ... 82
4.2.7.10 Předávání údajů dalším správcům a zpracovatelům ... 83
4.2.7.11 Ke GAP analýze a Posouzení vlivu na ochranu osobních údajů84
4.2.7.12 Zákonnost, korektnost, transparentnost a účelové omezení ... 85
4.2.7.13 Minimalizace, přesnost a omezení uložení ... 85
4.2.7.14 Integrita a důvěrnost ... 85
4.2.7.15 Přístup k právům subjektů ... 86

5 Zhodnocení výsledků ... 87
5.1 Použité metody ... 87
5.2 Dostupnost potřebných informací ... 87
5.3 Implementace napříč zkoumanými firmami ... 88
5.3.1 Bankovnictví ... 88
5.3.2 Internetový obchod ... 89
5.3.3 Hostingová firma ... 90
5.3.4 Výzkumná agentura a další ... 91

6 Závěr ... 92

7 Seznam použitých zdrojů ... 94

8 Přílohy 102
8.1 Příloha 1 - Grafy příjmů z reklam společností Google a Facebook 102
8.2 Příloha 2 - Vzor Identifikace zpracování 103
8.3 Příloha 3 – Webové stránky firem a komunikace s nimi 106
8.3.1 Stemmark 106
8.3.2 Českomoravská stavební spořitelna 107
8.3.3 Alza 110
8.3.4 ČSOB 112
8.3.5 Komerční Banka 120
8.3.6 AirBank 121
8.3.7 Ignum 122

Seznam obrázků

Obrázek 1 - Čas na prolomení MD5 56
Obrázek 2 - Průměrný čtvrtletní příjem Googlu z reklam na jednoho uživatele ... 102
Obrázek 3 - roční příjem z reklam společnosti Google 102
Obrázek 4 - Roční příjem Facebooku z reklam na jednoho uživatele 103
Obrázek 5 - Vzor pro identifikaci zpracování část 1 104
Obrázek 6 - Vzor pro identifikaci zpracování část 2 104
Obrázek 7 - Vzor pro identifikaci zpracování část 3 106
Obrázek 8 - STEM/MARK – informace o zpracování 106
Obrázek 9 - Českomoravská stavební spořitelna – umístění odkazu 107
Obrázek 10 - Českomoravská stavební spořitelna – struktura informací 109
Obrázek 11 - Alza.cz - informace o zpracování 110
Obrázek 12 - Alza.cz - dotazovací formulář 110
Obrázek 13 - Alza.cz - automatická odpověď 111
Obrázek 14 - Alza – ukázka vyžádaných dat 111
Obrázek 15 - Alza – odpověď na dotazník 111
Obrázek 16 - ČSOB umístění odkazu 112
Obrázek 17 - ČSOB – Informace o zpracování 113
Obrázek 18 - ČSOB žádost o údaje 115
Obrázek 19 - ČSOB – přehled údajů 1 116
Obrázek 20 - ČSOB – přehled údajů 2 117
Obrázek 21 - ČSOB – přehled údajů 3 118

Obrázek 22 - ČSOB Odpověď na žádost 119
Obrázek 23 - KB umístění odkazu 120
Obrázek 24 - KB informace o zpracování 120
Obrázek 25 - AirBank – Odpověď na dotazy 121
Obrázek 26 - Obrázek 26 - IGNUM – Umístění odkazu 1 122
Obrázek 27 - IGNUM – umístění odkazu 2 123
Obrázek 28 - IGNUM – souhlas s podmínkami 124

Seznam tabulek

Tabulka 1 - PZH kritéria 49
Tabulka 2 - PZH hodnocení rizika 49
Tabulka 3 - Ignum – Kritéria pro provedení DPIA 84

Seznam použitých zkratek

- Nařízení = GDPR = Obecné nařízení o ochraně osobních údajů = General Data Protection Regulation
- ÚOOÚ = úřad pro ochranu osobních údajů

1 Úvod

Už před příchodem jedenadvacátého století a s ním spojeným rozmachem internetu, neustále se rozvíjejícími počítačovými technologiemi a nástupem sociálních sítí můžeme najít důvody k ochraně osobních údajů. Nyní však díky těmto faktorům a mnoha dalším toto téma nabývá na daleko větší důležitosti než dříve. Ztráta osobních údajů se může na člověku projevit širokou škálou negativních důsledků. Relativně snesitelným případem může být například lavina nevyžádané pošty, ale může dojít i k mnohem závažnějším dopadům jako je ztráta údajů o platební kartě následovaná zmizením velkého finančního obnosu, nebo k extrémním případům jako ke krádeži identity a nesením odpovědnosti za kriminální činnost, která byla spáchána jménem okradené osoby.

Kvůli těmto a mnoha dalším hrozbám již bylo ve snaze omezit jejich výskyt vydáno mnoho zákonů, u nás například zákon na ochranu osobních údajů, nebo zákon o ochraně autorských práv. Vzhledem ke členství České republiky v Evropské Unii nabylo relativně nedávno na účinnosti také Obecné nařízení o ochraně osobních údajů (podle anglického názvu označované zkratkou GDPR) které si dává za cíl sjednotit přístup členských států k této problematice. Navzdory tomu, že se zásadní principy a mechanismy dosud zavedených právních norem příliš zásadně nemění a pro firmy, které zpracovávali osobní údaje v souladu se zákonem o ochraně osobních údajů, by teoreticky nemělo být zajištění souladu s tímto nařízením příliš náročné, v praxi dochází často ke komplikacím.

V této diplomové práci bude projednáváno především právě nařízení GDPR a jeho praktická aplikace na různé aspekty provozu firem a dalších institucí, které se zpracováním osobních údajů zabývají.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této diplomové práce je analyzovat aktuální postupy používané při zpracování osobních údajů a provést jejich porovnání s aktuálními legislativními nařízeními především pak s GDPR. Práce je zaměřena hlavně na používané systémy ve vybraných firmách a zabývá se uchováváním dat, jejich zpracováváním, jejich dostupností a povinnostmi firem s nimi nakládajícími. Dílčí cíle práce se zabývají analýzou používaných technologií a právních náležitostí s nimi spojenými, jakožto i právně konzultačních služeb poskytovaných třetími stranami a nově zavedené funkce pověřence pro ochranu osobních údajů. Jedním z výstupů práce je tvorba pomůcky pro kontrolu správnosti používaných systémů z hlediska platné legislativy a pro případné nalezení validních alternativ.

2.2 Metodika

Teoretická část práce se zabývá tématikou osobních údajů, jejich ochrany a možnými následky jejich ztráty, poškození, či odcizení. Práce se dále zabývá zákony vztahujícími se na osobní údaje a jejich zpracování, jako je například GDPR a obsahuje souhrn důležitých pojmů. Při tvorbě práce bylo využito odborné a vědecké literatury jakožto i zdrojů dostupných online. Práci dále tvoří analýza hrozeb, kterým mohou být osobní údaje vystaveny a jakožto i postupů používaných při prevenci těchto rizik.

Praktická část diplomové práce se zabývá používanými postupy ve vybrané skupině firem a jejich komparací s postupy předepsanými právními nařízeními (způsoby anonymizace, převodník identifikátorů). Dále se v této části rozebírají náklady vynaložené na zavedení validních postupů a jejich možnými alternativami a zefektivněním.

3 Teoretická východiska

3.1 Hodnota osobních údajů

Vzhledem k tomu, že osobní údaje vytvářejí celkem značnou ekonomickou hodnotu pro digitální trh, lze je mimo jiné z určitého úhlu pohledu považovat za ekonomická aktiva. (Nezmar, 2017 str. 20) Toto je velmi dobře vidět například u online platforem fungujících jako zprostředkovatel dat uživatelů a následně je prodávajících reklamním firmám. Tyto firmy pak mohou tyto informace analyzovat a využít pro zefektivnění personalizovaných reklam šitých na míru zákazníkovi.

3.1.1 Hodnota pro online platformy

Firmy jako například Google a Facebook využívají nabyté informace pro vylepšení svých služeb a tím pádem i ke zvýšení spokojenosti svých zákazníků. Dále je jich často využíváno k již zmiňovaným personalizovaným reklamám. Facebook zde využívá demografických údajů a osobních charakteristik jako je věk, pohlaví, zájmy nebo postoje jednotlivých uživatelů. Google pak využívá souborů cookies zaznamenávajících typy stránek, které uživatelé navštěvují, a následně je shlukuje do určitých skupin sloužících jako základ pro cílenou reklamu. Vzhledem k tomu, že obě zmiňované firmy jsou k dispozici zdarma, jejich hlavní příjem se skládá především z reklamy. (Nezmar, 2017 str. 20) Pro lepší představu, v letech 2015-2016 se průměrný čtvrtletní přínos z reklam na uživatele pohyboval kolem 6 dolarů. (Statista, 2019) Roku 2018 pak jen na reklamách Google utržil 116,32 miliard dolarů. (Statista, 2019) Co se Facebooku týče, roční výnos z reklam za jednoho uživatele v roce 2018 činil 24,96 dolarů. (Statista, 2019) (Grafy k dispozici v příloze č.1)

3.1.2 Hodnota pro firmy

Ze zpracování osobních údajů mohou dále firmy těžit i tak, že monitorují aktuální preference potenciálních zákazníků a případným uzpůsobením nabídek přímo na míru. Dalšími relevantními faktory jsou například recenze produktů, komentáře na sociálních médiích či údaje o použití produktů umožňující lepší zaměření na výzkum a inovace. Jako firmu úspěšně využívající osobní údaje za účelem zabezpečení internetových plateb je pak

možno uvést například PayPal. (Nezmar, 2017 str. 23) V odvětvích, kde tolik nejde o finanční stránku věci, pak není na škodu zmínit využití osobních údajů sanitkami a nemocnicemi.

3.1.3 **Benefity pro spotřebitele**

Přestože se při diskusích o zpracování osobních údajů z ohledu na samotné subjekty většinou do popředí dostávají hlavně negativa, nesmíme zapomenout, že tato činnost může mít i benefity. Již zmíněno bylo například zdravotnictví a pozitivních aspekty cílené reklamy. Dalšími poskytovanými výhodami jsou například slevy a odměny za členství.

Zajímavostí jsou pak také společnosti, které uživateli za možnost shromažďovat jejich údaje nabízejí určitý finanční obnos. Jako namátkové příklady lze zmínit Datacoup (Datacoup, 2019), Ocean Protokol nebo CitizenMe (CitizenMe, 2019). Tyto služby se však často potýkají s komplikacemi ať už v podobě ne zrovna lákavého finančního ohodnocení (BBC Capital, 2018) tak v podobě rychlého propadu hodnoty jimi nabízených tokenů (Cryptopotato, 2019).

Obecně lze pak říci, že uživatelé jsou ochotní svá data sdílet, když je jim jasně řečeno, jaké benefity jim daná služba na oplátku nabízí, přičemž preferují hlavně finanční odměny a slevy, ale nezavrhují ani zmíněné nabídky relevantních produktů. Z celkem pochopitelných důvodů pak upřednostňují poskytnutí například datum narození, bydliště a demografické informace před biometrickými údaji. (Microsoft, 2015)

3.2 **Obecné nařízení o ochraně osobních údajů**

GDPR (General Data Protection Regulation) představuje nový právní rámec ochrany osobních údajů v evropském prostoru, které má za cíl hájit práva občanů EU před neoprávněným zacházením s jejich údaji. GDPR se týká nejen všech firem a institucí, ale i online služeb a jednotlivců zpracovávajících osobní údaje. (GDPR, 2019)

Jako příklady dřívějších pokusů o vytvoření norem chránících soukromí můžeme uvést třebas nezávaznou směrnici OECD z roku 1980 která prvně definovala základní principy a mechanismy ochrany osobních údajů v podobě v jaké je používáme dnes. Přestože se nejednalo o závazné právní nařízení, ale spíše o návod, jak se k dané tematice stavit, měla tato směrnice znatelný celosvětový dopad.

Prvním opravdu závazným mezinárodním právním nástrojem v této kategorii pak byla až Úmluva č.108 (28. leden 1981), která dřívější směrnici dále rozvinula, a navíc se zabývala například otázkou přeshraničních toků informací. (Nulíček, 2018 stránky 57-58)

Co se pak týče ochrany osobních údajů z pohledu práva České republiky, právo na soukromí je vychází hlavně z několika ustanovení Listiny základních práv a svobod, dále se jím však zabývají například trestní zákoník, zákoník práce či zákon o elektronických komunikacích. (Poslaneská sněmovna, 1992)

Jako poslední významnou směrnicí před samotným Nařízením GDPR můžeme označit směrnici 95/46/EU (24.10.1995), která sloužila jako nástroj standardizace ochrany dat napříč státy evropské unie a do českého zákona byla zavedena pomocí zákona o ochraně osobních údajů. (Nezmar, 2017 str. 14) Od doby jejího zavedení však došlo k výraznému technologickému pokroku, a tak poněkud ztratila na efektivnosti. (Nezmar, 2017 str. 28) Tento nedostatek má řešit právě Nařízení GDPR, které bylo původně vyhlášeno 27. dubna 2016 a nabylo účinnosti 28.5.2018 (Evropský parlament a rada - GDPR, 2016).

3.3 Vymezení pojmů

Proto aby bylo možné Nařízení správně aplikovat v praxi je nejprve nutné si upřesnit význam jednotlivých klíčových pojmů, které se v něm vyskytují. K tomuto účelu slouží Článek 4 Nařízení, který obsahuje základní definice významných pojmů.

3.3.1 Osobní údaj

„Osobní údaj“ Nařízení definuje jako veškeré informace o identifikované, nebo identifikovatelné fyzické osobě, přičemž za identifikovanou lze osobu prohlásit, pokud ji lze přímo, či nepřímo určit především odkazem na určitý identifikátor, jako je například jméno, identifikační číslo, síťový identifikátor, nebo pomocí zvláštních prvků fyziologické, genetické, psychické, ekonomické, kulturní, nebo společenské identity této osoby. (Evropský parlament a rada - GDPR, 2016 str. 33)

Tento pojem je naprosto kritický z důvodu, že Obecné nařízení o ochraně osobních údajů se vztahuje výlučně jen na zpracování informací, které lze jako osobní údaje označit, a nikoliv na jiné informace, byť by jejich zpracování mohl člověk považovat za zásah do soukromí (takové informace mohou však stále spadat do působnosti jiných zákonů).

Dřívější již poměrně široká definice pojmu je oproti zákonu na ochranu osobních údajů Nařízením rozšířena o lokační údaje, síťový identifikátor a genetický aspekt lidské identity. (Zákon č. 101/2000 Sb, 2017 str. 2)

Za osobní údaje se nepovažují jen samotné identifikační údaje, podle kterých lze danou osobu určit, ale i veškeré informace, které se jí týkají, i když jsou samy o sobě či v kombinaci s dalšími informacemi pro identifikaci nepoužitelné (například počet dětí nebo zůstatek na bankovním účtu). Dále není rozhodující, zda se jedná o údaje zcela pravdivé či přesně měřitelné (v tomto směru není významný rozdíl mezi datem narození a posouzením, zda je osoba důvěryhodným věřitelem) ani nezáleží na formátu zachycení dané informace (například písemně, nebo audiozáznamem). Pro to, aby se data dala považovat za osobní údaj, musí se týkat žijící fyzické osoby. Ochrana osobnostních práv zemřelých podobně jako ochrana dobrého jména právnických osob do působnosti Nařízení nespadá. (Žůrek, 2018 str. 42)

Důležité je také určit, jaká osoba se považuje za identifikovatelnou. K tomu v kontextu Nařízení dochází, když ji správce, zpracovatel, nebo kdokoliv další dokáže za vynaložení rozumného úsilí a s případným využitím jím drženými nebo veřejnými údaji dokáže určit. Jako příklad reálně propojitelné identifikace lze uvést shromažďování identifikačních čísel telefonů provozovateli obchodních center za účelem sledování návštěvnosti. Samotní provozovatelé obchodních center nemají reálnou možnost identifikovat vlastníky jednotlivých telefonů, ale například orgány zodpovědné za stíhání trestné činnosti si mohou od operátora vyžádat informace potřebné k následnému vyvození místa a času pohybu konkrétních osob. Z tohoto důvodu se i takovéto informace považují za osobní údaje. Jako případ, kdy je možnost identifikace nadměrně složitá a její možnost se považuje spíše za hypotetickou, lze uvést zveřejnění agregovaných údajů o chudobě v konkrétních obcích statistickým úřadem. Za předpokladu znalosti místních poměrů a při výskytu pouze malého množství chudých osob by je bylo teoreticky možno identifikovat, ale vzhledem k potřebnému úsilí se jedná o možnost spíše akademickou. (Nulíček, 2018 stránky 77-79)

Jedním z nových typů údajů zmiňovaných ve Článku 4 Nařízení je takzvaný síťový identifikátor. Do této kategorie spadá například IP adresa (i dynamická), nebo cookies, ale vzhledem k projednávání dalších právních nařízení, které budou mít v tomto odvětví před GDPR přednost, není jisté, jak se bude k jejich zpracování zákon v budoucnu stavět.

Z pohledu Nařízení jsou však tyto údaje považovány za osobní, ačkoliv se při určitém úhlu pohledu dá říci, že se dotýkají věci a nikoliv člověka.

Jako opak osobních údajů jsou považovány údaje anonymní neboli informace, které se netýkají určené či určitelné osoby (například údaje o počasí), a údaje anonymizované. Jako anonymizované údaje se chápou ty, které byli dříve přiřaditelné ke konkrétnímu člověku, ale po jejichž úpravě toho již dosáhnout nelze. V zásadě lze tedy říct, že stále platí definice ze zákona na ochranu osobních údajů. (Zákon č. 101/2000 Sb, 2017 str. 2)

3.3.2 **Zpracování**

Jako „zpracování“ se z pohledu Nařízení rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, která je prováděna pomocí či bez pomocí automatizovaných postupů (například shromažďování, zaznamenávání, uspořádání, strukturování, ukládání, upravování, vyhledávání, nahlížení, použití, zpřístupnění přenosem, šíření, řazení či kombinování, omezení, výmaz nebo zničení). (Evropský parlament a rada - GDPR, 2016 str. 33)

Definice zpracování údajů se nabitím platnosti Nařízení v zásadě nezměnila oproti té současné, která je uvedena v zákoně na ochranu osobních údajů. I nadále se tedy jedná o systematickou činnost prováděnou za konkrétním účelem, bez ohledu na to, zda je výsledku dosahováno manuálně, elektronicky, pomocí softwarových nástrojů, nebo kombinací těchto postupů. (Zákon č. 101/2000 Sb, 2017 stránky 2-3)

Za zpracování je nutno označit i jednorázovou činnost provedenou pro dosažení specifického účelu. Například se může jednat o vedení personální evidence pro účel plnění pracovněprávních smluv, ale i jednorázové vyhledání údajů v této evidenci a jejich kombinace s veřejně dostupnými údaji se pak považuje za další samostatné zpracování.

Je vhodné zmínit, že i v případech, kdy subjekt dobrovolně zveřejní své osobní údaje na internetu, nemělo by docházet k jejich zpracování, pakliže k tomu správce postrádá vhodný právní důvod. (Nezmar, 2017 str. 35)

Jako zpracování je však třeba brát i některé méně nápadné operace a postupy, které by na první pohled zdánlivě nevyužívají osobních údajů. Jako příklad lze uvést internetový obchod, který umístil Facebookovou službu tlačítka „like“ na své stránky a způsobil tak, že data návštěvníků stránek byla shromažďována a zasílána provozovateli Facebooku bez jejich svolení i v případě, že této funkcionality nikdy nevyužily.

V případech, kdy je s daty manipulováno, a přesto se z právního hlediska nejedná o zpracování jde většinou o nepravidelný nahodilý důsledek jiné činnosti, jako je například servis či oprava technických prostředků pro zpracování dat, kdy může dojít k nárazovému přístupu k datům. I v těchto situacích však v praxi často dochází k ošetření pomocí smlouvy o ochraně důvěrných informací NDA. (Nulíček, 2018 str. 86)

3.3.3 **Profilování**

„Profilování“ je v Článku 4 Nařízení definováno jako forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení osobnostních aspektů dané fyzické osoby. Zejména se pak jedná o rozbor či odhad aspektů týkajících se pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování a místa častého výskytu. (Evropský parlament a rada - GDPR, 2016 str. 33)

V obecné rovině lze tedy profilování označit jako zpracování osobních údajů za účelem získání prediktivních informací na základě vytvořeného profilu složeného z charakteristik, vlastností a preferencí neboli s cílem s významnou mírou pravděpodobnosti předpovídat chování daného člověka. Spektrum možných využití pro profilování je široké a zahrnuje například tvorbu informačního základu pro zobrazování cílené reklamy podle dříve navštívených internetových stránek. (Nulíček, 2018 str. 87) Dalším příkladem může být třebas jeho využití ve finančních službách pro posouzení schopností klienta splácet hypotéku, zhodnocení zdravotního stavu, nebo hodnocení pracovního výkonu. (Nezmar, 2017 stránky 32,93)

3.3.4 **Pseudonymizace**

Za „pseudonymizaci“ považujeme zpracování osobních údajů takovým způsobem, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací. Tyto dodatečné informace jsou dále uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby se předcházelo jejich přiřazení identifikované nebo identifikovatelné fyzické osobě. (Evropský parlament a rada - GDPR, 2016 str. 33)

Výběr údajů pro provedení pseudonymizace je částečně subjektivní, ale měly být vybrány všechny významné údaje jako například rodné číslo. Při pseudonymizaci méně významných údajů jako datum narození či poštovní směrovací číslo dochází často ke ztrátě

jejich analytické hodnoty, a proto by mělo dojít alespoň k zavedení odvozených použitelných forem jako rok narození, či větší poštovní oblast. (Nezmar, 2017 str. 115)

Důležitým rozdílem oproti anonymizaci je skutečnost, že se nejedná o proces nevratný, ale výsledná data je možné stále za použití doplňkových informací přiřadit ke konkrétním fyzickým osobám. Z tohoto důvodu se pseudonymizovaná data i nadále z pohledu Nařízení považují za osobní údaje. (Nulíček, 2018 str. 88)

3.3.5 **Správce**

„Správce“ je Nařízením definován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura či jiný subjekt, který sám nebo spolu s jinými stanovuje účely a prostředky zpracování osobních údajů. (Evropský parlament a rada - GDPR, 2016 str. 33)

Drobnou změnou oproti dosavadní definici ze zákona na ochranu osobních údajů je to, že v Nařízení není přímo řečeno, že správce se na zpracování podílí a zodpovídá za něj. Vzhledem k tomu, že tyto skutečnosti vyplívají z dalších článků Nařízení, jedná se o změnu spíše kosmetickou. I nadále tedy platí, že správcem je osoba na jejíž popud je činnost zahrnující zpracování osobních údajů vykonávána. (Zákon č. 101/2000 Sb, 2017 str. 3)

Za výjimku z tohoto pravidla lze považovat situaci, kdy je povinnost provádět zpracování osobních údajů subjektu uložena zákonem. Jedná se například o zaměstnavatele a jejich povinnost vést evidenci odpracované doby a úrazů, poskytovatele zdravotních služeb, obce a další podobné případy. (Nulíček, 2018 str. 90)

3.3.6 **Zpracovatel**

Jako „zpracovatel“ se rozumí fyzická, nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který pro správce vykonává samotné zpracování osobních údajů. Často jím bývá samotný správce. (Evropský parlament a rada - GDPR, 2016 str. 33)

Podobně jako u definice správce se oproti zákonu na ochranu osobních údajů zpracovatel až na drobné detaily příliš významně nemění. (Zákon č. 101/2000 Sb, 2017 str. 3)

3.3.7 **Souhlas**

Jako „souhlas“ Nařízení definuje jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým dává subjekt údajů najevo své svolení ke zpracování svých osobních údajů. (Evropský parlament a rada - GDPR, 2016 str. 34)

Oproti definici v zákoně na ochranu osobních údajů Nařízení nyní přímo požaduje, aby byl souhlas udělen prohlášením, či zjevným potvrzením. Rozdíl spočívá v tom, že nyní se za validní souhlas nebude považovat například nečinnost subjektu, nebo předvyplněné zaškrtávací pole, které subjekt údajů aktivně nevymaže. Jako další ukázku lze uvést internetové stránky používající cookies u kterých se za souhlas dříve považovalo jejich pouhé používání, ale nyní je nutné aktivní potvrzení od uživatele. (Nezmar, 2017 str. 131) Dále je vhodné podotknout, že zatímco dříve bylo poskytnutí souhlasu bráno jako nejvhodnější právní titul ke zpracování osobních údajů, nyní je tomu právě naopak a správce by měl upřednostnit jiné důvody, proč dané zpracování provádí. (Nulíček, 2018 str. 128) Důvodem k tomu je například to, že poskytnutý souhlas je vždy možno odvolat (správně by to mělo být možné za vynaložení stejného úsilí jako bylo jeho poskytnutí) a dále například také to, že správce je povinen si vést záznamy o tom kdo souhlas udělil, kdy a jak k tomu došlo, o čem všem byl subjekt údajů informován a zda nebyl souhlas již odvolán. (Nulíček, 2018 str. 155) (Žůrek, 2018 str. 78) Je vhodné dodat, že v případě, že mezi subjektem údajů a správcem existuje výrazná nerovnováha moci (například: správcem je orgán veřejné moci, či zaměstnavatel) je vysoká šance, že poskytnutý souhlas nebude považován za svobodný, není-li jej možno vyjádřit jednotlivě ke konkrétním operacím zpracování. Podobně tomu tak často je, jeli souhlas vyžadován k poskytnutí služby pro jejíž výkon není nezbytný. (Nezmar, 2017 str. 133) (Evropský parlament a rada - GDPR, 2016 str. 8)

3.3.8 **Porušení zabezpečení**

„Porušením zabezpečení osobních údajů“ se rozumí porušení zabezpečení vedoucí k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí či zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. (Evropský parlament a rada - GDPR, 2016 str. 34)

K porušení zabezpečení může dojít jak činností zvenčí (kybernetické útoky, průmyslová špionáž) tak zevnitř organizace (neoprávněné poskytnutí osobních údajů třetí

osobě zaměstnancem firmy) přičemž výsledek může být jak úmyslný, tak učiněný nevidomky (nahodilé neúmyslné zničení informací). Samotným zabezpečením a ohlašováním jeho případných narušení se zabývají články 32 až 34 Nařízení.

Porušení zabezpečení se dá hrubě rozdělit do tří kategorií: porušení důvěrnosti, porušení dostupnosti a porušení integrity. Do první skupiny spadá především neoprávněné či náhodné zveřejnění nebo zpřístupnění osobních údajů. Jako porušení dostupnosti lze uvést ztráta přístupu k údajům u osob, které k tomu mají oprávnění, nebo úplné zničení dat. Poslední kategorie pak zahrnuje náhodné či neoprávněné pozměnění uchovávaných údajů.

V případě, že je za narušení zodpovědná konkrétní osoba, může se navíc jednat o trestný čin neoprávněného nakládání s osobními údaji.

3.3.9 **Genetický údaj, biometrický údaj, zdravotní stav**

Jako „genetické údaje“ se rozumí údaje o zděděných či získaných genetických znacích, které poskytují jedinečné informace o fyziologii a zdraví konkrétní fyzické osoby a vyplývají z analýzy jejího biologického vzorku.

Nápodobně se „údaje o zdravotním stavu“ týkají tělesného a duševního zdraví fyzické osoby, a to včetně údajů o poskytnutých zdravotních službách, jelikož ty také o jejím zdravotním stavu vypovídají.

Nařízení dále definuje pojem „biometrické údaje“ jako údaje vyplívající z konkrétního technického zpracování, které se týkají fyzických a fyziologických znaků nebo znaků chování dané fyzické osoby potvrzující její jedinečnou identifikaci. Jako příklad Článek 4 uvádí zobrazení obličeje, nebo daktyloskopické údaje. (Evropský parlament a rada - GDPR, 2016 str. 34)

Vzhledem k tomu, že za genetické údaje lze považovat téměř jakýkoliv biologický vzorek obsahující DNA či RNA ať už se jedná o sliny, vlasy s kořínkem nebo krev, bylo by hypoteticky možné za správce a zpracovatele osobních údajů možno považovat kohokoliv kdo s tímto materiálem přijde do styku, byť by se jednalo například o pouhé umývání nádobí, nebo výměnu prostěradla s vypadanými vlasy. Vzhledem k absurdním situacím, ke kterým by takovýto extrém vedl, se za zpracování genetických údajů považuje až aktivní rozbor těchto vzorků umožňující získání informací o dané osobě například v laboratoři.

Velmi podobně je na tom zpracování biometrických údajů. Při pořízení kvalitního záznamu je možno získat například individuální a měřitelné parametry obličeje, údaje o oční

duhovce, tělesných proporcích, otisky prstů či chodidel, nebo dokonce styl chůze, hlas a rukopis. Dokud však nedochází ke zpracování těchto informací specifickými technickými prostředky, nebo systémy umožňující identifikaci člověka, nemělo by se z pohledu Nařízení jednat o zpracování biometrických údajů.

Do kategorie informací o zdravotním stavu spadají pak například karty pacientů, lékařské recepty, údaje zdravotních pojišťoven či záznamy o zakoupení léků a jiných zdravotnických produktů. Dále lze pak zmínit identifikátory přiřazené během poskytování zdravotní péče, výsledky testů anebo informace o nemocích. Dle nařízení sem patří i informace o předpokládaném budoucím zdravotním stavu subjektu údajů. (Nulíček, 2018 stránky 96-98)

3.4 Zásady zpracování

Mezi důležité principy obsažené v Obecném nařízení o ochraně osobních údajů patří zásady, kterými by se každý měl správce při nakládání s osobními informacemi řídit. Jelikož tyto zásady a mechanismy byli zahrnuty již ve dřívějších směrnicích a úmluvách, nejedná se o úplné novinky, ale i tak dochází u většiny z nich v rámci Nařízení k dalším úpravám a zpřesněním.

3.4.1 Zásada zákonnosti

Tato zásada stanovuje, že zpracování osobních údajů lze provádět pouze na základě jednoho z definovaných právních titulů a současně nesmí být v rozporu se zákonem.
Nařízením stanovené tituly jsou:

1. Subjekt údajů udělil souhlas se zpracováním pro jeden nebo více účelů.
2. Zpracování je nezbytné pro plnění smlouvy se subjektem údajů.
3. Zpracování je nezbytné pro plnění právních povinností správce.
4. Zpracování je nutné pro ochranu životně důležitých zájmů fyzické osoby.
5. Zpracování je nezbytné pro splnění úkolu prováděného v zájmu veřejnosti, či při výkonu veřejné moci.
6. Zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, pakliže nejsou v rozporu se zájmy nebo právy a svobodami subjektu údajů.

V případě, že zpracování probíhá podle bodu 6 dochází také k takzvanému Balančnímu testování, jehož účelem je komplexně posoudit váhu oprávněného zájmu oproti základním právům a svobodám. Během tohoto testování by měl správce provést posouzení váhy oprávněného zájmu, posouzení důsledků zpracování pro subjekty údajů, následné vyvážení těchto dvou faktorů, a nakonec přijmout dodatečné záruky pro ochranu osobních práv a svobod. (Nulíček, 2018 str. 108)

Jako protiprávní zpracování se rozumí případy, kdy ke zpracování dochází za nelegitimním či nelegálním účelem. Tento zákaz se nevztahuje jen na zpracování v rozporu se samotným Nařízením, ale i v rozporu s právním řádem obecně. Pokud tedy zpracování probíhá v souladu s Nařízením, ale porušuje například občanský zákoník, stále dochází k porušení zásady zákonnosti. Jako další příklad porušení této zásady je zpracování údajů bez platného titulu uvedeného v článku 6 Nařízení, nebo zpracování citlivých údajů bez naplnění některé z článkem 9 uváděných výjimek. (Nezmar, 2017 stránky 53-54)

Dále je vhodné dodat, že ačkoliv není zásada zákonnosti přímo uvedena v zákoně o ochraně osobních údajů, je stále zajišťována povinností správce zpracovávat údaje na základě zákonných titulů v §5 odstavci 2. (Zákon č. 101/2000 Sb, 2017 str. 4)

3.4.2 **O korektnosti a transparentnosti**

Pod těmito zásadami se rozumí povinnost správce být otevřený ohledně toho, jak je s osobními údaji nakládáno a zajistit maximální míru informovanosti subjektu údajů.

V praxi kombinace těchto dvou zásad vede k tomu, aby správce subjekt specifickým způsobem informoval o tom, v jakém rozsahu dochází ke zpracování údajů. Dále tyto zásady souvisí s povinností neodůvodněně neodpírat subjektu přístup k údajům a informovat ho v případě závažných porušení zabezpečení. (Nulíček, 2018 str. 108) (Žůrek, 2018 str. 61)

Jako příklad spravedlivého a transparentního zpracování lze uvést situaci, kdy dojde k uzavření smlouvy s mobilním operátorem s vědomím, že si společnost uchová jméno a adresu pro fakturaci. Porušením zásady by pak bylo, kdyby bez jakýchkoliv dalších kroků byla data předána sesterské společnosti za účelem zaslání nabídky pojištění. (Nezmar, 2017 str. 52)

Jako rychlý způsob ověření, zda jsou tyto zásady dodržovány lze posoudit, zda správce splňuje následující body:

- Je upřímný ohledně své identity.

- Sděluje, jak budou informace zpracovány a komu budou zpřístupněny.
- Zpracovává osobní údaje takovým způsobem, který bylo při jejich poskytnutí možno rozumně předpokládat.
- Nezpracovává údaje způsobem, který by na subjekt mohl mít neoprávněný negativní dopad.

3.4.3 **Účelového omezení**

Zásada účelového omezení až na výjimky zakazuje správci zpracovávat údaje za jiným účelem, než za jakým byly původně shromážděny. Tuto zásadu lze považovat za jednu z nejdůležitějších, jelikož se od stanoveného účelu nadále odvíjí například minimalizace a omezení uložení. (Žůrek, 2018 str. 63)

Je vhodné uvést, že pro zásadu účelového omezení existuje výjimka o takzvaném dalším zpracování. Pakliže se jedná o některý z následujících čtyř případů, je z pohledu nařízení povoleno:

- Archivace ve veřejném zájmu pro historické či statistické účely.
- Subjekt údajů poskytne dodatečný souhlas.
- Zpracování je založeno na právu členského státu, nebo EU a představuje nutné a přiměřené opatření v demokratické společnosti.
- Správce provedl posouzení slučitelnosti a výsledkem bylo, že nový a stávající účel jsou slučitelné.

Oproti aktuální definici se tato zásada nijak výrazně nemění. (Zákon č. 101/2000 Sb, 2017)

Za předpokladu, že není účel stanoven zákonem, je definujícím momentem veškerého dalšího zpracování stanovení účelu, které musí proběhnout nejpozději v momentě shromáždění údajů. Takto definovaný účel musí být určitý, výslovně vyjádřený a legitimní.

Účel musí být stanoven dostatečně určitě na to, aby z něj vyplívalo jak (ne)budou osobní údaje zpracovány a aby bylo možné určit, zda je tomu tak v souladu s Nařízením. V zájmu správce je vhodné vyvarovat s jak příliš specifickým definicím, kterými by se mohl do budoucna příliš omezit, tak definicím přehnaně obecným („marketingové účely“ je vhodné zúžit například na „zasílání nabídek produktů“). Dále je vhodné neslučovat dohromady více samostatných účelů (tímto se nerozumí upřesnění jednotlivých částí

jednoho rozsáhlejšího účelu jako například rozložení „ochrany práv a právních nároků“ na „evidence a archivace dokumentů, komunikace se smluvní stranou, případné soudní vymáhání apod.“). Vzhledem k tomu, že účel je nutno posuzovat v kontextu dané situace, jen málokdy je možné obecně prohlásit účel za příliš vágní, nebo dostačující ve všech případech. (Nulíček, 2018 str. 109)

Jak již bylo řečeno výše, je možné provádět i takové zpracování, za jehož účelem nebyla data původně shromážděna. Při prvotním hrubém posuzování, zda jsou nový a původní účel slučitelné lze dospět ke třem různým závěrům: Kompatibilita je na první pohled jasná (údaje o adrese a bankovních informacích jsou opakovaně zpracovávány v rámci dodávání předplacené služby či zboží), účely jsou jasně neslučitelné (e-shop začne náhle poskytovat slevy na zboží podle instalovaného operačního systému) a k ověření je nutná další analýza (Zde je přihlíženo například k povaze shromážděných údajů, vztahu mezi subjektem a správcem, možným důsledkům dalšího zpracování a existenci vhodných záruk.). (Nezmar, 2017 str. 58)

V některých případech jsou organizace osvobozeny povinnosti účel oznamovat. K těmto situacím dochází, když dochází ke zpracování ke zřejmému účelu (např. šachový klub zpracovává údaje za účelem organizování turnaje). (Nezmar, 2017 str. 56)

Obecně lze prohlásit, že pro soulad s Nařízením je nutné, aby si byli jak správce, tak zpracovatel dokonale vědomi, jaká data zpracovávají a jakého účelu se snaží dosáhnout.

3.4.4 **Minimalizace**

Podle této zásady by měl správce zpracovávat jen takové údaje, které jsou relevantní pro dosažení stanovených cílů, a to pouze v takovém rozsahu, který je pro naplnění účelu nezbytně nutný. Jako příklad porušení této zásady lze uvést situaci, kdy organizátor školení požaduje po účastnících rodné číslo, které dále používá jako jejich jedinečný identifikátor (posloužilo by jakékoliv přidělené číslo). Dále je pak možno uvést situaci, kdy inkasní agentura hledá konkrétního dlužníka a během tohoto procesu identifikuje několik osob stejného jména, které nemají s případem nic společného. Ideálním řešením je pak smazání většiny údajů těchto osob a ponechání pouze základního záznamu pro předejití opakovaného prověřování téže osoby. (Nezmar, 2017 str. 61)

Oproti zákonu o ochraně osobních údajů Nařízení tuto zásadu nijak výrazně nemění.

Tato konkrétní zásada stojí v určitém rozporu například s tvorbou big data analýz, které si kladou za cíl naopak shromáždit co největší množství údajů. V takovýchto případech je nutné již zpočátku jasně definovat účel, nalézt vhodný právní titul a důsledně plnit informační povinnost. Druhou možností je poskytnutá data pravidelně anonymizovat (tento přístup bohužel v některých případech může vést až ke znehodnocení dat, například pokud šlo o sledování vývoje v čase, kde nelze provést propojení mezi jednotlivými údaji). (Nulíček, 2018 str. 113)

3.4.5 **Přesnosti**

Zásada přesnosti stanovuje, že veškeré osobní údaje musí být přesné a aktuální. Správci pak připadá povinnost nesprávné údaje opravit nebo vymazat.

Pro upřesnění je nutno uvést, že údaje nemusejí být nezbytně pravdivé. Například v situacích, kdy subjekt údajů poskytl špatné informace, není správce zodpovědný za jejich pravdivost. Dalším důležitým faktorem v posuzování přesnosti je účel zpracování, jelikož v případech, kdy je postačující pouze přibližný údaj, není jeho zpracování považováno za porušení této zásady.

Co se samotného zajišťování přesnosti při shromažďování a následném zpracování týče, ani Nařízení ani zákon o ochraně osobních údajů nestanovuje v tomto ohledu, žádné konkrétní postupy. Aktuální přístup ÚOOÚ je takový, že v závislosti na rozsahu a okolnostech musí každý zpracovatel přijmout systém opatření, který zpracování chybných a nepřesných údajů bude předcházet. Ze zákona však nevyplívá žádná nutnost nepřetržité kontroly, ale pouze povinnost opravit věrohodně ověřené chyby. Pravidelnost kontroly by měla odpovídat možnému riziku vzniku újmy. Z pochopitelných důvodů pak není nutné aktualizovat záznamy určené k archivaci. (Nulíček, 2018 str. 115) Podobně tomu tak platí i u ukládání nesprávných informací jako například chybná lékařská diagnóza, jelikož je nutná pro vysvětlení pacientovy léčby a případných následných zdravotních komplikací. V takovýchto případech je pouze nutné poznamenat, že se jednalo o chybnou informaci. (Nezmar, 2017 stránky 63,66)

3.4.6 **Omezení uložení**

Podle zásady omezeného uložení je správce povinen smazat či anonymizovat veškeré osobní údaje, které již nepotřebuje pro účel, za kterým byly shromážděny.

Některé kategorie osobních údajů mohou být zároveň potřebné pro více účelů, pokud však dojde k tomu, že přestane být některá z těchto kategorií potřebná, mělo by dojít k jejímu smazání případně k anonymizaci (Žůrek, 2018 str. 64). Nařízení nestanovuje žádné konkrétní minimální a maximální lhůty, pouze vybízí k posouzení vztahu mezi délkou uložení a stanoveným účelem. Jako důvody ke včasnému mazání pak patří mimo samotnou ochranu práv subjektů i fakt, že při dlouhém uchovávání narůstá riziko, že údaje již nejsou přesné a aktuální, a musí být i nadále zajišťována bezpečnost jejich uložení. Jako příklad k délce uchovávání můžeme uvézt dvě podobné situace zahrnující kamerový systém s účelem zabraňování trestné činnosti. Pokud je takový systém instalován v bance, záznamy je možné uchovávat i několik týdnů, jelikož o případném podvodu se může oběť dozvědět až po delší dob. V případě restaurace se na případné krádeže a podobné incidenty přijde relativně rychle a záznam tedy stačí uchovávat jen krátkodobě. (Nezmar, 2017 stránky 66-68)

Pokud je to nutné pro dodržení podmínek korektnosti a transparentnosti, měl by být subjekt informován o tom, jak dlouhou dobu budou jeho data uchovávána (je možná i relativní definice typu „do ukončení poskytování služby“).

Tato zásada nevyplývá jen z Nařízení ale i ze zákona o ochraně osobních údajů a v praxi se významně neliší. (Zákon č. 101/2000 Sb, 2017 str. 3)

I zde pak platí výjimka o uchovávání za účelem historického a vědeckého výzkumu, nebo pro statistické účely. (Nulíček, 2018)

3.4.7 **Anonymizace**

Pakliže správce dat osobní údaje anonymizuje, z pohledu Nařízení dojde k podobnému výsledku, jako kdyby byly údaje úplně smazán, jelikož se nadále nepovažují za osobní údaje.

Vzhledem k tomu, že při dnešních technologických možnostech již není něco jako absolutní anonymizace občas možné, musí se při posuzování, zda je fyzická osoba identifikovatelná, přihlédnout k tomu, jaké prostředky by bylo nutno vynaložit na určení oné osoby.

Pokud si správce vedle upravených údajů nechá i data původní, nejedna se o anonymizaci, nýbrž o pseudonymizaci.

Samotný způsob anonymizace se dá zhruba zařadit do jedné ze dvou kategorií, randomizace a generalizace. Mezi techniky randomizace spadá „noise addition“ (znepřesnění údajů), permutace (záměna hodnot s jiným subjektem údajů) a diferenciální utajení, do generalizace pak agregace a k-anonymita (seskupení subjektů s jinými, se kterými sdílí nějaké údaje), L-diverzita a t-blízkost (pokročilejší k-anonymita). (Nulíček, 2018 str. 120) Při následném posuzování anonymity údajů je nutno posoudit, zda je možno vyčlenit jednu osobu, zda je možno propojit více záznamů týkající se této osoby a zda je možné z dat vyvodit informace týkající se jí. U komplexních datových záznamů je toto bez předchozího provedení agregace téměř nemožné.

3.4.8 **Integrity a důvěrnosti**

Správci jsou ze zákona uloženy povinnosti zabezpečit zpracovávaná data. Ten musí přijmout vhodná technická a organizační opatření a zajistit tak integritu a důvěrnost uchovávaných osobních údajů. Pro soulad s touto zásadou je nutné navržení uspořádání bezpečnosti podle povahy uchovávaných záznamů, minimalizace potenciální škody, stanovení odpovědné osoby, ověření fyzické a technické bezpečnosti a připravenost na rychlé reakce v případě bezpečnostních incidentů. (Žůrek, 2018 str. 65) (Nezmar, 2017 str. 74)

3.4.9 **Odpovědnosti**

Zásadou odpovědnosti se rozumí povinnost splňovat všechny již uvedené zásady a být schopen tuto skutečnost prokázat.

Povinnost prokazovat soulad s ostatními zásadami je v Nařízení nová a pro její dodržení musí správce uchovávat důkazy o všech opatřeních, které přijal za účelem zajištění souladu s Nařízením.

3.5 **Zvláštní podkategorie osobních údajů**

3.5.1 **Citlivé údaje**

Kromě běžných osobních údajů definuje Nařízení takzvané citlivé osobní údaje. Vzhledem k tomu, že jejich zpracování může představovat větší ohrožení soukromí, než je tomu u údajů jiných, týká se ho několik dalších omezení.

Mezi citlivé údaje patří:

- Údaje vypovídající o etnickém, či rasovém původu.
- Informace o politických názorech, náboženském vyznání, filozofickém přesvědčení a členství v odborech.
- Genetické údaje.
- Biometrické údaje zpracovávané za účelem identifikace fyzické osoby. (Zde je nutné odlišit identifikaci (umožnění vyhledat subjekt v databázi porovnáváním 1: n) a autentizaci (ověření již jinými prostředky poskytnuté identity porovnáním 1:1))
- Údaje o zdravotním stavu a sexuálním životě a orientaci.

Velkým vlivem na obsah této kategorie byly právní předpisy z oblasti předcházení diskriminaci, což částečně vysvětluje fakt, že zde nenalezneme například údaje o platebních kartách a kartách a bankovních účtech, byť by jejich zneužitím mohla vzniknout závažná újma. (Nulíček, 2018 str. 172)

V případě zpracování citlivých údajů je mimo běžných povinností splnit alespoň jednu z následujících podmínek:

- Je poskytnut výslovný souhlas (vzhledem k úpravám podmínek běžného souhlasu je jediným zásadním rozdílem to, že běžný souhlas lze poskytnout konkludentně (vyplývá z činnosti subjektu údajů))
- Údaje jsou nezbytné pro plnění povinností v oblasti pracovního a sociálního práva a sociálního zabezpečení (například předání údajů zdravotní pojišťovně).
- Údaje jsou nutné pro ochranu životně důležitých zájmů (například při hromadných neštěstích se závažnými újmami na zdraví).
- Jedná se o oprávněnou činnost nadací, sdružení a jiných neziskových organizací s politickými, náboženskými, filozofickými, či odborovými cíli (Subjekt údajů je nebo byl členem, nebo s danou organizací pravidelně spolupracoval. Dále nelze údaje bez souhlasu šířit a jsou poskytnuty dostatečné záruky.).
- Údaje byly subjektem zjevně zveřejněny.
- Dochází k řešení právních nároků a soudních sporů.

- Zpracování je přiměřené ochraně veřejných zájmů na základě unijního či vnitrostátního práva.
- Údaje jsou použity pro účely zdravotní a sociální péče (Zpracovatelé jsou vázáni služebním tajemstvím, či jinou povinností mlčenlivosti.).
- Jedná se o zájem týkající se veřejného zdraví.
- Dochází k archivaci ve veřejném zájmu, vědeckému či historickému výzkumu, nebo statistickým měřením. (například sčítání lidu, které obsahuje údaje o rase a náboženství.)
- Zpracování genetických, biometrických a zdravotních údajů může být dále upraveno legislativou jednotlivých států. (Evropský parlament a rada - GDPR, 2016 str. 39)

3.5.2 **Údaje o trestní činnosti**

Tyto údaje již oproti zákonu o ochraně osobních údajů nespadají do kategorie citlivých údajů, ale z pohledu nařízení stojí samostatně. (Zákon č. 101/2000 Sb, 2017 str. 2) (Evropský parlament a rada - GDPR, 2016 str. 39) Na rozdíl od Zákona do této kategorie spadají veškeré osobní údaje spojené s rozsudky v trestních věcech a trestnými činy. Vzhledem k povaze nařízení by pod tuto ochranu neměly spadat údaje o bezúhonnosti, jelikož jejich zpřístupnění by nemělo subjekt údajů nijak poškodit. (Nulíček, 2018 str. 182) Obecně platí, že zpracování údajů o trestní činnosti by mělo probíhat pouze pod dozorem orgánu veřejné moci, nebo za oprávnění právem EU nebo členského státu.

3.5.3 **Zpracování nevyžadující identifikaci**

V případě, že pro daný účel není nutné, aby správce získával informace nutné pro identifikaci subjektu, není k tomu z pohledu Nařízení povinen. (Evropský parlament a rada - GDPR, 2016 str. 39) Toto se týká například internetových obchodů vedoucích si evidenci IP adres uživatelů za účelem zjištění návštěvnosti. Ačkoliv se IP adresa považuje za osobní údaj, vzhledem k tomu, že obchod nemůže pouze podle ní nikoho identifikovat, nemusí shromažďovat další data jen proto aby vyhověl případným stížnostem na její uchovávání. (Nulíček, 2018 str. 186)

3.6 Práva subjektu údajů

Jedním z dopadů Nařízení je rozšíření práv subjektů údajů s ohledem na jim poskytované informace. Konkrétně se tímto aspektem zabývají články 12 až 14, které odpovídají mimo jiné na otázky otevřenosti, komunikace a férovosti týkající se subjektu údajů. Články 15 až 22 se pak zabývají hlavně možnostmi subjektu do samotného zpracování zasahovat. Je dobré podotknout, že pokud nedochází k porušení základních práv a svobod mohou být některá práva omezena například z důvodů národní či veřejné bezpečnosti, řešení trestných činů, nebo ochrany práv jiných osob. (Evropský parlament a rada - GDPR, 2016).

3.6.1 Postupy pro komunikaci se subjektem

Správce je povinen přijmout vhodná opatření umožňující subjekt údajů informovat stručným, transparentním, srozumitelným a snadno přístupným způsobem a měl by k tomu použít jasných a jednoduchých jazykových prostředků. Informace by měli být k dispozici v písemné, či elektronické podobě, na vyžádání pak v některých situacích ústně. (Evropský parlament a rada - GDPR, 2016 str. 41) Oproti zákonu o ochraně osobních údajů zde tedy dochází ke změně, jelikož ten dříve neuváděl konkrétní požadavky na formu komunikace. (Nulíček, 2018 str. 191) V praxi se však nejedná o velký rozdíl, jelikož ÚOOÚ již dříve v tomto směru požadoval dostatečnou míru srozumitelnosti. (Úřad pro ochranu osobních údajů, 2013)

Ve zkratce lze tedy říci, že správce by měl splňovat následující body:

- Informační text by měl být členěn v podobě, která čtenáře nepřehltí nadbytkem zbytečných informací. Pro větší přehlednost je zde například možnost informace rozdělit na více částí a ty pak subjektu předkládat až v momentě, kdy je to pro něj relevantní. Další variantou jsou takzvané vrstvené podmínky ochrany osobních údajů, kde dojde k rozdělení informací na dvě až tři části podle jejich důležitosti a složitosti.
- Informace by měly být formulovány tak, aby jim cílový adresát byl schopen porozumět. Tomu je vhodné věnovat zvýšenou pozornost například v případech, kdy se očekává, že velkou částí adresátů tvoří děti či osoby se zrakovým postižením.

- Informace by měli být subjektům přímo předloženy, nebo by mělo být znatelně zjevné, jak se k nim dostat. Subjekt by neměl být nucen si je složitě dohledávat.
- Správce by se měl vyvarovat složitým dlouhým souvětím používající právnický jazyk a informace poskytnout konkrétně a jednoznačně. Obzvláště tomu tak je u vymezení účelu a právního titulu s jakým jsou data zpracována. (Nezmar, 2017 stránky 84-86)

Dalšími důležitými požadavky na komunikaci je povinnost reagovat na žádost subjektu do jednoho měsíce od jejího podání (prodloužitelné až na tři při dostatečném odůvodnění), ověřit totožnost žadatele v závislosti na potenciální závažnosti daného požadavku, a provádět tyto činnosti bezplatně, pakliže nejsou nedůvodné, či nepřiměřené. (Evropský parlament a rada - GDPR, 2016 str. 41)

3.6.2 **Informace a přístup k údajům**

Podobně jako zákon o ochraně osobních údajů i (Zákon č. 101/2000 Sb, 2017 str. 6) i Nařízení ukládá správci povinnost informovat subjekt údajů co nejdříve je to možné od okamžiku započetí zpracování.

Správce by měl poskytnout následující informace:

- Svou totožnost a kontaktní údaje.
- Kategorii zpracovávaných údajů.
- Účel zpracování a případné oprávněné zájmy na jejichž základě probíhá.
- Případné příjemce, kterým data poskytuje, či úmysl předat data do jiné země.

Pokud je to nutné pro zajištění spravedlivého a transparentního zpracování je třeba zahrnout i následující:

- Dobu, po kterou jsou údaje uchovávány.
- Existenci práva požadovat zpřístupnění, úpravu či výmaz údajů, odvolat souhlas, či podat stížnost u dozorčího úřadu.
- Skutečnost, zda je poskytnutí osobních údajů povinné a případné důsledky, pokud tomu tak není učiněno.
- Skutečnost, zda dochází k automatickému rozhodování či profilování a případným důsledkům této činnosti, (Evropský parlament a rada - GDPR, 2016 str. 42)

Dále je zde již výše zmíněná povinnost upozornit, pokud jsou údaje zpracovány za jiným účelem, než za jakým byly původně shromážděny, nebo pokud byly získány od jiné strany, než je subjekt údajů. Z pochopitelných důvodů není pak nutné informace poskytovat, pokud je doložitelné, že subjekt již informacemi disponuje, či by k tomu bylo nutné vyložit nepřiměřené úsilí. (Žůrek, 2018 str. 134) Další výjimkou je například dodržení povinnosti mlčenlivosti, či výslovného práva Unie či státu, které se na správce vztahuje. Pakliže to nijak nepříznivě neovlivňuje práva jiných osob, může si subjekt vyžádat plnou či částečnou kopii o něm uchovávaných údajů (podoba kopie se liší v závislosti na okolnostech, běžně se používají například soubory TXT, XML, JSON a CSV). (Evropský parlament a rada - GDPR, 2016 stránky 43-44) (Nezmar, 2017 stránky 85-86)

3.6.3 **Práva na opravu a výmaz**

Stejně jako u zákona o ochraně osobních údajů i z pohledu Nařízení platí, že subjekt má právo na opravu či doplnění údajů bez zbytečných prodlev (Na tyto změny by pak měly být upozorněny případné další strany, kterým byly údaje zpřístupněny.). (Žůrek, 2018 str. 138) Dále pak platí, že v případě, že uchovávané údaje již nejsou potřeba, dojde ke zrušení souhlasu, či přímo podání oprávněné stížnosti, dochází k protiprávnímu zpracování, nebo tomu tak udává zákon, měli by být údaje správcem bez zbytečného odkladu vymazány. I zde existují výjimky jako například právo na svobodu projevu, zákonem dané povinnosti, archivace ve veřejném zájmu, či výkon a obhajoba právních nároků. (Evropský parlament a rada - GDPR, 2016 str. 45) V některých situacích je pak také možno místo úplného výmazu dat přistoupit k takzvanému omezení zpracování. Údaje je pak možno uchovávat, ale bez dalšího souhlasu mohou být použita jen k hájení právních nároků, ochrany práv jiné osoby, nebo kvůli důležitému veřejnému zájmu. (Nezmar, 2017 stránky 87-88) (Nulíček, 2018 stránky 235-238)

Novinkou je pak takzvané právo na portabilitu (přenositelnost), které nabádá správce poskytnout nahromaděné údaje na vyzvání příslušnému subjektu údajů či určené třetí straně, a to v běžně strukturované strojově zpracovatelné podobě (XML, JSON, CSV a podobné formáty), jeli to technicky možné a nedojde-li k ohrožení práv dalších osob, či porušení jiného pro danou situaci relevantního zákona. (Pracovní skupina pro ochranu údajů (WP29), 2016 str. 19) Toto právo se vztahuje na případy, kdy jsou data zpracována na základě souhlasu, či plnění uzavřené smlouvy, byla poskytnuta samotným subjektem a k jejich

zpracování jsou využity automatizované prostředky. Toto právo bylo do Nařízení zahrnuto za účelem podpoření soupeření mezi jednotlivými správci, což by mělo vést ke zkvalitnění nabízených služeb. Přestože je toto právo cíleno hlavně na online prostředí, musejí se jím řídit i ostatní správci, což může vést k potenciálním komplikacím. (Nulíček, 2018 str. 242) (Nezmar, 2017 stránky 89-91)

3.6.4 Práva týkající se se automatizovaných systémů a právo vznést námitku

Článek č. 21 Nařízení umožňuje nově subjektu údajů vznést námitku nejenom proti zpracování za účelem přímého marketingu (takzvaná možnost opt-outu), jak tomu bylo doposud (Zákon č. 101/2000 Sb, 2017), ale i proti zpracování v oprávněném, či veřejném zájmu, nebo za účelem historického či statistického výzkumu. (Evropský parlament a rada - GDPR, 2016 str. 47) V případě podání námitky proti výzkumu, či zájmu je správce povinen přezkoumat, zda je zpracování konkrétních údajů opravdu nutné pro danou činnost a případně ho ukončit. Námitka proti přímému marketingu se považuje za absolutní. (Nulíček, 2018 str. 249)

Co se týče legislativy z pohledu automatického zpracování (například profilování), subjekt má právo na to být z něj vyjmut za předpokladu, že se nejedná o jednu z následujících situací:

- Je to nezbytné pro uzavření smlouvy. (například poskytnutí úvěru bankou)
- Je tomu povoleno zákonem, který zároveň udává vhodná opatření pro ochranu zájmů subjektu.
- Subjekt poskytl souhlas. (Nezmar, 2017 str. 94)

I při těchto případech je pak nezbytné poskytnout alespoň možnost vyžádat si lidský zásah ze strany správce a právo výsledné rozhodnutí napadnout, či se k němu jinak vyjádřit.

Je nutno podotknout, že toto právo platí pouze pokud se jedná o výhradní automatické zpracování (do procesu není nikde zapojen člověk), které má právní nebo jiné výrazné dopady. (Žůrek, 2018 str. 148)

Hlavním rozdílem oproti dřívější právní úpravě je, že nyní může úřad pro ochranu osobních údajů ukládat sankce až ve výši 20 milionů eur či 4 % celkového ročního obratu. Drobnou změnou je dále to, že subjekty jsou chráněny i proti některým neprávním dopadům automatického zpracování (Nulíček, 2018 stránky 255-256)

3.7 Správce a zpracovatel

3.7.1 Obecné povinnosti

Jako hlavní obecnou povinnost správce lze označit zajištění souladu své činnosti s Nařízením a následně tuto shodu prokázat s přihlédnutím ke kontextu, účelu a rizikům, kterým je zpracování vystaveno. Vzhledem k tomu, že případné dozorčí úřady, které jsou o zpracování informovány, nemohou reálně kontrolovat všechny aspekty jednotlivých činností, je kladen velký důraz právě na posuzování rizik. (Nulíček, 2018 str. 269) Co se týče samotného postupu tohoto posouzení, existuje několik doporučovaných metodik, které lze obecně shrnout do čtyř hlavních kroků:

1. Identifikace možných hrozeb: Sem patří například nezákonné překročení stanoveného účelu, přehnané shromažďování údajů, uchovávání po dobu delší než nutnou, narušení integrity, dostupnosti či důvěrnosti údajů, zpracovávání neaktuálních či chybných údajů, nebo třeba ztížení schopnosti subjektu uplatnit svá práva.
2. Identifikace potenciální újmy způsobené dotčeným osobám: Nařízení neudává přesný výčet, ale jako příklad můžeme uvést diskriminaci, krádež identity, finanční škodu, poškození pověsti nebo pozbytí různých práv a svobod.
3. Zhodnocení pravděpodobnosti, že k újmě dojde: Zde je nutné přihlížet například na počet zúčastněných osob, zapojení třetích stran do zpracování, rozdílné právní požadavky při předání do jiných zemí, slabá místa v použitých procesech či výskyt dřívějších problémů.
4. Zhodnocení závažnosti možné újmy: Zde hodnotíme množství a citlivost zpracovávaných údajů, zranitelnost citlivých osob a možný dopad na jejich finanční a ekonomickou situaci a důležité události v jejich životě.

Na základě tohoto zhodnocení situace je tedy správce povinen přijmout protiopatření za účelem minimalizování možných hrozeb.

Jeli to přiměřené, Nařízení dále nabádá k zavedení vnitropodnikových koncepcí předepisující zásady chování a procesy zpracování. (Evropský parlament a rada - GDPR, 2016 str. 49) Tyto koncepce by měly být pro zaměstnance srozumitelné, proveditelné, aktuální a mělo by jít ověřit, zda jsou skutečně dodržovány. Pro lepší přehlednost je tedy

vhodné je strukturovat do více vrstev obecnosti (například „Údaje budou adekvátně zabezpečeny“ vedoucí k „Při obdržení služebního notebooku je ověřeno, zda je disk zašifrován a zaměstnanec je vyzván ke změně hesla. “).

Je možné, aby několik různých firem či osob figurovalo jako takzvaní „společní správci“. K tomu dochází, když se podílí na určení účelu a prostředků zpracování a jsou pak povinováni si mezi sebou ujednat konkrétní práva a podíl na povinnosti týkající se dané činnosti. (Evropský parlament a rada - GDPR, 2016 str. 50)

3.7.2 **Zabezpečení údajů**

Podstata nařízení se v tomto ohledu nijak výrazně nemění oproti dřívějším právním úpravám. I nadále se od správce očekává, že bude periodicky posuzovat míru rizika a provádět relevantní protiopatření, zejména pak v oblastech náhodného či úmyslného zničení údajů, jejich pozměnění či ztrátě a neoprávněnému přístupu. (Nulíček, 2018 str. 315) Nařízením nejsou pevně stanoveny přesné postupy, ale očekává se, že správce přihlédne ke konkrétním okolnostem a aplikuje rozumnou kombinaci následujících prvků:

- Pseudonymizace a šifrování
- Zajištění důvěrnosti (rozličné metody autentizace a autorizace, systém rozdílných oprávnění…)
- Zajištění integrity (monitorování změn, uchovávání více verzí, hashování…)
- Zajištění dostupnosti (záložní zdroje, rozdělení služby a dat mezi více serverů...) – obzvláště důležité například ve zdravotnictví
- Zajištění odolnosti systému
- Zajištění případného včasného obnovení dostupnosti dat při technických problémech
- Pravidelné testování zavedených opatření

V případě, že dojde k porušení tohoto zabezpečení a nejedná se o drobnost, která by neměla mít žádný vliv na práva zainteresovaných osob (vždy je nutné narušení zdokumentovat), je správce povinen tuto skutečnost nejpozději do tří dnů od zjištění nahlásit danému kontrolnímu úřadu. Pokud je dopad porušení závažný, je dále nutno informovat i dotčené osoby. (Evropský parlament a rada - GDPR, 2016 str. 54)

Při posuzování, zda se jedná o porušení zanedbatelné, které není potřeba hlásit úřadu a případně dotčeným osobám by mělo být přihlédnuto k následujícím faktorům:

- Typ porušení (půlhodinová nedostupnost =/= úplná ztráta)
- Povaha, citlivost a objem dotčených osobních údajů (jméno zákazníka prodejny =/= údaje o platební kartě)
- Snadnost identifikace jednotlivců
- Závažnost případných důsledků
- Počet dotčených osob a jejich zvláštní charakteristiky (děti, mentálně postižené osoby)
- Zvláštní charakteristiky správce (nemocniční zařízení =/= prodejce mykologického časopisu)
- Obecné skutečnosti
  (Pracovní skupina pro ochranu osobních údajů (WP29), 2017 stránky 17-18)

3.7.3 **Posouzení vlivu zpracování**

Oproti dřívější právní úpravě jsou nyní správci povinni provádět takzvané „(Privacy/Data protection) Impact Assessment“ (PIA/DPIA). Výsledkem tohoto posouzení by měla být dokumentace umožňující zmírnění rizik, která zároveň slouží jako důkaz, že činnost probíhá v souladu s Nařízením. Provádění DPIA není však povinné pro každé zpracování dat, ale pouze pro typy, které mohou s vysokou pravděpodobností způsobit riziko pro práva a svobody fyzických osob (Nezmar, 2017 str. 100). Při posuzování rizik (lze nalézt o několik stránek výše s nadpisem „3.7.1 - Obecné povinnosti“) je tedy vhodné dávat pozor, zda zpracování neobsahuje některé z následujících faktorů:

- Profilování či jiné hodnocení (např.: banka porovnávající zákazníky oproti registru dlužníků)
- Automatické rozhodování s významnými důsledky
- Systematické monitorování
- Práci s citlivými údaji (nejen spadající do Nařízením vymezené kategorie, ale i údaje např. o platebních kartách nebo poloze) (Nepatří sem jednorázové výjimky jako například zjištění alergií hostů při organizaci firemního večírku.)
- Zpracování ve velkém rozsahu (pojem není přesně definován, ale je vhodné posoudit například počet osob, objem dat, četnost a zeměpisný rozsah zpracování)
- Kombinování více různých datových sad (získaných za rozdílným účelem)

- Údaje zranitelných osob (děti, osoby se zhoršenou schopností rozpoznávat důsledky svých akcí)
- Inovativní řešení aplikačních a organizačních řešení (například některé aplikace IoT technologií)
- Provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů

Jako obecné pravidlo pak platí, že pokud jsou splněny alespoň dva z těchto bodů, je nutné provést posouzení vlivu (v případě, že správce shledá že v těchto případech není posouzení vlivu nutné, měl by své důvody podložit dostatečnou dokumentací). Dále je tomu tak vždy nutno u systematického rozsáhlého rozhodování se závažným dopadem založeného na automatických systémech, rozsáhlého zpracování citlivých či trestních údajů, nebo rozsáhlého systematického monitorování veřejných prostor (PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ (WP29), 2017 stránky 7-8) (Nezmar, 2017 stránky 102-104)

Pro usnadnění určení nutnosti provedení DPIA vydal úřad pro ochranu osobních údajů přehlednější postup pro hodnocení jednotlivých kritérií. Při jeho použití je pak posouzení nutné v případě, že více než jedno z kritérií je kritické, nebo spolu s jedním kritickým nabývá alespoň dalších pět hodnotu „významné“. (Úřad pro ochranu osobních údajů, 2020)

Samotné posouzení vlivu může probíhat podle různých metodik, ale jejich výsledný produkt musí obsahovat alespoň následující komponenty:

- Systematický popis zamýšlených operací, účel a oprávněný zájem správce (dostatečně se zohledňuje povaha, rozsah, kontext a účel zpracování; zaznamenávají se údaje, jejich příjemci a doba uložení; je uveden funkční popis operace; jsou identifikována použitá aktiva; zohledňuje se dodržování kodexů)
- Posouzení nezbytnosti a přiměřenosti operací vzhledem k účelu (jsou stanovena opatření, která mají být v souladu se zásadami Nařízení a právy subjektů údajů)
- Posouzení rizik pro práva a svobody subjektů údajů (podrobnější rozpracování případného prvotního posouzení zohledňující například zdroje rizik a potenciální dopady)
- Plánovaná opatření k řešení rizik, záruky, bezpečnostní opatření, mechanismy k zajištění ochrany osobních údajů a doložení souladu s Nařízením

V případě, že posouzení odhalí příliš vysoká zbytková rizika, očekává se, že správce před zpracováním požádá dozorový orgán o konzultaci. Jako příklad těchto nepřijatelných

rizik jsou případy kdy se subjekty mohou setkat s významnými či nezvratnými důsledky, které nedokáží sami překonat, či situace, kdy je zřejmé že riziko jistě nastane. (Nezmar, 2017 str. 111)

Co se týče zpracování započatých před účinností Nařízení, není přímo uvedeno, zda je nutno provádět posouzení dodatečně, ale lze dojít k názoru, že je to nezbytné pouze, pokud dojde k výrazným změnám v jejich průběhu (přechod na nové technologie a podobně). (Nulíček, 2018 str. 352)

3.7.4 **Pověřenec pro ochranu osobních údajů**

Jednou z výrazných novinek, které Nařízení zavádí, je pozice takzvaného pověřence pro ochranu osobních údajů (Data protection officer). Nejedná se o koncept, který by byl úplnou novinkou (například v Německu a Francii už podobná pozice existovala už dříve), ale v České republice došlo k jeho zavedení až nyní s nástupem GDPR. (Pracovní skupina pro ochranu osobních údajů, 2016 str. 3)

Oproti řadovému zaměstnanci, kterému bylo správcem dáno na starost dodržování ochrany osobních údajů, se pověřenec liší v několika směrech. Jedním z hlavních rozdílů je to, že by mělo jít o pozici nezávislou, bez střetu zájmů, které by neměli být zaměstnavatelem ukládány žádné specifické pokyny. Jedná se tedy o samostatný poradní orgán, který se nestará o obchodní či jiný zájem organizace, ale informuje ji o případných porušeních Nařízením daných požadavků. Za samotné splnění požadavků pak stále zůstává zodpovědný správce, pověřenec zastává pouze dozorovou a konzultativní roli. (Nulíček, 2018 stránky 361-364)

Co se týče povinnosti jmenovat pověřence, nevztahuje se na všechny správce a zpracovatele nýbrž pouze následující skupiny:

1. Orgány veřejné moci a veřejné subjekty, kromě soudů při výkonu svých pravomocí.
2. Správci jejichž hlavní činnost spočívá ve zpracování vyžadující pravidelné a systematické monitorování subjektů údajů. – Toto zpracování musí být neoddělitelné od hlavní činnosti, nikoliv pouze jejím sekundárním důsledkem. (Patří sem například poskytování zdravotní péče, či provozování veřejných kamerových systémů. Opakem je pak třebas vyplácení mezd zaměstnancům nemocnice.)
3. Hlavní činnost správce se zabývá rozsáhlým zpracováním citlivých či trestních údajů. (Evropský parlament a rada - GDPR, 2016 str. 57)

I pokud není správce ze zákona povinen pověřence jmenovat, může tomu tak učinit dobrovolně. Pak musí ovšem splnit zmiňované podmínky nezávislosti. Důležitým faktem je také to, že pokud již organizace má zaměstnance zajišťující ochranu osobních údajů a nepřeje si pověřence jmenovat, měla by tyto pracovníky jasně odlišit, aby se na ně nevztahovalo případné riziko, že budou jako pověřenec posouzeni. (Nulíček, 2018 str. 365)

Co se týče samotné osoby pověřence, nemusí jít nutně o nově najatého zaměstnance. V případě, že dojde k zajištění požadované nezávislosti a prevenci střetu zájmů (předběžné určení, které pozice jsou s výkonem povinností neslučitelné, přijetí interních pravidel a podobně), není problémem jmenovat zaměstnance stávajícího. (Nezmar, 2017 stránky 164-165) (Žůrek, 2018 str. 109) Další z možností je také využití služeb společného pověřence, který bude svou roli plnit pro více různých správců. V tomto případě je pouze důležité, aby jej bylo možné snadno kontaktovat ze všech případných provozoven (vždy je vhodné zveřejnit alespoň e-mailovou adresu, telefonní číslo a adresu pro zasílání dokumentů) a dorozumět se v jazyce příslušného dozorového úřadu, či subjektu údajů. Ve všech těchto případech by mělo platit, že jmenovaná osoba má dostatečné znalosti o ochraně osobních údajů a příslušných národních a evropských předpisů ovlivňujících danou činnost. Potřebná výše těchto znalostí je pak závislá na citlivosti a rizicích konkrétního zpracování. (Pracovní skupina pro ochranu osobních údajů, 2016 stránky 8-9)

Pro lepší přehled následuje krátký souhrn úkolů, které by měl mít pověřenec na starost:

- Poskytování poradenství a informací správci a zpracovateli o jejich povinnostech daných Nařízením.
- Monitorování, zda jsou probíhající procesy v souladu s právními normami.
- Na požádání poskytnout poradenství ohledně posouzení vlivu daných činností.
- Spolupráce s dozorovým úřadem.
- Působení jako kontaktní místo pro dozorčí úřad a subjekty údajů.
- Ohledně vykonávání těchto činností je pověřenec vázán zásadou mlčenlivosti. (Evropský parlament a rada - GDPR, 2016 stránky 58-59)

Ze strany zaměstnávající organizace by se mělo pověřenci dostávat dostatečných zdrojů nezbytných k plnění jeho povinností. Příkladem bodů, které je vhodné zvážit budiž aktivní podpora ze strany vedení, dostatek času na plnění povinností, finanční zdroje a případné vybavení a pomocný personál, dostatečná známost pověřence v organizaci,

přístup k právním a technickým službám nebo dostatečné průběžné školení. (Nezmar, 2017 str. 174)

3.7.5 **Kodexy chování**

Jak již bylo zmíněno výše, jednou z povinností správce je prokazování, že zpracování, které probíhá pod jeho dohledem, je ve shodě s GDPR. K možnostem, jak toho dosáhnout nově přibývají takzvané „kodexy chování“ a „osvědčení“.

Kodexy chování jsou souhrny ustanovení, které si kladou za cíl pomocí samoregulací upřesnit požadavky Nařízení pro konkrétní odvětví, které jsou jím ovlivňovány. Tyto souhrny se však neuplatňují na všechny, kteří se v onom odvětví nachází, nýbrž pouze na správce, kteří se k jejich dodržování dobrovolně přihlásí. Výhodou pro tyto správce pak je například jednodušší dokazování jejich důvěryhodnosti, proces posuzování vlivu na ochranu údajů, či šance na zmírnění případných pokut za případné přestupky. Nevýhodou je pak především to, že se správce podřizuje dalšímu akreditovanému subjektu a to, že v případě nespokojenosti dozorového úřadu nemá výsledek dodatečné kontroly příliš velkou váhu. (Nulíček, 2018 stránky 383-387)

Samotné schvalování těchto kodexů si na starost berou příslušné dozorčí úřady, které je následně zaregistrují a zveřejní.

Osvědčení může nabývat například podobu pečeti, či známky a slouží ke snadnému zprostředkování informací subjektu jinému správci. Lze říci, že v oblasti zabezpečení znamenají něco podobného jako například značky „BIO“ nebo „Česká kvalita“ v potravinářském průmyslu. Na rozdíl od kodexů není cílem těchto značek optimální uplatnění Nařízení pro dané odvětví, ale pouze jeho určité zohlednění a dostatečného dodržení daných kritérií. Dále je také udělováno maximálně na dobu tří let. Co se výhod a nevýhod týče, jsou na tom osvědčení podobně jako kodexy. (Nulíček, 2018 stránky 389-391)

3.8 **Předávání údajů do zahraničí**

Může se stát, že správce či zpracovatel během své činnosti předá některé osobní údaje do země nepatřící do evropské unie (obzvláště u internetových služeb je toto často nezbytnou podmínkou jejich fungování). Vzhledem k tomu, že tyto země přímo nepodléhají působnosti

Nařízení (a nemusejí tedy nutně poskytovat stejnou úroveň ochrany jako země, které ano) je nutné, aby u těchto postupů docházelo k určitým preventivním opatřením.

Pro předejití případným nejasnostem je dobré zmínit, že jako předání se nepovažuje zveřejnění údajů na internetu způsobem, že k nim má přístup kdokoli z libovolné země na světě (Evropský soudní dvůr, 2003). Z pohledu nařízení se jedná o jakékoliv poskytnutí údajů správci či zpracovateli v zemi mimo EU, které splňuje obecné podmínky zákonnosti.

Co se týče zmiňovaných podmínek nutných pro předání, lze je zařadit do jedné z následujících tří kategorií.

3.8.1 **Předání na základě rozhodnutí o odpovídající ochraně**

Při tomto odůvodnění předání se odvolává na to, že země (případně mezinárodní organizace), do níž budou osobní údaje putovat, byla evropskou komisí posouzena a bylo shledáno, že dochází ke splnění podmínek ochrany osobních údajů v míře srovnatelné s EU. Tyto podmínky nemusí nutně splňovat celá země jako taková, nýbrž jen část jejího území nebo relevantní odvětví. (Nezmar, 2017 str. 154)

Je vhodné zmínit, že co se týče předávání údajů do Spojených států amerických (jejichž právní ochrana bez dodatečných opatření podmínky nesplňuje), jedná se o záležitost dlouhodobě problematickou. Dřívější program „Safe Harbour “, který měl zajišťovat ochranu práv Evropanů se ukázal nedostačující, jelikož nebyl americkými úřady respektován, a účinnost nového (2016) programu „Privacy Shield“, který Safe Harbour nahradil, byla již několikrát diskutována. Vzhledem k nejasné budoucnosti se tedy doporučuje při předávání údajů do USA využít dodatečných záruk a nespoléhat pouze na aktuální rozhodnutí evropské komise. (Nulíček, 2018 stránky 407-408)

3.8.2 **Předání na základě poskytnutých záruk**

Druhou kategorií je takzvané předání na základě vhodných záruk. V tomto případě Nařízení povoluje předání údajů, když jsou v dané zemi (organizaci) k dispozici vymáhatelná práva subjektů údajů a je splněn alespoň jeden z následujících bodů.

- Je přítomen právně závazný vymahatelný nástroj mezi orgány veřejné moci či veřejnými subjekty (například dohoda o zpracování jmenné evidence cestujících za účelem předcházení teroristickým útokům)

- Jsou určena závazná podniková pravidla
- Jsou používány standardní smluvní doložky
- Je dodržován schválený kodex chování či přítomno platné osvědčení
- Existují vlastní smluvní doložky mezi správci/zpracovateli, nebo vymáhatelná ustanovení pro ujednání orgánů veřejné moci. (Evropský parlament a rada - GDPR, 2016 str. 65)

3.8.3 **Výjimky pro specifické situace**

Během těchto specifických situací jsou většinou práva subjektu vystavena pouze malým rizikům, nebo existuje zájem, který nad právem na soukromí znatelně převažuje (ať už veřejný zájem či zájem samotného subjektu). U některých z těchto výjimek se očekává, že předání je pouze jednorázové či příležitostné. Těmi jsou předání nezbytné pro uzavření či splnění smlouvy mezi subjektem a správcem, nebo třetí osobou v zájmu subjektu (příkladem budiž pojištění sjednané rodičem dítěte), a předání nutná pro ochranu a výkon právních nároků. Je vhodné dodat, že zjednodušení administrativy není z pohledu Nařízení činnost nezbytná pro plnění smlouvy (Nulíček, 2018 str. 429). Ostatní výjimky umožňují opakované předávání, ale stále by mělo docházet k uplatňování určitých omezení. Do této skupiny patří případy, kdy byl subjekt dostatečně informován o rizicích a poskytl výslovný souhlas, předání nezbytné pro veřejný zájem (správa sociálního zabezpečení, dozor na finančních trzích, prevence chorob apod.), ochrana životně důležitých zájmů osob a předání z rejstříku určeného k informování veřejnosti. Pakliže není splněna ani jedna z těchto výjimek, je zde pak ještě nouzová možnost jednorázového předání v případě závažného oprávněného zájmu správce. Při této situaci je pak očekáváno balanční testování a informování dotčených subjektů. (Evropský parlament a rada - GDPR, 2016 stránky 67-68)

3.9 **Právní ochrana, odpovědnost a sankce**

Dle zákona má každý subjekt údajů, který má důvodné podezření, že zpracování osobních údajů, které se ho týkají, neprobíhá v souladu s Nařízením, právo obrátit se s touto stížností na příslušný dozorčí úřad. Důvodem pro tuto stížnost může být například nepřesnost zpracovávaných informací, shromažďování v rozsahu, který je pro uvedený účel přijatelný, nebo třeba úplná absence legitimního právního titulu. Dalším možným důvodem může být

ignorování subjektu, který se správce o těchto skutečnostech již snažil informovat. (Evropský parlament a rada - GDPR, 2016)

Po podání stížnosti by měl být úřadem subjekt dostatečně informován o průběhu a případném výsledku daného řízení. Je vhodné podotknout, že podání stížnosti nezbavuje subjekt práva na podniknutí jiných kroků jako například uplatnění nároku na škod či žaloba na ochranu osobnosti. Stejně tak by její nepodání nemělo při použití jiných prostředků ochrany býti subjektu žádnou překážkou. (Nulíček, 2018 str. 501)

Kromě zmiňovaného podání stížnosti dozorovému úřadu může subjekt při důvodném podezření na porušení jeho práv přejít přímo k podání žaloby u soudu. Toto by nijak nemělo ovlivnit případnou stížnost. (Evropský parlament a rada - GDPR, 2016)

V případě že porušením Nařízení došlo k újmě je, širší odpovědnost za tuto skutečnost nese správce. Zpracovatel je za újmu zodpovědný pouze pokud porušil povinnost, kterou Nařízení ukládá výslovně jemu, nebo pokud jednal nad rámec pokynů správce, nebo v rozporu s nimi.

Co se týče možné výše udělených peněžních sankcí, došlo oproti dříve platnému zákonu o ochraně osobních údajů k několika změnám. Jako horní hranici pokuty pro fyzickou osobu bylo Zákonem stanoveno 5 000 000 Kč, u právnické osoby tomu pak byl dvojnásobek. (Zákon č. 101/2000 Sb, 2017 str. 16) Úřad pro ochranu osobních údajů dříve povětšinou uděloval sankce v hodnotách deseti až statisíců. V posledních letech pak došlo ke značnému zvýšení (příkladem budiž pokuta 3,6 milionu za masivní únik osobních údajů a 4,25 milionu za opakované šíření nevyžádané reklamy), což si lze odůvodnit jako přípravu na přechod na přísnější GDPR.

Dle Nařízení by se měli být pokuty účinné, přiměřené a odrazující, za tímto účelem byl potenciální strop sankce za závažná porušení zvýšen na 20 000 000 EUR, nebo 4 % celosvětového příjmu podniku. Pokud se jedná o méně závažné porušení je maximální možná výše pokuty poloviční. Při ukládání by mělo být přihlédnuto k různým relevantním polehčujícím či přitěžujícím faktorům jako například:

- Výše příjmů v daném státě
- Zda k porušení došlo právnickou či fyzickou osobou
- Povaha, závažnost a trvání daného porušení
- Zda bylo porušení úmyslné, či z nedbalosti a případná relevantní dřívější porušení
- Kroky podniknuté ke zmírnění škody a dodržované kodexy chování (osvědčení)

- Míra odpovědnosti správce vzhledem k technickým a organizačním nařízením a spolupráce s dozorovým úřadem (Evropský parlament a rada - GDPR, 2016 stránky 87-88)

Cílem pak je, aby pokuta nebyla pro daného správce likvidační, ale zároveň došlo k dodržení zásady, že protiprávní jednání se nesmí vyplácet. I po vyplacení pokuty má stále správce povinnost uhradit případnou újmu. (Nulíček, 2018 str. 517)

3.10 **Implementace GDPR**

Vzhledem k tomu, že implementovat GDPR do běžných firemních postupů není úplně nejjednodušší, bývá vhodné tuto činnost rozdělit na více postupných kroků a přistoupit k nim formou projektového řízení. Prvním logickým krokem bývá seznámení se s požadavky kladené Nařízením, následně pak probíhá analýza aktuálního stavu podniku často označovaná jakožto „GAP analýza“.

3.10.1 **GAP analýza**

Jak již název napovídá, jedná se o techniku definování „mezery“ mezi aktuálním stavem („Kde jsme?“) a stavem požadovaným Nařízením („Kde chceme být?“). Obecně lze říci, že pokud firma již úspěšně implementovala zákon o ochraně osobních údajů, nemělo by z analýzy vyplynout příliš mnoho problémů.

Hlavními cíli GAP analýzy je zjistit následující:

- Sběrné uzly osobních údajů
- Struktura shromažďovaných dat
- Používané nástroje a jejich formální obsah (například formát formulářů)
- Jak byl získán případný souhlas
- Kdo (a na základě jakého oprávnění) má přístup k datům
- Způsob uchovávání a ochrany dat
- Systémy a aplikace používané ke zpracování
- V jakých procesech data figurují a jak probíhá jejich zpracování (a soulad těchto postupů s GDPR)
- Kontrola smluvních závazků týkajících se dat a vazby a smlouvy třetích stran
- Přístup k hodnocení dopadu na soukromí

- Proces řízení incidentů a schopnost na ně reagovat
- Návrhy a doporučení pro případný nesoulad s Nařízením (Nezmar, 2017 stránky 96-98)

Obvyklým postupem GAP analýzy bývá obvykle prvotní identifikace sběrných uzlů (kde jsou osobní údaje shromažďovány a vstupují do organizace – například: formulář na webu, dotazník u personalisty, zápis na recepci a podobně) a odpovědných osob, následovaná identifikací jednotlivých zpracování (Dá se využít různých vzorů jako například v příloze uvedený od A. Šefčíka a R. Dubravského). Po identifikaci zpracování bývá obvykle vypracován základní graf datových toků v organizaci, dojde k ověření validity jednotlivých používaných formulářů jakožto případně poskytovaného souhlasu a identifikaci smluvních vazeb. Po zhodnocení bezpečnosti jak listinných, tak digitálních informací pak dochází k výslednému sepsání GAP analýzy a přednesení případných návrhů ke zlepšení.

Výše neuvedeným krokem, který by však měl předcházet všemu ostatnímu, je angažování vedení organizace, jelikož bez asistence vrcholového managementu je prakticky nemožné, aby získané výsledky zcela odpovídaly skutečnému stavu.

Je vhodné zmínit, že často používanou praktikou na úřadech a firmách je zápis jména příchozího, času příchodu a odchodu, jména navštívené osoby a podpisu. Vzhledem k tomu, že podpis lze za specifických situací (Nikoliv pouze podpis na list papíru, kde závisí jen na výsledném vzhledu, ale do elektronického zařízení, kde lze měřit, jak byl daný podpis proveden.) považovat za biometrický údaj, který vyžaduje šetrnější zacházení, není jeho provádění pomocí tabletu vhodné. Listinné provedení v podobě návštěvních knih může rovněž vzhledem k trendu vývoje ochrany práv v budoucnu čekat určité omezení. (Pracovní skupina pro ochranu osobních údajů (WP29), 2012 str. 27)

3.11 **Rizika a jejich hodnocení**

Při zpracování osobních údajů se mohou vyskytnout případy, kdy nevhodným nakládáním z těmito údaji dojde k negativnímu ovlivnění příslušných subjektů. V některých případech může dojít k pouhé ztrátě údajů nebo zahlcování nevyžádanou poštou, ale v horších případech může dojít k vybrání bankovních účtů, nesení zodpovědnosti za trestnou činnost, či dokonce ohrožení na životě (příkladem budiž zveřejnění údajů policistů,

vězeňských důstojníků, či svědků u závažných trestných činů). (Policie ČR, 2019) (Nezmar, 2017 str. 74)

Při již zmiňované analýze rizik a posuzování vlivu dochází k identifikaci hrozeb možných při daném procesu zpracování. Jako jeden z možných postupů, jak k této identifikaci přistupovat je jednoduchá polokvantitativní metoda **PZH** (**P**ravděpodobnost, **Z**ávažnost, názor **H**odnotitelů). Metoda spočívá v přiřazení hodnot 1-5 jednotlivým proměnným a následnému spočtení hodnoty **R = P x Z x H**. Položka **H** zohledňuje více faktorů mající vliv na ohrožení a nebezpečí a spadá pod ní například počet ohrožených subjektů, čas trvání ohrožení, kategorie zpracovávaných údajů, úroveň zabezpečení (fyzické i kybernetické povahy), kumulace a dynamičnost rizik, vliv pracovních podmínek jakožto i další možné vlivy. Jednotlivé hodnoty proměnných si lze vyložit následujícím způsobem:

Tabulka 1 - PZH kritéria

Hodnota	Pravděpodovnost	Závažnost	názor Hodnotitelů
1	Nahodilá	Bez následku pro subjekty údajů	Zanedbatelný vliv
2	Nepravděpodobná	Minimální následky pro subjekty údajů	Malý vliv
3	Pravděpodobná	Bez trvalých následků pro subjekty údajů	Větší, nezanedbatelný vliv
4	Velmi pravděpodobná	Se závažnými následky pro subjekty údajů	Velký a významný vliv
5	Trvalá	Fatální následky ohrožující život subjektů údajů	Více významných a nepříznivých vlivů

Zdroj: (Nezmar, 2017 str. 126)

Po roznásobení jednotlivých proměnných získáme celkové bodové hodnocení rizika v rozmezí 1 až 125, podle kterého můžeme určit naléhavost přijetí případných protiopatření.

Tabulka 2 - PZH hodnocení rizika

Stupeň rizika	Celkové riziko R	Míra rizika
I	> 100	Nepřijatelné
II	51 - 100	Nežádoucí
III	11 - 50	Mírné
IV	3 - 10	Akceptovatelné
V	< 3	Bezvýznamné

Zdroj: (Nezmar, 2017 str. 127)

Podle metody PZH tedy můžeme rizika rozdělit do pěti kategorií. Jsou jimi:

- Zanedbatelné – Není třeba žádného zvláštního opatření, stačí na riziko pouze upozornit.
- Přijatelné – Je vhodné zvážit vynaložení nákladů na zlepšení či případné řešení. Většinou postačují opatření jako základní školení obsluhy, nebo běžný dozor.
- Mírné – V rozumném časovém úseku je nutné zavést opatření pro jeho snížení.
- Nežádoucí – Nutné urychleně provést bezpečnostní opatření a přidělit další zdroje.
- Nepřípustné – Je nutné úplné zastavení činnosti.

3.12 **IT technologie**

Jedním z důležitých aspektů, které je třeba brát na vědomí při implementaci GDPR v rámci podniku je prakticky nevyhnutelné používání počítačů a jiných informačních technologií. Mimo problémy zabývající se pohybem údajů například přes internet existují i méně často probíraná rizika.

3.12.1 **Reprografická zařízení**

Skutečnost, kterou mnoho lidí zapomíná brát na vědomí je fakt, že tiskárny nejsou pouhé „tupé“ přístroje, které nedokáží nic jiného než tisknout. Přesněji řečeno, k výkonu této činnosti jsou nezbytné komponenty podobné těm obsažené v běžném počítači (procesor, paměť a úložiště, OS, síťové připojení) a tudíž i zde hrozí rizika ztráty dat z toho vyplývající, ať už se jedná o fyzický přístup k pevnému disku (CBS News, 2010), napadení přes internet (Uniprint, 2017), nebo dojde k odchycení nezašifrovaného dokumentu putujícího po síti. Dalším mnohem přímějším ohrožením je prostá krádež/ztráta/přečtení dokumentu u tiskáren umístěných ve společných prostorách. Tomuto lze předcházet například využitím funkcí „soukromého tisku“, kterou některé tiskárny disponují (před započetím tisku je pak vyžadován například PIN kód nebo otisk prstu). (OE Canada Inc., 2019) Dále lze využít například čipových karet, či podobných zabezpečení.

3.12.2 **Další koncová zařízení**

Klíčovou roli, co se zabezpečení týče mají z pochopitelných důvodů i pracovní stanice (stolní počítače, notebooky) jednotlivých uživatelů a s nimi související vybavení.

Pro kontrolu a udržování bezpečnosti je vhodná začít samotnou fyzickou přístupností daného zařízení a zabezpečením například proti neoprávněné změně jeho hardwarové konfigurace. Tohoto lze dosáhnout například umístěním do prostor s omezeným přístupem, zavedením dohledového systému, nebo využití speciálního zámkového systému (Kensigton, 2019). Z ekonomických důvodů se dále používá například uzamčení běžným visacím zámkem. Přestože lze tento postup označit za relativně primitivní, jeho snadná dostupnost, cena a možnost zavedení společného klíče jej činí častou volbou u hromadných instalací jako například počítačové učebny. (Nezmar, 2017 str. 192)

Po vyřešení fyzické přístupnosti pak dochází k zabezpečení samotné softwarové stránky. Obvyklým postupem je používání dvojice hesel (jedno pro zabránění neoprávněné modifikace BIOSu („Basic Input Output System"), jedno pro samotné spouštění operačního systému). V případě modifikace BIOSu je velmi těžké tuto změnu rozpoznat z prostředí instalovaného OS, proto se na jeho ochranu používají složité technologie jako například HP Sure Start, které případné chyby automaticky detekují a opraví pomocí skryté zálohy. (HP, 2015) Tuto technologii je mimo stolní počítače a notebooky pak možno nalézt i v některých tiskárnách a podobných výrobcích. Podobně pak v některých případech (dostupné pro počítače s Windows 8.1 a 10) dochází k využití technologie UEFI Secure Boot, která při startu ověřuje, zda spouštěný kód má platnou bootovací certifikaci. (Časopis Chip, 2014) (Microsoft, 2018)

Kromě tiskáren, počítačů a podobných relativně masivních přístrojů je třeba brát na zřetel i zabezpečení těch snadno přenosných, jmenovitě pak mobilních telefonů. Základním opatřením by mělo být minimálně nastavení automatického zamykání obrazovky a nastavení alespoň čtyřmístného PIN kódu. Odhodlaného útočníka tato ochrana nezastaví ale přinejmenším odradí od náhodného prohlížení zvědavým kolemjdoucím. Problémem pak bývá, že složitá hesla, která by při případném útoku měla šanci obstát, není příliš pohodlné u telefonů používat. Vzhledem k tomu, že mnoho nových telefonů již nabízí možnost odemykání pomocí biometrických znaků jako je otisk prstu, nabízí se pak možnost kombinace biometriky a složitého hesla, které je nutné zadat jen jednou za delší časové období. (Nezmar, 2017 stránky 194-195)

3.12.3 **Mazání dat**

Jak již bylo zmíněno výše, jednou z povinností správce je mazání dat, které již nadále neslouží, žádnému účelu, či například dat, k jejichž odstranění byl subjektem údajů oprávněně vyzván. Za předpokladu, že nedojde k jejich pouhému označení jako „nezpracovávat“, nabízí se několik možností, jak daného cíle dosáhnout:

- Fyzická destrukce nosiče – Výhodou je jednoduchost provedení a relativní spolehlivost, logickou nevýhodou je nutnost nahradit úložiště novým.
- Obnovení továrního nastavení – Vhodné u zařízení bez přístupu k úložnému médiu jako takovému, nevýhodou je nemožnost se odchýlit od stavu poskytovaného výrobcem.
- Použití specializovaného softwaru – Umožňuje znovupoužití úložiště a v porovnání s ostatními postupy bývá levnější. Problémem je nepoužitelnost u některých typů médií a zdlouhavost důkladného procesu u velkých disků.
- Odborný zásah – Při předání dat dále je nutná určitá kontrola daného odborníka.
- Formátování – Samo o sobě nedostačující, ale vhodné jako doplňková metoda ke standardnímu přepsání dat. (Nezmar, 2017 stránky 72-73)

3.13 **Kybernetická bezpečnost**

Vzhledem k tomu, jak velkou roli hrají při dnešním zpracování osobních údajů počítačové technologie dává smysl, že správně fungující organizace by měla věnovat dostatečné úsilí na jejich zabezpečení. Mimo GDPR se tematikou bezpečnosti informací zabývá například řada norem ISO 27000 (obzvláště pak 27001 a 27018) (International Organization for Standardization, 2013). Tyto mezinárodní standarty definují další požadavky za účelem neustálého zlepšování bezpečnosti informací a zachování důvěrnosti, dostupnosti a integrity. (Krucek cybersecurity, 2019)

Při rozhodování zabývajícím se složitostí používaných postupů by měla brána na zřetel velikosti firmy, technologický vývoj, náklady na provedení, používané praktiky (například: při práci zaměstnanců z domova by mělo docházet k dostatečnému zabezpečení souborů sdílených přes internet) a povaha zpracovávaných osobních údajů. Mezi důležité aspekty kybernetické bezpečnosti patří například:

- počítačová bezpečnost – sem patří instalace firewallu, antivirové programy, častá aktualizace zabezpečení systému, šifrování elektronicky uchovávaných údajů, zálohování, likvidace starých počítačů a ochrana proti spywaru
- bezpečnost e-mailu – do této oblasti spadá používání skrytých kopií, šifrování mailů nebo kontrola při posílání na nezabezpečené servery
- zabezpečení faxu – používání krycích listů, potvrzení přijetí pomocí jiného druhu komunikace (např. telefonicky)
- školení zaměstnanců – používání silných hesel, zdrženlivost ve firemní korespondenci, podezřívavost vůči neobvyklým mailům („…Pro ověření přiložte číslo bankovního účtu a k němu příslušné heslo“ a podobné) a zásada okamžitého mazání spamu (Nezmar, 2017 str. 78)

3.14 **Document Management System**

DMS neboli „Document Management System“ jsou systémy pro správu elektronických dokumentů, kterých je v současné době čím dál více. Podle průzkumu z roku 2017, mělo takový systém zavedeno 74 % z dotazovaných amerických firem (Accusoft, 2017). Účelem těchto systémů je například usnadnění orientace ve více verzích téhož dokumentu, umožnění přístupu pouze ke složkám, ke kterým má uživatel oprávnění, zrychlení vyhledávání, či sdílení napříč firmou bez spoléhání se pouze na sdílený disk. (Software602 a.s., 2019) Obecně lze říci, že při nasazení správy elektronických dokumentů se řeší hlavně následujících šest kritérií: řízená distribuce dokumentů (sdílí jen autorizovaní pracovníci), zabezpečený přístup (hesla, monitorování přístupu a změn), prevence ztráty (zde se myslí založení papírových dokumentů), dodržování zákonných nařízení (katalogizace dokumentů potřebných pro případné kontroly), obnova po haváriích (ukládání mimo server či do cloudu) a archivace významných papírových dokumentů (práce s elektronickou kopií dokumentů které musejí být uchovány v papírové podobě). (Nezmar, 2017 str. 217) Je vhodné dodat, že kromě drahých softwarových programů existují i open source varianty jako například český DMS RAINBOW (Cost Cutting Solutions Ltd., 2019).

3.15 **Zabezpečení Wi-Fi**

Dalším z potenciálních rizik, na které je třeba si dát pozor je skutečnost, že co se týče komunikace, Wi-Fi sítě bývají často jejím nejslabším článkem. V případě, že dochází k připojení na server či pomocí aplikace, které posílaná data šifrují, v případě odposlechu přenášené informace nezíská útočník obvykle nic víc, než bezcennou smět jedniček a nul. Při komunikaci se servery, které tomu tak nečiní je ale vhodné využít tzv. tunelu VPN, který se postará o dodatečné zabezpečení. Nevýhodou tohoto řešení však je, že při použití VPN serverů může dojít k omezení rychlosti připojení, kvůli nutnosti obsloužit více uživatelů, kteří danou službu využívají. (Nezmar, 2017 stránky 218-221)

Obecně lze říci, že při používání Wi-Fi připojení je dobré mít nejnovější aktualizace firmwaru užívaného přístroje a případně periodicky přecházet na novější hardware umožňující nové metody zabezpečení. Dále je vhodné změnit výchozí tovární jméno a heslo routerů na nové a nepoužívat názvy sítí, které by případnému útočníkovy mohli poskytnout použitelné informace. Při nastavování vlastní Wi-Fi sítě je také třeba dát pozor na používaný typ šifrování. Při pohledu na českou statistiku lze například zjistit, že přijatelný typ zabezpečení WPA-2 používá z měřených 3 405 259 sítí pouze 63 % zatímco 14 % používá buď již prolomené WEP, nebo není zašifrováno vůbec. (Zde je vhodné připomenout, že sebelepší šifrování může být snadno prolomeno, pokud je nastaveno příliš jednoduché heslo) (Wifileaks, 2019) Pro případné návštěvníky je vhodné využít již relativně podporované funkce Guest network, která umožní připojení k internetu, ale je odříznutá od vnitřní sítě.

3.16 **Hesla a práce s nimi**

3.16.1 **Heslová politika**

Vzhledem k množství e-shopů, e-mailů, bankovních aplikací a dalších internetových služeb jejichž účty dnešní řadový člověk využívá lze bez zbytečné nadsázky tvrdit, že silnou heslovou politiku lze považovat za velmi významný prvek v ochraně údajů. I přesto lze bohužel prohlásit, že velká většina uživatelů internetu bere tento fakt na lehkou váhu. Při průzkumu z roku 2017 například vyšlo najevo, že pouze třetina dotazovaných si pro každý založený účet vytváří nové heslo a 10 % dokonce přiznalo, že pro všechny online účty používají pouze jedno stejné heslo. Při vymýšlení hesel pak dost velká část nepoužívá

doporučované postupy, jako kombinace velkých a malých písmen (53 %), či písmen a číslic (36 %). Dalším častým prohřeškem bývá sdílení hesel s rodinou (28 %), přáteli (11 %), či kusem papíru (22 %). (Kaspersky, 2017)

Jako základní pravidlo při práci s hesly lze ve výsledku prohlásit, že ani administrátor systému by neměl mít přístup k jeho nezašifrované podobě a při komunikaci s uživatelem například při jeho zapomenutí by mělo být využito například dočasných odkazů. (Nezmar, 2017 str. 224)

V celkem pochopitelných případech, kdy má uživatel problém zapamatovat si všechna svá složitá hesla lze pak využít speciálních programů jako je například 1Password nebo KeePass. Poté mu stačí vytvořit a zapamatovat si jedno velmi silné hlavní heslo, a přesto mít přístup k těm méně používaných například prostřednictvím mobilního telefonu. (1Password, 2019) (KeePass, 2019)

3.16.2 **Hashování**

Když už jsme u hesel, tématem, které je vhodné okrajově zmínit je takzvané hashování. Jedná se o jednosměrný proces, který pomocí snadno dostupných algoritmů vytvoří ze zadaného hesla jeho zašifrovanou podobu pevně dané délky. Dalším možným využitím tohoto postupu je také fakt, že při sebemenší změně původního textu dojde k razantní změně výsledku, a tudíž jej je možné aplikovat na celé dokumenty či aplikace za účelem kontroly jejich případné změny. (Nezmar, 2017 stránky 222-223)

Co se rozluštění původního textu týče potenciální útočník má k dispozici tři druhy postupů, kterými se může pokusit získat nezašifrovaná hesla: útok hrubou silou, slovníkové útoky a takzvané rainbow tables. Útok hrubou silou spočívá v opakovaném generování hashů pro všechny kombinace znaků a jejich porovnávání s požadovanou hodnotou. Účinnost tohoto postupu závisí především na složitosti daného hesla a jeho trvání se může pohybovat od několika milisekund po statisíce let.

Obrázek 1 - Čas na prolomení MD5

Čas potřebný k prolomení hashovaného hesla funkcí MD5 hrubou silou						
		Počet znaků hesla				
	Počet možných znaků	6	8	10	12	14
Jen malá písmena	26	15 ms	9 vteřin	2 hodiny	54 dnů	10 let
Malá a velká písmena	52	1 vteřin	45 minut	91 dnů	619 dnů	1 650 000 let
Malá a velká písmena, číslice	62	3 vteřiny	3 hodiny	1,3 roku	5 115 let	20 000 000 let
Malá a velká písmena, číslice, speciální znaky	95	36 vteřin	4 dny	94 roky	856 000 let	7 700 000 tisíciletí
Výpočet na Nvidia Geforce 1070 se schopností generovat cca 20 miliard MD5 hash tagů za vteřinu						

Zdroj: (Nezmar, 2017 str. 223)

Slovníkový útok využívá tendence uživatelů používat některé typy hesel (například „123456“, „hesloheslo“, „qwerty“, „michal“ a podobné). (TechRepublic, 2018) Zde tedy nastává paradoxně výhoda, pokud je v heslu gramatická chyba nebo pokud je použito méně rozšířené nářečí (ze strany mezinárodních útoků je do určité míry výhodou již samotná čeština). „Rainbow Tables“ jsou tabulky již předem vypočítaných hashů, zde v zabezpečení pomáhá hlavně délka hesla, jelikož již tabulka pro 9 znaků má i po podniknutí kroků pro její zmenšení velikost v řádu terabytů. (SOOM.cz, 2015)

3.17 **Nebezpečí virů**

Při práci s daty v elektronické podobě může mimo jiných incidentů dojít také k jejich ohrožení zapříčiněné virovým útokem. Existuje sice mnoho různých variant, jak nás může škodlivý software ovlivnit, ale zde kvůli obsáhlosti toho tématu zde krátce zmíníme pouze Ransomwarem, jelikož dopad této odrůdy útoků je pravděpodobně největší.

Ransomware (ransom = výkupné) je typ softwaru, který po své úspěšné instalaci zabrání uživateli v přístupu k počítači a následně požaduje platbu (nejčastěji v Bitcoinech či jiné kryptoměně; roku 2018 průměrně v hodnotě kolem jednoho tisíce dolarů (phoenixNAP, 2019)) za poskytnutí klíče k odemčení a dešifrování. (Nezmar, 2017 str. 229) Tento klíč pak často uživatel opravdu dostane, jelikož útočníci nemívají zájem dávat budoucím obětem důvod neplatit. Existují ale i případy, kdy propojení platby a dodání klíče nefungují a oběť jen zbytečně přijde o peníze. (Acronis, 2019)

Co se týče způsobu, jakým se cílový počítač nakazí, jako příklad lze uvést infikované e-mailové přílohy, často ve formátu doc nebo xls, které po spuštění vyžadují oprávnění pro

spuštění makra. Existují pak samozřejmě i varianty v podobě zip archivů či standardní spustitelné exe soubory.

Po spuštění pak následuje restart počítače a šifrování tvářící se navenek jako běžný program pro kontrolu disku. V některých případech je možné, že infekce kvůli nedostatečným oprávněním selže, avšak i zde může dojít ke spuštění dodatečného programu, který sice nezašifruje disk jako takový, ale dokáže tomu tak učinit na úrovni vytvořených dokumentů a instalovaných aplikací. (Network World, 2016)

Nejlepším způsobem, jak se těmto útokům bránit bývá proškolení zaměstnanců v rozeznávání podezřelých příloh a dodržování obecných zásad při pohybu na internetu. (Acronis, 2019)

3.18 **Online aspekty**

Vzhledem k celkem zřetelnému trendu současné doby čím dál více využívat služeb jako jsou cloudová úložiště, sociální sítě, e-shopy a další online služby, je celkem pochopitelné, že na organizace zabývající se těmito službami jsou kladeny mimořádné požadavky, co se bezpečnosti týče. Velká většina těchto omezení a doporučení již byla probrána v dřívějších částech této práce, proto zde uvedeme jen krátké shrnutí základních aspektů, které by měli být organizacemi v online prostředí dodržovány.

- V případě, že tomu tak není nutné, po uživatelích by nemělo být požadováno, aby se na našich stránkách přihlásili/registrovali (například pro pouhé prohlížení nabízeného zboží). Žádat o osobní informace bychom měli až v případě, že s námi zákazník hodlá obchodovat či nás jinak kontaktovat.
- Pokud shromažďujeme osobní informace, mělo by na webových stránkách existovat srozumitelné vysvětlení proč tomu tak uskutečňujeme.
- Uchovávané informace by měli být ukládány v zašifrované podobě.
- Pokud využíváme služeb dalšího zpracovatele, ve smlouvě s ním by mělo být jasně uvedeno, jaké má povinnosti týkající se zabezpečení použitých údajů.
- V případě, že na našich stránkách uvádíme obsah třetí strany (například reklamy a inzeráty), je vhodné zřídit kontaktní bod pro případné dotazy a stížnosti klientů (Nezmar, 2017 str. 233)

3.19 **Příklady dřívějších prohřešků**

Pro lepší přehled, jak mohou prohřešky (nejen) proti GDPR vypadat a jaké byli jejich následky, zde uvedeme několik příkladů (Business Insider, 2018):

V květnu 2017 byla ve Francii společnosti Facebook uložena pokuta činící 150 000 eur (v přepočtu cca 4 miliony Korun). Hlavním důvodem k tomu bylo, že za účelem profilování a cílené reklamy docházelo ke shromažďování aktivity uživatelů na internetových stránkách třetích stran pomocí cookies souborů, aniž by o tom byli uživatelé informováni. Facebook i přes poskytnutí tříměsíční lhůty na nápravu správní orgán ignoroval a uvedený problém odmítl řešit, což vedlo k uvedení sankce. (Nezmar, 2017 str. 256)

V září roku 2017 došlo díky chybě v zabezpečení k hackerskému útoku na účty služby Instagram, během kterého byly odcizeny telefonní čísla a e-maily příslušící odhadem k šesti milionům účtů. Tyto údaje byly následně nabídnuty k prodeji s cenou 10$ za položku. (Inc.com, 2017) O rok později pak došlo k náhlému růstu případů, kdy je uživatel odříznut od svého účtu a dojde ke změně například jeho biografie, jména, či kontaktních údajů. V tomto případě nebylo úplně jasné, jakým způsobem k odcizení účtů došlo. Co se týče škody, kterou společnost utrpěla, jednalo se především o reputaci a riziko, že mnoho uživatelů se rozhodne s platformou skončit a zůstane po nich pouze účet sloužící jako spambot zahlcující jejich odběratele nevyžádanými příspěvky. (Independent, 2018)

Jako několik příkladů úniků dat, které v nedávných letech nastaly pak můžeme uvést následující:

- Únik zašifrovaných hesel, e-mailových adres, čísel účtů a platebních informací zákazníků společnosti T-Mobile (2 miliony postižených osob) (Motherboard, 2018)
- Využitím chyby v kódu došlo o k úniku obecných (15 milionů) a citlivých údajů (14 milionů; lokalita, historie hledání, kontaktní údaje a další) přibližně 30 milionů uživatelů společnosti Facebook. (Business Insider, 2018)
- Údaje o 52,5 milionech uživatelů služby Google+. Šlo hlavně o jména, e-mailové adresy, věk a zaměstnání. Tento únik mimo jiné vedl k urychlení ukončení služby. (Business Insider, 2018)

- Analytický software Cambridgeské univerzity, který přímo či nepřímo shromáždil data údajně až o 87 milionech osob (toto číslo je nutné brát pro nedostatek zdrojů s rezervou; přímo ovlivněných bylo pouze přibližně 270 000 uživatelů, k dalším pak byl získán přístup v závislosti na jejich nastavení sdílení údajů s přáteli) a následně je předal například firmě zabývající se tvorbou cílených reklam na podporu volební kampaně současného amerického prezidenta Trumpa. (Business Insider, 2018)
- Hackerský útok na řetězec hotelů Marriott Starwood, při kterém byla odcizena databáze týkající se odhadem 500 milionů lidí a zahrnující mimo mailových adres například i údaje o platebních kartách. (Business Insider, 2018)
- Aktuální rekord podle některých zdrojů pak drží databáze Indických občanů Aadhaar. V tomto případě měla být údajně nedostatečným zabezpečením potenciálně postižena vice než miliarda osob. Vzhledem k tomu, že se jedná o unikátní vládní databázi, obsahuje Aadhaar prakticky veškeré relevantní informace o uvedených osobách. (ZDNet, 2018)

4 Vlastní práce

Hlavní náplň praktické části práce se zabývá porovnáváním aktuální legislativy (primárně Obecného nařízením o ochraně osobních údajů) s aktuálním stavem ve kterém se nacházejí organizace, které v rámci své činnosti provádějí zpracování osobních údajů. Pro provedení toho porovnání je nezbytné uskutečnění důkladného průzkumu, který přinese dostačující informace. Hlavními použitými způsoby shromažďování potřebných dat bude rozesílání dotazovacích mailů a studie webových stránek daných společností, avšak v případech, kde se naskytne příležitost dojde i k osobní návštěvě některé z poboček firmy a průzkumu přímo v terénu. Pro hodnocení, zda dané postupy dostatečně splňují předepsané požadavky bude využito mimo jiné znalostí získaných v teoretické části práce a dále materiálů, které již byli k podobným účelům vytvořeny a jejich kombinací.

Je nutné připomenout, že právě za účelem provedení úplné analýzy implementace GDPR byla samozřejmě zřízena pozice pověřence pro ochranu osobních údajů, který by v ideálním případě měl soulad s Nařízením zajistit. Účelem níže prováděných hodnocení je tedy často spíše dodatečná kontrola a je dosti pravděpodobné, že nedojde k odhalení žádných velkých nedostatků. V méně očekávaném případě, kdy nalezneme rozdíl mezi ideální a skutečnou situací však lze téměř jistě prohlásit, že upozorněním správce na případný nedostatek může dojít k odvrácení potenciálních budoucích problémů.

4.1 Posuzování

4.1.1 Sběr informací

Při posuzování jednotlivých firem je nutné nejdříve si objasnit, co všechno za informace budeme mít k dispozici a na která kritéria se budeme primárně zaměřovat. Prvním krokem bude prohledání veřejného registru zpracování osobních údajů. Tento krok není technicky vzato nutný, jelikož od 25.května 2018 (nástup GDPR) již správce nepodléhá oznamovací povinnosti. Jeho účelem je pouze získat přehled o tom, jak důkladně daná firma v minulosti dodržovala zákon o ochraně osobních údajů. Informace, které budeme v této databázi hledat jsou následující:

- Jaký právní titul používala firma ke zpracování osobních údajů? – Tuto informaci posléze porovnáme s tituly, které firma uvádí na svých stránkách.

Vhledem k tomu, že nejpoužívanějším odůvodněním dříve býval poskytnutý souhlas, jehož podmínky se s nástupem Nařízení poněkud zpřísnily, můžeme očekávat, že v tomto ohledu mohlo dojít k určitým změnám.

- Za jakým účelem byly osobní údaje zpracovávány?
- Jaké osobní údaje byly uchovávány? – Šlo pouze o základní popisné či adresní údaje, nebo docházelo ke shromažďování citlivých či dokonce biometrických údajů?
- Docházelo k předávání dat do zahraničí?

Po prozkoumání registru se přesuneme ke zkoumání internetových stránek, případně jiných dostupných médií. V této fázi se kromě porovnání zde uvedeného s registrem navíc snažíme zodpovědět na následující skupinu otázek:

- Jak dostupné, přehledné a srozumitelné jsou na stránkách poskytované informace?
- Má firma jmenovaného pověřence pro ochranu osobních údajů? Pokud ano, jsou jeho kontaktní údaje rozumně dostupné?

Poslední obecnou fází při sběru informací je rozesílání e-mailů s předpřipravenými dotazníky. Samozřejmě je možné, že na webových stránkách společnosti nalezneme daleko více než jsme doufali a dostane se nám odpovědí i na otázky které jsme původně plánovali získat za pomoci dotazníku. V případě, že k této události dojde, dotazník bude za účelem minimalizování nadbytečné práce na straně tázaného zkrácen, případně k jeho zaslání nedojde vůbec. Co se týče adresace těchto mailů, jejich cílem mohou být případné osoby na pozici pověřence pro ochranu osobních údajů, ale v případě jejich neexistence, nebo na základě jiných dalších vlivů budou cílena obecná kontaktní místa.

Cílem této činnosti bude zodpovědět na co nejvíce z následujících otázek:

- Jak rychle firma reaguje na dotazy? – V případě žádosti o poskytnutí podrobných informací má správce ve většině případů jednoměsíční lhůtu na vyřízení. U firem, u kterých budeme tyto informace požadovat, jde tedy o celkem důležitý faktor.
- Jak firma získává případný souhlas se zpracováním údajů? Jak jej dokazuje v případě sporů? – Vzhledem k tomu, že při spoléhání na souhlas leží důkazní břemeno na straně správce, je v jeho zájmu mít spolehlivou možnost poskytnutí souhlasu prokázat.

- Dochází k dalšímu zpracování?
- Jak jsou uchovávané údaje zabezpečeny? – Správce má povinnost zpracovávané údaje dostatečně zabezpečit a dobrým důkazem toho, že tuto povinnost bere vážně, jsou kroky, které za tímto účelem provedl.
- V případě, že firma rozesílá e-mailovou reklamu, umožňuje snadnou možnost opt-outu? – Rozesílání reklamy bez možnosti odhlášení odběru je nelegální. Zde se očekává, že všechny dotazované firmy odpoví kladně.
- Jak dlouho jsou osobní údaje jednotlivých subjektů uchovávány? – Informace je nutná pro posouzení dodržení zásady omezení uložení.
- Jak firma přistupuje k právu subjektu na portabilitu údajů? – Toto právo bude prověřováno hlavně v obecné rovině, ale u případů, kdy to bude možné, si autor práce vyžádá informace o své vlastní osobě.
- Dochází k nějakému automatickému rozhodování? – Otázka se bude soustředit hlavně na zjištění, zda nemůže být subjekt údajů tímto rozhodováním nějak poškozen.
- Jak jsou zabezpečeny přístroje jako tiskárny a počítače zaměstnanců? – Velká část dotazníku se zabývá zranitelností firmy vůči případným únikům či ztrátě zpracovávaných dat.
- Jak se firma zbavuje starých počítačů? – Podobně jako předchozí otázka, jde hlavně o posouzení bezpečnosti používaných postupů.
- Dodržuje firma nějaké kodexy/osvědčení? – Pokud firma splňuje nějaké oficiální standardy pro zabezpečení, je to při výsledném hodnocení velkou výhodou.
- Používá firma DMS? – Používání vhodného systému může vést k lepší bezpečnosti zpracovávaných dat.
- Má firma zkušenosti s ransomwarem? – V případě, že ke střetu s tímto problémem došlo, je vhodné vědět, jak se firma v chová v krizových situacích.
- Byla v dotazníku povolena makra? – Dotazník bude vybaven makrem, jehož jediným účelem bude poznačit, zda zaměstnanci odklikávají funkce, které mohou vést k potenciálnímu zanesení škodlivého softwaru. Nejedná se o

velmi spolehlivou metodu, ale i tak může přinést určitou informativní hodnotu.

Po získání všech těchto údajů může nastat čtvrtý krok, ve kterém dojde k osobní návštěvě některé z poboček za účelem získání podrobnějšího přehledu o tom, jak to v dané společnosti funguje. Nevýhodou již zmiňovaných dotazníků je totiž například jejich značná obecnost a fakt, že pokud by měli plně prozkoumat potřebnou tématiku, byly by téměř s absolutní jistotou ignorovány. Účelem osobní návštěvy je právě kompenzovat za tyto nedostatky.

4.1.2 **Hodnocení jednotlivých kritérií**

Vzhledem k tomu, že velké množství informací bude získáváno z elektronické komunikace a k přímému pěšímu průzkumu a osobnímu kontaktu s kvalifikovanými osobami dojde pouze u některých případů, je třeba si uvědomit, že hodnocení, které bude výsledkem této práce je v mnoha ohledech poněkud limitováno. Důkladný průzkum by vyžadoval plný přehled všech operací probíhajících ve firmě a přístup k datům a dokumentům s omezeným přístupem. Tato skutečnost ironicky vede k tomu, že pokud by firma autorovi práce dodala veškeré potřebné informace, s téměř úplnou jistotou by to znamenalo, že v implementaci Obecného nařízení o ochraně osobních údajů selhala.

Při hodnocení implementace bude hlavními posuzovanými kritérii dodržování zásad stanovených článkem 5 Nařízení, přičemž větší prostor se dostane zásadám o zákonnosti, korektnosti a transparentnosti a o integritě a důvěrnosti. Nyní následuje podrobnější popis kritérií:

- Zásada zákonnosti, korektnosti a transparentnosti – Zde se bude hodnotit například vhodnost použitého právního titulu či způsobu opatření souhlasu. Dále pak jde o posouzení, zda jsou informace poskytované dotčeným subjektům dostupné a dostatečně přehledné a srozumitelné. Jelikož případná existence Pověřence napomáhá při kontaktu se subjekty údajů, uvedeme případné informace, které se ho týkají sem.
- Zásada účelového omezení – Hodnotíme, zda je uvedený účel jasně definovaný a zda dává smysl.

- Zásada minimalizace – Zde se snažíme posoudit, zda činnosti, které firma provádí, a data, které shromažďuje, nejsou zbytečně přehnaná s ohledem na jí uváděný účel.
- Zásada přesnosti – Posuzujeme, zda informace, které firma uchovává, vyžadují pravidelnou aktualizaci. Dále pak hodnotíme, jak je daná aktualizace provedena a také to, zda při shromažďování údajů dochází k nějaké kontrole nezpochybnitelnosti zdroje, ze kterého jsou tyto údaje získávány.
- Zásada omezení uložení – Jelikož údaje, které firma uchovává ve velké většině případů postupně ztrácí na hodnotě, posuzujeme, zda doba jejich uchovávání rozumně odpovídá jejich potřebě. Této a následující zásady se pak také týká způsob, jakým se firma zbavuje zastaralých přístrojů, které mohou stále nějaké využitelné informace obsahovat.
- Zásada integrity a důvěrnosti – Zde řešíme hlavně přímo způsob, jak jsou v organizaci zabezpečena jednotlivá zařízení. V případě, že by došlo k odcizení, znepřístupnění, nebo poškození údajů, je to právě tato zásada, která trpí. Mezi parametry, které budeme hodnotit patří jak fyzická dostupnost hardwaru, tak používaný software, či lidský faktor v podobě například heslové politiky či předchozí zkušenosti s virovými útoky.
- Princip zodpovědného přístupu a prokazování souladu – Kromě povinnosti dodržovat jednotlivé zásady musí být správce navíc schopen v případě pochybností dokázat, že tak opravdu činí.
- Mezinárodní transfery – Vzhledem k tomu, že většina hodnocených firem bude pravděpodobně působit pouze na českém území, je nepravděpodobné, že se budeme zabývat předáváním údajů do zemí mimo Evropskou Unii. I přesto dojde alespoň k letmé kontrole, zda tomu tak nedochází a pokud ano, jaké jsou poskytované záruky.
- Práva subjektů – Kromě zkoumání přímo údajů jako takových zjistíme i to, zda správce dostatečně respektuje práva, která subjektu Nařízení přiznává. Zajímat nás bude například neodbytnost zasílaných obchodních sdělení, možnost vyžádat si kopii údajů, které jsou o subjektu uchovávány, nebo obecná reakční doba mezi kontaktováním firmy a její odpovědí na položené otázky.

4.1.3 Úprava použitých postupů po absolvování diplomantského semináře

Vzhledem k tomu, že získání podrobnějších informací o implementaci GDPR se ukázalo složitější, než byl prvotní odhad, většina zkoumaných firem skončila na úrovni porovnávání informací uváděných na internetových stránkách. Vzhledem k tomu, že údaje získané touto cestou jsou poměrně obecné a zároveň se zde vyskytuje riziko, že plně neodpovídají skutečnosti bylo nutné poněkud upravit, jakým směrem se bude práce ubírat.

Původní plánovaný rozsah práce se dále ukázal být příliš velký a výsledky průzkumů by tedy obsahovaly pouze obecné informace. Z těchto důvodů došlo ke zmenšení počtu zkoumaných subjektů a následně k zaměření se především na implementaci v jedné konkrétní firmě (IGNUM s.r.o.) u které je větší pravděpodobnost že budou k dispozici i podrobnější postupy a možnost ověřit si jejich uskutečňování v praxi.

Následující část práce lze tedy rozdělit na hodnocení firem na pomocí staré metodiky na základě studia a analýzy dokumentů a dotazníkového šetření s relativně obecnými závěry a na podrobnější hodnocení založené na rozhovorech s odpovědnými zaměstnanci a zúčastněném pozorováním přímo z provozu.

4.2 Zkoumané firmy

4.2.1 Výzkumná agentura STEM/MARK

Společnost STEM/MARK je agentura zabývající se prováděním marketingových výzkumů pro klienty z rozličné škály oborů. V závislosti na konkrétních požadavcích se jednotlivé prováděné průzkumy mohou značně lišit, ale obecně spadají buďto do kategorie kvalitativní (například hloubkový rozhovor, kde krom samotných odpovědí záleží i na jejich odůvodnění), nebo kvantitativní (například telefonáty zahrnující vyplňování dotazníku).

Návštěva veřejného registru a stránek firmy nám prozradí, že dříve byl hlavním používaným právním titulem poskytnutý souhlas, což vzhledem k povaze hlavní činnosti (výzkum trhu, marketing) dává smysl. Tituly jako oprávněný zájem a plnění smlouvy jsou pak využity při aktivitách týkajících se přímo zadavatelů konkrétních výzkumů. Zaměříme-li se na vztah firmy k respondentům, kategorie zpracovávaných údajů se poněkud různí podle typu průzkumu, minimálně se však jedná o kontaktní a základní sociodemografické údaje. Po shromáždění údajů pak dochází k jejich pseudonymizaci a výsledná data

předávaná žadatelům o průzkum lze dle firmy už považovat za anonymní. V tomto ohledu lze tedy říct, že na poli zákonnosti a jasně daného účelu si firma vede celkem dobře. Totéž se vzhledem k povaze činnosti dá pravděpodobně prohlásit i o minimalizaci. Lhůta, po které STEM/MARK maže uchovávaná data respondentů, je dle jejich tvrzení maximálně půl roku po dokončení daného průzkumu což opět vzhledem k povaze jejich činnosti lze považovat za relativně pochopitelné. Co se týče transparentnosti, odkaz na ze zákona poskytované údaje se nenachází v patičce nýbrž je mu přímo vyhrazen odstavec na domovské stránce. (viz obrázek v příloze číslo 3). Toto lze považovat za dostačující, ale autor této práce si dovolí tvrdit, že přidáním odkazu i do patičky by nebylo příliš složité a vedlo k ještě lepší dostupnosti. Je vhodné dodat, že při provádění telefonického výzkumu je dotazovaný informován o všech potřebných náležitostech pomocí předem připravené nahrávky. Co se transparentnosti týče, lze říci, že STEM/MARK si vede velmi dobře. Na dotazovací mail firma neodpověděla ani po dvou měsících. Zda mail pouze nedorazil, nebo firma nereaguje na žádosti se nepodařilo zjistit.

4.2.2 **Alza**

Vzhledem k tomu, že internetový obchod Alza.cz lze označit jako největší na českém trhu (už roku 2016 jeho roční tržby přesahovali 17 miliard Kč (Peak.cz, 2018), a nyní se pohybuje kolem pětadvaceti (Alza.cz, 2019)), je celkem pochopitelné, že při své činnosti zpracovává rozsáhlé množství osobních údajů a případné špatné nakládání s nimi by mohlo negativně ovlivnit velké množství zákazníků.

Podobně jako u jiných webových stránek i zde se informace o zpracování nachází v patičce, ale kromě běžného odkazu na mnohostránkové vysvětlení je tu i vyskakovací „bublina“, která poskytne rychlý přehled o účelu a oprávněnosti zpracování.

Jelikož se jedná o obchod fungující ve velkém na principu objednávek a dovozu zboží, je plně pochopitelné, že dochází ke zpracování základních identifikačních a kontaktních informací, které jsou k poskytování těchto služeb naprosto nezbytné. U některých služeb jsou pak shromažďovány další údaje za účelem ověření schopnosti splácet. Dále dochází například ke shromažďování údajů o IP adrese či webovém prohlížeči a používání souborů cookies (technických a funkčních, které jsou pro chod obchodu nutné, tak i soubory Google Analytics, které jsou pak využívány pro marketingové účely). Vzhledem k tomu, že tyto údaje jsou anonymizovány, nejsou z hlediska GDPR příliš

relevantní. Co se analytických cookies týče, Alza dokonce uvádí odkaz na zásuvný modul do prohlížeče, který je umožňuje zablokovat. Co se účelu uchovávaných údajů týče, spadají do kategorií nezbytnosti pro poskytování služby, péče o zákazníky (jako příklad lze uvést nahrávání hovorů se zaměstnanci callcentra, nebo třeba využívání již zmíněných Google analytics či A/B testování) a reklamní činnost. Z pohledu zásady o zákonnosti je zde tedy využito právních titulů plnění smlouvy, oprávněného zájmu (jako zajímavost lze uvézt ochrana proti nelegálnímu šíření e-knih pomocí jejich označení jménem a adresou kupce) a poskytnutého souhlasu (přímý marketing či ověření schopnosti splácet při prodeji „za Třetinku“). Ohledně předávání údajů třetím stranám, kontaktní a adresní údaje předávané kvůli dopravě jsou po doručení zboží neprodleně mazány a údaje o platebních kartách si uchovává použitá platební brána (Alza nemá v závislosti na individuálním nastavení buď vůbec, nebo pouze v anonymizované podobě). K dalšímu předávání dochází pak například při koupi elektronického obsahu (například předplatné časopisů), nebo při prověřování platební schopnosti u koupě na splátky (kromě rozličných registrů dlužníků se jedná například o Nikita Engine s.r.o. což je firma zabývající se Big Data analýzou). Obecně lze prohlásit, že co se zákonnosti transparentnosti a korektnosti týče, nebyly u Alzy nalezeny žádné výrazné nedostatky.

Doba, po kterou jsou osobní data uchovávána, se logicky liší v závislosti na druhu konkrétních údajů a účelu jejich shromažďování. Pokud jde o ta zaštítěná právním titulem poskytnutého souhlasu, jeho platnost vyprší po uplynutí 7 let. Tento časový úsek lze označit jako dlouhý, ale vzhledem k tomu, že souhlas lze zároveň kdykoliv odvolat, nemělo by to představovat problém. Podobně lze říci, že například uchovávání daňových dokladů po dobu 10 let je plně pochopitelné. Co by se možná dalo označit za lehce přehnané je uchovávání dat z uživatelských účtů 5 let po jejich zrušení, dle autora práce by bylo vhodnější přejít na uchovávání pouze základních dat za kratší dobu. Dále by šlo něco podobného říci o nahrávkách hovorů Call centra (až 1 rok) a kamerových záznamech (90 dní). Je pravda, že kamerové nahrávky mohou pomoci při výskytu případného protiprávního jednání, ale většině případů by měla být postačující lhůta jednoho až dvou týdnů. Uchovávání těchto záznamů téměř sedmkrát tak dlouho by se dalo hypoteticky ospravedlnit v případě, že pravidelně přinášejí významný užitek i po uplynutí autorem navrhované doby. Vzhledem těmto skutečnostem lze splnění zásady omezení uložení označit jako lehce diskutabilní.

Pokud jde o zásadu integrity, zasluhuje si ovšem Alza určitou pochvalu. Veškerá webová komunikace by měla být dle všeho šifrována, uchovávaná data uložena v často zahashované podobě na serverech s monitorovaným přístupem a při přihlašování je možnost zapnutí dvoufázového ověření pomocí SMS či mailu. Samotná hesla k uživatelským účtům jsou pak ukládána pouze v podobě hashovacích klíčů získaných metodou Bcrypt o dvanácti iteracích (tato metoda je obecně považována za bezpečnou, byť někdy lehce složitější na implementaci (Hacker Noon, 2018)).

V případě, že si zákazník chce provést opravu uložených údajů, je mu k dispozici standardní postup úpravy v nastavení účtu a pokud si přeje vyžádat informace, které o něm firma uchovává, nebo vymáhat jejich smazání, může tak dokonce učinit přímo pomocí zde se nacházejících tlačítek. Po vyžádání zaslání nahromaděných údajů došlo k jejich zaslání již během noci téhož dne (data jsou zasílána ve formátu xml, ukázka v příloze 4). Lze tedy prohlásit, že zásady přesnosti a plnění práv subjektů je prováděno v uspokojivé míře.

Pro zaslání zjednodušeného dotazníku bylo využito firmou nabízeného formuláře, a zároveň došlo k vyžádání si shromážděných údajů. Jako zajímavost se ukázalo, že tento formulář dle všeho neukládá ani základní formátování jako je zakončení řádku a poněkud delší dotaz skončil jakožto špatně čitelný jednolitý text. Byť pravděpodobnost takto dlouhých dotazů je minimální, lze celkem jistě prohlásit, že tento nedostatek může vést ke ztížení práce zaměstnanců, kteří se starají o zákaznickou podporu a nebylo by na škodu jej opravit. Je ovšem možné, že k deformaci dojde až při zaslání potvrzení na tazatelův e-mail a samotná komunikace tedy není ovlivněna (Po několika dalších zkušenostech s podobnými případy si autor práce nyní dovoluje předpokládat, že zde dochází přesně k tomu.). Na druhou stranu je formulář omezen typem souborů, které přijímá jako přílohu a automaticky tedy blokuje například excelovské dokumenty s podporou maker, či jiné potenciálně škodlivé koncovky.

Odpověď na odeslaný dotaz dorazila po deseti dnech a dá se tedy říci, že rychlost reakce na zákaznické otázky tohoto typu je relativně přijatelná. Ideální by samozřejmě bylo, kdyby doba byla kratší než týden, ale vzhledem k tomu, že zákonem daný limit je jeden měsíc a jednalo se o nestandardní dotaz, nejedná se ze strany Alzy o žádný prohřešek. Co se samotného obsahu odpovědi týče, kvůli smlouvě o mlčenlivosti a firemní politice nebyl dotazník vyplněn. Byla však zodpovězena otázka týkající se značné délky uchovávání

kamerových záznamů (90 dní). Vhledem k dřívějším případům důkazní nouze při zpětném odhalování trestné činnosti považuje firma tuto lhůtu za nezbytnou a oprávněnou.

Závěrem tedy můžeme říct, že internetový obchod Alza.cz požadavky na správnou implementaci GDPR splňuje, a to i v zásadě o omezení uložení, která zpočátku vzbuzovala určité pochybnosti.

4.2.3 **Českomoravská stavební spořitelna – centrála**

Jak již název napovídá, tato firma se zabývá poskytováním rozličných finančních služeb. Z těchto důvodů musí přirozeně zpracovávat velké množství osobních údajů a v případě, že by při těchto činnostech došlo například k jejich úniku či ztrátě, mohlo by dojít k výraznému negativnímu dopadu na rozsáhlou skupinu lidí. (Jen roku 2017 bylo uzavřeno více než 152 tisíc nových smluv o stavebním spoření, nemluvě o jiných poskytovaných službách) (Finance.cz, 2018).

4.2.3.1 Právní stránka

Při pohledu do rejstříku nalezneme tři typy registrovaných zpracování: nahrávání telefonických hovorů, zpracování fotografií zaměstnanců a vedení kamerového systému. Samotné zpracování, ke kterému dochází při procesech nezbytných například pro uzavření smlouvy zde uvedeno není. Zda zde byl dříve uveden nějaký podobný záznam není jisté, ale například vzhledem k číslování položek (002,003,004) lze spekulovat, že byl z nějakých důvodů odstraněn.

Co se týče webových stránek, odkaz na informace o zpracování se nachází v patičce všech stránek a byť není příliš výrazný, není problémem ho jednoduše nalézt. Po rozkliknutí zde můžeme nalézt rozsáhlé množství textu rozdělené do jednotlivých rozbalitelných kategorií jako například práva subjektu či zpracovávané údaje. Co se transparentnosti a přehlednosti týče, je zde velmi dobře vidět, že spořitelna (nyní spadající pod ČSOB) bere tyto zásady vážně.

Jako kategorie osobních údajů, které firma zpracovává, lze uvézt běžné identifikační a kontaktní údaje, ale dále sem spadají například informace o hardwaru a prohlížeči, které klient používá při elektronické komunikaci, výsledky neanonymních průzkumů, profilovací údaje (včetně informací o důležitých událostech v životě klienta, jako například stěhování),

ale i údaje o platební morálce či zdravotním stavu. Pro odůvodnění posledních dvou zmiňovaných kategorií firma uvádí skutečnost, že je tomu tak nutné pro řádně poskytování úvěrů a životního pojištění a dodává, že v případě citlivých údajů vždy navíc od zákazníku vyžaduje souhlas. Toto chování se dá s ohledem na druh poskytovaných služeb označit za plně pochopitelné.

Pokud jde o spořitelnou používané právní tituly, i ty jsou celkem přehledně rozepsány. Kromě běžného zpracování za účelem smlouvy či na základě souhlasu můžeme nalézt případy zpracování pro dodržování právních předpisů (zákony proti praní špinavých peněz, o stavebním spoření či o doplňkovém penzijním připojištění) nebo vlastní oprávněný zájem (marketing, posuzování pojistného rizika, prevence podvodného jednání, ochrana majetku). Lze tedy říci, že dochází k plnému využívání dostupných titulů a firma nespoléhá pouze na snadno zrušitelný souhlas.

Při určení délky uchovávání údajů ČSOB (a tedy i pod ní spadající spořitelna) využívá kombinaci zákona o bankách a oprávněného zájmu kvůli možným promlčecím lhůtám k tomu, aby některé údaje (například o platbách či úschově cenných papírů) uchovávala dvacet let, případně i déle. Zde autor práce přiznává, že při pohybu v tomto měřítku není plně kvalifikován k posouzení délky této lhůty, ale očekává, že při provedení dostatečných opatření by měla být připustitelná. Co se týče používání údajů za účelem odsouhlasené reklamy, nejpozdější termín pro smazání je 5 let po ukončení služby (případně rok, pokud klient nikdy nezačal používat). Tato lhůta přijde autorovi práce poněkud dlouhá, ale vzhledem k tomu, že souhlas lze snadno odvolat, neměla by představovat značný problém.

Vzhledem k rozsahu společnosti je dále pochopitelné, že dochází k situacím, kdy jsou osobní údaje předány třetím stranám. Nejde jen o sdílení v rámci ČSOB skupiny (například změna kontaktních údajů u klientského servisu, nebo marketingové účely), ale předávání údajů například České poště, poskytovatelům cloudových úložišť, nebo třeba advokátům. Tyto zpracování jsou pak prováděny primárně pod tituly souhlasu, plnění smlouvy, nebo dodržování právních povinností. Jelikož vyjmenovávat, byť jen všechny významnější příjemce dat a použité tituly by nemělo žádný praktický přínos, zmiňme dále pouze společnost KBC Group NV, které jakožto svému vlastníkovi ČSOB předává v rámci reportingu základní údaje o osobách, které jednají za jejich klienty.

Pověřenec pro ochranu osobních údajů byl firmou jmenován a kontakt na ni je k dispozici na webových stránkách.

4.2.3.2 Bezpečnostní politika firmy

Co se týče podrobnějšího chodu firmy, osobní průzkum a rozhovor přímo se zaměstnancem firmy přinesly následující informace (kvůli použití jakožto příklad pro porovnání s jinými firmami jsou zde uvedeny do větších podrobností):

- Stav tiskáren – Většina tiskáren používaných zaměstnanci Českomoravské stavební spořitelny se nachází v prostorách, které jsou dostupné pouze zaměstnancům firmy (pro vstup nutná čipová karta), přičemž pro provedení tisku je nutné buďto přiložit čipovou kartu, nebo použít zaměstnanecký kód pro tisk. Tento kód je jednou za přibližně 180 dní nově generován, přičemž zaměstnanec má možnost si jej posléze změnit. Lze tedy prohlásit, že šance náhodného úniku dat touto cestou je takřka nulová a případný neoprávněný úmyslný přístup někým mimo firmu je taktéž minimalizován.
- Stav počítačů – Jelikož se počítače nacházejí v kancelářích, ke kterým kromě přiřazených zaměstnanců (většinou 2-5) má klíče pouze ostraha a vedoucí oddělení, zamykat přímo jednotlivé počítače by bylo spíše ke škodě. Co se softwarového zabezpečení týče, k odemčení počítače je nutné mít jednak čipovou kartu (v případě její ztráty či poškození je přiděleno dočasné heslo), tak následně i přihlašovací údaje přímo do systému. Šance na přístup někým mimo firmu je tedy minimální. Samotní zaměstnanci jsou pak omezeni zablokováním možnosti cokoliv z počítače kopírovat na externí média. Jediným realistickým způsobem, jak by mohli údaje uniknout je tedy jejich odeslání například mailem, a i to je možné pouze na odděleních s přístupem na internet. Pro ochranu před případnými virovými útoky je na počítačích instalován antivirový program (zdroje v tomto případě si nejsou jisté, zda se jedná o AVG nebo jiný software).
- Zbavování se starých počítačů – V případech modernizace hardwarového vybavení kanceláří docházelo k přenesení starých sestav na jedno místo, kde posléze došlo ke zformátování disků a jejich vyčištění pomocí

specializovaného softwaru. V případě jejich následného prodeje tedy nehrozilo, že někdo získá na nich dříve zpracovávané citlivé údaje. Tato informace oproti ostatním pochází z doby ještě před účinností GDPR, ale vzhledem ke zpřísnění požadavků lze očekávat, že nyní prováděné postupy jsou buď stejné, nebo ještě přísnější.

- Školení a heslová politika – Heslo k přístupu do systému si zaměstnanec minimálně jednou za rok nastavuje nové, přičemž musí splňovat alespoň základní minimum osmi znaků a kombinace velkých a malých písmen a číslic. Dále je pak vhodné zmínit, že školení ohledně e-mailové komunikace, ochrany údajů a dalších podobných tematik probíhají online v intervalech jednoho až dvou let v závislosti na daném typu.
- Zacházení s dokumenty – Pro správu dokumentů je ve firmě zaveden systém s rozdílně nastavenými oprávněními podle konkrétních rolí, jakou daný zaměstnanec zastává. Oproti pouhému sdílenému disku, nebo předávání souborů přes mail jde o mnohem bezpečnější postup, nemluvě o tom, že při velikosti firmy se jedná o jedinou reálně proveditelnou možnost.
- Stav Wi-Fi – Přístup k bezdrátové síti je chráněn heslem, které se dle všech zjištěných informací mění jednou za den. Firma neposkytuje otevřenou síť pro návštěvníky a heslo je přístupné pouze určitým osobám, nebo na vyžádání.
- Další poznatky – Kromě výše řečených postupů je vhodné zmínit, že firma jednou za čas provádí namátkové kontroly zaměřené například na zacházení s citlivými dokumenty (čtěte: „Vytištěné složky zákazníků neleží volně na stole po skončení pracovní doby a podobně.“).

Centrála Českomoravské stavební spořitelny se, alespoň pokud se jedná o zde uvedené poznatky, dá označit jako relativně ukázkový příklad toho, jak by měla být ochrana dat implementována.

4.2.4 ČSOB

Známá také jakožto Československá obchodní banka, a. s., ČSOB je bankovní instituce poskytující služby jak fyzickým, tak právnickým osobám. Ačkoliv se původně

jednalo o organizaci vlastněnou českým/československým státem, roku 1999 došlo k jejímu prodeji belgické společnosti KBC Group. Koncem roku 2018 měla skupina ČSOB více než 3,6 milionu klientů a 265 poboček (ČSOB, 2019) z čehož plyne značné množství zpracovávaných údajů, a tedy i vysoká zodpovědnost za správné zavedení nezbytných opatření.

Vzhledem k tomu, že ČSOB a výše probíraná ČMSS spadají nyní pod stejného vlastníka, je celkem pochopitelné, že způsob implementace Nařízení je v mnoha ohledech podobný. Z tohoto důvodu se bude tato část práce zabývat pouze krátkým porovnáním dotčených institucí.

Jak je už celkem zvykem, odkaz na podrobnější informace o zpracování lze nalézt v patičce většiny stránek. Podobně jako u ČMSS jsou stránky ve formě rozbalitelných tematických celků, takže návštěvník nemá problém nalézt odpověď na konkrétní otázky. Při zběžném pohledu na obsah těchto odstavců je zřejmé, že se jedná o tentýž text s drobnými úpravami, to vzhledem k jeho modulární povaze a stejným vlastníkům firem nelze označit jako překvapení. Při detailnějším prozkoumání si lze všimnout, že stránky ČSOB obsahují některé odstavce navíc (jako příklad lze uvést postoj ke zpracování biometrických údajů). Jako obstojnou hypotézu lze tedy považovat, že obsah stránek ČSOB byl do těch ČMSS zkopírován a následně upraven a očesán o nadbytečné odstavce.

Jako významné pozitivum lze označit dvě přehledné tabulky, které se na informačních stránkách nacházejí. První se nachází hned pod hlavičkou a obsahuje příklady zpracování, ke kterým dochází při běžných aktivitách, kterých se zákazník a banka účastní. Díky tomu není ihned nutné, aby se návštěvník nořil do rozsáhlého textu, ale i tak měl přístup k základnímu přehledu Kdy, Proč a které údaje ČSOB zpracovává a zda jde tyto případy nějak ovlivnit. Druhou je přehled hlavních právních předpisů, které se zpracováním zabývají a konkrétních odvětví a procesů, které ovlivňují.

Jako další krok průzkumu fungování firmy byla 29.9. zaslána žádost o poskytnutí zpracovávaných osobních údajů (viz přílohy). Odpověď na ni dorazila již za tři dny, což vzhledem k zákonné jednoměsíční lhůtě lze považovat za ukázkové plnění povinností.

Závěrem lze tedy říct, že co se dodržování zásad GDPR týče, průzkum neodhalil u skupiny ČSOB, pokud ignorujeme níže uvedenou zajímavost, žádná zásadní porušení. Firma používá prakticky celé spektrum právních titulů a má jmenovaného pověřence pro každou společnost. Zákazníci mají k dispozici přehledný souhrn informací a v případě zájmu

o výpis shromážděných dat firma reaguje velice rychle. Údaje, které jsou uchovávané dávají smysl vzhledem ke stanoveným účelům a umožňují jednoduchou aktualizaci. Za předpokladu, že kroky prováděné v Českomoravské stavební spořitelně jsou standardem napříč celou skupinou ČSOB, zásada o integritě a důvěrnosti také není brána na lehkou váhu. Výše zmiňovanou zajímavostí je to, že jako dobu uložení údajů o klientech je až 20 let a u zaměstnanců dokonce 45 (alespoň dle informací v zaslaném výpisu uchovávaných osobních údajů). Dle všeho se jedná pouze o ve výpisu uvedené údaje (hlavně ty základní identifikační) zatímco podrobnosti o transakcích a další důvěrnější dokumenty mají trvanlivost 5-10 let v závislosti na typu. Jestli krom základního přehledu je o zaměstnancích uchováváno ještě něco dalšího se nepodařilo autorovi práce zjistit. Byť je tato lhůta pravděpodobně dostatečně odůvodněná (vést si alespoň základní evidenci o bývalých zaměstnancích lze označit jako smysluplné), lze ji vyzdvihnout jako příklad situace, kde podstata Nařízení může poněkud kolidovat se „selským rozumem“. Vzhledem k tomu, že údaje nebudou pravděpodobně dále aktualizovány, informace jako bydliště, telefon a mail by pravděpodobně porušovali zásadu o přesnosti. Zde se autor práce necítí dostatečně kvalifikovaný na to, aby situaci řádně posoudil, a proto ji pouze zmiňuje jako zajímavost.

4.2.5 **Air/Bank**

Jako další zástupce z oblasti bankovnictví byla vybrána Air/Bank, která na český trh vstoupila 22.listopadu 2011. Oproti jiným bankám se soustředí spíše na poskytování služeb menším klientům, zatímco větší firmy přenechává jiným. Roku 2017 měla Air/Bank více než 600 tisíc klientů což ji z tohoto hlediska umístilo na osmou pozici (Finance.cz, 2018). K hodnocení byla banka vybrána pro porovnání s výše zmíněnou ČSOB, oproti které je stále relativně malá.

Návštěva veřejného rejstříku ukázala, že před nabitím účinnosti GDPR firma pro odůvodnění zpracování osobních údajů používala primárně v té době univerzálně aplikovaný souhlas subjektu. Právní tituly, jako je ochrana majetku a dodržování smlouvy, nastoupily většinou až spolu s Nařízením.

Hledání podrobnějšího vysvětlení zpracování osobních údajů trvalo poněkud déle, jelikož na rozdíl od předchozích zkoumaných institucí na ně nemá AirBank na stránkách žádný viditelný odkaz, ale je nutné hledat v dokumentech ke stažení. Vzhledem k tomu, že

se jedná o statické PDF hledání konkrétních informací je o něco složitější, než například u ČMSS a ČSOB, jelikož zde nejsou k dispozici rozbalovací kategorie. Navzdory těmto faktům je ale dokument stále ještě relativně přehledný a zásada transparentnosti tedy zůstává dodržena. Jako možné zlepšení by zde tedy autor práce mohl doporučit inspirovat se u konkurence a založit pro osobní údaje samostatnou stránku s odkazem v patičce webu.

Co se zásad účelového omezení a minimalizace týče, banka zpracovává mimo jiné identifikační, kontaktní a charakteristické údaje a informace o vedených službách. Všechna tato data jsou vzhledem k povaze firmy a poskytovaných služeb pochopitelná a odůvodněná mimo jiné. Dále dochází například k nahrávání telefonních hovorů na což je zákazník upozorněn pouze v případě, že je na straně volajícího. Jako odůvodnění je zde použita snaha nenatahovat hovor a nemarnit zákazníkův čas. Tímto by pravděpodobně k žádnému hrubému porušení zásady o transparentnosti docházet nemělo. Jedná se o běžně používanou praktiku a zákazník byl o tomto faktu nejspíš již dříve informován například při podepisování smlouvy. Obecně lze říci, že se pravděpodobně jedná o příklad situace, kdy doslovné dodržování zásady není úplně nutné. V dokumentu firmy lze dále najít tabulku obsahující přehled běžných zpracování, včetně kategorie údajů a odůvodnění. Další drobnou zajímavostí je, že dochází k uchovávání biometrických údajů (konkrétně vizuální záznam ručního podpisu včetně doplňkových údajů pořizovaný zařízením SignPad). Tyto údaje jsou uchovávány v zašifrované podobě. V dokumentu je zde uvedeno, že dokud nedojde k rozšifrování, nejedná se o citlivé údaje. S tímto tvrzením autor této práce úplně nesouhlasí, jelikož dešifrovací klíč je firmě stále k dispozici, ale uznává že se jedná spíše o nešťastnou formulaci. Co se vytváření analytických modelů a přímého marketingu týče, firma buďto zpracovává údaje anonymizované, nebo nabízí možnost zasílání odmítnout. Ve výsledku lze říci, že nebylo nalezeno žádné porušení zásad minimalizace a účelového omezení.

K nevratnému mazání údajů klientů dochází 10 let po ukončení smluvního vztahu. Kamerové údaje jsou uchovávány 35 dní, záznamy z bankomatů 60 a webové formuláře s žádostí o kontakt 1 měsíc. Všechny tyto lhůty lze označit jako dodržující zásadu o omezení uložení.

Jde-li o práv subjektu údajů na přenositelnost, výmaz, či poskytnutí výpisu údajů, firma na ně upozorňuje, ale jelikož autor práce ani nikdo z jeho okolí s Air/Bank nikdy neměl uzavřenou smlouvu, nelze ověřit rychlost jejich plnění. Kontakt na pověřence je veřejně dostupný.

Jako následující krok proběhlo zaslání dotazníku, jehož přijetí bylo potvrzeno téměř okamžitě. Z odpovědi bylo zřejmé, že ke kontrole e-mailů používá firma antivirus Kaspersky, který verzi dotazníku obsahující makra okamžitě smazal, a proto byla zaslána alternativní verze bez nich.

Na dotazník AirBank reagovala již následující den. Jelikož firma považuje konkrétní způsob technické implementace za bezpečnostně citlivé téma (což lze v rámci hodnocení označit jako pozitivní prvek), bylo ale zodpovězeno jen několik otázek. Tiskárny jsou zabezpečeny nutností použít zaměstnaneckou čipovou kartu, což slouží jako prevence úmyslného odcizení dokumentů, tak neúmyslného smíchání s jinými dokumenty. Připojení k Wifi zaměstnanců je možné jen ze specifických zařízení a síť je oddělená od té pro návštěvníky (která je navíc zabezpečena periodicky se měnícím heslem). Toto přispívá k ochraně před narušením bezpečnosti případným útočníkem. Jako poslední informaci AirBank poskytla fakt, že údaje klientů jsou uchovávány již od počátku firmy pod přiřazeným identifikátorem, a ne například pod rodným číslem. Díky tomu je možné s nimi pracovat v pseudonymizované podobě, což snižuje potenciální škodu v případě částečném úniku dat.

4.2.6 **Komerční banka**

Posledním zkoumaným zástupcem na poli bankovnictví byla zvolena Komerční banka, jelikož spadá mezi trojici s největším počtem klientů (Finance.cz, 2018).

Podobně jako u AirBank bylo ve veřejném rejstříku zpracování k nalezení mnoho činností odůvodněných právním titulem souhlasu subjektu, bylo zde však i více případů, které se na souhlas nespoléhaly.

Co se týče přístupnosti aktuálních informací o zpracování osobních údajů, webové stránky nevybočují a obsahují běžně používaný odkaz v patičce vedoucí na stránku s obsahem rozděleným do kategorií.

Jako hlavní zákonné tituly používá KB hlavně plnění povinností (ochrana trhu, daňové povinnosti…), plnění smlouvy a oprávněný zájem (bezpečnost…) zatímco udělený souhlasu používá jen pro personalizovaný marketing a několik vedlejších služeb (TelcoScore, některé typy platebních karet). Pokud jde o kategorie zpracovávaných údajů, jedná se opět o standardní kombinaci identifikačních a kontaktních údajů spolu se sociodemografickými daty a majetkovými poměry používanými například ke zjištění

schopnosti splácet. Zásady zákonnosti, transparentnosti a účelového omezení nevykazují žádná výrazná porušení.

Jelikož KB uveřejňuje i informační memorandum týkající se zaměstnanců naskytla se možnost porovnání délky uchovávaných údajů zaměstnanců s délkou stanovenou u ČSOB. Jako lhůtu pro uchovávání osobních údajů řadových zaměstnanců potřebnou pro dostatečné splnění právní povinnosti uvádí Komerční Banka 30 let (na Slovensku 70), pro hlasové záznamy 5 let a pro záznamy z IS 10 let. U žadatelů u zaměstnání a externistů je doba pochopitelně kratší a to 6 měsíců po skončení náboru (24 se souhlasem), respektive 5 let (10 Slovensko). Data klientů bývají uchovávána něco přes 10 let po ukončení smluvního vztahu. Ignorujíce slovenské lhůty můžeme stále prohlásit, že podobně jako u ČSOB jde o relativně dlouhou dobu během, které data téměř jistě ztratí na přesnosti. Jelikož je jako důvod uvedeno dodržování povinnosti, můžeme do určité míry předpokládat, že předpokládat, že zde dochází k povolenému archivování. Dodržení zásady omezení uložení je tedy opět poněkud diskutabilní, ale pravděpodobně ve výsledku označitelná jako procházející.

4.2.7 **Ignum**

4.2.7.1 Úvodem

Jako hlavní firma pro posouzení implementace GDPR byla vybrána hostingová společnost IGNUM sídlící na Praze 3. Důvodů pro zvolení této společnosti je několik. Jedná se o firmu zabývající se poskytováním webového hostingu, prodejem SSL certifikátů a registrováním doménových jmen a při její činnosti tedy běžně dochází nejen ke standardnímu zpracování osobních údajů, ale často i k jejich předávání do zahraničí (ať už v rámci Evropské Unie nebo mimo ni). Dalším důvodem je skutečnost, že u této firmy bylo coby aktuální zaměstnanec relativně snadné na vlastní oči získat přehled o tom, jak jsou předpisy skutečně implementovány a nebylo nutné spoléhat se na e-mailovou komunikaci u které je riziko, že druhá strana údaje neposkytne vůbec, nebo pravdivost jí sdělených informací nelze nijak jednoduše potvrdit. Kromě studie materiálů zveřejněných na webových stránkách jsou tedy informace čerpány i z osobní praxe a polostrukturovaných rozhovorů se služebně staršími zaměstnanci firmy.

Jakožto zaměstnanec firmy je autor práce pochopitelně vázán smlouvou o mlčenlivosti, a proto zde nemohou být některé postupy rozvedeny do úplných detailů.

4.2.7.2 Veřejně dostupné informace

Veřejně se lze k informacím o zpracování údajů dostat jednak na stránkách ignum.cz, kde se nacházejí v patičce pod názvem „Smlouvy a licence“ (Ignum s.r.o., 2018), tak na stránkách domena.cz, kde se nachází přímý odkaz „Zásady ochrany osobních údajů“. V prvním případě hledání podmínek trvá o něco déle, ale stále se lze umístění označit za dostačující.

Jako hlavní právní titul ke zpracování údajů je firmou používáno plnění uzavřené smlouvy a dodržování povinností stanovených zvláštními zákony. V některých případech je dále zpracování odůvodněno oprávněným zájmem. Při provádění objednávek je dále od zákazníka požadován souhlas s podmínkami v závislosti na typu poskytované služby (Ignum s.r.o., 2020).

Hlavními zpracovávanými kategoriemi jsou identifikační a kontaktní údaje zákazníků, ale jedná se i o údaje o objednávkách a platbách, kontaktech uložených v účtu, logy přístupů a provedených operací a cookies soubory. Naprostá většina těchto informací je nezbytná pro naplnění smlouvy, zbytek je odůvodněn například shromažďováním za účelem zkvalitnění služeb. Co se zdroje dat týče, bývá jím obvykle sám zákazník (ať už se jedná o vyplňování údajů online, nebo zasílání papírových formulářů).

Jako doba uchovávání údajů z účtu zákazníka je uvedeno 5 let po ukončení smlouvy. Stejná lhůta ve většině případů platí i pro údaje uchovávané kvůli registraci domén (například u NIC.CZ se některé údaje drží až po 10 let) (NIC.CZ, 2018).

Vzhledem k pracovní náplni firmy je celkem pochopitelné, že k předávání údajů dalším správcům a zpracovatelům dochází takřka neustále. Jmenovitě se jedná například o služby registrování domén, správa SSL certifikátů, uchovávání telefonických záznamů či pořizování balíčků firmy Microsoft.

Velká část informací v dalších odstavcích již není v plném rozsahu běžně k dispozici na webových stránkách, ale byli získány pomocí polostrukturovaných rozhovorů přímo ve firmě.

4.2.7.3 Další právní a organizační charakteristiky

Jedním z drobných překvapení při zkoumání firmy se ukázala skutečnost, že Ignum s.r.o. aktuálně nemá stanoveného Pověřence pro ochranu osobních údajů. Obsazení této pozice bylo společností v minulosti několikrát probíráno, ale ve výsledku ke jmenování nedošlo. Ačkoliv by se dalo předpokládat, že poskytování registrátorských služeb jmenování GDPR Pověřence vyžaduje, při opětovném nahlédnutí do Nařízení lze usoudit, že zákon firmě jeho jmenování neukládá. Firma není orgánem veřejné moci, informace k jejichž zpracování dochází nespadají ani do kategorie citlivých ani trestních údajů a jediné monitorování které firma provádí se netýká zákazníků, ale pouze například funkčnosti poskytovaného webhostingu. Z pohledů Nařízení je tedy jmenování Pověřence plně dobrovolné a nedochází zde k žádnému porušování zákona. Na druhou stranu by obsazení pozice mohlo pomoci v případě potenciálních budoucích incidentů, které by se zpracování údajů týkaly.

4.2.7.4 Uchovávané údaje

Údaje zpracovávané firmou jsou uchovávány především v elektronické podobě a jsou uloženy ve dvou propojených zákaznických systémech (Ignum s.r.o., 2020). První je systém používaný pro doménové registrace, SSL certifikáty a některé typy mailových hostingů. Druhou je databáze používaná účty spravujícími webhosting a zbytek mailových služeb. Existence dvou různých systémů se dá považovat za problém, jelikož nejen poněkud mate zákazníky, ale dále vede ke zbytečným duplicitám a ztěžuje fakturování a udržování aktuálnosti všech informací. Do jisté míry je tím tedy narušena například schopnost správně dodržovat zásadu přesnosti. Při dalším zkoumání se ukázalo, že firma již nějakou dobu pracuje na sloučení těchto dvou databází a v budoucnu lze tedy očekávat, že tento nedostatek zmizí.

V prvopočátcích firmy byla hesla k uživatelským účtům uchovávána v plaintextu, ale aktuálně jsou v naprosté většině případů v zahashované podobě. Mezi výjimky, ve kterých je původní heslo čitelné, patří například mailová služba MS Exchange, kde ze stany zákaznické podpory dochází k dodatečnému nastavování. Po dokončení objednávky je zákazník je informován o nutnosti heslo po prvním přihlášení změnit.

Co se týče informací uchovávaných mimo firemní systémy, jde například o nahrávky hovorů a vyplněné papírové formuláře které klienti poslali poštou. Nahrávky jsou uchovávané společností Daktela po dobu 3 až 6 měsíců (Daktela, 2018)Formuláře po protřídění na recepci a následném zpracování jsou uchovávány v zabezpečených prostorách, ve kterých se je třeba se při vstupu prokázat přiděleným čipem. Fyzická dostupnost dokumentů pro nepovolané osoby lze tedy považovat za dostatečně ztíženou.

4.2.7.5 Zabezpečení

Přístup k údajům v elektronické podobě, které tvoří výraznou většinu, probíhá primárně přes počítače jednotlivých zaměstnanců. Vzhledem k tomu, že například u oddělení zákaznické podpory je celkem často využíváno možnosti práce z domova, nelze prohlásit, že fyzické zabezpečení těchto počítačů je na nejvyšší možné úrovni, ale jelikož se jedná o činnost nezbytnou pro chod firmy, žádné výrazné omezení přenášení není v tomto případě použitelné. Jedním z možných kroků, kterým by se dalo zabezpečení zvýšit, by bylo stanovení přísnější heslové politiky. Z vnitropodnikových nařízení plyne, že všechny počítače musí být zaheslovány, ale nejsou pevně stanoveny žádné minimální požadavky a spoléhá se především na rozhodovací schopnosti jednotlivých zaměstnanců. Byť v praxi by zavedení oficiální heslové politiky pravděpodobně mnoho nezměnilo, jelikož většina počítačů by ji již pravděpodobně splňovala, jednalo by se o další bezpečnostní prvek předložitelný případné kontrole.

V prostorách firmy je k dispozici Wi-Fi připojení zabezpečené heslem. Pakliže se zaměstnanec připojí do některého ze systémů přes ní (nebo například z domova), je od něj vyžadováno ještě dodatečné připojení k firemní VPN.

Jde-li o ochranu proti virům a dalšímu škodlivému softwaru, u části počítačů se spoléhá na základní Windows Defender, případně na antivirus, který si dle vlastního uvážení instaluje přímo zaměstnanec, ale například servery a počítače zákaznické podpory jsou chráněny dodatečně zakoupeným antivirem značky ESET. Podobně firma přistupuje i k aktualizacím operačního systému, kde jsou u většiny počítačů zapnuty automatické aktualizace, zatímco u serverů řeší plánování updatů firemní administrátoři.

O dalším softwarovém vybavení počítačů jednotlivých zaměstnanců se žádný úplný přehled nedodržuje a je jim dána relativní volnost v tom, jaké programy si na ně doinstalují.

Pokud jde o instalaci a spouštění počítačových her na služebních strojích (mimo práci), není nijak postihováno, ale preferovaným stavem je jejich využívání pouze pro služební účely.

4.2.7.6 Sdělování informací a změna dat

Jednou z velmi často se opakujících situací jsou případy, kdy zákaznickou podporu kontaktuje osoba, která potřebuje zjistit nebo změnit údaje o účtu či doméně, se kterou nemá oficiálně nic společného, nebo je dotaz podán způsobem, pomocí kterého nelze ověřit, že je pro obdržení informací dostatečně oprávněn. Příkladem může být žádost o změnu údajů u domén vedených na jméno bývalého zaměstnance, zapomenutí nastaveného mailu či třeba telefonát z neregistrovaného čísla. Kvůli velkému množství proměnných zde sice nelze jednoduše uvést všechna řešení, ale velmi častou odpovědí v těchto případech bývá krom prostého odkázání na autorizovaný typ komunikace, či úředně ověřený formulář, například poskytnutí domény, pod kterou je zapomenutý e-mail veden (například místo josef.novak@zahradnictvi.cz pouze @zahradnictvi.cz). Obecně lze prohlásit, že právě v tomto odvětví působí snaha o dodržování GDPR určité komplikace. Problematické je zde například to, že údaje označené jako veřejně dostupné se mohou doménu od domény lišit. V některých případech tedy může teoreticky dojít k tomu, že i když by z hlediska Nařízení bylo poskytnutí údajů v pořádku, je zákazník odkázán na jinou formu komunikace.

V případě že o poskytnutí informací žádá například policie, ke komunikaci dochází buďto pomocí datové schránky, nebo osobně.

4.2.7.7 Zaměstnanci

Při nástupu jsou zaměstnanci přiděleny přístupové údaje k základním podnikovým systémům a dochází k zapůjčení služebního notebooku s nezbytným softwarem a založení firemní emailové schránky. Další funkce a oprávnění jsou zpřístupněny až při/po proškolení v dané tematice. Toto vede ke snížení výskytu situací, ve kterých by došlo například k neúmyslné ztrátě uchovávaných dat. Při ukončení pracovního úvazku jsou všechny tyto přístupy zrušeny a u účtů které nejsou závislé na firemním systému je neprodleně nastaveno nové heslo.

K uchovávání hesel nesmí zaměstnanec z pochopitelných důvodů používat papírové poznámky ani soubory v běžných textových formátech, ale správci hesel jako je například KeePass jsou povoleny.

Jde-li o samotné zaškolení, krom instruktáže spojené přímo s náplní pracovní činnosti firma hradí například účast na celodenních seminářích organizovaných českým registrem CZ.NIC na témata internetové bezpečnosti. Jak již bylo zmíněno výše, všichni zaměstnanci podepisují dohodu o mlčenlivosti.

Souhrnně lze tedy prohlásit, že z pohledu proškolení zaměstnanců nebyly nalezeny žádné závažné nedostatky.

4.2.7.8 Kamerový systém

Prostory firmy jsou monitorovány kamerovým systémem se záznamem. Kamery jsou rozmístěny například u vstupu do kanceláří, společné kuchyně či na střeše, ale kromě zasedací místnosti a toalet lze prohlásit, že většina prostor firmy je alespoň do určité míry pod dohledem. Důvodem pro instalaci kamer je především ochrana majetku a do malé míry přehled příchodů a odchodů návštěv. Jelikož se jedná o zařízení s relativně nízkým rozlišením, nebylo by příliš relevantní, jestli některá z kamer zabírá i monitor některého ze zaměstnanců, ale i přesto je až na jednu výjimku rozmístění takové, že k tomu nedochází.

O přítomnosti kamerového systému je návštěvník informován cedulkou u vstupu a v případě zaměstnanců navíc během školení. Záznamy jsou dostupné pouze vedoucímu administrátorů a jedné další osobě a doba jejich uchovávání je až 90 dní (běžně jsou mazány po 7 dnech, ale v případě nutnosti je možné je obnovit až 60-90 dní zpět).

Lze říci, že kamery ve své současné podobě nepředstavují kritický zásah do soukromí, ale jelikož se stále jedná o monitoring na pracovišti, bylo by vhodné upřesnit, zda jeho zavedení bylo opravdu nezbytné, například kvůli dřívějším incidentům.

4.2.7.9 Řešení bezpečnostních incidentů a používané technologie

Během zkoumání toho, jak se firma staví k ohlašování a řešení bezpečnostních incidentů, se ukázalo, že, alespoň co se týče úniků dat či jiných těžkých narušení bezpečnosti, Ignum s.r.o. se doposud kritickým problémům úspěšně vyhýbal. Nelze říci, zda jsou všechny potřebné postupy mezi zaměstnanci dostatečně zažité pro případ že by došlo k náhlé závažné

situaci. Jako vhodné preventivní opatření by se pak nabízelo větší upřesnění povinností správce či již výše zmiňované jmenování pověřence pro ochranu osobních údajů.

Jde-li o incidenty týkající se nikoliv úniků, ale nedostupnosti a ztráty dat, firemní postupy jsou v tomto směru značně pokročilé. Běh počítačové sítě a serverů je monitorován open source systémem Nagios (Ignum s.r.o. - IT, 2020) a pokud není v prostorách firmy přítomen alespoň jeden službu konající technik, je rychle k zastižení na telefonu.

Jako další programy, které firma ve větším měřítku využívá lze zmínit chatovací program Slack pro urychlení komunikace mezi odděleními, Chatra pro kontakt se zákazníky na webových stránkách, nebo virtuální ústředna Daktela (Ignum s.r.o. - helpdesk, 2020).

Jako další krok podniknutý pro předcházení bezpečnostním incidentům lze jmenovat pravidelné zálohování databází, serverů a jednotlivých zákaznických e-mailových schránek. V případě serverů jde o zálohy přírůstkové, u webhostingů a mail hostingů o zálohy plné. Pakliže by došlo k výskytu požáru jsou pak místnosti chráněny dusíkovým hasicím systémem.

Zbavuje-li se firma zastaralých počítačů, nedochází k fyzickému zničení disků, ale pouze k jejich několikanásobnému smazání a přepsání náhodnými daty. I tento postup lze považovat za dostačující.

Při dotazování na předchozí incidenty související s počítačovými viry a ransomwarem se celkem očekávaně ukázalo, že v minulosti občas došlo k zavirování zákaznických hostingů, což mohlo v krajních případech způsobit krátkodobou nestabilitu některých systémů, ale přímo počítače zaměstnanců doposud žádné zásadní problémy neměly.

4.2.7.10 Předávání údajů dalším správcům a zpracovatelům

Vzhledem k povaze primární činnosti firmy dochází k předávání údajů dalším správcům u velké části zákaznických objednávek, především se pak jedná o komunikaci s doménovými registry různých zemí a případnými dalšími registrátory. Jelikož důkladnější kontrola, byť jen několika z těchto registrů, by daleko přesahovala rozsah této práce, zde dojde pouze k okrajovému zmínění několika příkladů.

Velká část registrů a registrátorů se nachází na území evropské unie a podobně jako na Ignum se na ně tedy vztahuje obecné nařízení o ochraně osobních údajů. Do této kategorie spadá například NIC.CZ, NIC.SK, maďarské Silicium Network, EURid, nebo německé

RRPPROXY. Jak již bylo zmíněno výše, rozdílné registry se staví různě například ke zveřejňování údajů. Zatímco u českých domén jsou krom jména vlastníka a většinou i jeho sídla ostatní údaje skryty, u EU domén lze zjistit i jeho kontaktní e-mail, a u slovenských i telefon. Někdy při registraci domén (ruských, čínských a v některých případech irských) bývá registrem požadována kopie dokladů, což se z pohledu GDPR dá označit jako přehnané. Obecně lze prohlásit, že předání údajů probíhá v souladu s Nařízením, ale jeho implementace je napříč jednotlivými partnery očekávaně nekonzistentní.

4.2.7.11Ke GAP analýze a Posouzení vlivu na ochranu osobních údajů

GAP analýza se dá označit jako jeden z výchozích kroků pro správnou implementaci GDPR. Při hodnocení firmy Ignum se tedy, v případech, kdy tomu bylo možné, autor práce inspiroval právě touto metodikou. Pro úplné dodržení metodiky by bylo nutné nejen například větší zapojení vedení firmy, ale dále by kolidovalo s autorovým výkonem pracovní činnosti. I přes tyto komplikace došlo k uspokojivému zodpovězení většiny cílových otázek, které metodika pokládá (kdo má přístup k datům, jak jsou údaje zabezpečeny, jaké jsou používány systémy, proces řízení incidentů…).

Další zmiňovanou praktikou je Posouzení vlivu na ochranu osobních údajů a analýza, zda je nutné toto posuzování provádět. Během dotazování se ukázalo, že v minulosti během analýzy firma dospěla k rozhodnutí, že provádět Posouzení vlivu není nutné. Při zhodnocení dostupných informací podle kritérií pro nutnost provádět DPIA (Úřad pro ochranu osobních údajů, 2020) autor této práce došel k podobnému závěru (viz. tabulka níže). Některé body nebyly významné vůbec, a zatímco firma zpracovává například platební údaje zákazníků, nebo kamerové záznamy zaměstnanců, žádné z kritérií se nedá označit jako kritické.

Tabulka 3 - Ignum – Kritéria pro provedení DPIA

Hodnocení rizikovosti kriterií	Kritické	Významné	Nízké
Profilování, či jiné hodnocení			**X**
Automatické rozhodování s významnými důsledky			**X**
Systematické monitorování		**X**	
Práce s citlivými údaji		**X**	
Zpracování v rozsáhlém měřítku		**X**	
Slučování více datových souborů		**X**	
Údaje zranitelných osob			**X**
Inovativní řešení			**X**
Obtížně uplatnitelná práva subjektu			**X**

4.2.7.12 Zákonnost, korektnost, transparentnost a účelové omezení

Po zvážení dostupných informací lze prohlásit, že jde-li o tyto zásady, nedochází u firmy Ignum s.r.o. k žádným významným přestupkům. Použité právní tituly dávají s ohledem na uvedené účely smysl a stejně tak způsob opatřování souhlasu se zpracováním údajů. Informace o zpracování jsou k dispozici na stránkách, byť v jednom ze tří případů nejsou přístupné jedním kliknutím, a jsou v dostatečně srozumitelné podobě. Jako potenciální slabinu lze označit, že společnost nemá jmenovaného Pověřence. I zde se však nejedná o porušení Nařízení.

4.2.7.13 Minimalizace, přesnost a omezení uložení

Při zadávání údajů je zákazník povinen vyplnit pouze informace nezbytně nutné pro plnění smlouvy. V případě, že zákazník vyplní údaje navíc, je po něm vyžadován dodatečný souhlas. Vždy se však jedná o údaje, které jsou relevantní pro registraci nebo pro případné budoucí ověření zákazníka (jedná se o často se vyskytující situaci, nikoliv o uchovávání typu „co kdyby“). Jde-li o dobu po kterou jsou rozličná data uchovávána, jedná se často o lhůty, které si stanovuje přímo registr a firma je tedy nedokáže přímo ovlivnit. I v těchto případech však nebývají doby uchovávání příliš přehnané.

Například u údajů doménových kontaktů je nutné provádět pravidelnou aktualizaci o čemž bývá zákazník periodicky upozorňován přímo příslušným registrem. Už jen vzhledem k množství těchto kontaktů není možné, aby byly údaje aktualizovány automaticky a dochází k tomu tedy pouze na podnět osoby, jejíž oprávnění bývá potvrzováno buďto pomocí emailu na pevně danou adresu, nebo úředně ověřeným formulářem. Zásada přesnosti je tedy dodržována.

4.2.7.14 Integrita a důvěrnost

Jak již bylo zmíněno výše, jde-li o zabezpečení údajů a zajištění jejich dostupnosti zákazníkům, lze tyto zásady považovat za splněné. V některých případech stále dochází k dočasným výpadkům připojení, ale problémy bývají rychle vyřešeny. Tyto výpadky by měli být i nadále redukovány například zaváděním novějšího serverového vybavení. Ani při zkoumání dalších faktorů nebyly odhaleny žádné závažné nedostatky. Jako návrh pro

případné zlepšení by se dalo uvést zavedení přísnější heslové politiky a aktualizace některých vnitropodnikových směrnic.

4.2.7.15 Přístup k právům subjektů

Od odebírání reklamních sdělení se lze odhlásit buďto v nastavení uživatelského účtu nebo přímo odkazem v zasílaných e-mailech a jejich zasílání tedy práva zákazníka neporušuje. V případě, že si zákazník přeje smazat nepoužívaný účet, stačí mu se do něj přihlásit a o zrušení požádat zákaznickou podporu. Jde-li o reakční dobu na případné dotazy a požadavky, firma se snaží reagovat do hodiny, ale v závislosti na typu dotazu a vytížení může odpověď přijít později. Pokud se jedná o žádosti, které vyžadují například exportování údajů z databáze, vyřízení obvykle proběhne až následující den. Obecně lze však prohlásit, že práva, na která má zákazník nárok, jsou dodržována.

5 Zhodnocení výsledků

5.1 Použité metody

Jako hlavní zdroje informací pro první polovinu praktické části práce sloužila studie materiálů veřejně dostupných na internetových stránkách firem doplněná o dotazníkové šetření. Vzhledem k účelu dotazníků a malému počtu obesílaných firem nebylo využito předpřipravených šablon jako nabízejí například stránky vyplnto.cz, nebo survio.com, ale byly vytvořeny v programu MS Excel a jednou z testovaných skutečností bylo, zda v nich u některé z firem nedojde k povolení maker. V některých případech soubory neprošly automatickou kontrolou a bylo nutné zaslat variantu bez maker, v ostatních se vrátila pouze textová odpověď na zlomek zasílaných otázek. Spouštění potenciálně nebezpečného obsahu zaměstnanci dotazovaných firem tedy nakonec nebylo možné vyvodit.

Jako další způsob pro získání informací posloužil polostrukturovaný rozhovor. Této metody bylo využito u dvou firem, a to primárně u Ignum s.r.o. a v menší míře u Českomoravské stavební spořitelny. U ČMSS šlo pouze o postupy týkající se řadových zaměstnanců, zatímco u Ignumu zahrnoval i další organizační a technické dotazy.

V druhé půli praktické části práce bylo velké množství informací dále čerpáno z osobních zkušeností a opakovaného pozorování aktivity ve firmě.

Výsledné hodnocení napříč firmami lze pak brát jako indukci s hypotézou „Implementace GDPR v českých firmách je na přijatelné úrovni“, respektive místo implementace jako celku brát pouze dodržování jednotlivých zásad.

5.2 Dostupnost potřebných informací

Při vypracovávání tohoto dokumentu se jako hlavní problém ukázala složitost zjišťování konkrétnějších informací o implementaci GDP napříč prakticky všemi zkoumanými firmami. Zatímco obecné informace o zpracování, jako je například účel, kategorie údajů, délka uchovávání a další spadají pod zásady zákonnosti a transparentnosti, bylo možné jednoduše získat z internetových stránek jednotlivých firem, ke konkrétně používaným postupům a vnitřním směrnicím se často nepodařilo dostat vůbec. Důvodem je především to, že poskytnutí těchto informací, by se dalo při určitém úhlu pohledu vyložit právě jako porušení hodnocených postupů. V naprosté většině případů tedy zkoumání

implementace skončilo pouze u hodnocení na venek sdělovaných postupů, jejichž skutečnou pravdivost nelze z velké části nijak dokázat. U firmy, kde byly informace poskytnuty pak bylo nutné si dávat pozor při rozhodování, které lze v práci přímo uvést a o kterých se zmínit pouze nepřímo. Byť komplikace přímo souvisejí s tématem práce a byly tedy do jisté míry předpokládány, jejich dopad na její průběh byl větší, než se očekávalo.

5.3 Implementace napříč zkoumanými firmami

Důkladněji rozepsané příklady implementace v jednotlivých firmách již byly uvedeny v předchozí části práce. V následujících několika odstavcích tedy dojde hlavně ke shrnutí společných znaků v jednotlivých zkoumaných odvětvích a poukázání na případné odchylky či zajímavosti.

5.3.1 Bankovnictví

Jako hlavní zástupci na poli bankovnictví a pojišťovnictví byly vybrány firmy Air Bank, Komerční Banka, Českomoravská stavební spořitelna a Československá obchodní banka. O všech těchto zkoumaných subjektech lze říci, že alespoň po stránce zákonnosti a transparentnosti berou Nařízení vážně. Veřejně dostupné informace o zpracování osobních údajů byly přehledné a krom Air Bank byly k dispozici nejen v podobě statického PDF souboru, ale i jako přehlednější HTML.

Ve všech případech dle očekávání dochází hlavně ke zpracovávání identifikačních a kontaktních údajů na základě právního titulu „Plnění smlouvy“ nebo „Dodržování právních povinností“. Okrajově se pak jedná i o zpracování na základě oprávněného zájmu či souhlasu (například pro marketingové účely).

Při posuzování zásad minimalizace a přesnosti také povětšinou nedocházelo k nalezení žádných významných nedostatků, ale napříč všemi firmami se dala pozorovat překvapivě dlouhá doba uchovávání údajů. ČSOB uchovává některé zaměstnanecké údaje až 45 let, slovenské pobočky KB dokonce 70. Podobně tomu bývá i u některých údajů o klientech. Jelikož nebyly k dispozici dostatečné informace o tom, které kategorie údajů jsou uchovávány po takto dlouhou dobu, nebylo možné dojít k jednoznačnému závěru, ale dá se předpokládat, že lhůta by měla být mnohem kratší.

Informace relevantní pro zásadu integrity a důvěrnosti a bezpečnostní postupy obecně se bohužel podařilo získat jen u ČMSS, a i v tomto případě pouze v omezené míře. Na základě toho, že v ostatních směrech se společnosti jevily dosti podobně lze ovšem do určité míry očekávat, že i implementace této zásady by se napříč firmami neměla výrazně lišit. Ve výsledku se tedy dá předpokládat, že firmy zabývající se finančnictvím budou na zabezpečení a firemní předpisy klást značný důraz.

Kromě poněkud pochybné doby uchovávání údajů lze obecně prohlásit, že implementace GDPR v bankovním odvětví (alespoň v aspektech k jejichž hodnocení byly k dispozici dostatečné informace) splňuje požadavky, které jsou nařízením ukládány.

5.3.2 **Internetový obchod**

Jako další odvětví pro zkoumání implementace GDPR byly vybrány internetové obchody, konkrétně tedy jakožto jejich zástupce Alza.cz. Ostatní obchody pak byly zkoumány pouze okrajově pro porovnání některých aspektů.

Podobně jako u bankovnictví, jde-li o zásady zákonnosti, korektnosti a transparentnosti, lze opět prohlásit, že nebyly odhaleny žádné závažné nedostatky. Použitými právními tituly jsou především „plnění smlouvy“, „souhlas“ a „oprávněný zájem“ přičemž například u koupě na splátky dochází k důkladnějšímu zpracování údajů za účelem ověření zákazníkovi schopnosti splácet. Ve všech případech lze rozsah zpracování označit jako odpovídající danému účelu. Podobně jako u v předchozím odvětví, i zde lze pozorovat o něco delší dobu uchovávání některých údajů, než by se mohlo na první pohled zdát nutné, ale v ve většině případů je buďto odůvodněná, nebo lze na rozhodnutí zákazníka zkrátit. Jako příklad lze uvést odvolání souhlasu s uchováváním údajů za účelem marketingu a 90denní doba uchovávání kamerových záznamů kvůli předchozím zkušenostem (v porovnání s 14 dny u Mall.cz a CZC). Údaje o zákaznících se v ostatních případech napříč obchody uchovávají v závislosti na tom, zda provedli nějaký nákup, buďto po dobu několika měsíců, nebo let, což lze obecně označit jako opodstatněné.

Jde-li například o právo na portabilitu nebo opravu údajů, minimálně u Alzy ho lze bez jakýchkoliv problémů uplatnit pomocí automatického systému. Reakční doba na dotazy pak také splňovala relevantní normy.

5.3.3 **Hostingová firma**

Posledním zkoumaným odvětvím byly hostingové firmy / registrátoři internetových domén, konkrétně společnost Ignum s.r.o. U dalších firem zabývajících se poskytováním těchto služeb (Active24, Wedos, Gransy s.r.o …) k došlo pouze k pročtení zveřejněných materiálů za účelem porovnání s Ignumem, ve kterém bylo zkoumání výrazně důkladnější. Zmínitelným rozdílem je pak například to, že společnost Active 24 využívá služeb pověřence pro ochranu osobních údajů, zatímco ostatní nemají na tuto pozici stanovenou, jelikož to není požadováno zákonem. Jde-li o informace poskytované na stránkách nejlépe zpracované jsou dle autora práce ty firmy Wedos jelikož oproti ostatním poskytují nejvíce relevantních informací (U Active 24 je pak dobré vyzdvihnout přehlednou tabulku partnerů, kterým v některých případech údaje předává).

Jelikož podrobně zkoumána byla pouze firma Ignum, nemůžeme s jistotou tvrdit, že zpracování probíhá ve všech hostingových firmách stejně, ale na základě dostupných údajů můžeme do určité míry předpokládat, že nedochází k velkým rozdílům. O Ignumu a částečně i o odvětví hostingových firem můžeme říci následující.

Jelikož to zákon nevyžaduje, není prováděno DPIA a jmenování Pověřence je také spíše výjimkou. Obecně jsou však zásady jako zákonnost, korektnost, transparentnost a účelové omezení dodržovány podobně jako uchovávání pouze minimálních potřebných údajů. Dodržování zásady přesnosti je vzhledem k množství dat obtížné hlídat jinak než pomocí automaticky zasílaných zpráv přímo od registrů, ale samotná aktualizace údajů již probíhá bezproblémově.

Podobně jako u ostatních odvětví se i zde lhůty pro uchovávání počítají převážně v letech. U dokumentů se pohybují v rozmezí 5-10 let, u nahrávek telefonátů půl roku a u kamerových záznamů maximálně 90 dní. Všechny tyto doby bývají pak relativně opodstatněné.

Integrita a důvěrnost bývá taktéž dodržována a problémy s nimi se vyskytují převážně v podobě drobností, jako jsou krátkodobé nedostupnosti některých dat, nespecifikovaná heslová politika zaměstnanců, nebo horší dostupnost některých směrnic.

Předávání údajů do zahraničí je v tomto odvětví pochopitelně nezbytné, ale většinou se jedná pouze o základní identifikační údaje a nedochází tedy ke komplikacím. Existují však i výjimky, kdy registr vyžaduje například kopii občanského průkazu. V těchto

případech bohužel firmy nemohou situaci ovlivnit a zákazník musí na podmínky buď přistoupit, nebo vyhledat doménu s jinou koncovkou. Ačkoliv uchovávání kopie dokladů lze označit jako přehnané, nejedná se o situaci, kterou by bylo možné vytýkat přímo zkoumaným hostingovým/registrátorským společnostem.

Jde-li o dodržování práv zákazníků například na smazání uchovávaných údajů, nebyly zde nalezeny žádné závažné přestupky. Pokud jde o právo na portabilitu, jeho uplatnění může trvat déle, ale stále se jedná o rozmezí několika dní, což zákonem stanovenou měsíční lhůtu s výraznou rezervou splňuje. (Wedos, 2018) (Active24, 2018) (Gransy s.r.o., 2018)

5.3.4 **Výzkumná agentura a další**

Od podrobnějšího hodnocení výzkumné agentury STEM/MARK bylo, stejně jakožto u pražského dopravního podniku, telefonních operátorů a několika dalších zástupců z bankovního sektoru, upuštěno kvůli přehnaně velkému rozsahu, kterého by práce při jejich zahrnutí dosáhla.

U výzkumné agentury úvodní hodnocení vycházelo v souladu s GDPR, ale pro nedostatečnou počáteční komunikaci bylo pozastaveno a kvůli změně hlavního zaměření práce zůstalo nedokončeno.

6 Závěr

Ačkoliv fakt, že osobní údaje mají nezanedbatelnou hodnotu, není žádnou novinkou, díky stále většímu rozmachu internetových technologií pozbývají některé dřívější předpisy na jejich ochranu na aktuálnosti. I když se zde zmiňovanou hodnotou nemyslí pouze riziko krajních případů jako je krádež identity, ale i ty méně invazivní jako využívání shromážděných informací pro cílenou reklamu, je nutné nebrat potenciální ohrožení dat (ať už ze strany lidské chyby, úmyslného poškození nebo neovlivnitelnými událostmi) na lehkou váhu. Za tímto účelem nabylo 28.5.2018 účinnosti obecné nařízení pro ochranu osobních údajů (také známé pod anglickou zkratkou GDPR). Toto nařízení se týká jak firem, tak jednotlivců zabývajících se zpracováním osobních dat a klade si za cíl hájit práva evropských občanů a chránit je před nevhodným zacházením s jejich údaji.

Tato diplomová práce si kladla za cíl prozkoumat, zda a jak důsledně je Nařízení dodržováno napříč firmami působícími v české republice. Toto hodnocení mělo za cíl vzít nejen obecně dostupné informace, ale i v praxi používané firemní postupy pro sběr, uchovávání a další zpracování dat a porovnat je s doporučenými postupy ze strany GDPR a dalších legislativních nařízení.

Při shromažďování teoretických podkladů velmi rychle vyšlo najevo, že Nařízení a ochrana osobních údajů obecně je velice spletité téma a byť obsahuje mnohé instrukce pro to, jak mají používané postupy vypadat (například souhrn zásad, které by měl každý správce dodržovat, jako je transparentnost nebo účelové omezení) a jak dodržování hodnotit (GAP analýza, posouzení dopadu zpracování na ochranu osobních údajů), pro některé aspekty není možné jednoduše stanovit, jaké postupy jsou ještě v pořádku a jaké již není možné v považovat za v souladu se zákonem. Z tohoto důvodu je někdy hodnocení implementací ve firmách spíše námětem na dlouhou diskuzi než pouhým zaškrtnutím několika položek v tabulce.

Původně měla praktická část této práce zahrnovat i telefonní operátory a zástupce dalších odvětví, jako jsou školy, ubytovací zařízení a dopravní podnik, ale tento rozsah byl nakonec z rozličných důvodů zmenšen pouze na společnosti zabývající se financemi, internetové obchody a hostingové firmy.

Při samotném hodnocení firem se jako hlavní problém ukázala být nedostupnost přesnějších vnitřních postupů a nutnost z větší míry spoléhat na dotazníky a studium

materiálů dostupných volně na internetových stránkách. V několika případech bylo však k dispozici i přímé pozorování běhu firmy a zkoumání pomocí rozhovorů se zaměstnanci.

Při velkém zestručnění výsledků práce lze prohlásit, že z výsledků jednotlivých hodnocení lze vyvodit, že velké firmy působící v české republice kladou na dodržování GDPR velký důraz a snaží se splňovat všechny požadovaná kritéria. U menších firem pak občas dochází k různým nedostatkům plynoucím z nutnosti zavádět další organizační opatření, ale i v těchto případech nebyly nalezeny žádné kritické problémy.

Jako další přínos této práce lze pak krom samotných výsledků hodnocení označit i poukázání na některé méně dostačující postupy přímo ve firmách což by mělo vést k jejich případnému budoucímu zlepšení.

7 Seznam použitých zdrojů

1Password. 2019. Password Manager for Families, Businesses, Teams. *1Password.* [Online] 2019. [Citace: 8. 7 2019.] https://1password.com/.

Accusoft. 2017. The Importance of Document Management and Security. *accusoft.com.* [Online] 1. 5 2017. [Citace: 6. 7 2019.] https://www.accusoft.com/blog/the-importance-of-document-management-and-security/.

Acronis. 2019. Jak se účinně bránit ransomwaru. *Acronis - softwarové nástroje pro zálohování a ochranu dat.* [Online] 8. 2 2019. [Citace: 10. 7 2019.] https://www.acronis.cz/ochrana-proti-ransomwaru/?gclid=EAIaIQobChMIyq6G14uq4wIVh6MYCh06cgUTEAAYASAAEgKnx_D_BwE.

Active24. 2018. Prohlášení o ochraně osobních údajů. *active24.cz.* [Online] 18. 5 2018. [Citace: 11. 2 2020.] https://www.active24.cz/privacy.

Alza.cz. 2019. Alza.cz - největší obchod s počítači a elektronikou. *Alza.cz.* [Online] 29. 8 2019. [Citace: 19. 1 2020.] https://www.alza.cz/.

—. 2019. Alza.cz 2018: obrat 25 miliard . *Alza.cz - největší obchod s počítači a elektronikou.* [Online] 30. 1 2019. https://www.alza.cz/alzacz-2018-obrat-25-miliard.

BBC Capital. 2018. BBC Capital. *Can you make money selling your data?* [Online] 21. 9 2018. [Citace: 27. 5 2019.] http://www.bbc.com/capital/story/20180921-can-you-make-money-selling-your-data.

Business Insider. 2018. Facebook suspends Cambridge Analytica, a controversial data-analysis firm linked to the Trump campaign. *Business Insider.* [Online] 16. 4 2018. [Citace: 15. 7 2019.] https://www.businessinsider.com/facebook-suspends-cambridge-analytica-strategic-communication-laboratories-2018-3.

—. 2018. Google+ will shut down 4 months early after Google discovered a 2nd bug affecting user data for more than 52 million. *Business Insider.* [Online] 10. 12 2018. [Citace: 15. 7 2019.] https://www.businessinsider.com/google-plus-early-shut-down-second-data-breach-2018-12.

—. 2018. Hackers stole millions of Facebook users' highly sensitive data — and the FBI has asked it not to say who might be behind it. *Business Insider.* [Online] 10. 10 2018.

[Citace: 15. 7 2019.] https://www.businessinsider.com/facebook-30-million-users-affected-hack-fbi-asked-not-to-reveal-source-2018-10.

—. 2018. Here's how to check if you were one of the 500 million customers affected by the Marriott hack. *Business Insider.* [Online] 30. 11 2018. [Citace: 15. 7 2019.] https://www.businessinsider.com/marriott-starwood-hotel-hack-data-breach-how-to-check-if-you-were-affected-2018-11.

—. 2018. The 21 scariest data breaches of 2018. *Business Insider.com.* [Online] 30. 12 2018. [Citace: 26. 6 2019.] https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#7-cambridge-analytica-87-million-15.

CBS News. 2010. Digital Photocopiers Loaded With Secrets. *cbsnews.com.* [Online] 19. 4 2010. [Citace: 27. 6 2019.] https://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/.

CitizenMe. 2019. CitizenMe - Features. *CitizenMe.* [Online] 2019. [Citace: 27. 5 2019.] https://www.citizenme.com/public/wp/business/pricing/.

Cost Cutting Solutions Ltd. 2019. [Online] 2019. [Citace: 6. 7 2019.] http://www.cost-cutting.cz/.

Cryptopotato. 2019. IEO's Nightmare: Ocean Protocol Lost 80% Following Its IEO On Bittrex. *Cryptopotato.* [Online] 5. 5 2019. [Citace: 2019. 5 27.] https://cryptopotato.com/ieos-nightmare-ocean-protocol-lost-80-following-its-ieo-on-bittrex/.

Časopis Chip. 2014. UEFI Secure Boot: Příliš bezpečný start PC. *chip.cz.* [Online] 13. 1 2014. [Citace: 2. 7 2019.] https://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-08-2013/uefi-secure-boot-prilis-bezpecny-start-pc/.

ČMSS. 2019. Českomoravská stavební spořitelna, ČMSS. *ČMSS.* [Online] 9. 8 2019. [Citace: 19. 1 2020.] https://www.cmss.cz/.

—. 2019. Informace o zpracování osobních údajů. *ČMSS.* [Online] 9. 8 2019. [Citace: 19. 1 2020.] https://www.cmss.cz/informace-o-zpracovani-osobnich-udaju.

ČSOB. 2019. O ČSOB a skupině. *ČSOB portál.* [Online] 2019. [Citace: 29. 9 2019.] https://www.csob.cz/portal/csob/o-csob-a-skupine.

—. 2019. Úvodní stránka . *ČSOB.* [Online] 29. 9 2019. [Citace: 19. 1 2020.] https://www.csob.cz/portal/.

Daktela. 2018. Daktela - Informace o ochraně osobních údajů (GDPR). *daktela.com.* [Online] 25. 5 2018. [Citace: 10. 1 2020.] https://www.daktela.com/informace-o-ochrane-osobnich-udaju-gdpr/.

Datacoup. 2019. Datacoup - How it works. *Datacoup.* [Online] 2019. [Citace: 27. 5 2019.] http://datacoup.com/docs#how-it-works.

Evropský parlament a rada - GDPR. 2016. GDPR (obecné nařízení). *Úřad pro ochranu osobních údajů.* [Online] 27. 4 2016. [Citace: 19. 10 2018.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31512.

—. 2016. GDPR úplné znění. *Úřad pro ochranu osobních údajů.* [Online] 27. 4 2016. [Citace: 29. 5 2019.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32394.

Evropský soudní dvůr. 2003. Rozsudek ve věci C-101/01. *InfoCuria.* [Online] 6. 11 2003. [Citace: 14. 6 2019.] http://curia.europa.eu/juris/document/document.jsf?docid=48382&doclang=CS.

Finance.cz. 2018. Kdo vlastní české stavební spořitelny? *Finance.cz - daně, banky, kalkulačky, spoření, kurzy měn.* [Online] 6. 11 2018. [Citace: 9. 8 2019.] https://www.finance.cz/516367-vlastnici-stavebnich-sporitelen/.

—. 2018. Která banka má nejvíce klientů? *Finance.cz - daně, banky, kalkulačky, spoření, kurzy měn.* [Online] 17. 10 2018. https://www.finance.cz/496071-kdo-vlastni-ceske-banky/.

GDPR. 2019. Co je GDPR? *Obecné nařízení o ochraně osobních údajů prakticky.* [Online] 2019. [Citace: 29. 5 2019.] https://www.gdpr.cz/gdpr/.

Gransy s.r.o. 2018. Zásady ochrany osobních údajů. *subreg.cz.* [Online] 20. 5 2018. [Citace: 15. 2 2020.] http://subreg.cz/pd_subreg_cz.pdf.

Hacker Noon. 2018. The Bcrypt Protocol… is kind of a mess. *Hacker Noon.* [Online] 3. 11 2018. https://hackernoon.com/the-bcrypt-protocol-is-kind-of-a-mess-4aace5eb31bd.

HP. 2015. BIOS-Level Technology | HP Sure Start | HP. *HP.com.* [Online] 2. 12 2015. [Citace: 2. 7 2019.] https://www.youtube.com/watch?v=10xH_puklMU.

Ignum s.r.o. - admin. 2020. Volná místa - Linux admin. *Ignum.cz.* [Online] 2020. [Citace: 10. 1 2020.] https://www.ignum.cz/ostatni/o-nas/kariera/volna-mista/linux-admin/.

Ignum s.r.o. - helpdesk. 2020. Volná místa - Technická podpora. *Ignum.cz.* [Online] 2020. [Citace: 10. 1 2020.] https://www.ignum.cz/ostatni/o-nas/kariera/volna-mista/zakaznicka-podpora/.

Ignum s.r.o. - IT. 2020. Volná místa - IT technik. *Ignum.cz.* [Online] 2020. [Citace: 10. 1 2020.] https://www.ignum.cz/ostatni/o-nas/kariera/volna-mista/it-technik/.

Ignum s.r.o. 2020. Doména.cz - Podmínky a pravidla. *Domena.cz.* [Online] 2020. [Citace: 10. 1 2020.] https://www.domena.cz/terms-and-conditions.

—. 2018. Ignum - Zásady ochrany osobních údajů. *Ignum.cz.* [Online] 25. 5 2018. [Citace: 10. 1 2020.] https://www.ignum.cz/ostatni/smlouvy-a-licence/zasady-ou/.

—. 2020. Webcontrol - nový účet. *Ignum.cz.* [Online] 2020. [Citace: 10. 1 2020.] https://www.ignum.cz/webcontrol/signup/.

Inc.com. 2017. 6 Million Instagram Accounts Hacked: How to Protect Yourself. *Inc.com.* [Online] 6. 9 2017. [Citace: 26. 6 2019.] https://www.inc.com/joseph-steinberg/6-million-instagram-accounts-hacked-how-to-protect.html.

Independent. 2018. People's Instagram accounts are being mysteriously taken over by Russians, and they can't get them back. *The Independent | News | UK and Worldwide News | Newspaper.* [Online] 25. 9 2018. [Citace: 15. 7 2019.] https://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-hack-accounts-russia-breached-take-over-accounts-how-locked-2018-a8553776.html.

International Organization for Standardization. 2013. Řada norem ISO/IEC 27000. *Risk Analysis Consultants, s.r.o.* [Online] 10 2013. [Citace: 4. 7 2019.] http://www.iso27000.cz/.

Kaspersky. 2017. Kaspersky Lab Survey Show Users' Bad Password Habits . *Kaspersky Antivirus Protection & Internet Security Software.* [Online] 16. 1 2017. [Citace: 6. 7 2019.] https://me-en.kaspersky.com/about/press-releases/2017_bad-password-habits.

KeePass. 2019. KeePass Password Safe. *KeePass Password Safe.* [Online] 2019. [Citace: 8. 7 2019.] https://keepass.info/.

Kensigton. 2019. Kensington security solutions. *kensington.com.* [Online] 2019. [Citace: 27. 6 2019.] https://www.kensington.com/solutions/product-category/security/.

Komerční Banka. 2019. Hlavní stránka. *KB.cz.* [Online] 29. 10 2019. [Citace: 19. 1 2020.] https://www.kb.cz/cs/.

Krucek cybersecurity. 2019. Co je ISO/IEC 27001? *krucek.cz.* [Online] 2019. [Citace: 4. 7 2019.] https://www.krucek.cz/cz/qualifications/iso-iec-27001/?gclid=CjwKCAjwx_boBRA9EiwA4kIELiMOCUGcMZAE3JkQGArOo3XTR6Pq5Nm76cw05h7oS-nDg8PxO8TGQBoC7-4QAvD_BwE.

Microsoft. 2015. Microsoft Research reveals understanding gap in the brand-consumer data exchange. *Microsoft news.* [Online] 3. 6 2015. [Citace: 27. 5 2019.] https://news.microsoft.com/apac/2015/06/03/microsoft-research-reveals-understanding-gap-in-the-brand-consumer-data-exchange/.

—. 2018. Secure the Windows 10 boot process. *Microsoft.com.* [Online] 11. 16 2018. [Citace: 2. 7 2019.] https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process.

Motherboard. 2018. Hackers Stole Personal Data of 2 Million T-Mobile Customers. *VICE - Original reporting and documentaries on everything that matters in the world.* [Online] 24. 8 2018. [Citace: 15. 7 2019.] https://www.vice.com/en_us/article/a3qpk5/t-mobile-hack-data-breach-api-customer-data.

Network World. 2016. Petya ransomware is now double the trouble. *Network World.com.* [Online] 13. 5 2016. [Citace: 10. 7 2019.] https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html.

Nezmar, Luděk. 2017. *GDPR, praktický průvodce implementací.* Praha : Grada, 2017. ISBN 978-80-271-0668-4.

NIC.CZ. 2018. Nic.cz - zásady ochrany osobních údajů. *Nic.cz.* [Online] 22. 5 2018. [Citace: 10. 1 2020.] https://www.nic.cz/files/documents/20180525_Zasady_zpracovani_osobnich_udaju_final.pdf.

Nulíček, Michal. a kol. 2018. *GDPR/Obecné nařízení o ochraně osobních údajů - praktický komentář.* Praha : Wolter Kluwer, 2018. ISBN 978-80-7598-068-7.

OE Canada Inc. 2019. Using Private Print . *oecanada.com.* [Online] 2019. [Citace: 6. 27 2019.] https://www.oecanada.com/using-private-print/.

Peak.cz. 2018. Česká e-commerce stále roste. Vládne jí pětice obřích e-shopů. *Peak.cz – peníze, ekonomika, analýzy, komentáře.* [Online] 27. 6 2018. https://www.peak.cz/ceska-e-commerce-stale-roste-vladne-petice-obrich-e-shopu/2492/.

phoenixNAP. 2019. 27 Terrifying Ransomware Statistics & Facts You Need To Read. *phoenixNAP Global IT Services Blog.* [Online] 31. 1 2019. [Citace: 10. 7 2019.] https://phoenixnap.com/blog/ransomware-statistics-facts.

Policie ČR. 2019. Ztráta identity. *policie.cz.* [Online] 2019. [Citace: 26. 6 2019.] https://www.policie.cz/clanek/ztrata-identity.aspx.

Poslaneská sněmovna. 1992. LISTINA ZÁKLADNÍCH PRÁV A SVOBOD. *Parlament České republiky, Poslanecká sněmovna.* [Online] 16. 12 1992. [Citace: 29. 5 2019.] https://www.psp.cz/docs/laws/listina.html.

Pracovní skupina pro ochranu osobních údajů (WP29). 2012. Opinion 3/2012 on developments in biometric technologies. *Evropská komise.* [Online] 27. 4 2012. [Citace: 24. 6 2019.] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

—. 2017. Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679. *Úřad pro ochranu osobních údajů.* [Online] 3. 10 2017. [Citace: 8. 6 2019.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30234.

Pracovní skupina pro ochranu osobních údajů. 2016. Pokyny k funkci pověřence pro ochranu osobních údajů. *Ministerstvo průmyslu a obchodu.* [Online] 13. 12 2016. [Citace: 9. 6 2019.] https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/gdpr-dokumenty/2018/1/Preklad-Metodiky-poverence-WP29.pdf.

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ (WP29). 2017. Guidelines on Data Protection Impact Assessment. *Evropská komise.* [Online] 4. 4 2017. [Citace: 8. 6 2019.]
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwim7_7A49niAhUOLFAKHRHjC40QFjAAegQIBBAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D44137&usg=AOvVaw1ikLQwC5a4vpP-FE-OUzwa.

Pracovní skupina pro ochranu údajů (WP29). 2016. Pokyny týkající se práva na přenositelnost údajů. *Úřad pro ochranu osobních údajů.* [Online] 13. 12 2016. [Citace: 3. 6 2019.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31882.

Software602 a.s. 2019. DMS s řízeným oběhem dokumentů. *Software602 a.s.* [Online] 2019. [Citace: 6. 7 2019.] https://www.602.cz/reseni/dms-s-rizenym-obehem-

dokumentu/?gclid=EAIaIQobChMIwsqz4PKf4wIVwprVCh1GlAcgEAAYAiAAEgId3_D_BwE.

SOOM.cz. 2015. Rainbow tables tajemství zbavené. *SOOM.cz.* [Online] 1. 2 2015. [Citace: 8. 7 2019.] https://www.soom.cz/clanky/1165--Rainbow-tables-tajemstvi-zbavene.

Statista. 2019. Google's average revenue per monthly active user from 1st quarter 2015 to 4th quarter 2016 (in U.S. dollars). *Statista.* [Online] 2019. [Citace: 27. 5 2019.] https://www.statista.com/statistics/306570/google-annualized-advertising-arpu/.

—. 2019. Advertising revenue of Google from 2001 to 2018 (in billion U.S. dollars). *Statista.* [Online] 2019. [Citace: 27. 5 2019.] https://www.statista.com/statistics/266249/advertising-revenue-of-google/.

—. 2019. Facebook's annualized revenue per user from 2012 to 2018 (in U.S. dollars). *Statista.* [Online] 2019. [Citace: 27. 5 2019.] https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/.

StemMark. 2019. Marketingový výzkum a analýza dat - STEM/MARK. *stemmark.cz.* [Online] 7. 8 2019. [Citace: 19. 1 2020.] https://www.stemmark.cz/.

TechRepublic. 2018. Brute force and dictionary attacks: A cheat sheet. *techrepublic.com.* [Online] 17. 12 2018. [Citace: 8. 7 2019.] https://www.techrepublic.com/article/brute-force-and-dictionary-attacks-a-cheat-sheet/.

Uniprint. 2017. Printer Hacking – A Very Real Enterprise Data Security Breach. *uniprint.net.* [Online] 28. 9 2017. [Citace: 2019. 6 27.] https://www.uniprint.net/en/printer-hacking-data-security-breach/.

Úřad pro ochranu osobních údajů. 2018. GDPR stručně. *Úřad pro ochranu osobních údajů.* [Online] 2018. [Citace: 21. 10 2018.] https://www.uoou.cz/gdpr%2Dstrucne/ds-4843/archiv=0&p1=3938.

—. 2013. K plnění informační povinnosti. *Úřad pro ochranu osobních údajů.* [Online] 21. 3 2013. [Citace: 31. 5 2019.] https://www.uoou.cz/k-plneni-informacni-povinnosti/d-1596.

—. 2019. K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA). *Úřad pro ochranu osobních údajů.* [Online] 2019. [Citace: 27. 5 2019.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33193.

—. 2020. Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů. *uoou.cz.* [Online] 10. 1 2020. [Citace: 2. 2 20.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

—. 2018. Základní příručka k GDPR. *Úřad pro ochranu osobních údajů.* [Online] 2018. [Citace: 21. 10 2018.] https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938.

Wedos. 2018. Zásady zpracování osobních údajů zákazníkůWEDOS v souladu s GDPR. *wedos.cz.* [Online] 25. 5 2018. [Citace: 11. 2 2020.] https://www.wedos.cz/wp-content/uploads/2019/06/zasady-zpracovani-osobnich-udaju.pdf.

Wifileaks. 2019. *Wifieaks.* [Online] 5. 7 2019. [Citace: 6. 7 2019.] http://www.wifileaks.cz/statistika.php.

Zákon č. 101/2000 Sb. 2017. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. července 2017. *Úřad pro ochranu osobních údajů.* [Online] 1. 7 2017. [Citace: 21. 10 2018.] https://www.uoou.cz/zakon%2Dc%2D101%2D2000%2Dsb%2Do%2Dochrane%2Dosobnich%2Dudaju%2Da%2Do%2Dzmene%2Dnekterych%2Dzakonu%2Dve%2Dzneni%2Ducinnem%2Dod%2D1%2Dcervence%2D2017/ds-3109/p1=3109.

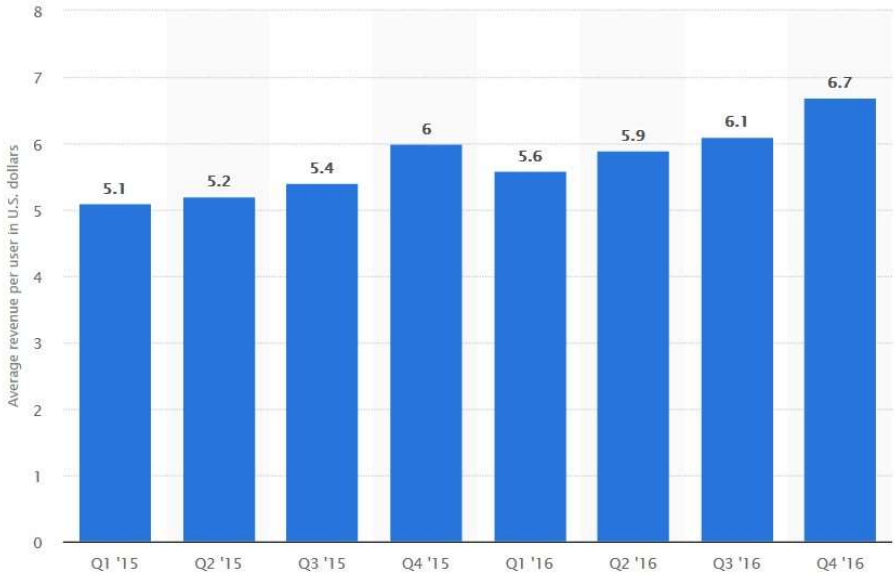
ZDNet. 2018. A new data leak hits Aadhaar, India's national ID database. *Technology News, Analysis, Comments and Product Reviews for IT Professionals | ZDNet.* [Online] 23. 4 2018. [Citace: 15. 7 2019.] https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/.

Žůrek, Jiří. 2018. *Praktický průvodce GDPR. Včetně úplného znění GDPR.* Olomouc : ANAG, 2018. ISBN 978-80-7554-152-9.

8 Přílohy

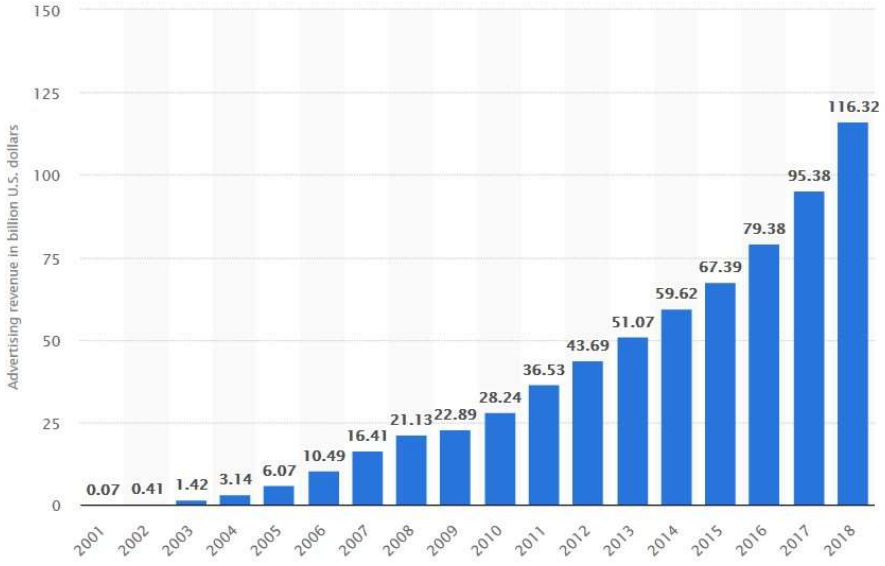
8.1 Příloha 1 - Grafy příjmů z reklam společností Google a Facebook

Obrázek 2 - Průměrný čtvrtletní příjem Googlu z reklam na jednoho uživatele



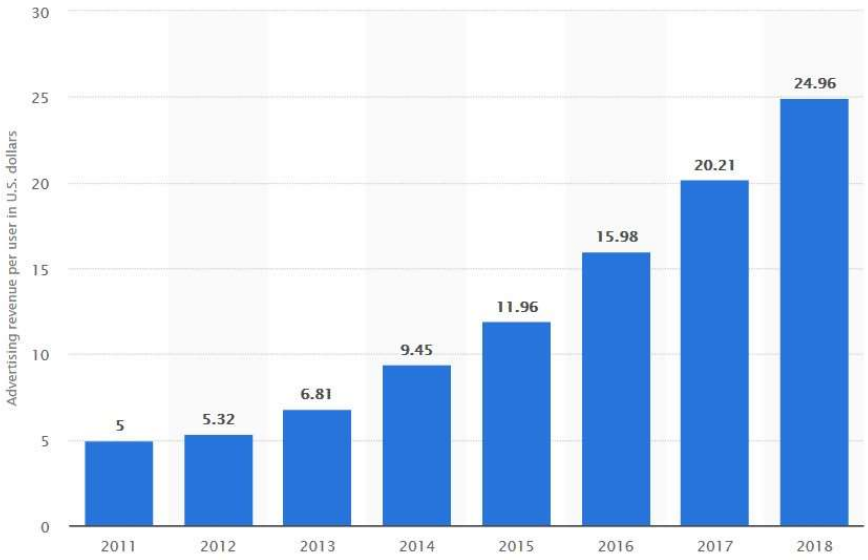
Zdroj: (Statista, 2019)

Obrázek 3 - roční příjem z reklam společnosti Google



Zdroj: (Statista, 2019)

Obrázek 4 - Roční příjem Facebooku z reklam na jednoho uživatele

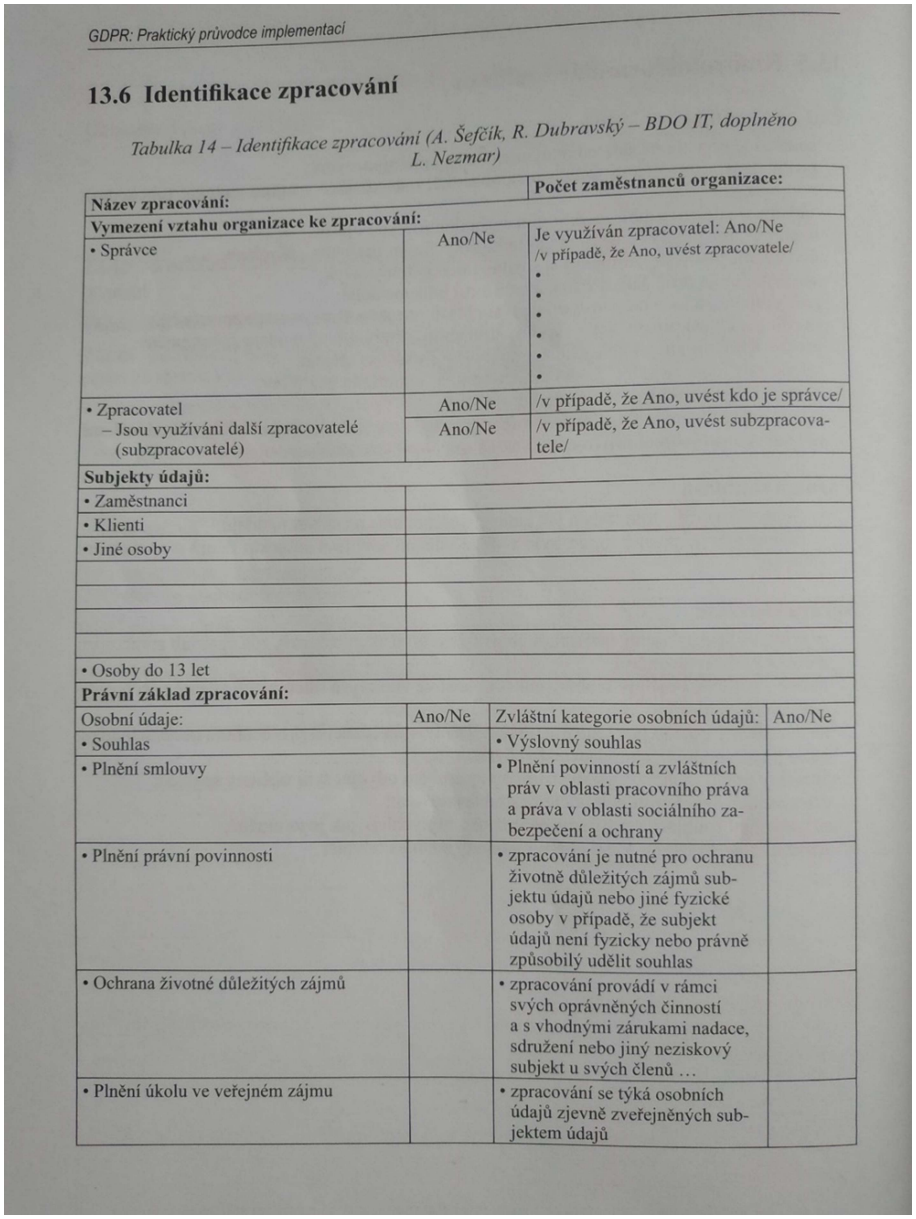


Zdroj: (Statista, 2019)

8.2 Příloha 2 - Vzor Identifikace zpracování

Jedná se o dotazník vytvořený Antonínem Šefčíkem a Romanem Dubravským použitelný pro identifikaci typu zpracování během GAP analýzy. (Nezmar, 2017 str. 296)

Obrázek 5 - Vzor pro identifikaci zpracování část 1



13.6 Identifikace zpracování

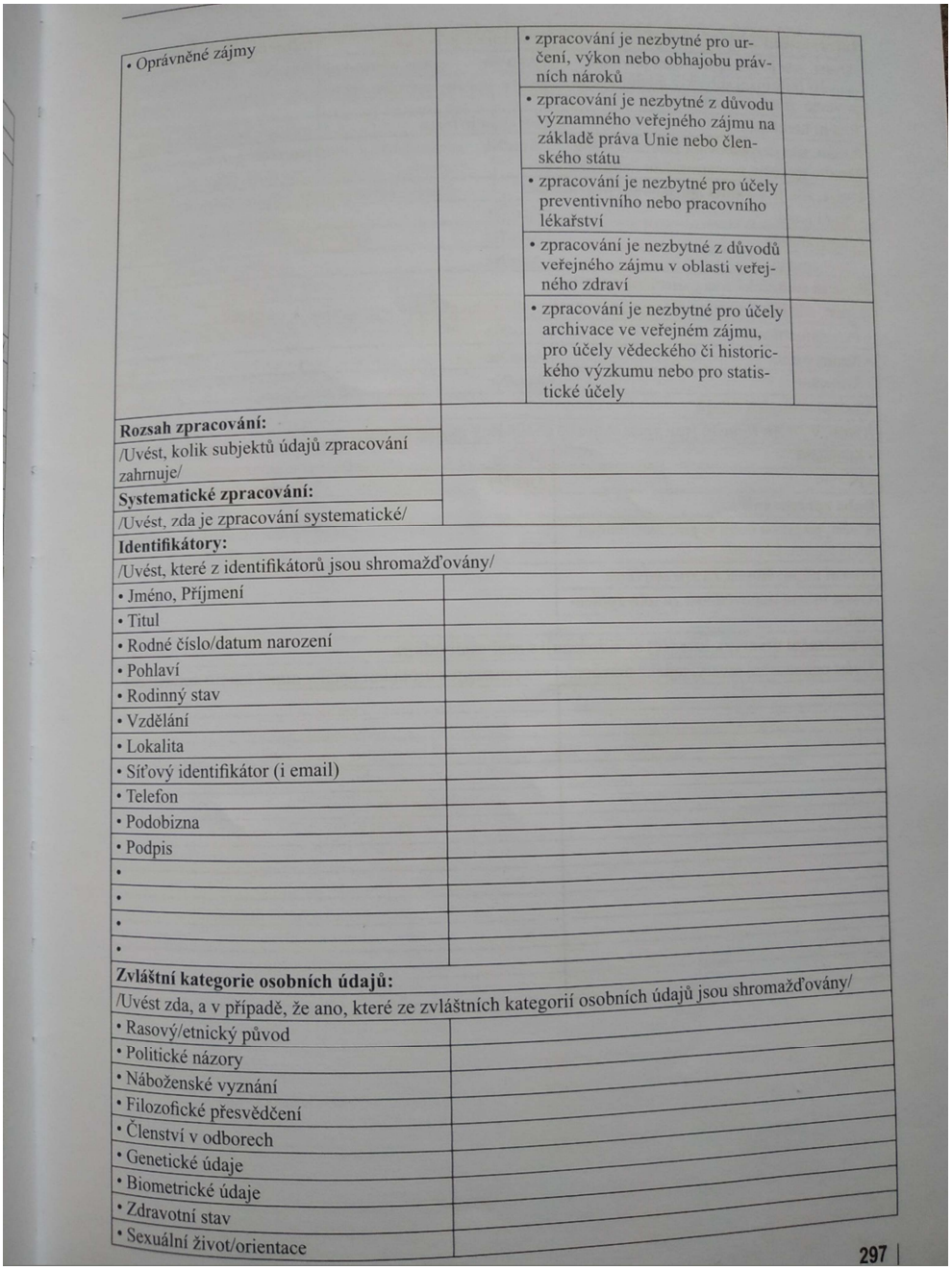
Tabulka 14 – Identifikace zpracování (A. Šefčík, R. Dubravský – BDO IT, doplněno L. Nezmar)

Název zpracování:		**Počet zaměstnanců organizace:**
Vymezení vztahu organizace ke zpracování:		
• Správce	Ano/Ne	Je využíván zpracovatel: Ano/Ne /v případě, že Ano, uvést zpracovatele/ • • • • • •
• Zpracovatel	Ano/Ne	/v případě, že Ano, uvést kdo je správce/
– Jsou využíváni další zpracovatelé (subzpracovatelé)	Ano/Ne	/v případě, že Ano, uvést subzpracovatele/
Subjekty údajů:		
• Zaměstnanci		
• Klienti		
• Jiné osoby		
• Osoby do 13 let		

Právní základ zpracování:			
Osobní údaje:	Ano/Ne	Zvláštní kategorie osobních údajů:	Ano/Ne
• Souhlas		• Výslovný souhlas	
• Plnění smlouvy		• Plnění povinností a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany	
• Plnění právní povinnosti		• zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas	
• Ochrana životné důležitých zájmů		• zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt u svých členů …	
• Plnění úkolu ve veřejném zájmu		• zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů	

Zdroj: (Nezmar, 2017 str. 296)

Obrázek 6 - Vzor pro identifikaci zpracování část 2

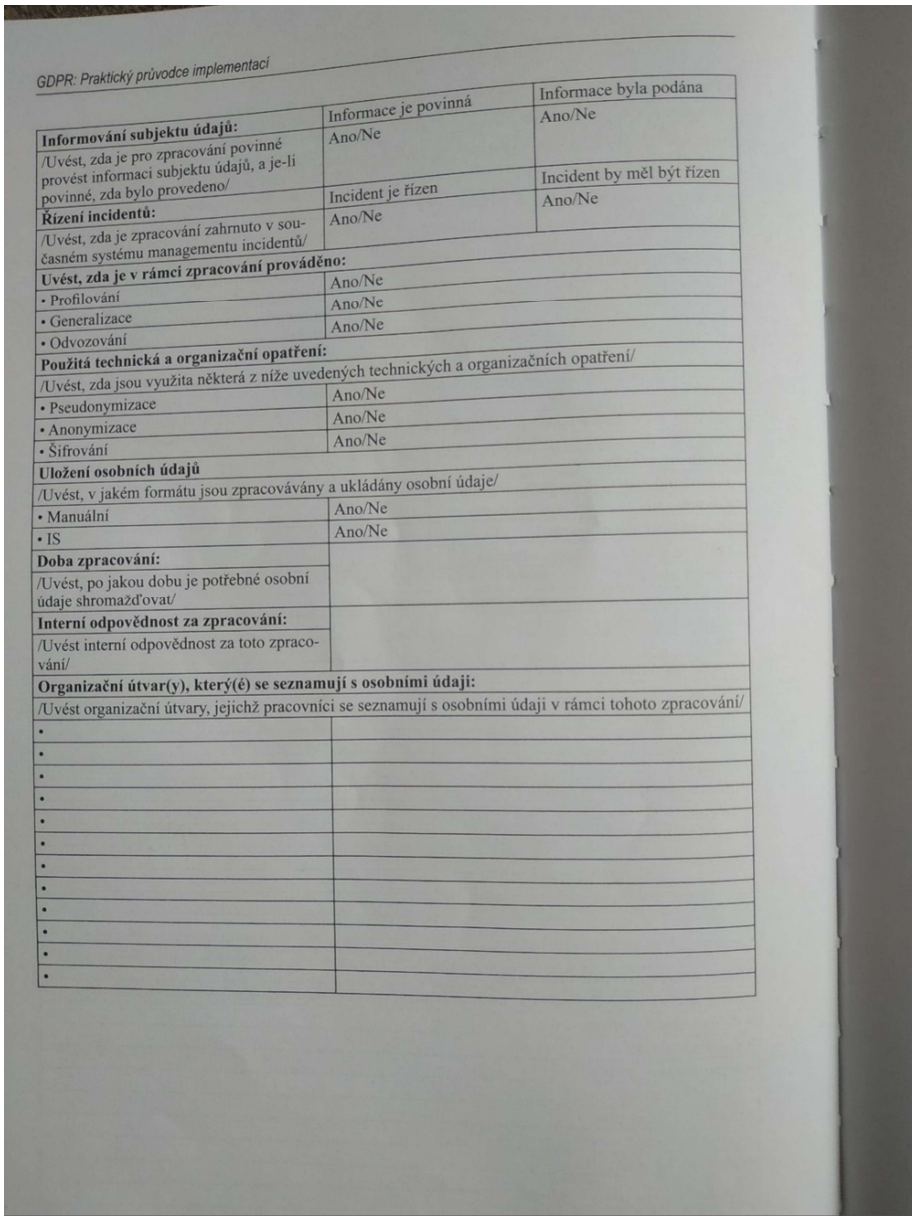


• Oprávněné zájmy		• zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků	
		• zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu	
		• zpracování je nezbytné pro účely preventivního nebo pracovního lékařství	
		• zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví	
		• zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely	
Rozsah zpracování:			
/Uvést, kolik subjektů údajů zpracování zahrnuje/			
Systematické zpracování:			
/Uvést, zda je zpracování systematické/			
Identifikátory:			
/Uvést, které z identifikátorů jsou shromažďovány/			
• Jméno, Příjmení			
• Titul			
• Rodné číslo/datum narození			
• Pohlaví			
• Rodinný stav			
• Vzdělání			
• Lokalita			
• Síťový identifikátor (i email)			
• Telefon			
• Podobizna			
• Podpis			
•			
•			
•			
•			
Zvláštní kategorie osobních údajů:			
/Uvést zda, a v případě, že ano, které ze zvláštních kategorií osobních údajů jsou shromažďovány/			
• Rasový/etnický původ			
• Politické názory			
• Náboženské vyznání			
• Filozofické přesvědčení			
• Členství v odborech			
• Genetické údaje			
• Biometrické údaje			
• Zdravotní stav			
• Sexuální život/orientace			

297

Zdroj: (Nezmar, 2017 str. 297)

Obrázek 7 - Vzor pro identifikaci zpracování část 3



GDPR: Praktický průvodce implementací

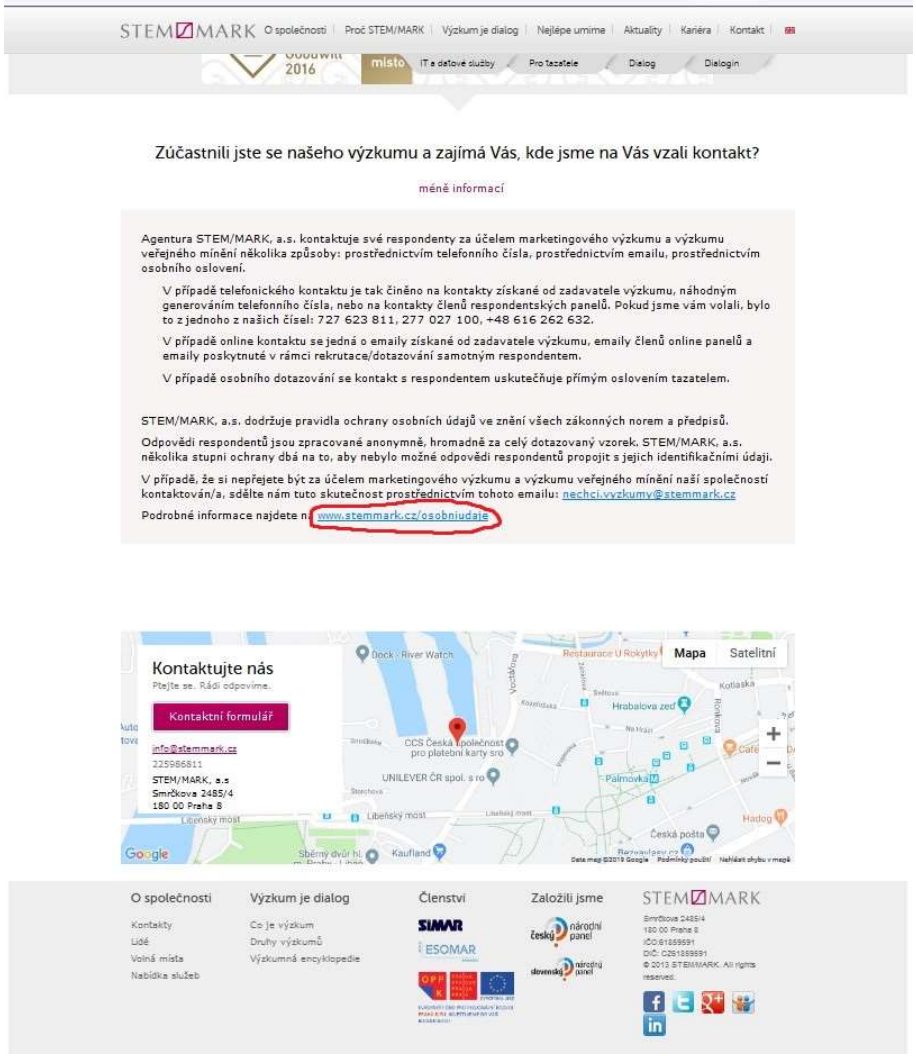
Informování subjektu údajů: /Uvést, zda je pro zpracování povinné provést informaci subjektu údajů, a je-li povinné, zda bylo provedeno/	Informace je povinná Ano/Ne	Informace byla podána Ano/Ne
Řízení incidentů: /Uvést, zda je zpracování zahrnuto v současném systému managementu incidentů/	Incident je řízen Ano/Ne	Incident by měl být řízen Ano/Ne
Uvést, zda je v rámci zpracování prováděno:		
• Profilování	Ano/Ne	
• Generalizace	Ano/Ne	
• Odvozování	Ano/Ne	
Použitá technická a organizační opatření:		
/Uvést, zda jsou využita některá z níže uvedených technických a organizačních opatření/		
• Pseudonymizace	Ano/Ne	
• Anonymizace	Ano/Ne	
• Šifrování	Ano/Ne	
Uložení osobních údajů		
/Uvést, v jakém formátu jsou zpracovávány a ukládány osobní údaje/		
• Manuální	Ano/Ne	
• IS	Ano/Ne	
Doba zpracování: /Uvést, po jakou dobu je potřebné osobní údaje shromažďovat/		
Interní odpovědnost za zpracování: /Uvést interní odpovědnost za toto zpracování/		
Organizační útvar(y), který(é) se seznamují s osobními údaji:		
/Uvést organizační útvary, jejichž pracovníci se seznamují s osobními údaji v rámci tohoto zpracování/		
•		
•		
•		
•		
•		
•		
•		
•		
•		
•		
•		
•		

Zdroj: (Nezmar, 2017 str. 298)

8.3 Příloha 3 – Webové stránky firem a komunikace s nimi

8.3.1 Stemmark

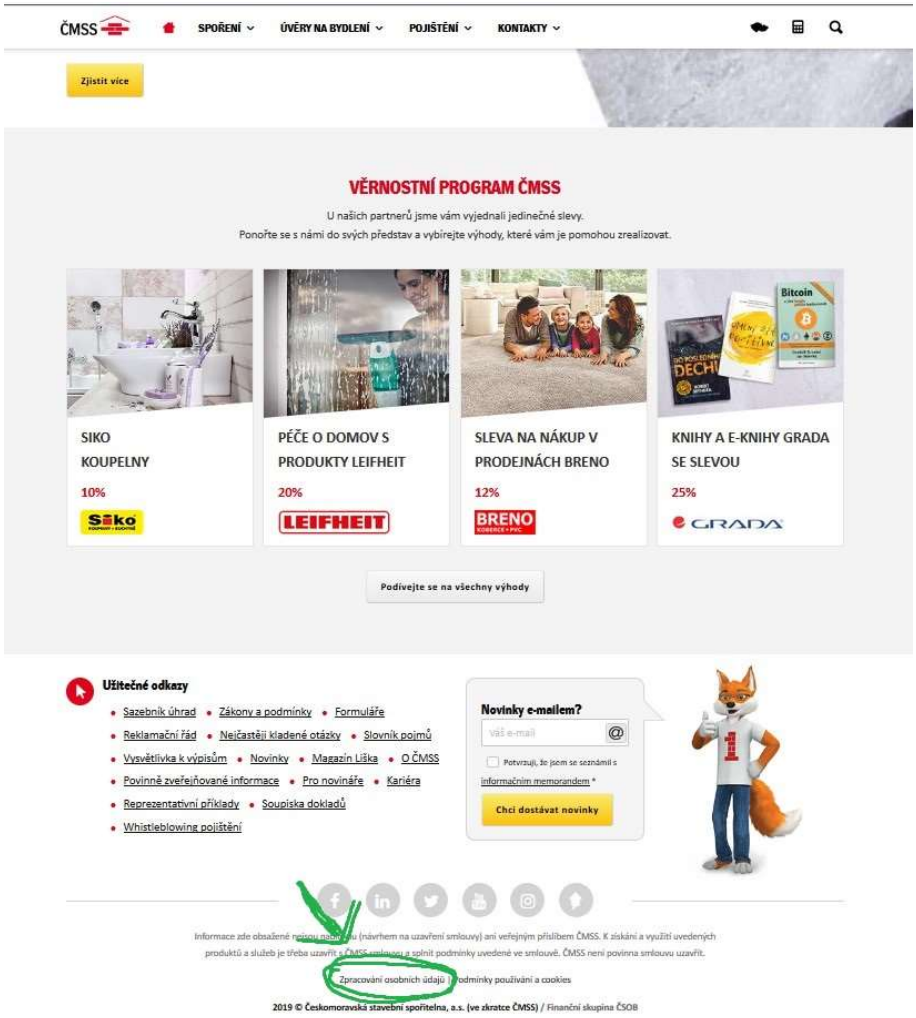
Obrázek 8 - STEM/MARK – informace o zpracování



Zdroj: (StemMark, 2019)

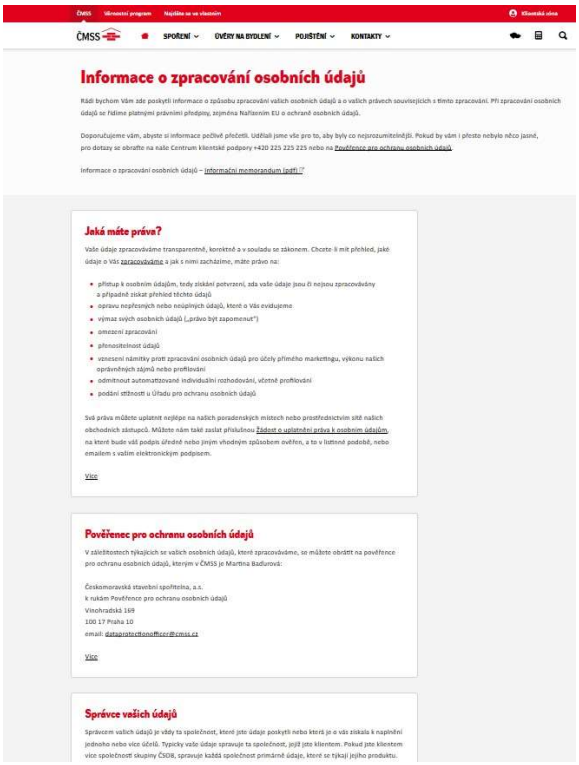
8.3.2 Českomoravská stavební spořitelna

Obrázek 9 - Českomoravská stavební spořitelna – umístění odkazu



Zdroj: (ČMSS, 2019)

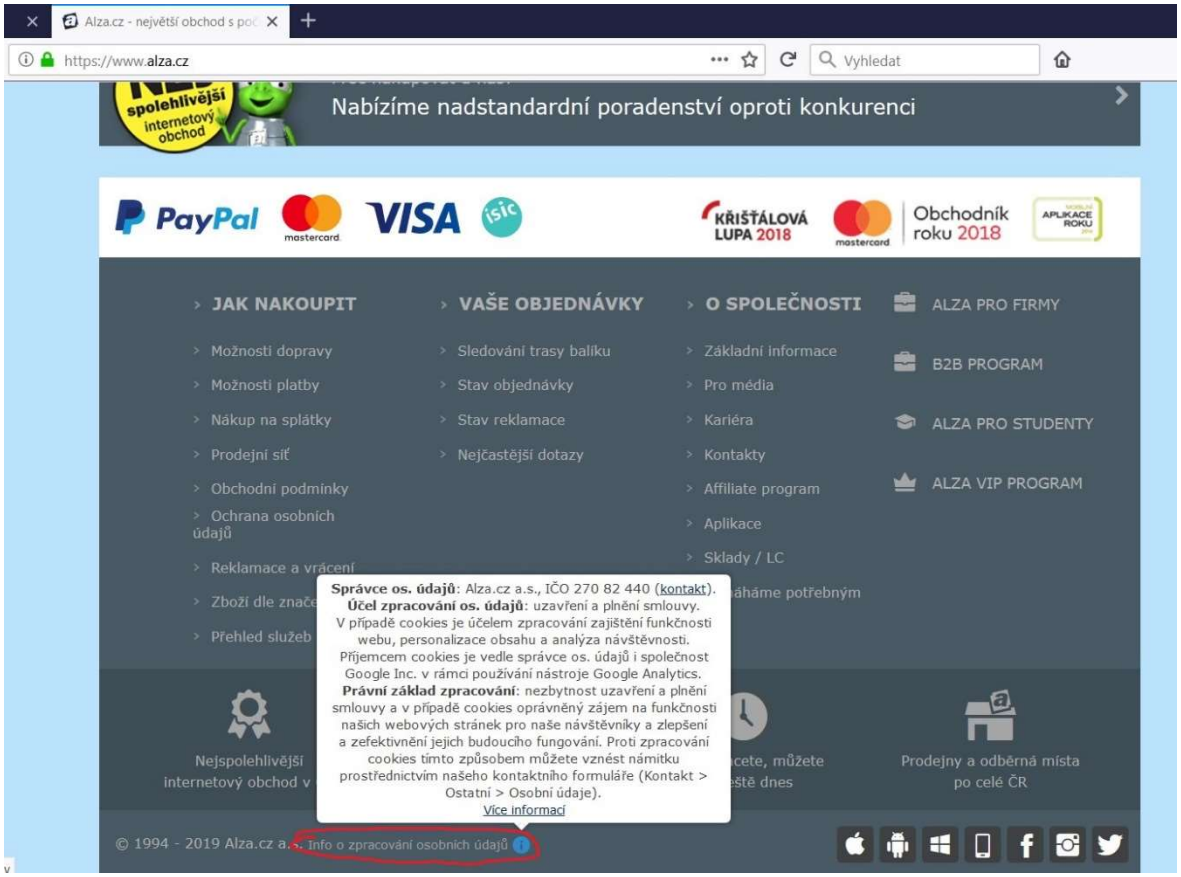
Obrázek 10 - Českomoravská stavební spořitelna – struktura informací



Zdroj: (ČMSS, 2019)

8.3.3 **Alza**

Obrázek 11 - Alza.cz - informace o zpracování

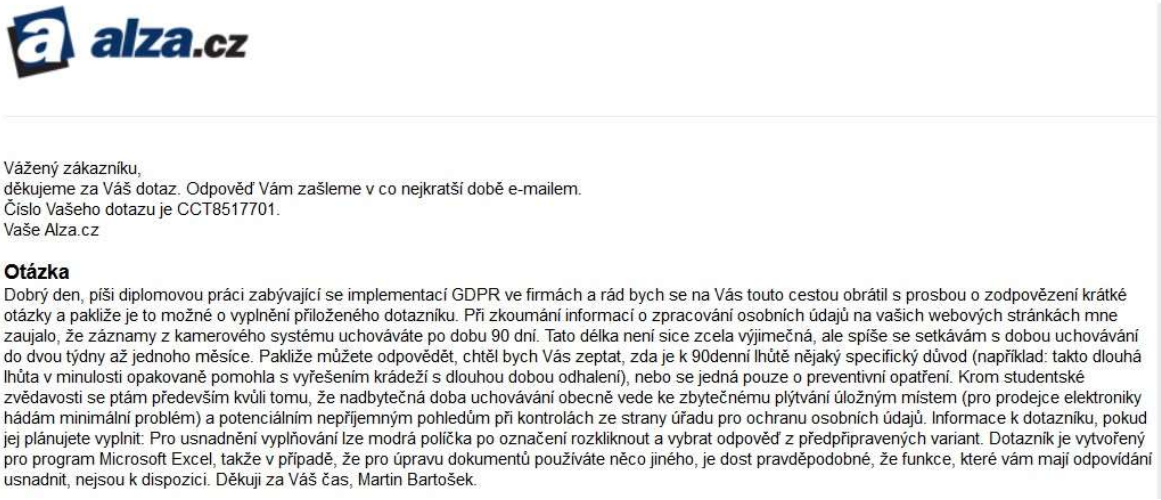


Zdroj: (Alza.cz, 2019)

Obrázek 12 - Alza.cz - dotazovací formulář

Zdroj: Komunikace s Alza.cz

Obrázek 13 - Alza.cz - automatická odpověď



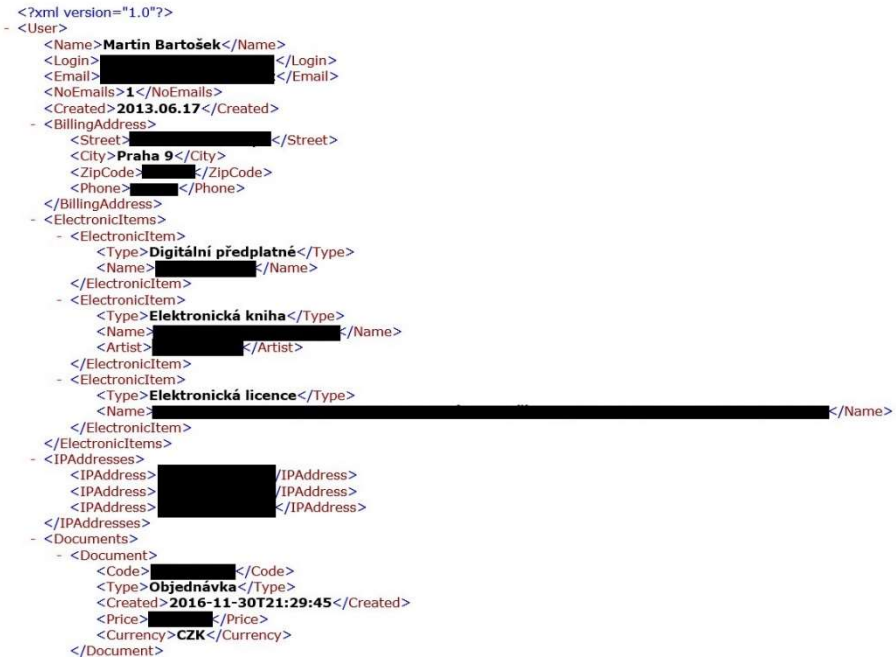
Vážený zákazníku,
děkujeme za Váš dotaz. Odpověď Vám zašleme v co nejkratší době e-mailem.
Číslo Vašeho dotazu je CCT8517701.
Vaše Alza.cz

Otázka

Dobrý den, píši diplomovou práci zabývající se implementací GDPR ve firmách a rád bych se na Vás touto cestou obrátil s prosbou o zodpovězení krátké otázky a pakliže je to možné o vyplnění přiloženého dotazníku. Při zkoumání informací o zpracování osobních údajů na vašich webových stránkách mne zaujalo, že záznamy z kamerového systému uchováváte po dobu 90 dní. Tato délka není sice zcela výjimečná, ale spíše se setkávám s dobou uchovávání do dvou týdny až jednoho měsíce. Pakliže můžete odpovědět, chtěl bych Vás zeptat, zda je k 90denní lhůtě nějaký specifický důvod (například: takto dlouhá lhůta v minulosti opakovaně pomohla s vyřešením krádeží s dlouhou dobou odhalení), nebo se jedná pouze o preventivní opatření. Krom studentské zvědavosti se ptám především kvůli tomu, že nadbytečná doba uchovávání obecně vede ke zbytečnému plýtvání úložným místem (pro prodejce elektroniky hádám minimální problém) a potenciálním nepříjemným pohledům při kontrolách ze strany úřadu pro ochranu osobních údajů. Informace k dotazníku, pokud jej plánujete vyplnit: Pro usnadnění vyplňování lze modrá políčka po označení rozkliknout a vybrat odpověď z předpřipravených variant. Dotazník je vytvořený pro program Microsoft Excel, takže v případě, že pro úpravu dokumentů používáte něco jiného, je dost pravděpodobné, že funkce, které vám mají odpovídání usnadnit, nejsou k dispozici. Děkuji za Váš čas, Martin Bartošek.

Zdroj: Komunikace s Alza.cz

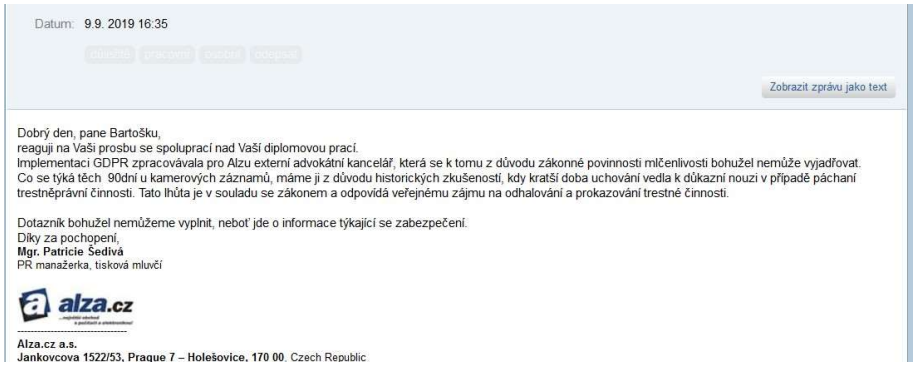
Obrázek 14 - Alza – ukázka vyžádaných dat



```
<?xml version="1.0"?>
- <User>
    <Name>Martin Bartošek</Name>
    <Login>[redacted]</Login>
    <Email>[redacted]</Email>
    <NoEmails>1</NoEmails>
    <Created>2013.06.17</Created>
  - <BillingAddress>
      <Street>[redacted]</Street>
      <City>Praha 9</City>
      <ZipCode>[redacted]</ZipCode>
      <Phone>[redacted]</Phone>
    </BillingAddress>
  - <ElectronicItems>
    - <ElectronicItem>
        <Type>Digitální předplatné</Type>
        <Name>[redacted]</Name>
      </ElectronicItem>
    - <ElectronicItem>
        <Type>Elektronická kniha</Type>
        <Name>[redacted]</Name>
        <Artist>[redacted]</Artist>
      </ElectronicItem>
    - <ElectronicItem>
        <Type>Elektronická licence</Type>
        <Name>[redacted]</Name>
      </ElectronicItem>
    </ElectronicItems>
  - <IPAddresses>
      <IPAddress>[redacted]/IPAddress>
      <IPAddress>[redacted]/IPAddress>
      <IPAddress>[redacted]</IPAddress>
    </IPAddresses>
  - <Documents>
    - <Document>
        <Code>[redacted]</Code>
        <Type>Objednávka</Type>
        <Created>2016-11-30T21:29:45</Created>
        <Price>[redacted]</Price>
        <Currency>CZK</Currency>
      </Document>
```

Zdroj: Komunikace s Alza.cz

Obrázek 15 - Alza – odpověď na dotazník


Datum: 9.9. 2019 16:35

Zobrazit zprávu jako text

Dobrý den, pane Bartošku,
reaguji na Vaši prosbu se spoluprací nad Vaší diplomovou prací.
Implementaci GDPR zpracovávala pro Alzu externí advokátní kancelář, která se k tomu z důvodu zákonné povinnosti mlčenlivosti bohužel nemůže vyjadřovat.
Co se týká těch 90dní u kamerových záznamů, máme ji z důvodu historických zkušeností, kdy kratší doba uchování vedla k důkazní nouzi v případě páchaní trestněprávní činnosti. Tato lhůta je v souladu se zákonem a odpovídá veřejnému zájmu na odhalování a prokazování trestné činnosti.

Dotazník bohužel nemůžeme vyplnit, neboť jde o informace týkající se zabezpečení.
Díky za pochopení,
Mgr. Patricie Šedivá
PR manažerka, tisková mluvčí

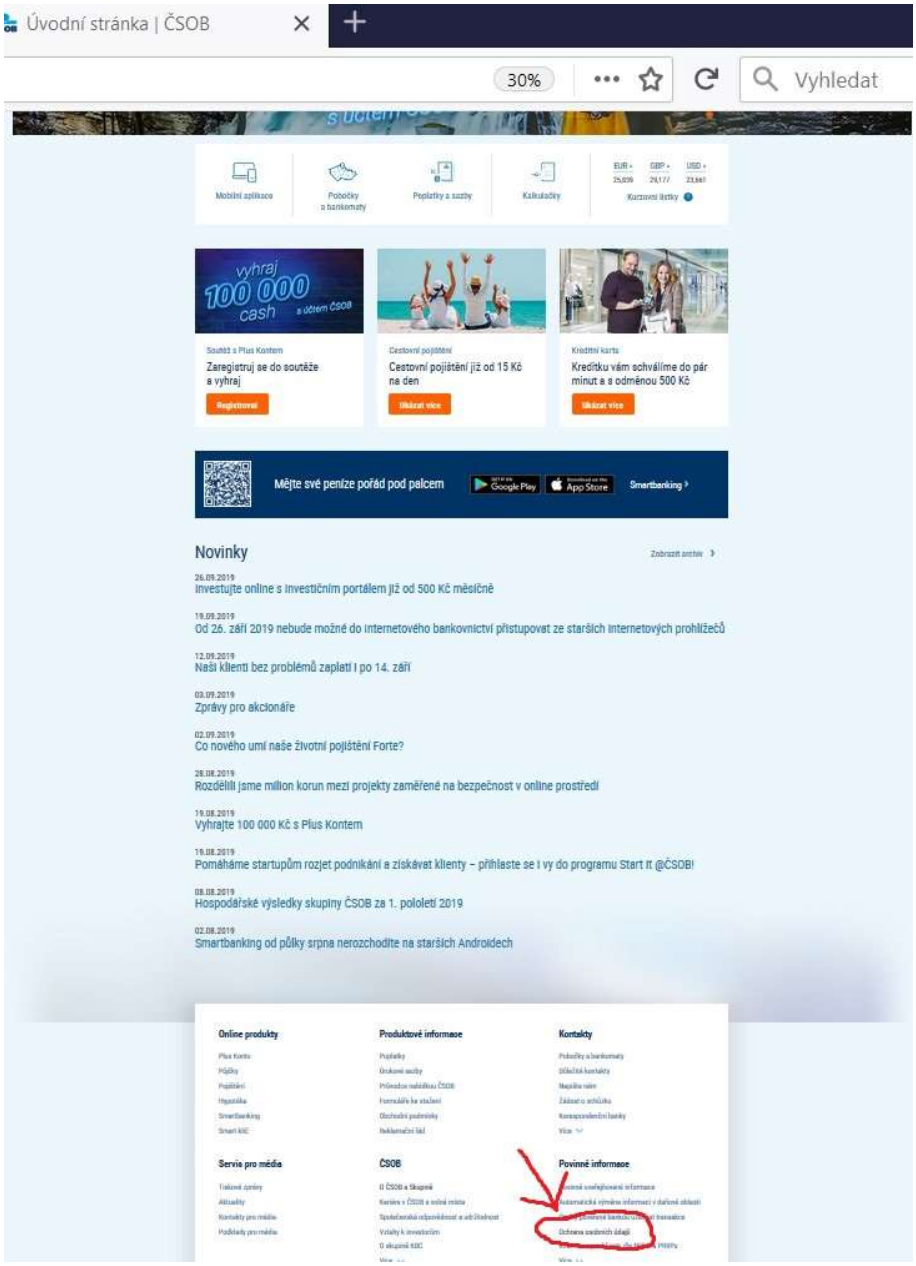
alza.cz

Alza.cz a.s.
Jankovcova 1522/53, Praque 7 – Holešovice, 170 00, Czech Republic

Zdroj: Komunikace s Alza.cz

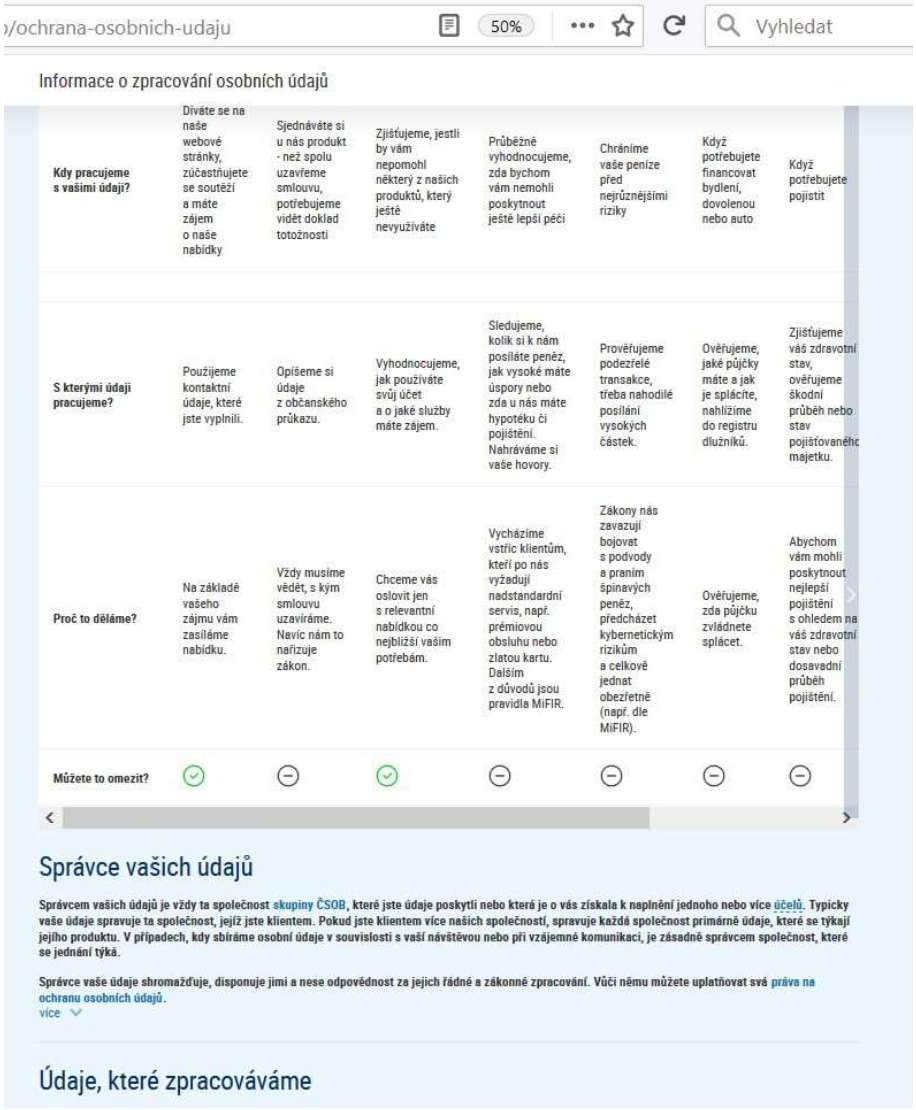
8.3.4 **ČSOB**

Obrázek 16 - ČSOB umístění odkazu



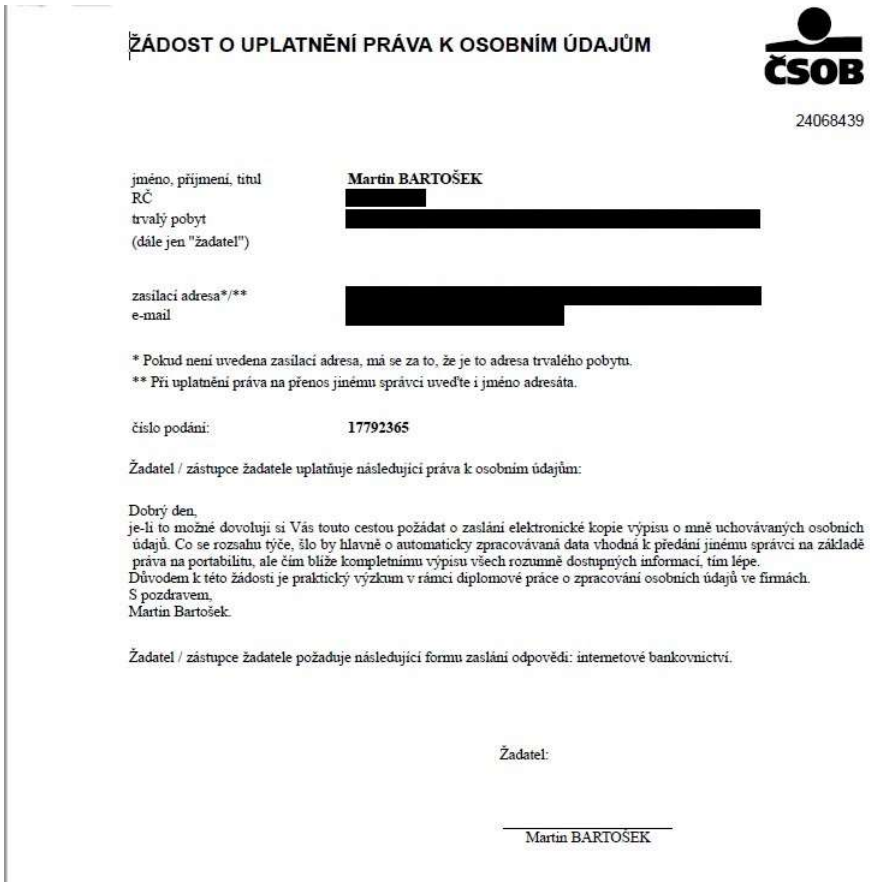
Zdroj: (ČSOB, 2019)

Obrázek 17 - ČSOB – Informace o zpracování



Zdroj: (ČSOB, 2019)

Obrázek 18 - ČSOB žádost o údaje



ŽÁDOST O UPLATNĚNÍ PRÁVA K OSOBNÍM ÚDAJŮM

ČSOB

24068439

jméno, příjmení, titul: **Martin BARTOŠEK**
RČ: [redacted]
trvalý pobyt: [redacted]
(dále jen "žadatel")

zasílací adresa*/**: [redacted]
e-mail: [redacted]

* Pokud není uvedena zasílací adresa, má se za to, že je to adresa trvalého pobytu.
** Při uplatnění práva na přenos jinému správci uveďte i jméno adresáta.

číslo podání: **17792365**

Žadatel / zástupce žadatele uplatňuje následující práva k osobním údajům:

Dobrý den,
je-li to možné dovoluji si Vás touto cestou požádat o zaslání elektronické kopie výpisu o mně uchovávaných osobních údajů. Co se rozsahu týče, šlo by hlavně o automaticky zpracovávaná data vhodná k předání jinému správci na základě práva na portabilitu, ale čím blíže kompletnímu výpisu všech rozumně dostupných informací, tím lépe.
Důvodem k této žádosti je praktický výzkum v rámci diplomové práce o zpracování osobních údajů ve firmách.
S pozdravem,
Martin Bartošek.

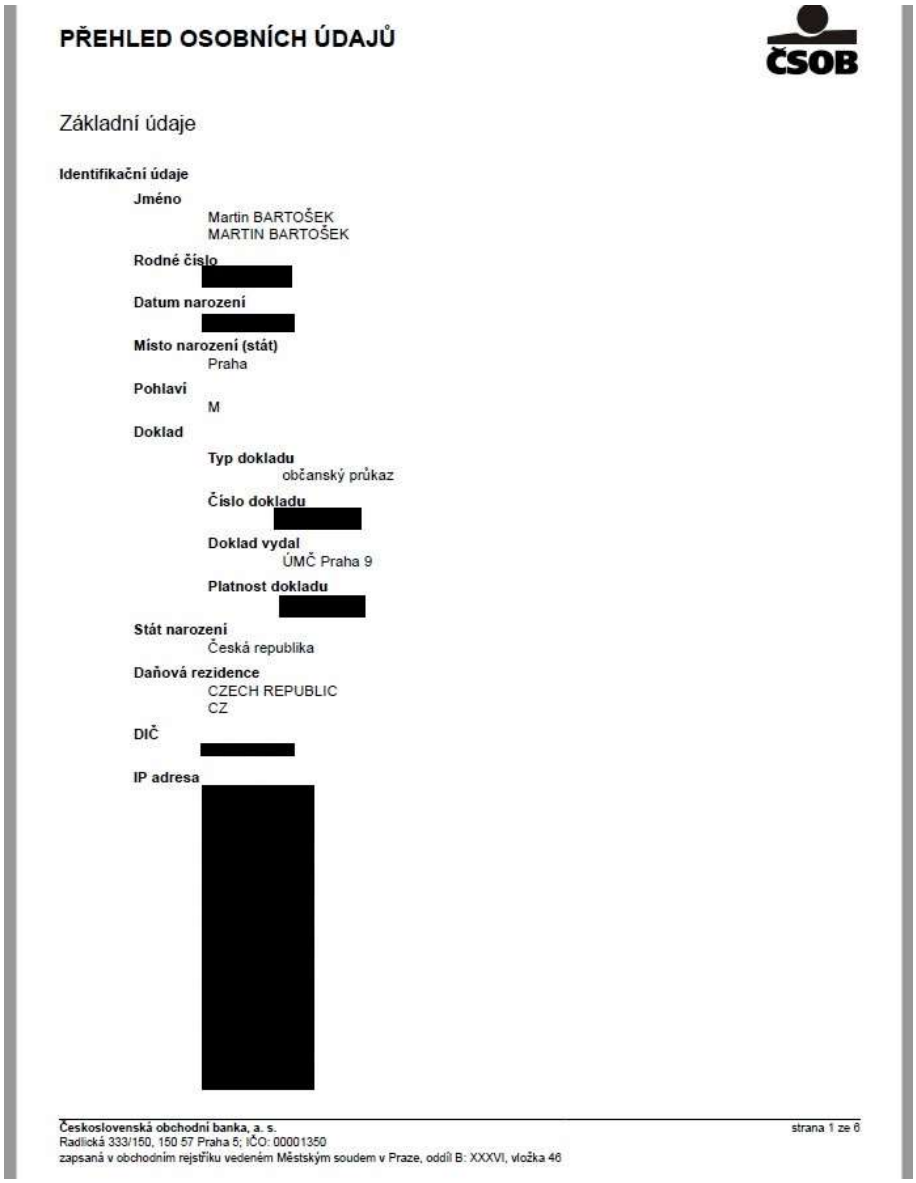
Žadatel / zástupce žadatele požaduje následující formu zaslání odpovědi: internetové bankovnictví.

Žadatel:

Martin BARTOŠEK

Zdroj: Komunikace s ČSOB

Obrázek 19 - ČSOB – přehled údajů 1



PŘEHLED OSOBNÍCH ÚDAJŮ

ČSOB

Základní údaje

Identifikační údaje

Jméno
Martin BARTOŠEK
MARTIN BARTOŠEK

Rodné číslo
[redacted]

Datum narození
[redacted]

Místo narození (stát)
Praha

Pohlaví
M

Doklad

Typ dokladu
občanský průkaz

Číslo dokladu
[redacted]

Doklad vydal
ÚMČ Praha 9

Platnost dokladu
[redacted]

Stát narození
Česká republika

Daňová rezidence
CZECH REPUBLIC
CZ

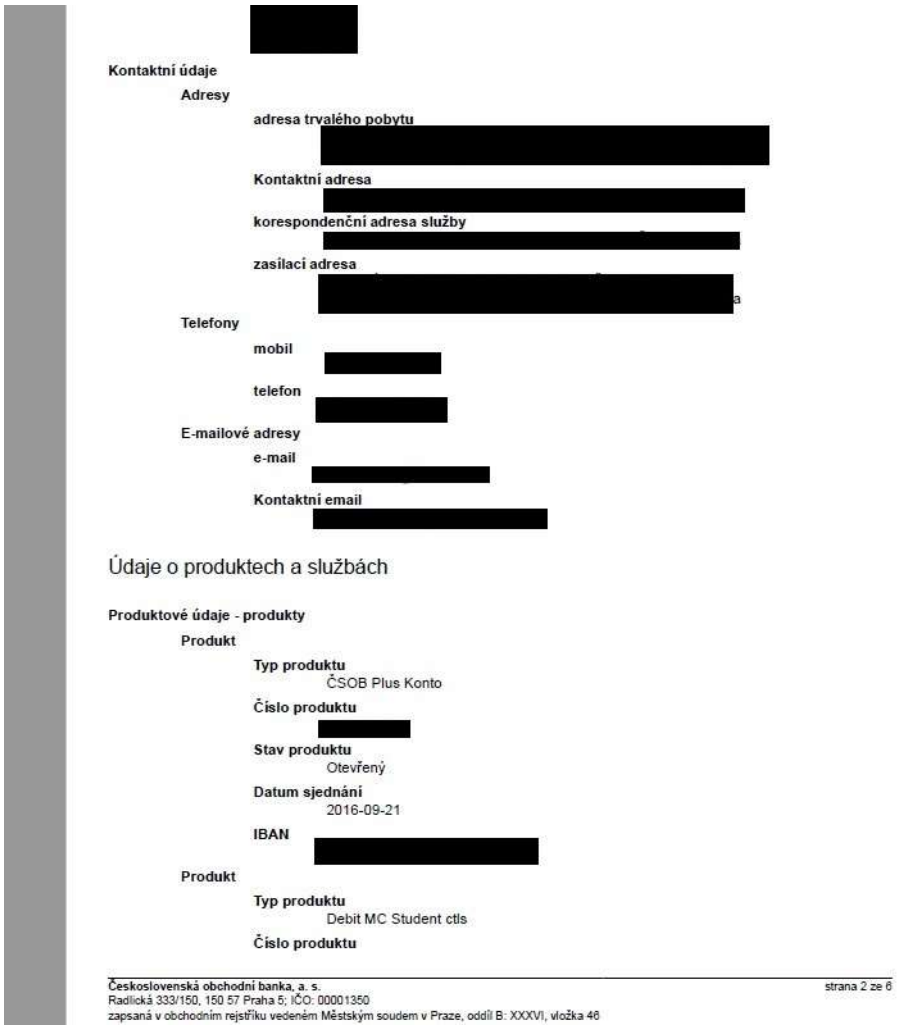
DIČ
[redacted]

IP adresa
[redacted]

Československá obchodní banka, a. s. strana 1 ze 6
Radlická 333/150, 150 57 Praha 5; IČO: 00001350
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B: XXXVI, vložka 46

Zdroj: Komunikace s ČSOB

Obrázek 20 - ČSOB – přehled údajů 2



[redacted]

Kontaktní údaje

Adresy

adresa trvalého pobytu
[redacted]

Kontaktní adresa
[redacted]

korespondenční adresa služby
[redacted]

zasílací adresa
[redacted]

Telefony

mobil
[redacted]

telefon
[redacted]

E-mailové adresy

e-mail
[redacted]

Kontaktní email
[redacted]

Údaje o produktech a službách

Produktové údaje - produkty

Produkt

Typ produktu
ČSOB Plus Konto

Číslo produktu
[redacted]

Stav produktu
Otevřený

Datum sjednání
2016-09-21

IBAN
[redacted]

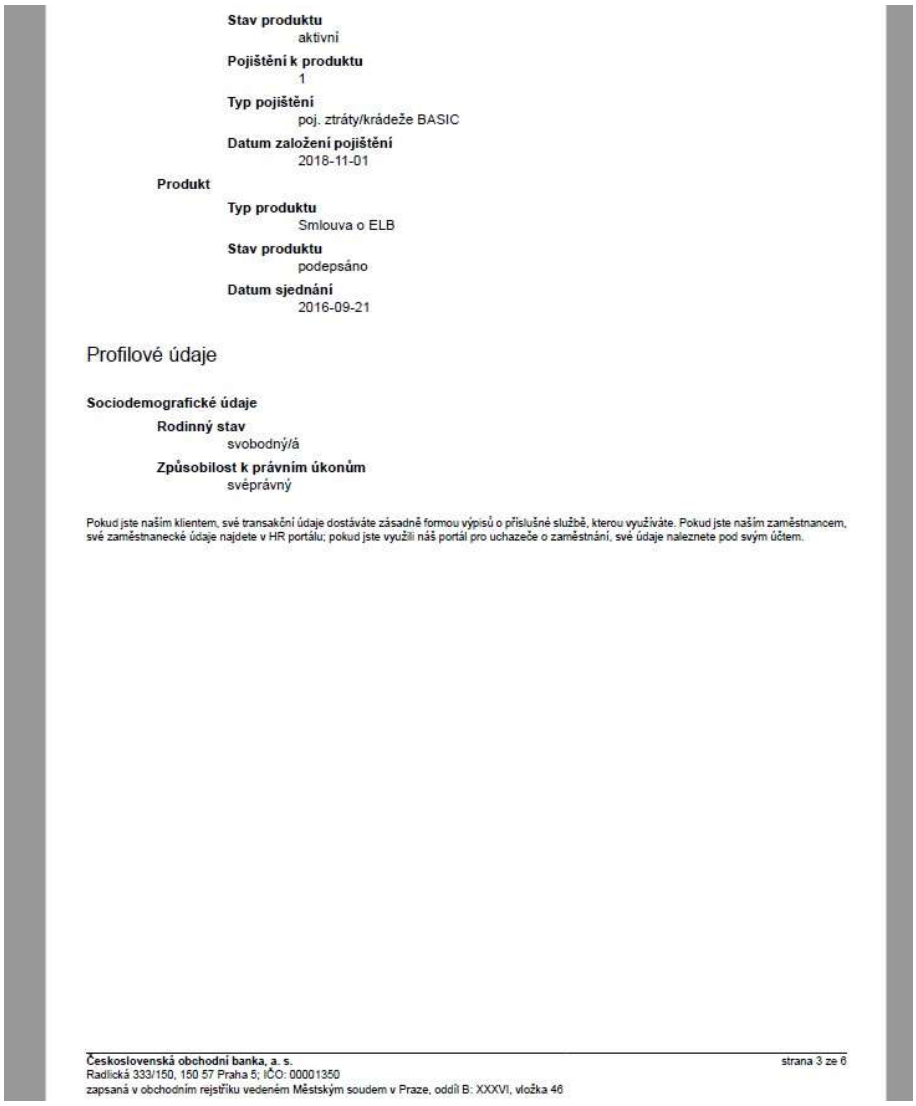
Produkt

Typ produktu
Debit MC Student ctls

Číslo produktu

Zdroj: Komunikace s ČSOB

Obrázek 21 - ČSOB – přehled údajů 3



Stav produktu
aktivní

Pojištění k produktu
1

Typ pojištění
poj. ztráty/krádeže BASIC

Datum založení pojištění
2018-11-01

Produkt

Typ produktu
Smlouva o ELB

Stav produktu
podepsáno

Datum sjednání
2016-09-21

Profilové údaje

Sociodemografické údaje

Rodinný stav
svobodný/á

Způsobilost k právním úkonům
svéprávný

Pokud jste naším klientem, své transakční údaje dostáváte zásadně formou výpisů o příslušné službě, kterou využíváte. Pokud jste naším zaměstnancem, své zaměstnanecké údaje najdete v HR portálu; pokud jste využili náš portál pro uchazeče o zaměstnání, své údaje naleznete pod svým účtem.

Zdroj: Komunikace s ČSOB

Obrázek 22 - ČSOB Odpověď na žádost

ČSOB

Martin BARTOŠEK
[redacted]
Česká republika

Vážená paní, vážený pane,

zasíláme Vám vyjádření k Vaší žádosti o uplatnění práva k osobním údajům číslo **17792365** ze dne **29.09.2019**.

Potvrzujeme, že zpracováváme osobní údaje, které se Vás týkají, a posíláme Vám jejich přehled a další informace. Poskytnuté údaje a informace jsou platné ke dni vyřízení Vaší žádosti. Pokud Vám zde nějaký osobní údaj nebo informace chybí, neváhejte se na nás obrátit na kontaktech uvedených níže. Přehled neobsahuje údaje, které Vám nejsme oprávněni poskytnout, ani údaje, které nejsou z povahy věci dále průběžně používány.

Na Vaši žádost posíláme v příloze požadované osobní údaje tak, jak vyžadují příslušné právní předpisy. Jedná se o údaje, které zpracováváme automatizovaně, tedy pouze v našich informačních systémech, na základě Vašeho souhlasu nebo podepsané smlouvy. Upozorňujeme však, že neručíme za integritu přenesených dat. Součástí nejsou údaje, které Vám nejsme oprávněni poskytnout, ani údaje, které nejsou z povahy věci dále průběžně používány.

V případě, že jsme Vaší žádosti nevyhověli nebo s jejím vyřízením nesouhlasíte, můžete nás kontaktovat se žádostí o prošetření nebo podat podnět našemu pověřenci pro ochranu osobních údajů, e-mail: dataprotectionofficer@csob.cz. Aktuální kontakty naleznete v informačním memorandu (viz první strana a část "Jaká máte práva?"), odkaz na memorandum se nachází níže. Jste také oprávněni podat stížnost u dozorového úřadu, případně pak žádat o soudní ochranu. Stížnost se podává k Úřadu na ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7. Podrobnější informace k podání stížnosti naleznete na stránkách úřadu www.uoou.cz nebo Vám je Úřad může sdělit na telefonním čísle 234 665 111.

Více informací najdete v našich Informacích o zpracování osobních údajů na stránce www.csob.cz/osobni-udaje. Nemáte-li přístup k internetu, požádejte nás o jeho poslední verzi v jakékoliv pobočce nebo na bezplatné lince 800 300 300.

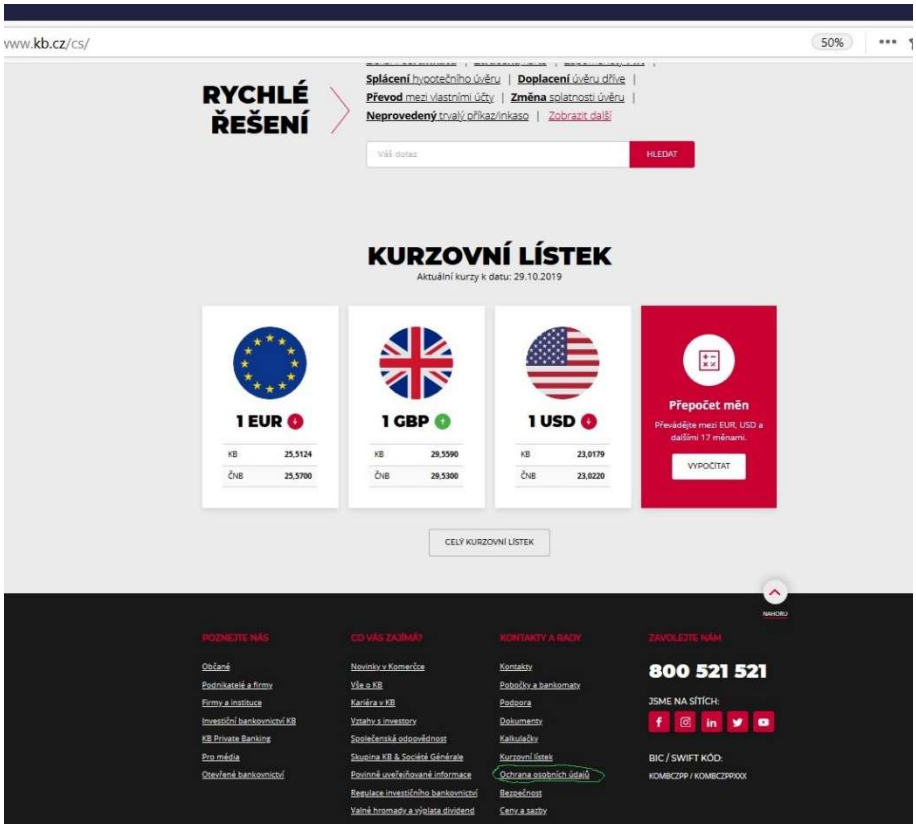
S pozdravem

V Praze dne 2.10.2019

Zdroj: Komunikace s ČSOB

8.3.5 **Komerční Banka**

Obrázek 23 - KB umístění odkazu



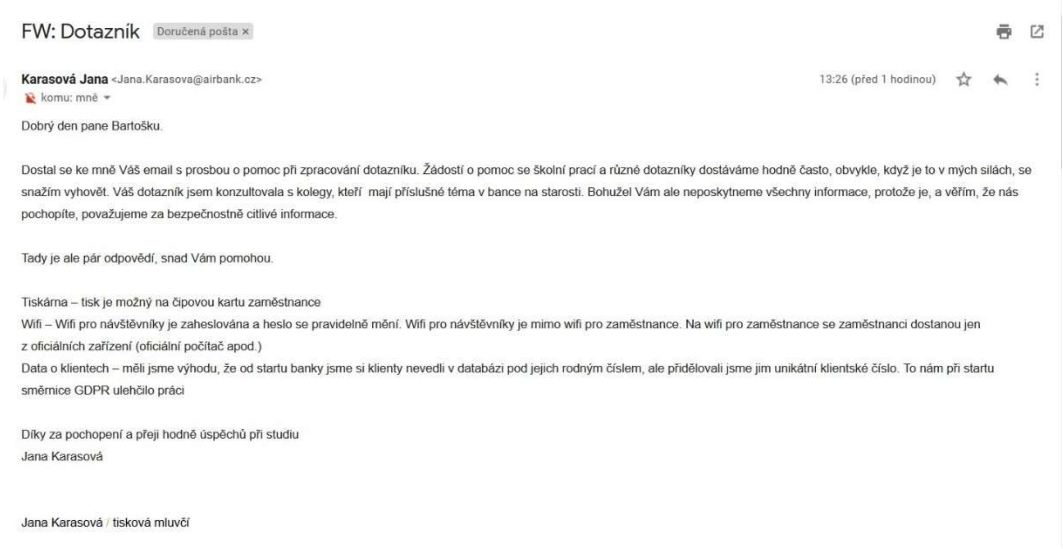
Zdroj: (Komerční Banka, 2019)

Obrázek 24 - KB informace o zpracování

Zdroj: (Komerční Banka, 2019)

8.3.6 **AirBank**

Obrázek 25 - AirBank – Odpověď na dotazy



FW: Dotazník Doručená pošta ×

Karasová Jana <Jana.Karasova@airbank.cz> 13:26 (před 1 hodinou)

komu: mně

Dobrý den pane Bartošku.

Dostal se ke mně Váš email s prosbou o pomoc při zpracování dotazníku. Žádostí o pomoc se školní prací a různé dotazníky dostáváme hodně často, obvykle, když je to v mých silách, se snažím vyhovět. Váš dotazník jsem konzultovala s kolegy, kteří mají příslušné téma v bance na starosti. Bohužel Vám ale neposkytneme všechny informace, protože je, a věřím, že nás pochopíte, považujeme za bezpečnostně citlivé informace.

Tady je ale pár odpovědí, snad Vám pomohou.

Tiskárna – tisk je možný na čipovou kartu zaměstnance
Wifi – Wifi pro návštěvníky je zaheslována a heslo se pravidelně mění. Wifi pro návštěvníky je mimo wifi pro zaměstnance. Na wifi pro zaměstnance se zaměstnanci dostanou jen z oficiálních zařízení (oficiální počítač apod.)
Data o klientech – měli jsme výhodu, že od startu banky jsme si klienty nevedli v databázi pod jejich rodným číslem, ale přidělovali jsme jim unikátní klientské číslo. To nám při startu směrnice GDPR ulehčilo práci

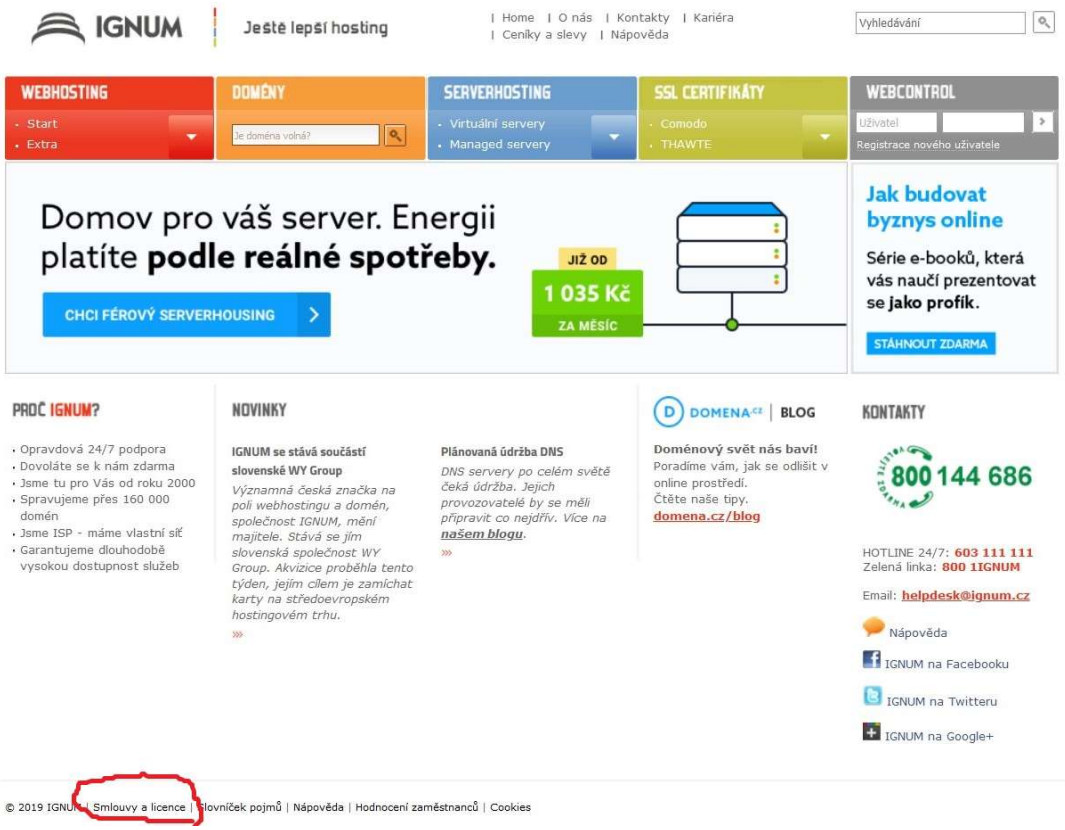
Díky za pochopení a přeji hodně úspěchů při studiu
Jana Karasová

Jana Karasová / tisková mluvčí

Zdroj: Komunikace s Komerční Bankou

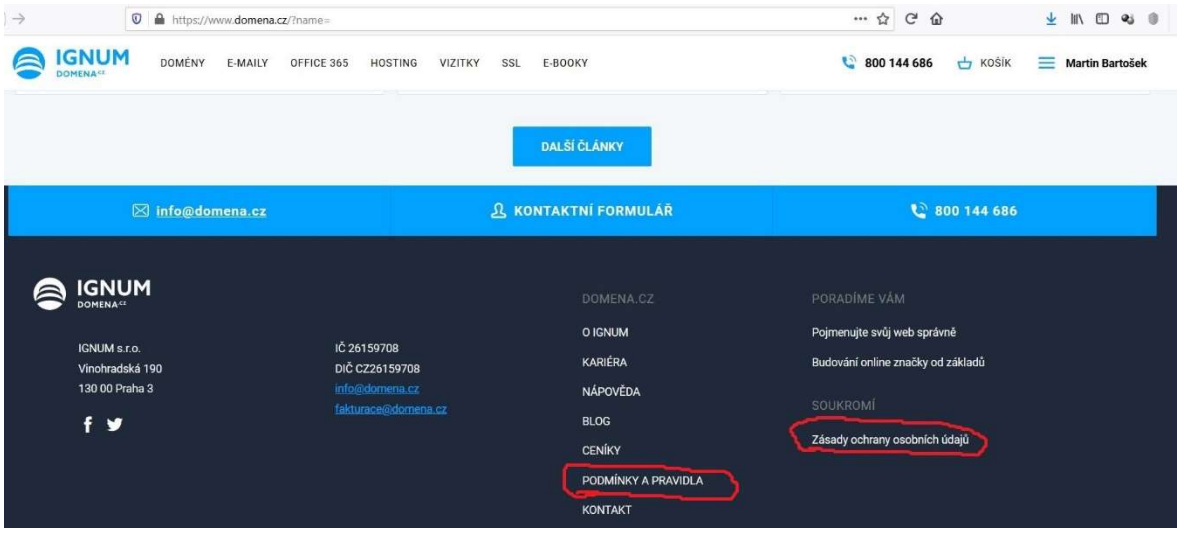
8.3.7 **Ignum**

Obrázek 26 - Obrázek 26 - IGNUM – Umístění odkazu 1



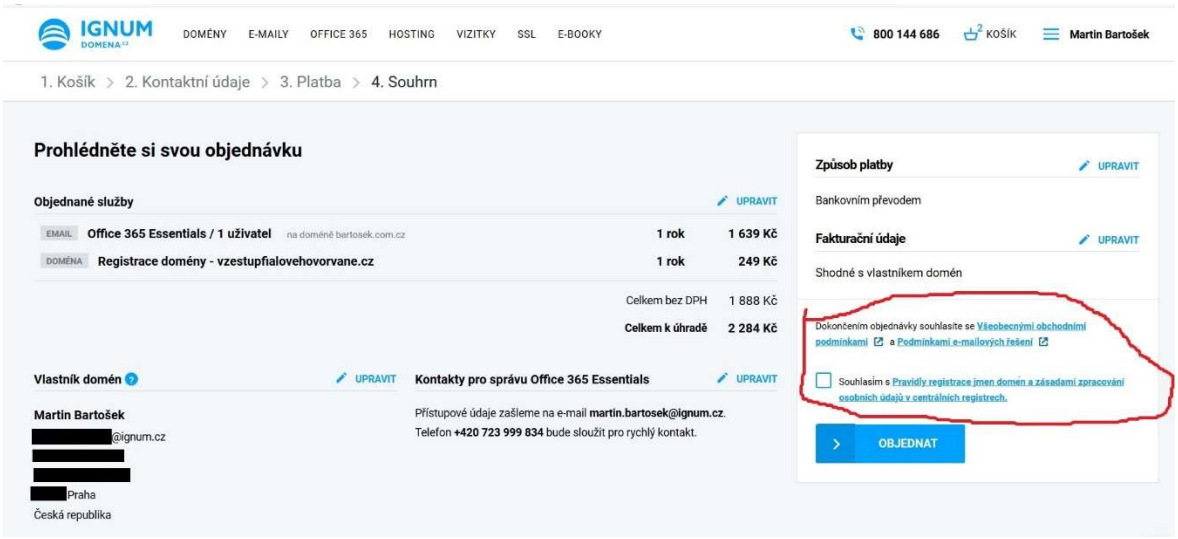
Zdroj: (Ignum s.r.o., 2020)

Obrázek 27 - IGNUM – umístění odkazu 2



Zdroj: (Ignum s.r.o., 2020)

Obrázek 28 - IGNUM – souhlas s podmínkami



Zdroj: (Ignum s.r.o., 2020)