FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Analýza dopadů GDPR v oblasti webových služeb
Student:	Michal Šanda
Vedoucí:	Ing. David Buchtela, Ph.D.
Studijní program:	Informatika
Studijní obor:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2018/19

Pokyny pro vypracování

Cílem práce je analýza dopadů GDPR na webové služby, které monetizují návštěvnost webových stránek skrze reklamní systémy.

1. Vypracujte stručnou rešerši o zákonech ovliňujících zacházení s osobními údaji
2. Seznamte se s GDPR a analyzujte důležité části pro webové služby
3. Analyzujte dopady GDPR v závislosti na obchodních aktivitách, zejména v oblasti webových služeb a zjištěné poznatky případně zakreslete s využitím vhodných diagramů
   a) srovnání druhů zpracovávaných dat a jejich využití (před a po zavedení GDPR)
   b) spojování dat z různých zdrojů včetně veřejných
4. Analyzujte dopady GDPR webové služby využívající monetizaci reklamního prostoru na používané reklamní systémy a technologie v ČR
5. Pro praktickou část analyzujte procesy v projektu ElateMe
   a) určete problémová místa
   b) navrhněte změny vzhledem k nové legislativě
   c) vypracujte nutné dokumenty pro regulátora (ÚOOÚ)
   d) spočítejte náklady, které je nutné vynaložit v rámci tohoto projektu a GDPR

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 3. ledna 2018

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Analýza dopadů GDPR v oblasti webových služeb

Michal Šanda

Katedra softwarového inženýrství

Vedoucí práce: Ing. David Buchtela, Ph.D.

13. května 2018

Poděkování

Chtěl bych poděkovat Ing. Davidu Buchtelovi, Ph.D. za vedení této práce a nápomocné rady, kdykoliv to bylo třeba. Dále bych chtěl poděkovat Bc. Michalovi Maněnovi a Matěji Macháčkovi, za možnost podílet se na vývoji aplikace ElateMe. Další poděkování patří Vlastimilu Vybíhalovi za poskytnuté materiály. Nakonec bych chtěl poděkovat své rodině za morální podporu po celou dobu studia a především mé mamince za opravy gramatických chyb.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 13. května 2018 .....

České vysoké učení technické v Praze

Fakulta informačních technologií

Odkaz na tuto práci

Šanda, Michal. *Analýza dopadů GDPR v oblasti webových služeb.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

Tato práce se zabývá příchodem Obecného nařízení o ochraně osobních údajů (dále jen GDPR) a změnám o proti zákonu o ochraně osobních údajů č. 101/2000 Sb. Práce analyzuje povinnosti vzhledem k současnému zákonu a poukazuje na nové změny a dopady na webové služby a jejich monetizaci. Praktická část pak analyzuje procesy v projektu ElateMe a navrhuje jejich změny vzhledem GDPR, dále se zabývá nutnými dokumenty a finančními náklady. Teoretická část pak může sloužit jako souhrn podstatných částí nařízení pro další webové aplikace.

Klíčová slova GDPR, Obecné nařízení o ochraně osobních údajů, osobní údaje, webové služby, dopady GDPR, monetizace

Abstract

This thesis is about General Data Protection Regulation (GDPR) and its changes compared to privacy law no. 101/2000 Sb. It analyzes obligations with respect to the current law and highlights new changes and impacts to web applications and its monetization. The practical part analyzes processes in ElateMe project and suggests modifications in view of GDPR. It also deals with necessary documents and financial expenses. Theoretical part might serve as a summary of the directive's mandatory parts, that can be used in other web services.

Keywords GDPR, General Data Protection Regulation, Privacy policy, web services, impact of GDPR, monetization

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Kolem problematiky GDPR se v současnosti vyskytuje řada informací, některé jsou správné, jiné naopak zavádějící či až nepravdivé. Nařízení jako takové je velice rozsáhlé a snaží se pokrýt a sjednotit většinu případů zpracování osobních údajů. Tato práce by se měla pokusit udělat jasno v oblasti webových aplikací využívající monetizaci, která je pro řadu vydavatelů nejlepší způsob, jak přijít k nějakému zisku. Cílem práce je poukázat na stav před příchodem GDPR – tedy zejména zákon o ochraně osobních údajů (č. 101/2000 Sb.) – dále je porovnat s novými skutečnostmi s příchodem obecného nařízení a udělat tak situaci jasnější, v praktické části pak navrhnout změny vzhledem k GDPR v projektu ElateMe.

Novými skutečnostmi by především měli být příchod pověřence pro ochranu osobních údajů, pohledu na profilaci, cookies a nutná dokumentace. Dále bych se v práci rád zaměřil na to, co je obecné nařízení a co už je směrnice ePrivacy, tyto dvě věci jsou často nesprávně zaměňovány.

Praktická část, jak již bylo popsáno výše, se zabývá navržení změn vzhledem k GDPR na projekt ElateMe, analýzou kritických míst a nutných dokumentů pro ÚOOÚ tak, aby vše bylo v souladu s novou legislativou.

Část I

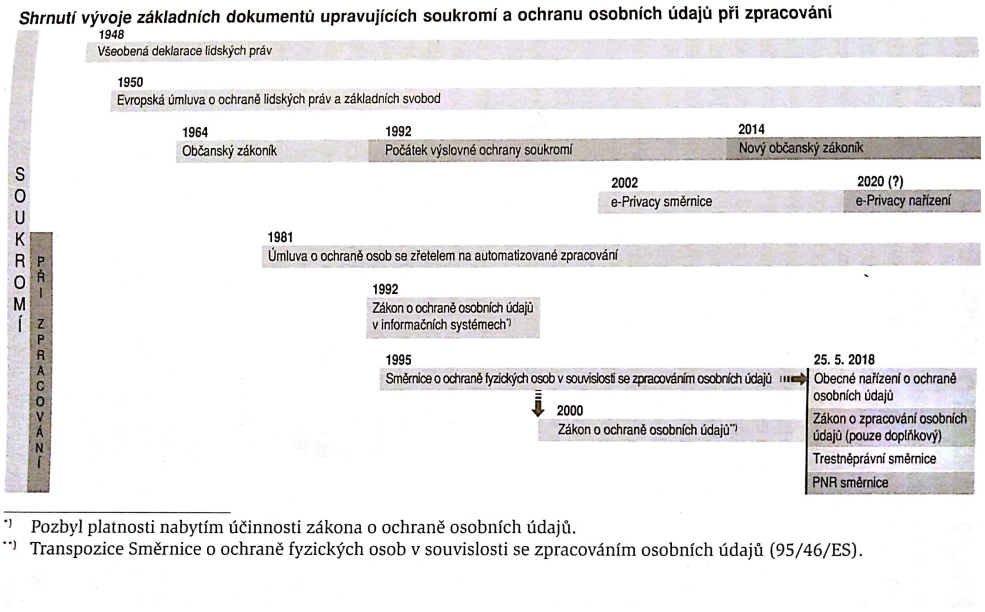
Teoretická část

Kapitola 2

Současné zákony upravující ochranu osobních údajů

Zákon, který by v České republice upravoval nakládání s osobními daty má u nás relativně krátkou historii, která začíná teprve v roce 2000. Jedná se o v současné době platící a v české legislativě vymahatelný zákon o ochraně osobních údajů č.101/2000 Sb., čerpáno z [1]. Dohled nad jeho dodržováním pak přebírá Úřad pro ochranu osobních údajů (dále jen ÚOOÚ), ke kterému má správce tzv. oznamovací povinnost (§16) až na výjimky, které může určit zvláštní zákon. Ta spočívá v předání ÚOOÚ následujících údajů: identifikační údaje správce, účely za kterým jsou data zpracována, příjemci a doba po kterou jsou osoby zpracovány.

Tento zákon čeká novelizace, protože od konce května 2018 vstupuje v platnost Obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů známý především pod zkratkou jako GDPR. Vývoj zákonů, které se týkají osobních údajů nejlépe ilustruje obrázek 2.1 na straně 6.



Obrázek 2.1: Vývoj zákonů platných v ČR upravující nakládání s osobními údaji, převzato z[1]

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

Tímto zákonem se zavádí základní pojmy **správce** a **zpracovatel** (§4 odst. j a k). Správce je z pohledu zákona každý, kdo určuje co se s osobními údaji bude dít, tyto povinnosti však může dále delegovat na zpracovatele. Tím může být např. externí firma (outsourcing).

Naopak „***Příjemcem*** *je každý jemuž jsou osobní údaje zveřejněny*“ (§4 odst. o), příkladem může být člověk, kterému je sdělíme. Klíčové pro webové služby je shromažďování resp. zpracování dat o jejich uživatelích a to především ze dvou důvodů. První důvod je, že zpracování údajů je nezbytné pro funkčnost aplikace jako takové – s tím se setkáváme například u internetových obchodů, kdy bez údajů nelze vyfakturovat zboží. Dalším a v současnosti velice lukrativním důvodem je (především behaviorální) reklama.

Dále v textu bude zákon o ochraně osobních údajů č. 101/2000 Sb. označován zkratkou **ZOÚ**.

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

2.2 Pozice ÚOOÚ

Pozice ÚOOÚ je nezávislá a má vlastní část rozpočtu – řídí se pouze platnými zákony a je to také jediná cesta, jak provést případné změny. Jeho funkce je dále dozorová, konzultační a samozřejmě řešení sporů.

2.3 Jaká data jsou považována za osobní údaje?

Podle výše zmíněného ZOÚ §4 české legislativy jsou za osobní údaje považovány infromace (nebo jejich kombinace) určeného nebo určitelného subjektu údajů – například jméno a příjmení spolu s datem narození, data tedy mohou mít různou podobu. Záleží tedy zda subjekt lze identifikovat přímo či nepřímo. Obecně lze rozdělit osobní údaje takto[3]:

- identifikační – jméno a příjmení, rodné číslo, ...,
- popisné – číslo bankovního účtu, ...,
- citlivé – náboženské vyznání, ...
- a další, ...

Podobně v současné době nahlíží zákon 101/2000 Sb. i na identifikátory jako je IP či MAC adresa, tyto údaje slouží k identifikaci síťového prvku a záleží tedy na kontextu v kterém tato data máme uložena [4].

IP adresa je problematická tím, že v dnešní době, kdy řada internetových poskytovatelů používá technologii NAT, z čehož vyplývá, že za jednou IP adresou se může skrývat více koncových uživatelů. Podobné to je i s MAC adresou, kterou většina zdatnějších uživatelů zvládne změnit. Přístup k IP adrese se mění s příchodem GDPR, kterému se budeme věnovat později v kapitole 3.3 na straně 20 a dále pak v nařízení známé jako ePrivacy.

2.4 Nahodilost sběru osobních údajů

Nahodilý sběr osobních údajů lze ukázat na příkladu, který řada z nás potkává – například v autě v případě, že používáme kameru. Ta zaznamenává průběh jízdy a záznam nám tak může posloužit jako důkazní materiál. **Zákon 101/2000 Sb. na tuto situaci myslí a nevztahuje se na ní, ale pouze v případě nejsou-li osobní údaje dále zpracovávány** (§3 odst.4), v případě nehody tento záznam lze použít pro pojišťovnu nebo jako důkazní materiál.

2.5 Citlivé údaje

Některé osobní údaje mají zvláštní povahu a v zákonu č. 101/2000 Sb. je najdeme pod pojmem citlivé údaje. Často se jedná o údaje, které by mohly subjekt diskriminovat. Namátkou se jedná o data týkající se národnosti nebo náboženského přesvědčení, odsouzení za trestné činy, zdravotního stavu nebo biometrických údajů, díky kterým lze subjekt jednoznačně identifikovat (§4 odst. b). Jedná se tedy skutečně o údaje, které v častých případech nechceme nikomu sdělovat.

Zpracovávat takováto data můžeme jen za podmínek, že nám subjekt dal výslovný souhlas – v případě sociální sítě například aktivním zaškrtnutím. Tento souhlas musíme být schopni doložit po celou dobu zpracování těchto dat. Toto lze v případě webových služeb nejjednodušeji a nejčastěji vyřešit zapsáním příslušné informace do databázového systému. Dále je v tomto případě nutné, aby subjekt byl informován o tom, za jakým účelem souhlas dává (§9 odst. a).

Samozřejmostí by pak pro správce i zpracovatele mělo být dodržování bezpečnostních interních směrnic tak, aby subjekt, který zpracování odsouhlasil neutrpěl žádnou újmu na své osobnosti (§10) – například omezením počtu přístupů k produkční databázi atp.

2.6 Povinnosti při zpracování osobních údajů

Podle §13 ZOÚ je povinen správce (a případně zpracovatel) přijmout taková opatření, aby nemohlo dojít k náhodnému či neoprávněnému přístupu a jinému zneužití osobních dat. Zároveň jsou povinni dokumentovat opatření vedoucí k zajištění ochrany. Pokud se jedná o automatizované zpracování dat je nutné zajistit aby se systémem, který data zpracovává, pracovala jen oprávněná osoba – to lze zajistit rozdělením práv a povinností jak v rámci organizace, tak v rámci systému (ať už se jedná o celý operační sytém nebo databázi, . . .). Zároveň zákon ukládá vést záznamy, které umožní ověřit kdy a kdo s osobními daty pracoval. V IT praxi se tedy bude jednat nejčastěji o logování přístupů a modifikací. Samozřejmost, která by měla být každému vlastní, je zachování mlčenlivosti a to i po skončení zaměstnání.

2.6.1 Zásady pro zacházení s osobními údaji

Povinnosti pro zpracování osobních údajů podle ZOÚ lze shrnout do následujících bodů:

1. musí být stanoven účel za kterým chceme informace zpracovávat,

2. informace musí být přesné,

3. informace smějí být uchovány jen po dobu nezbytnou pro jejich zpracování,

4. nesdružovat osobní informace, které byly získány rozdílným způsobem.

Subjekt údajů má právo vznést žádost o informaci o zpracování osobních údajů. Správce je povinen se řídit §12 ZOÚ a tyto informace předat. Obsahem je pak **proč – účel zpracování, co – samotná data a případně povaha v souvislosti s využitím pro rozhodování**.

Dále je správce (resp. zpracovatel) povinen data odstranit, jakmile pomine účel, pro které byla zpracována (§5).

2.6.2 Zpracování bez souhlasu subjektu

Zpracovávat osobní údaje v případě webových služeb můžeme bez souhlasu, je-li splněn podle ZOÚ §5 odst. 2 některý z těchto odstavců zákona:

(a) *Vyplývá to pro nás z jiné právní povinnosti*

(b) *Je to nezbytné pro plnění smlouvy*

(c) *Je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů*

(d) *Jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním předpisem*

(e) *Pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce*

(f) *Pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti*

(g) *Jedná-li se o zpracování výlučně pro účely archivnictví*

V případech, které nejsou uvedeny výše, je nutný souhlas. Možnosti, kdy si lze takto počínat jsou tedy i v současném zákoně jasně dané a otázkou je spíše dodržování tohoto zákona.

2.6.3 Předávání osobních údajů dalším správcům

Z pohledu webových služeb a reklamy na internetu nás bude zajímat především §5 odstavec 6. Tento odstavec právně upravuje situaci, kdy chceme osobní údaje předat jinému správci. Tato situace například nastává tehdy, pokud sbíráme data o uživatelích za účelem cílené reklamy, nebo pokud máme například

dceřinou společnost. Vzhledem k tomu, že Česká republika je členským státem Evropské unie (dále jen EU), platí volný pohyb pro předávání informací na jejím území (ZOÚ §27 odst. 1). Podobně tomu je tak u zemí, které přijali Úmluvu č. 108 [5].

Do zemí, které nejsou členy EU a nepřijali onu výše zmíněnou úmluvu, lze osobní údaje předat jen za předpokladu, že to nezakazuje zákon platný v ČR nebo zákon (případně rozhodnutí) jemu nadřazený (viz obrázek 3.1 na straně 16). K takovému zpracování je pak třeba souhlas subjektu, ÚOOÚ a prokázání, že v dané zemi existují záruky, které stále při nejmenším podobně chrání subjekt údajů (ZOÚ §27 osdt. 3). Chceme-li předat osobní údaje jinému správci musíme splnit tyto podmínky (ZOÚ §5 odst. 6):

(a) *Údaje subjektu byly získány v souvislosti s činností správce nebo se jedná o zveřejněné osobní údaje*

(b) *Údaje budou využívány pouze za účelem nabízení obchodu a služeb*

(c) *Subjekt byl o této skutečnosti informován správcem a nevyslovil nesouhlas*

Správce, který takto osobní údaje obdrží je již dále předat nesmí (§5 odst. 7). Pokud uživatel (resp. subjekt osobních údajů) s předáním osobních údajů a dalším zpracováním nesouhlasí, musí nesouhlas udělit písemně. V případě, že byly předány údaje jako je jméno,příjmení a adresa je správce povinen informovat o vyslovení nesouhlasu ostatní správce, kterým tyto údaje sdělil (ZOÚ §5 odst. 8). Sám tyto údaje však dále zpracovávat může a to právě za účelem vyřazení (ZOÚ §5 odst. 9). Podobný, ale rozšířený princip bude požadovat i GDPR.

Příkladem může být internetový obchod s náhradními díly pro automobily – máme nasbíraná data o uživatelích, kteří náš obchod používají – víme tedy například věk, kolik v průměru utratí a co nakupují. Tato data jsou cenná, jednak pro nás z pohledu predikce dalšího chování uživatele, ale stejně tak cenná jsou v oblasti reklamy, kdy si můžeme představit například automobilku, která chce zacílit svou reklamu na specifického uživatele, který je nějak starý a víme kolik utrácí (je tak větší šance, že si u nás něco koupí) více viz kapitola 4 na straně 37.

2.7 Zákon o elektronických komunikacích č. 127/2005 Sb.

Z pohledu webových služeb je důležitý §89 tohoto zákona, který pojednává o důvěrnosti komunikací. Zároveň je tato část důvodem toho, proč nyní vídáme

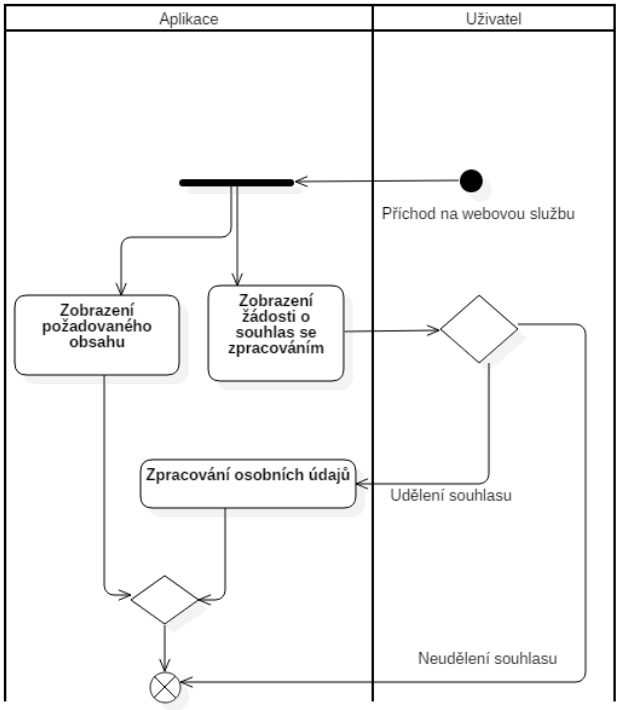
skoro na každém webu lištičku s oznámením o tom, že web, který jsme navštívili používá soubory cookies. Zároveň přesně tato část implementuje částečně směrnici ePrivacy (viz kapitola 3.1 na straně 15) a její pohled právě na problematiku cookies. Odstavec 3 tohoto zákona zní „*Každý, kdo hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu* ***k údajům uloženým v koncových zařízeních*** *účastníků nebo uživatelů, je povinen tyto účastníky nebo uživatele předem prokazatelně* ***informovat o rozsahu a účelu*** *jejich zpracování a je povinen nabídnout jim* ***možnost*** *takové zpracování* ***odmítnout****, . . .* “. Rozdíl oproti ePrivacy je tedy takový, že směrnice nařizuje režim **opt-in** (viz obrázek 2.3 na straně 12) – tedy dobrovolné povolení ještě před začátkem, ale náš zákon povoluje **opt-out** – což je samozřejmě opak předchozího, kdy uživatel ve výchozím stavu souhlasí, ale má možnost odmítnout. Příklad takového informování ukazuje obrázek 2.2 na straně 11.

Obrázek 2.2: Cookies na službách Economia a.s., zdroj[2]

2.8 Pokuty

Hranice pokut v současném zákoně se pohybuje v případě fyzických osob od 100 000 – 5 000 000 Kč v závislosti na tom, o jaké provinění se jedná a také na jeho rozsahu. Do výše 100 000 Kč lze udělit pokutu v případě porušení

[2] Economia. *Cookies na službách Economia a.s.* 2018. Dostupné také z: `http://napoveda.centrum.cz/index.php?/Knowledgebase/Article/View/145/7/cookies-na-sluzbach-economia-as`.



Obrázek 2.3: Vysvětlení principu opt-in

mlčenlivosti, do 1 000 000 Kč pak za přestupky jako je shromažďování více dat než kolik potřebuje k udanému účelu či jiné porušení povinností, a nejvyšší sazbu lze udělit v případě, že se jedná o velký rozsah nebo citlivá data (ZOÚ §44).

V případě právnických osob a podnikatelů se hranice pokut pohybují od 5 000 000 do 10 000 000 Kč a jedná se o stejný princip jako v případě osob fyzických, tedy nižší sazba v případě banálnějšího porušení povinností a ta nejvyšší v případě velkého rozsahu či citlivých údajů (ZOÚ §45).

Speciální případy jsou pak takové, kdy se jedná o porušení zákazu zveřejnění jiným právním předpisem – ať už jde o fyzické nebo právnické osoby, lze uložit pokutu až do výše 1 000 000 Kč, v případě, že ten, kdo se provinil použil tisk, film, nebo např. počítačovou síť je možné udělit pokutu až 5 000 000 Kč (ZOÚ §44a a §45a).

2.9 Shrnutí

Shrnutí lze rozdělit do dvou částí. První jsou povinnosti provozovatele webové aplikace, a to zejména informování subjektů o zpracování osobních údajů, jeho důvodu, doložení jejich souhlasů a zajištění řádné bezpečnosti (zejména pokud se jedná i o údaje citlivé). Dále pak informovat o tom, že má uživatel právo vyslovit nesouhlas s jejich zpracováním. Tyto informace se nejčastěji vyskytují ve všeobecných obchodních podmínkách(§1827 odst. 2 NOZ), ke kterým musí mít uživatel přístup a ideálně by je poskytovatel aplikace měl nabízet ke stažení například v PDF formátu – toto, však vzhledem k GDPR již nebude stačit [7] a souhlas bude muset být oddělený, nařízení se tak snaží předejít situacím, kdy se jedná o tzv. „wall of text“, tedy mnoho textu, který v důsledku uživatelé nečtou a ihned ho odsouhlasí.

Praktický dopad na uživatele je tedy takový, že právě nejčastěji v obchodních podmínkách narazí na příslušnou kategorii s výše popsanými informacemi a souhlas udělí, například zaškrtnutím check-boxu u kterého je popisek, že uživatel souhlasí s obchodními podmínkami, případně je zde další, který povoluje zpracování osobních údajů. Tato informace se pak uloží například do databáze provozovatele, aby splnil dle zákona povinnost doložení souhlasu o zpracování osobních údajů.

Kapitola 3

Obecné nařízení o ochraně osobních údajů – GDPR

Toto nařízení bude v České republice a celé Evropské unii platně vymahatelné od 25.5.2018. GDPR tak nahradí a především sjednotí zákony o ochraně osobních údajů všech členských zemí. Je dobré si uvědomit, že některé země (např. Německo) již podobné zákony mají a přechod by tedy neměl být až tak bolestivý, jak ho občas prezentují média – Kateřina Hrubešová (SPIR) pro Tiscali Media, konáno 13.11.2017, Václavské nám. 793/36, Praha 1. Znění GDPR lze nalézt v [1], ze kterého jsem čerpal.

3.1 GDPR a jeho pozice v české legislativě

Pozici GDPR v české legislativě můžeme odvodit z obrázku 3.1 na straně 16. Evropské právo je tedy nad našimi zákony a tak jsme jako členský stát povinni dodržovat vymahatelnost. Stejně jako v případě zákona č. 101/2000Sb. bude ÚOOÚ plnit funkci kontroly, dozorového, konzultačního úřadu a informačního kanálu – i v současnosti můžeme nalézt většinu podstatných informací a jejich výklad přímo na webu `www.uoou.cz` a v případě nutnosti požádat o konzultaci.

Jako první je vhodné představit si zmiňované právní akty EU. Samotnému GDPR předcházela směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, podobně tomu je u ePrivacy v první „vlně“ přichází jako **směrnice**, což pro každou členskou zemi znamená, že do určité doby musí dosáhnout nějaké implementace – nicméně je na každém státě jakou cestu si zvolí. Dalším důležitým pojmem je **nařízení**, která jsou **právně závazná** a platná ihned jakmile začne jejich platnost. Dalším faktem je, že nařízení platí plošně v celé EU, tudíž má funkci i sjednocující [8]. Řada nařízení včetně Obecného nařízení o ochraně osobních údajů umožňuje jednotlivým státům

s některými „požadavky“ hýbat v rámci mezí nařízení a zároveň platných zákonů v dané zemi – v řadě případů tedy bude třeba novelizace stávajících zákonů.

3.1.1 Pracovní skupina WP29

Novinkou s příchodem GDPR je pracovní skupina (po vstupu nařízení v platnost se bude jednat o sbor) WP29, která vydává vodítka upřesňující výklad nařízení. Skupina se skládá ze zástupců odpovědných úřadů jednotlivých zemí, Evropských komisařů a Evropské komise [2]. Lze si představit, že se prakticky jedná o úřad nad úřady a zároveň evropskou verzi našeho ÚOOÚ.

Obrázek 3.1: Hiearchie práva v ČR, zdroj[3]

Důležitým faktem je, že vodítka jako taková slouží jako „možnost výkladu“. Často jsou zde příklady z praxe, ale stále se nejedná o zákon a při využívání je třeba být opatrný.

3.1.2 ÚOOÚ a příchod GDPR

ÚOOÚ bude mít opět funkci dozorového úřadu, který bude dohlížet na dodržování obecného nařízení, stejně jako v případě zákona o ochraně osobních údajů bude plnit i funkci osvěty a prevence či konzultací pro správce (funkce tedy zůstává stejná). Samozřejmostí je pak prošetřování stížností [2].

[3]Kučera, Zdeněk. *Prezentace k přednášce na FIT ČVUT - Úvod do předmětu, právo a IT* [online] [cit. 2018-03-25]. Dostupné z: `https://edux.fit.cvut.cz/courses/BI-PAI/_media/lectures/1-2017.ppt`.

Vzhledem k sjednocujícímu principu GDPR se zavádí tzv. **mechanismus jednotnosti**. Ten zabraňuje odlišnému výkladu obecného nařízení v odlišných zemích resp. jejich dozorových úřadech (recitál 135,136 a kapitola 7 nařízení) a tedy v případě sporného výkladu nebo v případě nutnosti vzhledem k nadnárodnímu rozsahu rozhodne sbor. Tak se zajistí, že rozhodnutí bude nejlepší možné vzhledem ke všem členům (o sboru resp. pracovní skupině viz předchozí kapitola 3.1.1).

Zásadní změna pro všechny správce, kteří zpracovávají osobní údaje nadchází v **konci ohlašovací povinnosti** ÚOOÚ. S principem GDPR však přichází na správce větší zodpovědnost, protože budou muset sami doložit a tedy zároveň dokumentovat, že s osobními údaji zacházejí v souladu s obecným nařízením [10]. Dalším důležitým faktem je, že **v případě úniku dat či narušení bezpečnosti** musí tuto skutečnost správce **nahlásit do 72 hodin** právě ÚOOÚ [11]. V případě, že únik dat může mít nějaké větší následky, správce je povinen tuto skutečnost oznámit i samotnému subjektu údajů (článek 33 a 34 nařízení).

3.2 GDPR vs. ePrivacy

Mnoho lidí zaměňuje nebo slučuje GDPR s nařízením o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích – zkráceně ePrivacy (– Kateřina Hrubešová (SPIR) pro Tiscali Media, konáno 13.11.2017, Václavské nám. 793/36, Praha 1). Jde však o dvě odlišné věci. Aktuální je především GDPR, nařízení ePrivacy by mělo vejít v platnost později. Od roku 2002 platilo ePrivacy jako směrnice a není zcela jasné, kdy začne platit jako nařízení (viz obrázek 2.1 na straně 6), stejného názoru je i ÚOOÚ [12].

GDPR na rozdíl od ePrivacy nahlíží na ochranu osobních údajů obecně, řeší jak případy uvnitř firem či organizací, tak ty, které se dotýkají osob z „venku“ – zákazníků, pacientů, apod. Směrnice resp. nařízení ePrivacy se, jak již název napovídá, specializuje na internet a komunikaci. Návrh nařízení je možné najít na serveru `http://eur-lex.europa.eu`, který zpřístupňuje zákony Evropské unie. Vzhledem k tomu, že není jasné kdy vejde v platnost, lze očekávat jistou toleranci od dozorových úřadů.

ePrivacy [13][14] upravuje nakládání s daty, zejména takovými jako jsou(čl. 4) metadata elektronické komunikace (odst. c), veřejně dostupné seznamy (d), elektronická pošta (e), přímý marketing (f). Dále ePrivacy říká, že **data elektronických komunikací** (tímto se rozumí jak obsah, tak metadata – viz článek 4 odst. 3) jsou důvěrná až na výjimky, kdy data může zpracovat poskytovatel elektronické komunikace, které toto nařízení povoluje (čl. 5 a 6).

Jedná se o případy, kdy je to nezbytné pro přenos komunikace nebo v případě, že se jedná o bezpečnost. Dále poskytovatel může zpracovat **metadata** (t.j. například údaje o poloze, či jiné údaje pro přenos viz článek 4 odst. 3c) pokud:

- je to nezbytné pro kvalitu služeb,
- je to nezbytné pro vyúčtování, odhalení zneužívání služby,
- **koncový uživatel k tomu dal souhlas** a účel nelze splnit anonymizováním informace.

Zpracovávat **obsah** za účelem poskytnutí konkrétní služby je možné, pokud dotčený uživatel nebo uživatelé dali souhlas. Poskytovatel po obdržení dat musí data buď smazat nebo anonymizovat. V případě informací důležitých například pro výše zmíněné vyučtování, mohou být příslušná data uchována do konce vyučtovacího období (čl. 7). Nemělo by tedy již docházet například k případům, kdy na základě obsahu zpráv mezi uživateli, se jim začne zobrazovat reklama na dané téma aniž by předtím byl udělen souhlas.

„*Využití funkcí koncového zařízení pro zpracování a uchování, jakož i shromaždování informací o software a hardware, jinými subjekty, než jsou dotčení koncoví uživatelé, se zakazuje, s výjimkou těchto důvodů*:“ (článek 8)

- je to nezbytné pro přenos komunikace,
- **koncový uživatel dal souhlas**,
- je to nezbytné pro poskytování služby informační společnosti požadované koncovým uživatelem,
- měření návštěvnosti internetových stránek – pokud měří poskytovatel informační služby.

Podobně pak pro shromažďování informací platí, že informace lze uchovávat, jen po dobu nutnou ke spojení nebo je zde oznámení o jejich shromažďování, které je jasně vidět. Souhlas se zpracováním může uživatel kdykoliv odvolat, jedná se o podobné principy, které používá i GDPR.

3.2.1 Pokuty za porušení ePrivacy

Pokuty lze rozdělit do tří skupin (článek 23): První skupina jsou pokuty, které mají možnost stanovit si členské státy – jedná se o případy týkající se volání a pro webové služby tedy ne úplně podstatné (porušení čl. 12, 13, 14).

Další kategorie je pro nás zajímavější a to porušení článků 8, 10, 15 a 16. Obsah prvního z článků je popsán výše na straně 18. Článek 10 hovoří o informovanosti o ochraně soukromí v internetu a musí nabízet možnost, která zabraňuje uchování informace v zařízení třetím stranám. Dokážeme si představit, že toto se týká především internetových prohlížečů a souborů cookie. Informace musí přijít již při instalaci a je vyžadován uživatelův souhlas s nastavením. Článek 15 se týká veřejných seznamů. Nakonec článek 16 pojednává o nevyžádaných sděleních (neboli spamu) a to jak písemném, tak prostřednictvím volání. Doslova říká, že přímý marketing lze uplatnit, pouze máme-li souhlas koncového uživatele s výjimkou toho, pokud je získáme při prodeji produktu. V tomto případě lze potenciálního zákazníka oslovit, avšak musí být jednoduchá možnost tyto sdělení zrušit a tuto možnost musíme připomínat s každým sdělením. Samozřejmostí pak je, že sdělení musí být jasně označena, že jde o marketing.

„*V těchto případech je* ***horní hranice pokuty až 10 000 000 EUR*** *nebo až* ***2% z celkového ročního obratu celosvětově za předchozí finanční rok*** *v případě jedná-li se o podnik. Horní hranice bude ta z částek, která bude vyšší.*“ (článek 23 odst. 2).

Třetí a poslední kategorie pokut je ta nejvyšší – jedná se o „*. . .* ***až 20 000 000 EUR nebo 4% z celkového ročního obratu v případě podniku****, podle toho, která z hodnot bude vyšší*“ (článek 23 odst. 5). Jedná se o porušení článků 5, 6, 7 a 18. Článek 5 zakazuje zasahování do elektronické komunikace – např. odposlechy, monitorování. Článek 6 pak nařizuje zpracování dat jen pokud je to nezbytné pro například kvalitu služeb nebo bezpečnost, nebo za předpokladu, že koncový uživatel souhlasil se zpracováním. Článek 7 viz výše v kapitole 3.2 strana 18. A nakonec porušení článku 18 – porušení nařízení dozorového úřadu.

Pokuty jsou tedy vyšší než na které jsme v České republice zvyklí, ale vzhledem k tomu, že se bude jednat o nařízení pro všechny členské státy, lze částky považovat za adekvátní.

3.2.2 Shrnutí

ePrivacy tedy upravuje nakládání s daty elektronické komunikace. Nejzásadnější jsou z pohledu webových aplikací odstavce, které se týkají povinností na software – snadno si lze transponovat, že se bude jednat například o internetové prohlížeče a nastavení toho, jaké soubory cookie mají akceptovat. Princip je opět podobný jako u GDPR – nepoužívat nadbytečné informace, informace zpracovávat jen po dobu, po kterou je skutečně potřebujeme a nepoužívat koncová zařízení uživatele, aniž by o tom věděl. Další zásadní změny jsou v principu opt-in používání koncového zařízení – opět se bude týkat především

souborů cookie, spolu s tím jsou samozřejmě důležité lhůty pro uchovávání dat. V současné době upravuje práci s cookie zákon o elektronických komunikacích, který však ePrivacy v tomto případě nereflektuje a povoluje přístup opt-out [15] viz 2.7 na straně 10. V případě reklamních systémů tedy budou nejspíše značné komplikace a bude záležet na finálním znění.

3.3 Co jsou osobní údaje s příchodem GDPR?

Řada článků a informací ohledně GDPR na první pohled vypadá, že se snaží vyvolat revolučnost tohoto nařízení. Pokud si však přečteme definici osobního údaje: „*Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor)...*“ v GDPR (čl. 4 odst 1) a v zákonu 101/2000Sb. zjistíme, že definice osobního údaje se vlastně nijak nerozšířila, tohoto názoru je i ÚOOÚ, viz web úřadu [16].

To, zda jde o osobní údaj, nezáleží na tom, zda subjekt identifikovat ihned (přímo), nebo je k tomu potřeba zpracování vícero subjektů (nepřímo). Důležitý je fakt, že subjekt údajů vůbec lze takto identifikovat [15]. Tento výklad se v dostupné literatuře opakuje v různých příkladech.

Zajímavá informace pro webové prostředí je, že recitál GDPR uvádí rovnou jako příklad identifikátorů fyzických osob **lokační** a především **síťové identifikátory**. Jedná se o recitál č.30, který zmiňuje adresy internetoveho protokolu, soubory cookies, či RFID a doslova říká, že „*... tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají použity k profilování fyzických osob a k jejich identifikaci*“. Recitál tedy do jisté míry dělá jasno o jaká data resp. jaké formy jde a které kategorie dat budou problémové. Dále je to jistý náznak toho, že profilování a s ním spojená behaviorální reklama bude problémem.

V tomto kontextu se velice často objevuje v dostupných zdrojích [15][17] rozsudek, který označil dynamickou IP adresu za osobní údaj. Podle mého názoru se na tuto skutečnost dá nahlížet dvěma způsoby. První je z pohledu uživatele, kdy skutečně dochází k ochraně jeho soukromí v případě, že by adresu někdo ukládal. Druhý pohled je pak z pohledu technického, kde se naskytují otázky, co všechno by museli případně jednotliví prostředníci udělat, aby šlo daného uživatele skutečně vystopovat. Nicméně z uvedené skutečnosti výše na tom nezáleží, podstatné je, že existuje způsob jak koncového uživatele identifikovat. O tom, zda je to správně či není, by se dalo polemizovat.

3.3.1 Citlivé osobní údaje s příchodem GDPR

GDPR kategorii citlivých údajů vyloženě nemá, nicméně se jedná spíše o přejmenování na „zvláštní kategorie dat“. U této kategorie dat, stejně jako obecně u definice osobních údajů, se toho velice nezměnilo. Změny lze nejlépe ukázat tabulkou 3.1 na straně 21, kterou jsem vytvořil z dostupné literatury [2]. Pohled na informace o sexuálním životě zůstává stejný a jedná se samozřejmě o citlivá data. Změna v tomto směru je v přidání sexuální orientace jako citlivého údaje resp. informaci patřící do zvláštní kategorie dat. Naopak národnostní původ nyní již do zvláštní kategorie spadat nebude. Biometrické údaje jsou v GDPR zvláštní kategorií osobních dat v případě „*. . . jsou-li zpracovávány za účelem jedinečné identifikace fyzické osoby*“[4] – oproti tomu zákon č. 101/2000 Sb. má definici pro biometrické údaje, že je to údaj, který umožňuje přímou identifikaci nebo autentizaci subjektů údajů (§4 odst. b). U trestních věcí a činů je to trochu složitější – do zvláštní kategorie nespadají, ale zpracování takových údajů vyžaduje dozor orgánu veřejné moci nebo k tomu musíme být oprávněni nějakou právní úpravou (kapitola 2 – článek 10)[2]. Tyto změny jsou zajímavé zejména z pohledu projektů, které mají profily uživatelů – např. seznamky, tam zcela jistě lze nalézt sexuální orientaci. Naopak v případě, kdy nějaká webová služba zpracovává informace o trestních věcech, bych očekával znalost legislativy ze strany provozovatele a tedy minimálního dopadu.

Tabulka 3.1: Srovnání pohledu na citlivé údaje

GDPR	**Zákon č. 101/2000 Sb.**
X	národnostní původ
sexuuální život	sexuální život
sexuální orientace	X
biometrické údaje *	biometrické údaje
trestní věci a činy **	odsouzení za trestný čin

3.4 Zpracování osobních údajů a profilace

Předtím než se budu věnovat problematice profilování a zpracování osobních údajů je třeba podívat se na definice těchto pojmů – zpracování definuje v kapitole první článek 4 odstavec 2, profilaci se pak věnuje článek 4 odstavec 4.

Pojem zpracování o proti současnému zákonu o ochraně osobních údajů č. 101/2000 Sb. zůstává stejný. Novým pojmem se stává **profilování**. Profi-

[4] Žůrek, Jiří. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. Právo (ANAG)., 2017. ISBN 978-80-7554-097-3, str. 52.

lování znamená takové automatizované zpracování osobních údajů, po kterém můžeme subjekt nějakým způsobem ohodnotit. Často se jedná o uživatelovu interakci v rámci webové aplikace a její následné predikce do budoucna, čehož využívají reklamní systémy – lze tak například vyselektovat určité spektrum uživatelů, u kterých je pravděpodobné, že reklamě podlehnou. Dále se i v GDPR nachází pojmy správce a zpracovatel, kde správce určuje, co se bude s osobními údaji dělat a zpracovatel pak jen zpracování vykonává a tedy ani zde nejsou žádné změny významu [11].

3.4.1 Kdy lze data zpracovat?

Data lze zpracovávat, existuje-li alespoň jeden právní důvod – u webových aplikací se nejčastěji bude jednat o případy, které definuje článek 6 a následující odstavce:

a) *subjekt dal souhlas,*

b) *jde o zpracování, které je nezbytné pro splnění smlouvy,*

c) *jde o zpracování, které je nezbytné pro splnění právní povinnosti, která se vztahuje na správce,*

f) *jde o oprávněný zájem správce.*

Nejlepší vysvětlení odstavců bude ukázání na příkladech. Prvním příkladem je případ, kdy subjekt dává souhlas se zpracováním osobních údajů za účelem zasílání obchodních sdělení třetích stran; pod zpracováním nezbytné pro plnění smlouvy si představuji například uzavření bankovního účtu po internetu; právní povinnosti mohou představovat například povinnost ukládání daňových dokladů po dobu 10ti let. Poslední položku – oprávněný zájem – lze využít v případě, že zájmy správce převažují a zároveň neporušují práva subjektu údajů – například některé analytické nástroje při správném nastavení a nebo zaznamenávání IP adresy do logů v systému s cílem předejít kybernetickému útoku.

Smlouvy se kterými se na internetu můžeme setkat, mohou mít různé podoby. Jedná se o Click-wrap, Click-trough a Browse-wrap. Click-wrap smlouvy jsou tvořeny nejčastěji oknem, kde jsou dostupné smluvní podmínky a nejsou uzavřené, dokud uživatel neklikne na tlačítko nebo nezaškrtne požadované políčko. Click-trough smlouvami se proklikává uživatel několikrát, nejčastěji se s tímto případem setkáváme u internetových obchodů, kde nejdříve vidíme produkty, které jsme si dali do košíku, jejich počet, v dalším kroku pak vyplníme kontaktní či platební údaje, až dojdeme na rekapitulaci a dokončíme objednávku. Browse-wrap je pak smlouva, která je uzavřená už jen tím, že na

daný obsah uživatel kouká, musí zde ale být viditelné její podmínky. Viditelnost podmínek resp. špatná implementace je také jeden z největších problémů tohoto typu smluv [19].

3.4.2 Spojování dat

V definici zpracování GDPR a i v zákonu č. 101/2000 Sb. je zmíněno kombinování dat. Tedy v případě, že správce osobních údajů chce spojit údaje z různých zdrojů nasbíraných za rozdílným účelem bude potřebovat stejně jakémkoliv jiném zpracování právní základ, který mu to umožní – může se tedy jednat např. o souhlas subjektu nebo případně i o odůvodněný oprávněný zájem. Navíc článek 6 odst. 4 pojednává o zpracování pro jiný účel, než-li byl ten původní a je tedy nutné posoudit vazby mezi účely, okolnosti, povahu, důsledky a vhodné záruky. V případě veřejných zdrojů v situaci, kdy má data o nějakém subjektu a chce je spojit s veřejně dostupnými daty, bude postup stejný [20].

3.4.3 Zásady zpracování osobních údajů

Oproti zákonu o ochraně osobních údajů, který má část „Práva a povinnosti při zpracování osobních údajů“ má obecné nařízení článek 5 „Zásady zpracování osobních údajů“. Těchto zásad je celkem osm – **zákonnost, korektnost a transparentnost, účelové omezení, minimalizace údajů, přesnost, omezení uložení, integrita a důvěrnost** a nakonec **odpovědnost**. Tyto zásady lze víceméně nalézt i v zákonu o ochraně osobních údajů [2] a kapitola 2.6.1 na straně 8. Zákonnost spočívá v tom, aby existoval alespoň jeden právní důvod ke zpracování. Korektnost a transparentnost pak říká, že správce nesmí skrývat účel, rozsah a předávání osobních údajů. Dále musí být stanoveny přesně účely, za kterými daná data správce zpracovává. Minimalizace pro správce pak znamená, že by neměl ukládat více údajů, než je skutečně nezbytné. Zásada přesnosti je právo subjektu údajů na korektnost údajů a správce je tedy povinen při žádosti subjektu údaje aktualizovat nebo opravit. Dále by data neměla být uložena déle, než po nezbytně nutnou dobu pro jejich zpracování. Nakonec samozřejmě by všechna data, která spadají do osobních údajů měla být „*. . . zpracována způsobem, který zajistí náležité zabezpečení osobních údajů, . . . pomocí vhodných technických či organizačních opatření*“ – článek 5 odst 1 písmeno f. Považuji za nezbytné zmínit, že způsob zabezpečení by měl vždy zohledňovat o jaká data jde a jaký je jejich rozsah a objem – článek 32 obecného nařízení – v této oblasti vzniká velice často mezi správci a zpracovateli zbytečná panika. V případě, že nejde o zvláštní kategorie dat (citlivé údaje) lze usuzovat, že bude stačit běžně dostupné zabezpečení - např. spojení HTTPS, přístup na servery pomocí certifikátů a omezení počtu osob, které tento přístup mají, atp. Nakonec článek stanovuje správci odpovědnost a schopnost doložení dodržení faktů výše uvedených a

z toho tedy vyplývá vedení dokumentace a zdůvodnění proč jsou dané údaje potřeba.

3.4.4 Kdy může jít o oprávněný zájem?

Oprávněný zájem je jeden z termínů z GDPR, který v rámci možností dává šanci správcům a zpracovatelům nechtít pokaždé při zpracování osobních údajů souhlas subjektu údajů. I tento princip má ale pochopitelně svá pravidla. Recitál č. 47 říká, že předpoklad pro oprávněný zájem lze využít **pokud** „***. . . nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem***“, dále je přípustná možnost, kdy subjekt údajů je zákazníkem nebo jsou mu správcem nabízeny nějaké služby – ve všech případech by toto zpracování měl subjekt z kontextu očekávat. Tedy většina běžných úkonů – kdy uživatel může očekávat nějaké zpracování – by měla být stále bez souhlasu. Dále recitál výslovně uvádí, že **přímý marketing lze považovat za oprávněný zájem**, dále recitál č. 49 připouští oprávněný zájem v případech, kdy se jedná o bezpečnost komunikace či bezpečnost sítě. V případě, že jde o přímý marketing může subjekt údajů kdykoliv **vznést námitku** v celém rozsahu – a to ať už na počátku nebo v dalším zpracování, které se týká marketingu – musí na to být upozorněn a toto upozornění musí být zřetelné (recitál 70 a článek 21). Po vznesení námitky údaje již nadále nemůžou být zpracovávány.

3.4.5 Profilace uživatelů

Pro zjištění, jak obecné nařízení nahlíží na profilaci je opět dobré začít v recitálu samotného nařízení. Již v předchozí kapitole 3.3 na straně 20 je zmíněn recitál číslo 30, který síťové identifikátory a identifikátory cookies vidí jako možnost k profilování a v kombinaci s jedinečnými identifikátory mohou jednoznačně identifikovat konečný subjekt. Recitál 72 nám sděluje, že na profilování se vztahují pravidla tohoto nařízení a ponechává Evropskému sboru pro ochranu osobních údajů možnost vydávat pokyny v tomto směru (článek 70 pís. f). Vzhledem k zásadě transparentnosti musí být subjekt údajů informován o profilování, k čemu slouží a co se stane, pokud ho povolí nebo zakáže (recitál 60), dále pak kdo jsou příjemci oněch údajů a pokud je to možné, tak i přístup k nashromážděným informacím (recitál 63, článek 13 pís. f a článek 15 pís. h). Vzhledem k různým výkladům a problematičnosti se tomuto tématu věnuji v kapitole 3.5 na straně 25.

3.4.6 Předávání dat třetím stranám

Podobně jako u zákona o ochraně osobních údajů i v případě nařízení se jedná prakticky o 3 (resp. 4) druhy třetích stran – čemuž odpovídají i rizika (viz kapitola 3.7.1 na straně 33). První je předání údajů správci či zpracovateli

na území stejného státu (u nás ČR), následuje předání v rámci EU, předání mimo EU a s trochu jiným náhledem pak předání do USA. Ve všech případech musí mít správce (zpracovatel) právní důvod (viz článek 6 a 9).

V případě EU shledávám situaci stejnou jako v případě současného zákona o ochraně osobních údajů – jedná se tedy o volný pohyb. V případě, že se jedná o předání mimo EU, opět je situace obdobná jako u současného zákona – data lze předat v případě, že daná země je schválena Evropskou komisí (EK) a je schopna nějakým způsobem zajistit odpovídající ochranu. Obdobně to funguje v případě, že země na seznamu není – v tomto případě lze využít tzv. vhodných záruk, kdy lze využít například standardních smluvních doložek přijatých EK, případně doložkou mezi správci s povolením dozorového úřadu. V případě USA je využit „Privacy shield“ k jehož dodržování se společnost z USA přihlásí a pak lze data předávat [2].

3.4.7 Dopady a shrnutí

V oblasti definice osobních údajů, resp. dat jako takových, se toho moc nezměnilo, většina z požadovaných zásad je již nějakým způsobem obsažena ve stávajícím zákonu č. 101/2000 Sb. Totéž se týká pojmů jako je správce a zpracovatel. Novinkou je pojem profilace a problém síťových identifikátorů, včetně souborů cookies (zejména po případném vstupu směrnice ePrivacy v platnost). Tato část zákona je velice specifická a i přes dostupné komentáře se naskytuje řada otázek. Článek nařízení – Automatizované individuální rozhodování, včetně profilování – který o této problematice pojednává, je z mého pohledu napsán dosti obecně a jen stěží si pod ním lze představit něco konkrétního. Bohužel (z pohledu koncového uživatele možná bohudík) to spíše vyznívá v jeho prospěch a nejspíše v nejednom případě to bude znamenat fatální následky na poli webových služeb a především v internetové reklamě.

3.5 Automatizované individuální rozhodování, včetně profilování

Stejně jako tato kapitola se jmenuje i článek 22 v obecném nařízení. První odstavec říká, že „***Subjekt údajů má právo nebýt předmětem žádného zpracování včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká***“ – tento odstavec se nepoužije v případě, kdy je to nezbytné k uzavření smlouvy, v případě, že je to povolené právem nebo v případě máme-li výslovný souhlas od subjektu údajů. Dále stanovuje odstavec číslo 3 vhodná opatření na „ochranu práv a svobod“ a oprávněných zájmů.

Při čtení tohoto článku mi vyskočilo hned několik otázek, které by bylo vhodné z pohledu této práce zodpovědět, protože z pohledu informatiky si bohužel tento článek lze vyložit různě. Otázka, zda subjekt musí vznést námitku proti profilování, či je ve výchozím stavu zakázáno, komentuje literatura tak, že se jedná spíše o zákaz až na výjimky. V komentáři se dále dočteme, že by v průběhu roku 2017 měly být dostupné pokyny ze strany pracovní skupiny WP29 [15](o WP 29 viz kapitola 3.1.1 na straně 16). Na webu ÚOOÚ, je již příslušná kategorie, kde lze nalézt i přeložené doporučené postupy [21].

3.5.1 Výklad dle WP29

Přeložená vodítka k této problematice [22] začínají upřesněním definic, kde jedním z jednodušších výkladů profilace je, že je to každá činnost, která díky analýze nějakého chování zařadí uživatele do nějaké kategorie a to ať na základě chování v minulosti nebo predikce do budoucnosti. Jako příklad je zde uvedena problematika cílení produktů a služeb (tedy behaviorální reklama), zároveň je zde uvedeno, že záleží na okolnostech zda-li se jedná o automatizované rozhodování podle článku 22 odstavce 1.

Automatizované rozhodování dle pokynů WP29 se může částečně překrývat právě s profilováním – jak již vyplývá z výše uvedeného – jedná se o schopnost rozhodnout „***čistě technologickými prostředky, bez lidského zásahu***“.

Dokument uvažuje v profilování ve třech případech (kapitola I písmeno C):

- *obecné profilování*,
- *rozhodování založení na profilování* – případ kdy člověk rozhoduje na základě vypracovaného profilu,
- *výhradně automatizované rozhodování, včetně profilování* – případ, kdy člověk do procesu vůbec nezasahuje.

3.5.2 Zákaz profilování?

V kapitole II tohoto dokumentu se dočteme, že ve výchozím stavu platí zákaz automatizovaného rozhodování včetně profilování, nicméně poslední odstavec dodává, že zákaz se „*... uplatní pouze, pokud rozhodnutí založené výhradně na automatizovaném zpracováním včetně profilování, má na někoho právní účinek nebo obdobně významný dopad.*“. Kapitola II sekce A upozorňuje, že nelze uměle lidskou činnost dosadit do tohoto procesu – muselo by se jednat o nějakou smysluplnou činnost či rozhodnutí. Osobně mě více zajímá výklad sousloví „právní účinek nebo obdobně významný dopad“ – právě tomuto se věnuje sekce B druhé kapitoly.

3.5.3 Právní účinek a obdobně významný dopad

Jak již zmiňuji výše a je to poznamenáno i na začátku této sekce, **nařízení neobsahuje definici sousloví právního účinku a obdobného významu**, proto musíme hledat právě ve vodítkách WP29. Práce se věnuje především webovým službám a monetizaci, profilování se týká především cílené reklamy a tu zmiňuje právě tento dokument. Skupina WP29 je toho názoru, že ve většině případů se profilace významně jednotlivců nedotýká – výjimkou jsou případy **dotěrnosti, očekávání a přání dotčených osob, způsobu doručení reklamy nebo konkrétních zranitelných míst subjektu údajů**. Příkladem dává osobu, která má finanční problémy a zobrazuje se jí reklama na půjčky. Další příklad je v případě, že profilování stanoví odlišné ceny nějakého produktu nebo služeb a daný subjekt na něj pak nemůže dosáhnout. Tedy případ v praktické části, kdy se jedná o sbírky na přání, které vytvoří uživatel sám pro sebe a následně se mu bude podle interakcí zobrazovat reklama, by měl dle mého názoru podléhat souhlasu.

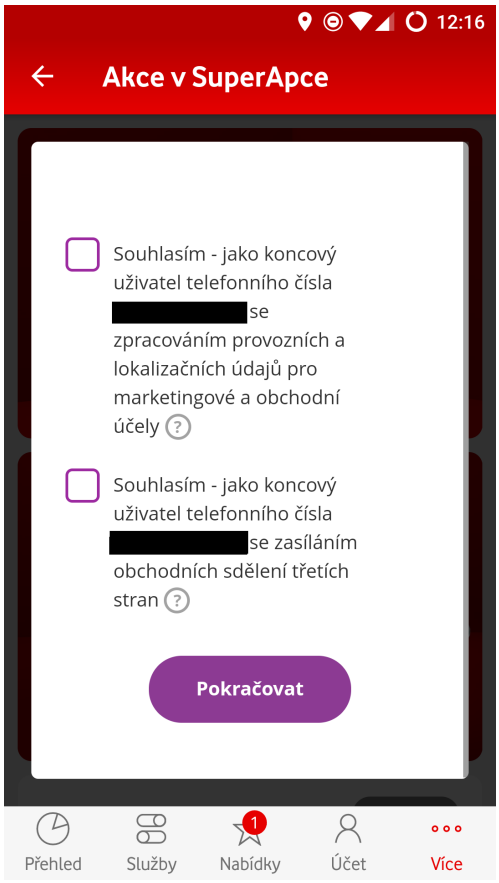
Dokument tedy přináší trochu světla do této problematiky, nicméně pouze z právního hlediska. Z pohledu implementace to vypadá, že bychom museli kontrolovat, kdo používá koncové zařízení nebo některá data úplně přestat využívat. Nastává otázka, zda tedy nevyžadovat souhlas v souvislosti s profilováním a reklamou vždy a být tak z pohledu nařízení kryti, i když to není nutně vždy vyžadováno.

Další specifickou skupinou (a to tedy nejen pro profilování) jsou děti (kapitola IV postupů od WP29). Výklad sice vyloženě nezakazuje profilaci, ale opět se dostává do podobného problému jako u dospělých – zmiňuje totiž příklad nezletilého hráče, na kterého cílí reklama s mikrotransakcemi a tak i on se stává „rizikovým“ – opět bychom v ideálním stavu měli nějak rozlišovat, kdo skutečně za koncovým zařízením sedí. Je to skutečně nezletilý hráč a nebo jen člověk, který hraje hry s mikrotransakcemi a nic zásadnějšího na internetu nevyhledává? Nebo bychom neměli používat cílenou reklamu na hráče vůbec? Behaviorální reklama sice stojí na statistických metodách, ale i tak má jisté odchylky.

3.5.4 Souhlas

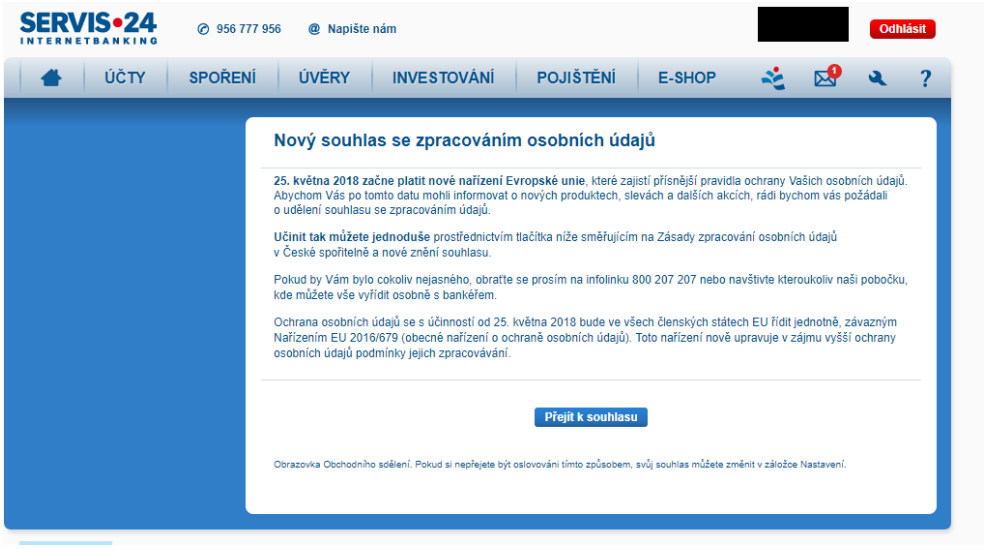
V odstavcích výše se vyskytuje možnost souhlasu – tento souhlas musí být udělen nějakou aktivitou – a musí být jasně zřetelné k čemu byl udělen a čeho se týká a jaký má na uživatele dopad v případě udělení či neudělení. Ostatně tak by to mělo být u každého souhlasu, který je vyžadován v důsledku tohoto obecného nařízení. Udělování souhlasů se v poslední době se již promítá do reality, jak například ukazují obrázky 3.2 na straně 28 a 3.3 na straně 29 z aplikace Můj Vodafone [23] a z internetového bankovnictví České spořitelny

[24], přičemž druhý ze zmíněných souhlasů je dle mého názoru diskutabilní – napadá mě totiž otázka zda-li po kliknutí na tlačítko dám skutečně souhlas a nebo mě skutečně jen přesměrují na nějaký další formulář (v textu se uvádí, že souhlas udělím kliknutím)? Nemělo by zde být tlačítko odmítnout místo vynucení klikání do horizontálního menu v případě, že souhlas dávat nechceme? Souhlas by měl být dobrovolný a ne vynucený, na druhou stranu z pohledu obchodních modelů je pochopitelné, že se správci budou snažit formulovat žádosti takovým způsobem, aby jim uživatel vyhověl (ale stále to musí být v mezích nařízení).



Obrázek 3.2: Vyžádání souhlasu v aplikaci Můj Vodafone, zdroj[5]

[5] Vodafone Czech Republic a.s. *Můj Vodafone* [online]. Verze 3.1 [cit. 2018-05-10]. Dostupné z: `https://play.google.com/store/apps/details?id=com.zentity.vodafone&hl=cs`.



Obrázek 3.3: Vyžadování souhlasu v aplikaci internetového bankovnictví České spořitelny, zdroj[6]

3.5.5 Dopady a shrnutí

Profilování by tedy ve výchozím stavu nemělo být přímo zakázané pokud jsme schopni zajistit, že nebude mít právní či obdobné následky pro subjekt profilace. V případě, že to zajistit nemůžeme, je profilace bez souhlasu zakázána. V oblasti webových služeb lze tedy očekávat mnoho žádostí o souhlas v podobných podobách, jako je tomu díky současnému zákonu o elektronických komunikacích(kapitola 2.7 na straně 10), obohacených o nezbytné informace. V případě, že souhlas nelze dát či vyžadovat lze očekávat necílenou reklamu nebo nerespektování GDPR (vysokým pokutám navzdory). Na tento fakt – čekání na první rozsudek nebo rozhodnutí ÚOOÚ – poukazuje i literatura [15], která nepřímo přiznává, že ačkoliv v ČR nemáme vyloženě precedentní systém, lze očekávat, že v těchto případech tomu tak bude.

3.6 Pověřenec pro ochranu údajů

Pověřenec pro ochranu údajů – často označován z anglického výrazu **Data Protection Officer jako DPO** je nově vytvořená pozice z obecného nařízení, pod touto zkratkou bude označen i dále v této práci. Kolem této nově vytvořené pozice se opět vytvořila značná bublina, že je pověřenec povinný pro všechny, kdo zpracovávají osobní údaje – tak to ale není.

[6] Česká spořitelna, a. s. *SERVIS 24* [online] [cit. 2018-05-10]. Dostupné z: `https://www.servis24.cz`.

3.6.1 Kdy je DPO povinný?

GDPR nařizuje jmenovat DPO ve třech případech zpracování (článek 37 odst. 1):

(a) „*Zpracování provádí orgán veřejné moci či veřejný subjekt*“

(b) „*Jedná se o* ***hlavní činnost v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů***“

(c) „*Hlavní činnosti správce (zpracovatele) spočívají v rozsáhlém zpracování dat spadajících do zvláštní kategorie (citlivé údaje) nebo trestních věcí a činů*“

Na to, aby se na správce vztahovala povinnost jmenovat DPO, je nutné, aby podmínky v odstavci b) **nastávaly společně** – a to tedy rozhodně nenastává v každém případě. Každý správce by se měl rozhodnout, uda do této kategorie spadá, pokud ne, tak by měl vypracovat písemnou analýzu, ze které by mělo vyplývat proč tomu tak je. Tato skutečnost zároveň odpovídá tomu, že GDPR nutí správce dokazovat, že jejich zpracovávání údajů je v souladu s nařízením. Pojem hlavní činnost si lze v prostředí webových aplikací ilustrovat na sociální síti. Rozsáhlé zpracování pak závisí na počtu záznamů, době po kterou data potřebuje ke zpracování, ale dle WP29 sem například spadá zpracování osobních údajů vyhledávačem pro potřeby behaviorální reklamy. Za pravidelné monitorování lze pak dle literatury označovat právě již několikrát zmíněné profilování [2].

3.6.2 Povinnosti DPO

Náplň práce DPO (článek 38 a 39), by měl mít patřičné znalosti z oblasti, které se zpracování týká. Ve společnosti má pak **nezávislou pozici a nemůže být za plnění svých úkolů sankcionován**. Jeho náplň práce je dokumentovat a dohlížet na zpracování osobních údajů, řešení sporů a celkově, co se týče osobních údajů být kontaktní osobou. Nakonec by bylo dobré zmínit, že **zodpovědnost je stále na správci nebo zpracovateli**.

3.7 Posouzení vlivu na ochranu osobních údajů – DPIA

GDPR oproti zákonu o ochraně osobních údajů nahlíží na povinnosti správců (a zpracovatelů) odlišným způsobem – dává jim již několikrát zmíněnou větší zodpovědnost, čemuž nasvědčuje i zrušení oznamovací povinnosti (viz kapitola

3.1.2 na straně 17), která je zdůvodněna tak, že GDPR má zkrátka jiné mechanismy. Jedním z těchto mechanismů je právě „Posouzení vlivu na ochranu osobních údajů“ – v angličtině **„Data Protection Impact Assessment“ – zkráceně DPIA** - článek 35 nařízení. Toto posouzení je nutné v případech, které můžou mít za následek **vysoké riziko pro práva a svobody fyzických osob** (článek 35 odst. 1) a následně by pak mělo sloužit především k zmírnění či eliminaci rizik a zároveň slouží i k dokumentaci v případě dokládání pro dozorový úřad. GDPR jako takové uvádí případy (odstavec 3), kdy je DPIA nutné, jedná se zejména o automatizované zpracování a profilování (viz kapitola 3.5 na straně 25), zvláštní kategorie dat (resp. citlivé údaje) a rozsáhlé monitorování veřejně přístupných prostor. Třetí odstavec mluví o nutnosti, nicméně opět neříká, co je rozsáhlé zpracování a je dosti obecný – toho využívá odstavec 4, který uvádí, že **dozorový úřad sestaví a zveřejní seznam druhů zpracování kdy je nutné DPIA**. Obdobně to platí pro případy, kdy to nutné není (odstavec 5) – tyto seznamy pak předává dozorový úřad sboru. V současné době, kdy je tato práce psána je na webu ÚOOÚ vystaven dokument, který je návrhem a je určen k veřejné diskuzi (do 15. 3. 2018) – tato práce tedy bude vycházet z tohoto návrhu [25].

Dokument navrhuje použití tzv. kriteriální analýzy – správce či zpracovatel ohodnotí, jak s danými údaji zachází a na základě toho určí, zda-li se jedná o vysoké riziko. Dokument dále připouští tři hodnoty ohodnocení – červená, žlutá, zelená – kde červená je vysoká hodnota a zelená nejnižší. Oněch kritérií se nachází v dokumentu celkem 15, **na to, aby správce spadal do kategorie s vysokým rizikem musí mít hodnotu dvou a více kritérií (viz tabulka 3.2 na straně 32). červených nebo jednu hodnotu kritickou a zároveň alespoň pět hodnot žlutých**.

3.7.1 Důležitá kritéria pro webové aplikace

Vzhledem k rozsáhlosti výše zmíněného dokumentu od ÚOOÚ, bych rád zmínil alespoň kategorie, které mi z pohledu webový služeb a aplikací přijdou nejdůležitější, tyto kategorie jsou zvýrazněné v tabulce 3.2 na straně 32.

První kritérium – určení míry monitorování subjektu údajů má dvě možnosti. První možnost, která je označena červenou, zní „subjekty údajů jsou identifikovatelné/identifikované a lokalizovatelné“ – v poznámce se pak můžeme dočíst, že se jedná zejména o zpracování pohybu. Druhá možnost zní stejně, ale místo lokalizace pojednává o rozpoznatelnosti – jedná se tedy především o obrazový materiál.

Druhé kritérium – údaje shromažďované o subjektech údajů má dvě červené kategorie, první z nich se týká trestních věcí a činů, druhá pak profilování a automatizovaného rozhodování. V poznámce se pak můžeme dočíst, že by se

Tabulka 3.2: Kritéria podle návrhu ÚOOÚ

1. Určení míry monitorování subjektu údajů
2. Údaje shromažďované o subjektech údajů
3. Míra a zranitelnosti subjektů údajů
4. Dostupnost osobních údajů
5. Rozsah a zpracování osobních údajů
6. K zasaženému území z hlediska subjektů údajů
7. K uplatnění práv subjektů údajů ke zpracování osobních údajů
8. Přístupnost osobních údajů
9. Soustavnost zpracování osobních údajů
10. K předávání
11. K působnosti správce nebo zpracovatele
12. K rozložení správce nebo zpracovatele v území
13. Ke složitosti systému zpracovávajícího osobní údaje u správce
14. Vazby na jiné subjekty
15. Inovativnost řešení

mělo jednat například i o údaje z logů. Dále jsou zde 3 žluté odpovědi, které se týkají především identifikace subjektu údajů a to spojení jména a příjmení či údajů o platebních kartách. Zelené jsou pak údaje o chování a údajů, jako je výška či věk.

Dalším z vybraných kritérií je rozsah a zpracování osobní údajů, kde dokument dělá v těchto pojmech konečně jasno. Jedná se o:

velký rozsah zpracování – od 10001 a/nebo nad 20 přistupujících osob

střední rozsah zpracování – od 5001 a/nebo od 3 do 20 přistupujících osob

malý rozsah zpracování – do 5000 a/nebo do 2 přistupujících osob

Dalším vybraným kritériem je soustavnost zpracování osobních údajů, zde jsou jen dvě kategorie – žlutá a zelená. Rizikovější z nich a tedy žlutá kategorie je dlouhodobé, soustavné a systematické zpracování, zelená pak krátkodobé, jednorázové, dočasné či příležitostné zpracování.

Posledním vybraným kritériem je předávání osobních údajů, které se dělí do tří kategorií – nejkritičtěji jsou označeny případy, kdy se data předávají do států, kde není zajištěna ochrana na úrovni EU. Dále je žlutá kategorie se státy, kde je ochrana zajištěna nebo jsou zde vhodné (obdobné) záruky. Jak již lze čekat, nejbezpečnější je pak nepředávání údajů mimo Evropskou unii.

3.7.2 Obsah samotného posouzení

Literatura uvádí čtyři povinné kategorie, které by dokument měl mít. Jedná se o systematický popis zamýšlených operací a to i včetně oprávněných zájmů, posouzení rizik a nezbytnosti dat, posouzení rizik pro subjekty údajů, bezpečnostní opatření k řešení rizik, včetně záruk (článek 35 odst.7)[2]. Dále lze přihlížet ke kodexu chování (článek 35 odst. 8 a článek 40).

3.7.3 Případy kdy DPIA není nutné

Návrh [25] obsahuje i seznam případů, kdy DPIA není nutné provádět. Jedná se například o lékařské služby do 5 000 pacientů, dále zpracování za účelem účetnictví nebo obchodní činnosti, která používá jen nezbytné údaje a nejsou dotčena ve velké míře práva subjektů údajů, tedy v případě profilování a automatizovaného rozhodování je nutné DPIA vypracovat.

Vypracování DPIA není nutné úplně ke všem operacím, ale pouze k těm, které jsou nejkritičtější směrem k právům uživatele [2]. Tedy například v případě oprávněného zájmu, kdy se zaznamenávají IP adresy do logovacího souboru kvůli bezpečnosti, není vypracování nutné.

3.7.4 Dopady a shrnutí

Pokud tedy správce či zpracovatel spadá do kategorie, kdy musí mít vypracované DPIA, měl by mít smysluplně u rizikových procesů zdokumentováno, jak a proč s daty zachází, kdo k nim má přístup a jak jsou zabezpečena. Návrhový dokument ÚOOÚ pak dělá jasno i v dalších kategoriích zejména v pojmu rozsahů pro kapitolu 3.5 na straně 25.

3.8 Práva subjektů údajů

Práva subjektů údajů částečně vyplývají již z kapitoly 3.4.3 na straně 23. Ve shrnutí se jedná o:

(a) přístup k údajům,

(b) právo na opravu,

(c) právo na výmaz,

(d) právo na omezení zpracování,

(e) právo na vznešení námitky,

(f) právo na přenositelnost.

Přístup k údajům by obecně měl být v nějakém smysluplném formátu, aby z něj bylo jasné o jaká data vlastně jde. V dalších dvou bodech – oprava a výmaz – bez dalšího vysvětlování je jasné o co jde, nicméně lehce problémový může nastat proces zálohování v případě, kdy jsou data například exportována z databáze a následně „zabalena“ nějaký kompresním algoritmem. Omezení zpracování (článek 18) lze využít na přechodnou dobu například z důvodu ověření správnosti dat nebo v případě, že subjekt vznesl námitku. V případech, kdy jsou data zpracovávána na základě souhlasu nebo výslovného souhlasu, případně jde o data z profilování, je správce povinen na žádost poskytnout nasbírané údaje jinému správci ve strojově čitelné podobě (Právo na přenositelnost - článek 20). Vzhledem k tomu, že nařízení mluví o těchto právech velice obecně, a víceméně není žádný standard, např. pro předávání dat, bude velice zajímavé sledovat vývoj dění v této oblasti po nástupu nařízení v platnost.

Dalším otazníkem v této kategorii je článek 19, nařizující oznamovací povinnost pro správce ostatním správcům v případě, že data smazal nebo opravil – nařízení uvažuje výjimky a to v případě, kdy lze prokázat, že je oznámení nemožné nebo vyžaduje tzv. nepřiměřené úsilí. V řadě případů tedy bude nutné vymyslet i proces pro takováto oznámení. V komentáři [15] se správně poukazuje na to, že v případě, že správce upozorní druhého o aktualizaci údajů, je druhý správce taktéž povinen údaje opravit (mělo by to být jasné už jen z principu korektnosti). V případě výmazu dat, však komentář říká, že ačkoliv upozornění o výmazu je pro dalšího správce stejné jako kdyby ho vznesl subjekt údajů, nicméně správce jemuž byla data předána, by měl posoudit individuálně, zda-li je žádost oprávněná.

Tabulka 3.3: Tabulka porušení podléhající nižší pokutě, převzato z[7]

10 000 000 EUR nebo, jde-li o podnik, 2 % obratu za porušení:	
Správce a tam, kde připadá v úvahu i zpracovatel	povinností při zabezpečení ochrany osobních údajů
	podmínek pro najmutí a spolupráci se zpracovatelem
	povinnosti vyhotovit záznamy o činnostech zpracování
	povinnosti spolupráce s dozorovým úřadem
	povinností při ohlašování, resp. oznamování případu porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů
	povinnosti posoudit vliv na ochranu osobních údajů a absolvovat předchozí konzultaci
	povinností týkajících se jmenování a podmínek pověřence
	povinnosti ustanovit zástupce pro správce nebo zpracovatele usídleného mimo Evropskou unii
	povinnosti týkající se činnosti při získávání osvědčení

3.9 Pokuty

Dalším velmi častým tématem GDPR jsou bezesporu pokuty. Chceme-li mluvit o částkách je třeba říci, že se prakticky jedná o dvě kategorie, podobně jako je tomu u ePrivacy, viz kapitola 3.2.1 na straně 18. Je potřeba si uvědomit, že pokuty v obecném nařízení mají především funkci „strašáka“, aby na správce (zpracovatele), zpracovávající osobní data, byla dostatečná páka nařízení dodržovat, dalším faktem je, že pokuty jsou pro všechny členské země (stejně jako v případě ePrivacy) a tedy pro některé země je taková výše pokut přirozenější.

Jak již bylo popsáno výše, jedná se opět o dvě kategorie, první je pokuta 10 000 000 EUR nebo 2 % z celosvětového ročního obratu, druhá pak 20 000 000 EUR a 4 %. Za co lze pokuty obdržet, pěkně ilustruje literatura [2] resp. obrázky 3.3 na straně 35 a 3.4 na straně 36.

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

Tabulka 3.4: Tabulka porušení podléhající vyšší pokutě, převzato z[8]

20 000 000 EUR nebo, jde-li o podnik, 4 % z obratu za porušení:	
Správce a tam, kde připadá v úvahu i zpracovatel	zásad a zákonnosti zpracování
	podmínek vyjádření souhlasu
	podmínek pro zpracování zvláštních kategorií osobních údajů
	práv subjektu údajů
	podmínek pro předávání osobních údajů do třetí země
	povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které Obecné nařízení umožňuje upravit na vnitrostátní úrovni
	povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 Obecného nařízení nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1 Obecného nařízení
	nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 Obecného nařízení (nápravné pravomoci) nebo neposkytnutí přístupu při uplatnění dozorové pravomoci

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

Kapitola 4

Reklama na internetu

Nedělitelnou součástí internetu a webových aplikací je beze sporu reklama. Úplně nejzákladnější rozdělení reklamy na internetu lze ilustrovat na tabulce 4.1, toto rozdělení se dotýká spíše „míst“ či webových forem aplikací. Toto rozdělení je již překonané – v současné době se používají především bannery s cílenou reklamou na uživatele, které můžou mít rozdílný původ co se algoritmů týče. Mnohem zajímavější z pohledu informačních technologií je podívat se na formy reklamy jako takové. Můžeme je rozdělit buď tím, co a jak zobrazují (případně kde) nebo jakým způsobem za ni inzerent zaplatí.

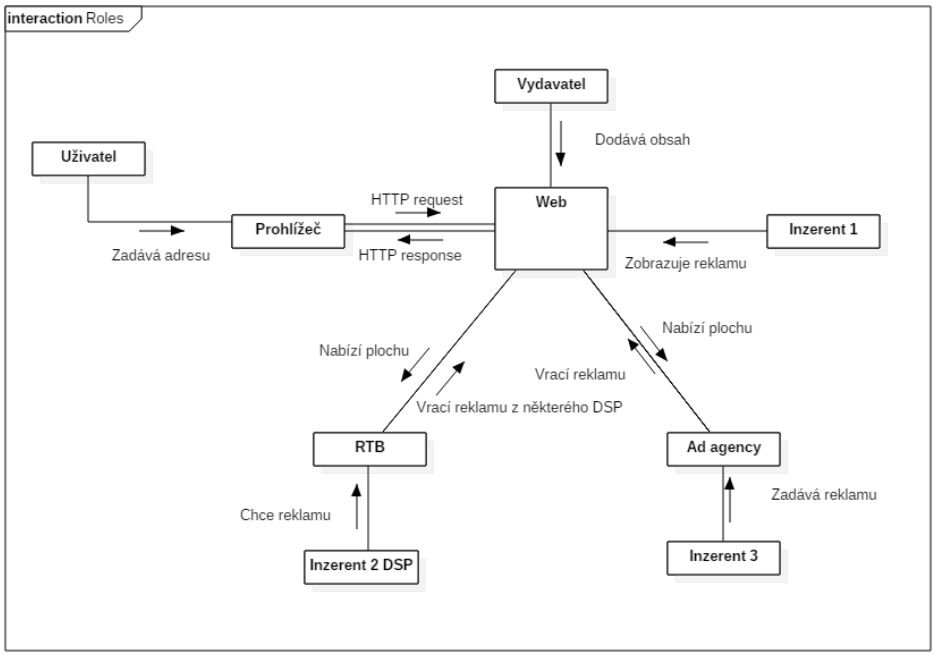
Tabulka 4.1: Dělení reklamy na internetu, převzato z[9]

Způsob	**Finanční náklady**	**Časová náročnost**	**Doba odezvy**
Reklama v massmédiích, billboardy, atp	velké	střední	krátká
Reklama na známých stránkách na internetu	střední	malá	krátká
Zařazení do katalogů vyhledávacích serverů	minimální	velká	dlouhá
Odkazy ze známých stránek	minimální	střední	krátká
Diskusní skupiny	minimální	velká	dlouhá
Elektronická pošta	minimální	střední	krátká
Registrace podobných URL	malé	velká	střední

Specifickou kategorií jsou zápisy do katalogů, které podle mého názoru do několika let úplně zmizí. O proti tomu kontextová reklama je specifická tím, že se nejčastěji zobrazuje, jak již název napovídá, v nějakém kontextu – typický příklad je, když se vyhledávač snaží upřednostnit nějaké vyhledané (a inzerované) odkazy před těmi ostatními.

Speciálním typem, který je z pohledu legislativy nejproblematičtější, bude reklama behaviorální, která se zobrazuje na základě chování uživatele na in-

[9] Stuchlík, Petr; Pegner, Martin; Dvořáček, Martin. *Marketing a reklama na internetu*. Praha: Grada, 1998. ISBN 80-7169-630-7.



Obrázek 4.1: Vztahy mezi jednotlivým subjekty v prostředí webové aplikace a reklamy

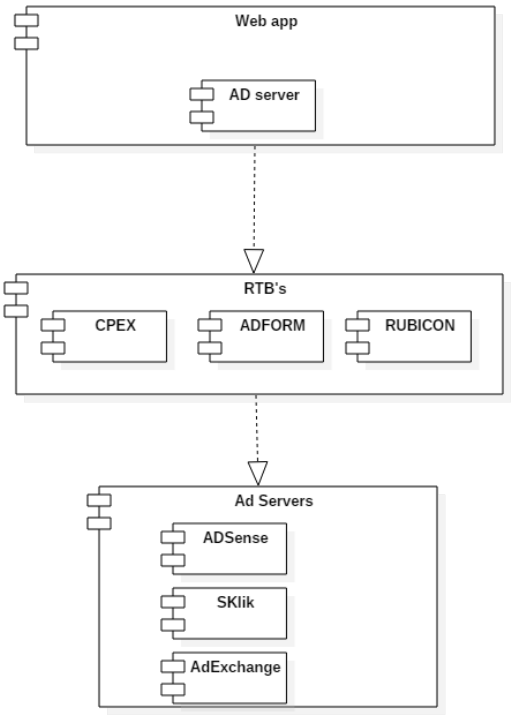
ternetu a využívá dnes často zmiňované soubory cookies. Tomuto tématu se budeme věnovat v kapitole 4.2 na straně 39.

Dále je potřeba si uvědomit, že řada vydavatelů jako je například Tiscali Media, obsah nabízejí zdarma a reklama je pro ně prakticky jediný způsob, jak generovat nějaký zisk. Změny legislativy tedy v některých případech budou nejspíše znamenat i změnu obchodního modelu, nebo zaniknutí služeb – příkladem může být známý portál Spoluzaci.cz. Vztahy v reklamě ve webových aplikacích lze ilustrovat obrázkem 4.1.

4.1 Rozdělení reklamy podle plateb

Podíváme-li se na reklamu z pohledu toho jak se za ní platí, můžeme ji rozdělit takto:

- přímý prodej,
- **PPC** – Pay per click,
- aukce resp. platforma **RTB**.

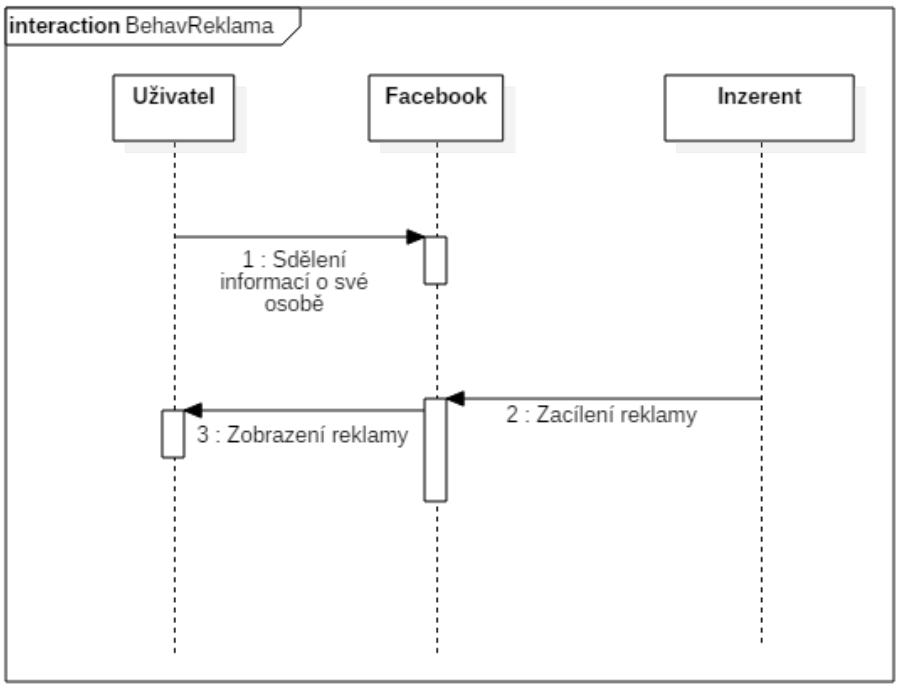


Obrázek 4.2: Kaskáda přes reklamní platformy

Tento pohled společně s kapitolou 4.2 pro nás bude ten nejzajímavější. Přímý prodej reklamy se dnes vyplatí především na webových aplikacích velkých vydavatelů a jejich partnerů. Pokud tato reklama nebude behaviorální, tak koncového uživatele a jeho osobních údajů se to samozřejmě nedotkne. Problémy však nastávají v případě, využíváme-li nějaký reklamní server, který do vztahu inzerent a koncový uživatel vstupuje jako prostředník. Existují však i další možnosti, kdy požadavek na zobrazení reklamy „probublá“ přes několik služeb (obrázek 4.2 na straně 39). Jedná se o případ, kdy například v aukci není vhodná reklama k dispozici a nabídka je podstoupena dále mimo aukční model do ostatních služeb např. AdSense. Nemáme tedy zcela pod kontrolou u koho nabízená plocha skončí.

4.2 Behaviorální reklama

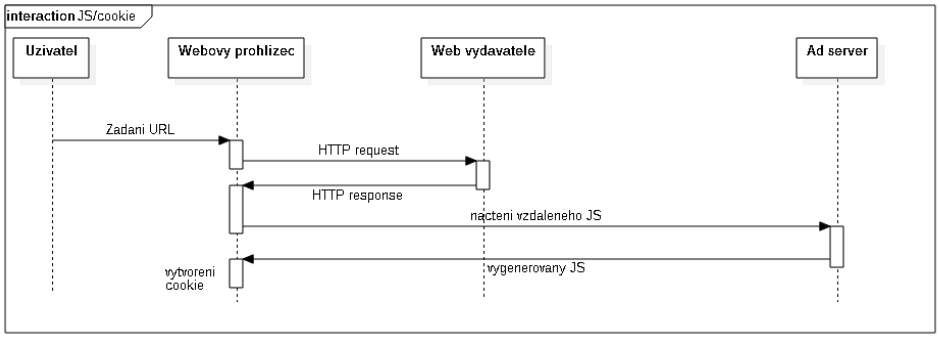
S příchodem nových platforem jako jsou společnosti Facebook a Google se reklama na internetu změnila. Stále je to reklama, která má za cíl uživatele přivést na nějaké jiné stránky, typicky s nějakým produktem, službou či jiným obsahem. Co se tedy změnilo? Změnil se se způsob, jak reklamu na uživatele cílit a také systém toho, jak reklamu na internetu zobrazovat.



Obrázek 4.3: Obecné znázornění cílené reklamy

Nejlépe lze novou situaci popsat na sociální síti Facebook (viz obrázek 4.3 na straně 40). Tato společnost má velkou základnu uživatelů, kteří každý den o sobě dobrovolně nahrávají další a další data. Jedná se jednak o textové příspěvky, ale i o fotografie, nebo například informace v profilu o oblíbených sportech. Ze všech těchto dat lze udělat tzv. profilaci – ze které lze dále předpovědět další uživatelovo chování.

Profilace obecně je založená na tzv. cookies, což je soubor uložený v prohlížeči uživatele a ostatní servery jsou schopny si spárovat identifikátory v něm uložené. Pokud budeme hledat informace týkající se právě těchto souborů, dozvíme se, že jde o záznam nějakých informací – lepší pohled na situaci i díky přicházejícímu GDPR (a v budoucnosti ePrivacy) je nahlížet na cookies spíše jako na mechanismus. Takto se dívali na cookies i tvůrci známého (a dnes již ukončeného) prohlížeče Netscape [27]. Tuto teorii podporuje fakt, jakým způsobem funguje zobrazování reklamy a identifikace uživatele. Uživatel zadá URL stránky (resp. webové aplikace), web zpět odešle HTTP odpověď s kódem, prohlížeč kód zobrazí a načte vzdálené soubory, včetně vzdálených javascript skriptů. Právě tyto skripty mohou pocházet od reklamního serveru (Ad serveru). Načtený kód se vykoná, vytvoří se soubor cookie, který se využije na webové aplikaci.Tento



Obrázek 4.4: Cookie a vzdálený JavaScript

fakt ilustruje obrázek 4.4 na straně 41. Ono kouzlo je ale v tom, přijdeme-li na **jinou webou stránku, která bude využívat služeb stejného Ad-serveru tak se použije pro zobrazení reklamy právě tentýž cookie**. Soubory cookie jsou vázány na doménu, která je vytvořila – nejčastěji třetí strana reklamního systému. Z tohoto důvodu je také problém v souvislosti s ePrivacy. Dále je tento typ reklamy zajímavý i z hlediska návratové hodnoty – behaviorální reklama je totiž více než dvakrát efektivnější než reklama necílená [28] .

4.3 PPC reklama

Zkratka PPC znamená „Pay per click“, největším hráčem na tomto poli v mezinárodním žebříčku je dle mého názoru Google se službou AdSense resp. AdSense a AdWords.

4.3.1 AdSense a AdWords

AdSense použijeme v případě, že chceme zobrazit reklamu na našich stránkách a funguje jako kontextová reklama. AdWords je protičlánek služby AdSense, službu AdWords využívají inzerenti, kteří chtějí nějakou reklamu zobrazovat. Služba jako taková má poměrně striktní pravidla, co lze inzerovat a co ne – službu může použít kdokoliv a není uzavřená jen pro velké vydavatele, kteří mnohdy využívají (někdy i svoje) uzavřené služby v rámci svého portfolia webů a aplikací.

Z pohledu GDPR a zmíněné kaskády zde nastává otazník ve chvíli, kdy použijeme zobrazení reklamy z jiné URL, což nám AdSense umožňuje [29]. V případě, že se bude jednat o další reklamní systém, který si zvolíme my a bude se jednat o behaviorální reklamu, je nutný souhlas. Ale v případě, že by to

byl reklamní systém, který přenechává plochu automaticky dalším systémům, je možné udělit nejspíš souhlas jen s předáním údajů prvnímu reklamnímu systému – neměli bychom totiž kontrolu nad tím, co se zrovna v tuto chvíli zobrazilo, resp. přes kolik dalších prostředníků požadavek prošel.

4.3.2 eTarget

Osobně služba eTarget připadá jako nejčastější z českých PPC zástupců. eTarget je jednou ze služeb, která se z uzavřených stala otevřenou – nicméně i tak se snaží o kvalitní obsah v podobě pravidel na vlastní domény a aktuálnost obsahu [29]. V současnosti navíc nabízí i vlastní DSP (viz kapitola 4.4 na straně 42) [30].

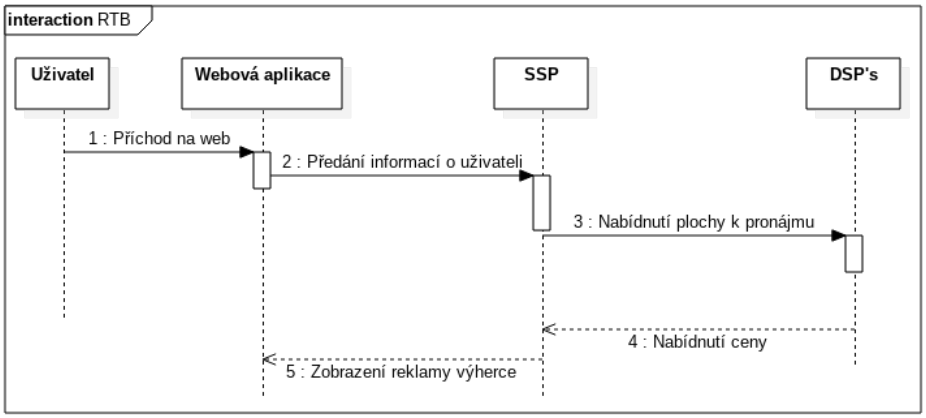
4.4 Real Time Bidding

S příchodem profilace, vyšších rychlostí internetu a zvětšením kapacit úložišť se na trhu objevil model pro nákup a prodej reklamy, který nejčastěji můžeme vidět pod zkratkou **RTB**. Jedná se o real-time aukční model, který má dvě základní části:

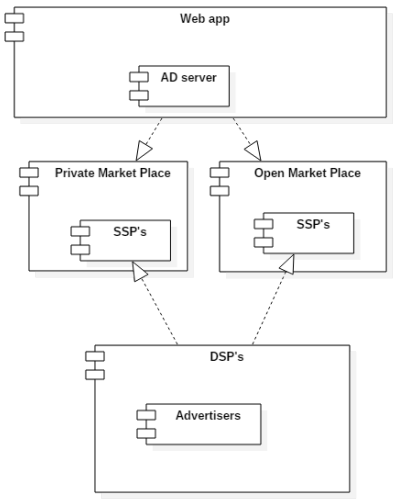
- **SSP** – Supply Side System,
- **DSP** – Demand Side Platform.

RTB je tedy platforma – nebo chcete-li algoritmus – který nabízí plochu k pronájmu inzerentům. Sám o sobě neví nic o ceně za jednotlivou impresi, ta se určí v reálném čase právě na základě nabídek v aukci [28]. První část – SSP – figuruje na straně vydavatele, který chce vydělat na reklamě umístěné na jeho ploše, vytvoří aukci a nabídne ji DSP. DSP má roli přihazujícího. Pro lepší představu průběh vyjadřuje obrázek 4.5 a 4.6. Princip je stejný jako v tom nejtriviálnějším obchodním modelu – „levně nakoupit a draze prodat“. Zde je třeba zmínit, že plochy ve webové aplikaci, která používá profilaci, jsou cennější než jen „obyčejná plocha k pronájmu“ viz 4.2 na straně 41. Pojmy „Private makret place“ a „Open market place“ představují něco podobného jako velkoobchodní a maloobchodní ceny při nákupu v obchodě, v případě PMP se jedná o lepší ceny o proti OMP, které jsou běžné.

Jmenujme si alespoň dva zástupce z platformy RTB. Z globálního světového měřítka stojí za zmínění **Rubicon**. Na domácí půdě pak **CPEX**, který se chlubí členstvím vydavatelů jako je Annonce, Mafra či partnerství s Tiscali.cz. Dále se můžeme dočíst, že se CPEX pokrývá 85 % české online populace.



Obrázek 4.5: Komunikace mezi jednotlivými částmi systému RTB



Obrázek 4.6: Schéma jednotlivých částí RTB

Dále se můžeme setkat s pojmem **DMP** – Data Management Platform. Na DMP můžeme v tom nejtriviálnějším případě nahlížet jako na real-time centralizovanou databázi [28]. Do této „databáze“ se sbírají data o uživatelích a o třetích stranách. Tato data lze dále analyzovat a vizualizovat. Jedná se tedy o nástroj pro vyhodnocování.

4.5 Analytické nástroje

S reklamou jsou nedílně spojené analytické nástroje nabízející nejrůznější vizualizace dat o příchozí návštěvnících. Samotná data jsou často o tom, odkud uživatel přišel, z jaké země nebo jak dlouho na dané stránce setrval. Nejrozšířenější službou v této oblasti je Google Analytics, který nabízí taktéž řadu nastavení. Další velmi rozšířenou službou je Facebook Analytics.

4.5.1 Google Analytics

Služba Google Analytics je jeden z nejpoužívanějších nástrojů v oblasti analýzy přístupů k dané webové aplikaci. V případě, že se rozhodneme tuto službu použít, vstupuje Google do celého procesu zpracování osobních dat jako zpracovatel.

Společnost má na svých stránkách postup, jakým způsobem lze omezit odesílání údajů do služby Analytics – zajímavostí možná pro některé z nás může být upozornění, že jednoznačná identifikace se může vyskytovat i v samotných odkazech a tomu bychom se pochopitelně měli vyhnout. V případě IP adresy je možné sledovací kód upravit tak, aby se vynechala poslední část z adresy (ať už IPv4 nebo IPv6) – údajně se ale tímto postupem sníží přesnost určení odkud uživatel přišel [31].

Dále Google Analytics umožňuje omezení doby uložení údajů o uživatelích a to od 14 do 50 měsíců nebo navždy [32].

I přes odlišný zákon o telekomunikacích, se dle mého názoru lze v tomto případě inspirovat u Nizozemska. Na stránkách zdejšího úřadu na ochranu osobních údajů lze nalézt přímo postup [33], co by správce měl provést v případě, že chce používat Google Analytics a zároveň využít oprávněného zájmu z GDPR.

4.5.2 Facebook Analytics

Společnost Facebook jde v tomto případě trochu jiným směrem, v dokumentech zveřejněných na stránkách pro vývojáře lze najít průvodce, který by měl usnadnit vývojáři rozhodnutí zda potřebuje souhlas či nikoliv.

V textu jsou uvedeny příklady, kdy je vhodné žádat o souhlas uživatele – jeden z nich se týká blogu, který využívá analýzy demografických údajů pomocí souborů cookie a právě tuto možnost nabízí služba Facebook Analytics. Na rozdíl od Googlu zde není možnost, která by umožňovala tato data nějak omezit. Dále se v průvodci můžeme dočíst jakým způsobem o souhlas požádat, kde jednou z možností je používat bannery obdobné těm, které se používají v případě souborů cookie a navádět uživatele k tomu, jak souhlas může udělit

– ostatně tuto možnost jsem již zmiňoval i v předchozích kapitolách [34]. V případě této služby je tedy vhodné jít cestou opt-in.

V posledních dnech se v aplikacích společnosti Facebook začala objevovat upozornění s žádostí o revizi uživatelských nastavení soukromí, dále Facebook nabízí uživatelům popis k čemu soubory cookie využívá [35].

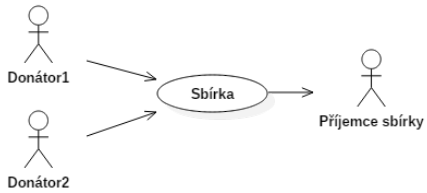
Část II

Praktická část

Kapitola 5

O projektu ElateMe

Projekt ElateMe (ElateMe s.r.o.), jak již název napovídá, nabízí uživatelům službu, jak někomu udělat radost v případě narozenin, svátků a podobných událostí, kdy bychom chtěli někoho obdarovat. Tento projekt je dílem několika dílčích částí, které vznikaly zde na Fakultě Informačních Technologií ČVUT v rámci předmětu Softwarový projekt nebo jako závěrečné práce. Princip aplikace je takový, že uživatel může založit sbírku na nějaký dárek, ať už pro sebe nebo někoho dalšího a ostatní mohou přispívat nějakým finančním obnosem po nějakou předem určenou dobu. V případě, že se stanovená částka vybere, je následně vyplacena (viz obrázek 5.1 na straně 49).



Obrázek 5.1: Princip sbírky

Za projektem jako CEO stojí Matěj Macháček, CTO je Bc. Michal Maněna, který ve spolupráci s Ing. Jiřím Chludilem vede projekty v rámci předmětu Softwarový projekt na Fakultě Informačních Technologií ČVUT.

Samotná webová aplikace je napsána v programovacím jazyce React, za kterým stojí společnost Facebook. Sociální sít Facebook se využívá i nadále, protože v současnosti je účet na této sociální síti jediná možnost, jak se do aplikace přihlásit – nicméně v plánu je rozšíření o registraci přímo na stránkách

projektu. Projekt jako takový tedy funguje na relativně jednoduchém principu, jedním z dalších cílů je profilování uživatelů na základě interakcí mezi nimi a předání získaných dat jako cookie třetím stranám, které by o to měly zájem – zde se jeví jako nejpravděpodobnější různé internetové obchody.

V současnosti projekt vystupuje na internetu pod názvem „Wowee“ a lze ho najít na adrese `http://wowee.cz`.

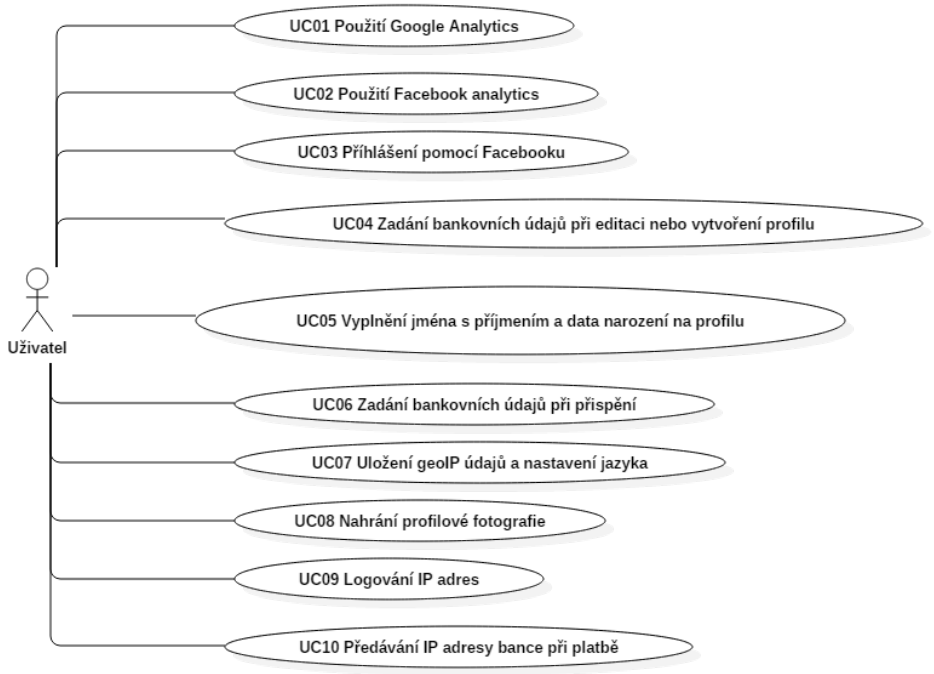
5.1 Popis praktické části

Kapitola 6 na straně 51 se zabývá zjištěnými procesy a navrhuje jejich změny. Dále kapitoly 7 na straně 69, 8 na straně 79 a kapitola 9 na straně 83 se zabývají dokumenty a nutnými informacemi pro ÚOOÚ. Kapitola 10 na straně 85 se zabývá finančními náklady, které souvisejí se změnami, které GDPR přináší.

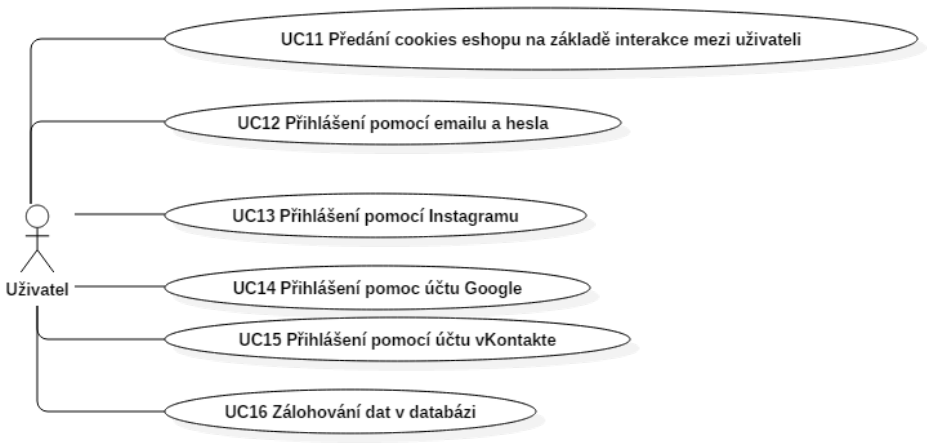
Kapitola 6

Zjištěné případy užití

Na základě schůzek s CTO projektu byla zjištěna současná místa, kde je možnost nějakého způsobu zpracování osobních dat v případech uvedených na obrázku 6.1 na straně 51. Dále projekt počítá s rozšířeními, které jsou uvedeny na obrázku 6.2 na straně 52. Tyto případy, respektive jejich procesy bude nutné analyzovat a v případě, že to bude nutné, zajistit nejlepší možný soulad s GDPR – např. oprávněný zájem.



Obrázek 6.1: Procesy, kde je možné, že dochází ke zpracování osobních údajů



Obrázek 6.2: Budoucí plánované procesy

6.1 Kritická místa

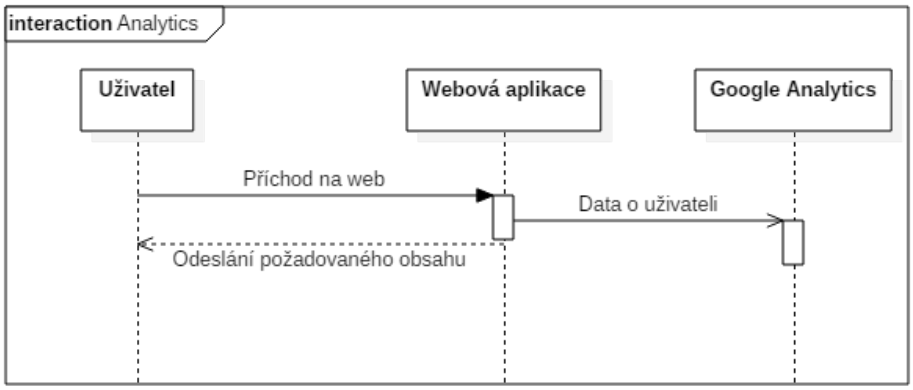
Případy užití nabízejí hned několik oblastí z oblasti osobních údajů – řada případů užití (dále jen UC) je zpracování jen u správce, některé jsou případy, kdy ElateMe je příjemcem resp. třetí stranou pro nějakého jiného správce a samozřejmě tu máme i případ, kdy i ElateMe předává osobní údaje třetím stranám. Z mého pohledu je nejkritičtějším místem rozhodně profilování a v případě zálohování odstranění (nebo anonymizace) dat subjektu údajů, v případě odebrání souhlasu nebo žádosti o výmaz. Dále pak možné případy, kdy nebude možné rozlišit, zda-li jde o osobní údaje, či nikoliv a (WP136 skupiny WP29 to ilustruje na případně IP adres) v takovém případě měl být dán souhlas subjektu údajů nebo podobný právní důvod.

UC01 – Využívání služeb Google Analytics

Používání služby Google Analytics je jedním z nejzákladnějších kroků všech provozovatelů webových služeb, kteří chtějí mít přehled nad tím kdo, kdy a co navštívil. V případě informacích o uživateli jde především o demografické údaje, odkazy které navštívil a odkud přišel. Jak putují data je znázorněno na obrázku 6.3 na straně 53.

Řešení vzhledem k GDPR

Využil bych postupu omezení sběru osobních údajů zmíněného v kapitole 4.5.1 na straně 44, díky kterému lze využít oprávněný zájem. Postup začíná přijetím ustanovení, které lze nalézt v nastavení služeb – Google bude vstupovat do dat pouze jako „editor“ resp. zpracovatel. Druhým bodem je „oříznutí“



Obrázek 6.3: Komunikace s Google Analytics

IP adresy, které lze nalézt i přímo v dokumentaci služby Google Analytics. Dalším bodem v postupu je omezení, resp. vypnutí sdílení dat se společností Google například pro reklamu. Předposledním bodem v dokumentu je nepoužití funkce UserID a konečně posledním je sdělení, že je nutné tyto informace poskytnout v zásadách ochrany osobních údajů.Samozřejmostí pak stále zůstává možnost opt-out [33]. Nově začala služba také nabízet omezení doby, po kterou data budou uchována, na výběr je z 14, 26, 38 a 50 měsíců nebo bez omezení. Doporučil bych využít omezení na 50 měsíců. V případě opt-out u analytických služeb a konkrétně u společnosti Google lze využít rozšíření do prohlížeče, které uživatele vyjme – nicméně v případě, že se uživatel rozhodne rozšíření nepoužít je implementace opět na správci, kde jediné globální řešení vidím identifikátor cookie a uložení záznamu do databáze. Princip by byl takový, že po příchodu uživatele na web by aplikace zkontrolovala, jestli je uživatel v příslušné tabulce „vyjmutých uživatelů“ a pokud ano, uživatel by nebyl zahrnut do analytických dat. Na takovýto krok, vzhledem k souboru cookie nám bude stačit oprávněný zájem, protože uživatel žádá o vyjmutí, jiné technické řešení nepřipadá v úvahu a uživatel může takové zpracování očekávat.

UC02 – Použití Facebook Analytics

Služba Facebook Analytics funguje podobně jako Google Analytics, zachytává akce, které se dějí v aplikaci a následně je zpracuje do grafického výstupu pro analytiky.

Na stránkách služby se můžeme dočíst o tom, jaké údaje lze zobrazit o jednotlivých lidech – jedná se o věk a pohlaví, **město, země, jazyk, pracovní pozice, úroveň vzdělání a rodinný stav**, tučně zvýrazněné informace **jsou**

dostupné pokud se jedná zároveň o uživatele služeb sociální sítě Facebook. Facebook a jeho služba Analytics zpracovává údaje o uživatelích jménem provozovatele a je tedy zpracovatel.

Řešení vzhledem k GDPR

Pro řešení je nutné analyzovat blíže proces, co se s daty vlastně děje. Uživatel, který přijde na webovou stránku je zanalyzován na základě souboru cookie a tato informace je předána do analytického prostředí služby. Dále v případě, že se jedná o uživatele sociální sítě, jsou přidány tučně zvýrazněné údaje z odstavce výše. Proces kombinování se dá rozdělit na dva případy dat. První jsou data směrem od sociální sítě Facebook, která spravuje jako správce a nabízí je ke kombinování s druhým typem dat a to s těmi, které máme k dispozici my v rámci aplikace po příchodu uživatele. Uživatel by dle mého názoru měl o takovém kombinování dat vědět a souhlasit s ním, to odpovídá přístupu opt-in z kapitoly 4.5.2 na straně 45.

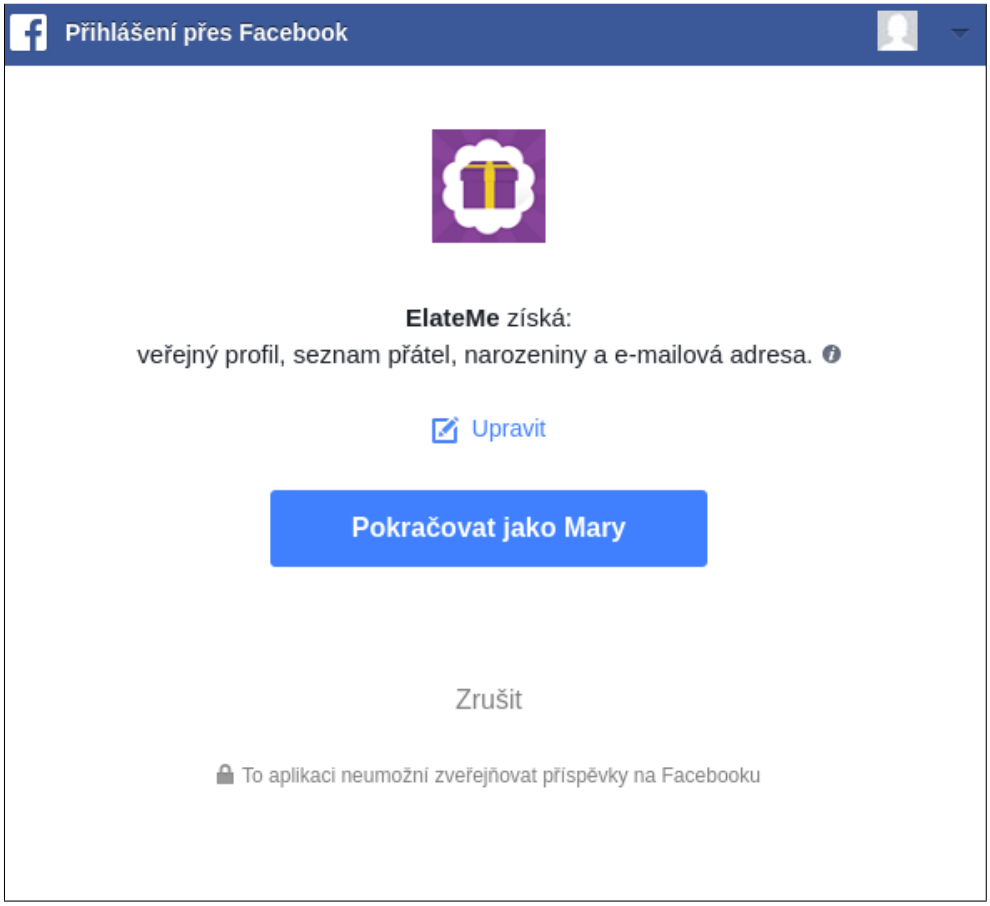
Řešením může být tedy například zobrazení lišty s informací, že takové analytické nástroje aplikace chce použít a žádá o uživatelův souhlas. Druhou variantou a dle mého názoru lepším řešením je používat Facebook Analytics až po přihlášení do služby, kdy po prvním přihlášení můžeme zobrazit dialogové okno, ve kterém můžeme tuto službu zmínit resp. ji přidat k ostatním požadovaným souhlasům, napsat důvody proč ji chceme používat, včetně důsledků pro uživatele a nakonec si vyžádat souhlas potvrzením. Druhá varianta se jeví jako lepší, protože stránka, na kterou uživatel přijde poprvé bez přihlášení, nebude přesycena nějakými upozorněními.

UC03 – Přihlášení pomocí Facebooku

V případě přihlášení pomocí účtu na sociální síti, se při prvním použití po kliknutí na tlačítko uživateli zobrazí dialogové okno. V tomto okně má možnost potvrdit vyžadovaná práva aplikace, viz obrázek 6.4 na straně 55. Aplikace si pak prostřednictvím Facebook API může synchronizovat daná data, která uživatel v předchozím kroku povolil a v tomto případě jsou tedy data předány ze strany Facebooku aplikaci ElateMe, **uživatel tedy dává v současné podobě souhlas Facebooku s předáním dat**.

Řešení vzhledem k GDPR

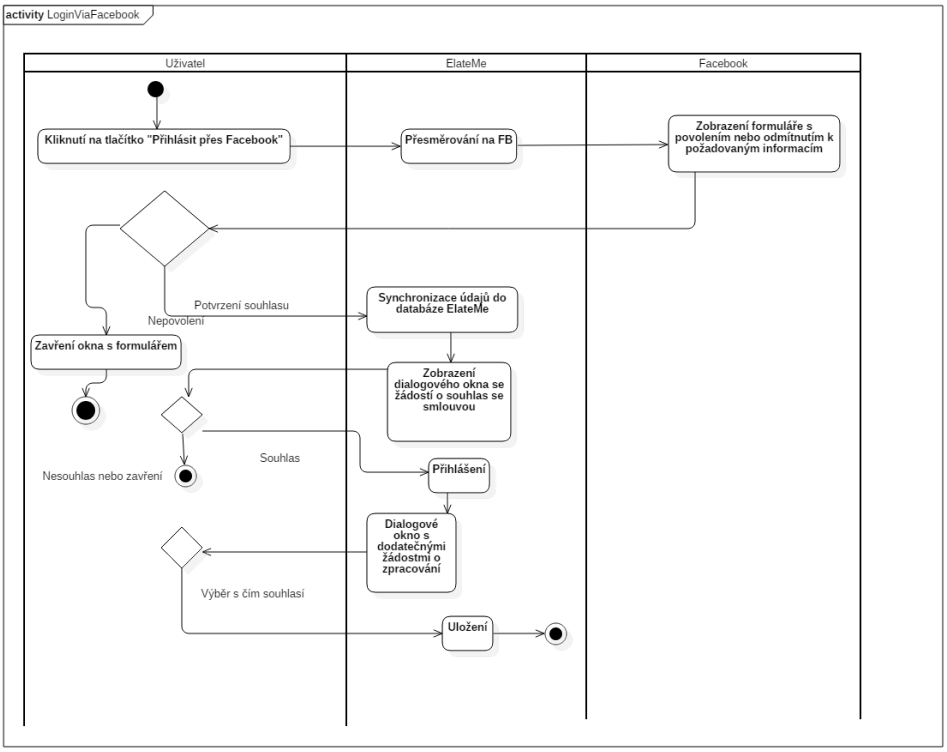
V případě, že data, která nám Facebook poskytl chceme dále zpracovávat, potřebujeme právní základ. Jedním z právních základů je oprávněný zájem, který lze využít v případě, že práva a svobody subjektu nepřevažují nad zájmy správce. Dále k oprávněnému zájmu hovoří recitál GDPR č.47. Tento recitál dává za příklad zákazníka a poskytovatele služeb, dodává však, že je nutné posoudit, zda subjekt může takové zpracování v dané situaci očekávat. Můj



Obrázek 6.4: Potvrzení přístupu aplikace k profilovým informacím

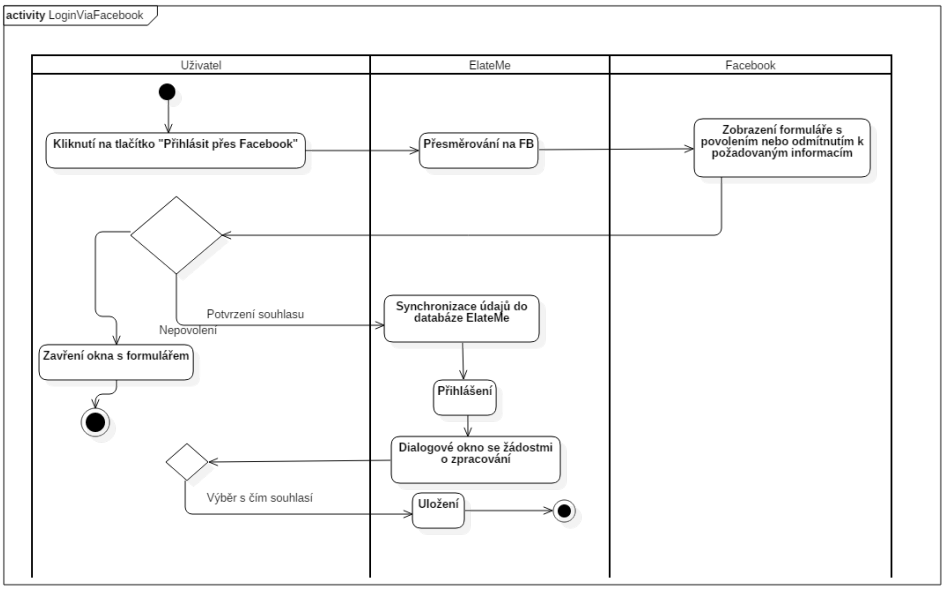
návrh řešení je tedy následující: Jedná-li se o zpracování osobních údajů za **účelem přihlášení**, lze tato data zpracovat na základě **oprávněného zájmu** a tedy po odsouhlasení uživatele můžeme data synchronizovat do databáze aplikace. Následně se uživatel může přihlásit. **Data, která zpracovávat dále nemůžeme, jsou data, která jsme dostali navíc z profilu uživatele – v tuto chvíli není zřejmé proč a na co je chceme**.

V případě dat, která aplikace požaduje dále ze sociální sítě Facebook v rámci dialogového okna 6.4 na straně 55, se jedná o další účel zpracování. Je tedy opět nutné využít z některých právních základů, které nám nařízení nabízí. V tomto případě podle mého názoru nelze použít oprávněný zájem, protože jak již je popsáno výše není jasné (a už vůbec ne uživateli zřejmé), co se s údaji bude dít. V tomto případě připadají v úvahu dvě možnosti – zpracování na základě **plnění smlouvy nebo vyžádání souhlasu se zpracováním**. V případě plnění smlouvy bude nutné uzavřít smlouvu mezi Ela-



Obrázek 6.5: Activity diagram pro přihlášování s účtem Facebook a smlouvními podmínkami

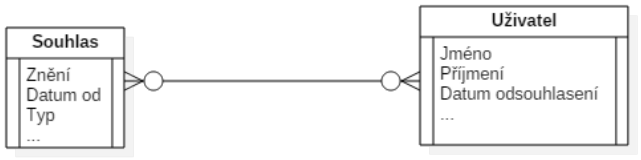
teMe a uživatelem, v této smlouvě lze vyžádat údaje **pouze pro účely nabízené služby** a nikoliv nad rámec (např. profilování je již zpracování navíc). V případě smluvního vztahu je tedy legitimní požadovat ve smlouvě jméno, příjmení, datum narození, profilovou fotografii a číslo bankovního účtu společně s kódem banky pro účely nabízené služby (profil uživatele, sbírky a komentáře)(viz obrázek 6.5 na straně 56). Další zpracování jako je zmíněné profilování a předávání dat třetím stranám, bude podléhat souhlasu samotného uživatele. Tento souhlas si tedy bude nutné vyžádat odděleně. Druhá varianta je jít cestou vyžádání souhlasu samotného subjektu údajů (viz 6.6 na straně 57). V této variantě je problémové odmítnutí poskytnutí služeb, protože nebyla uzavřena smlouva a uživatel tedy nemusí souhlas se zpracováním udělit. Takový postup by byl fér vůči uživateli a bude zároveň v souladu s nařízením. Účel tohoto zpracování je zobrazení uživatelova reálného jména a příjmení společně s datem ostatním uživatelům, aby bylo možné mu vytvořit sbírku a komentovat ji nebo předvyplnění údajů v případě přispění. V případě, že by uživatel chtěl jen procházet sbírky, které vytvořili jeho přátelé, nemusely by být tyto údaje zpracovány a v případě komentářů by se zobrazil jeho e-mail,



Obrázek 6.6: Verze, kde se vyžaduje souhlas se zpracováním

při přispění na sbírku, by se však stejně nevyhnul vyplnit dodatečné údaje.

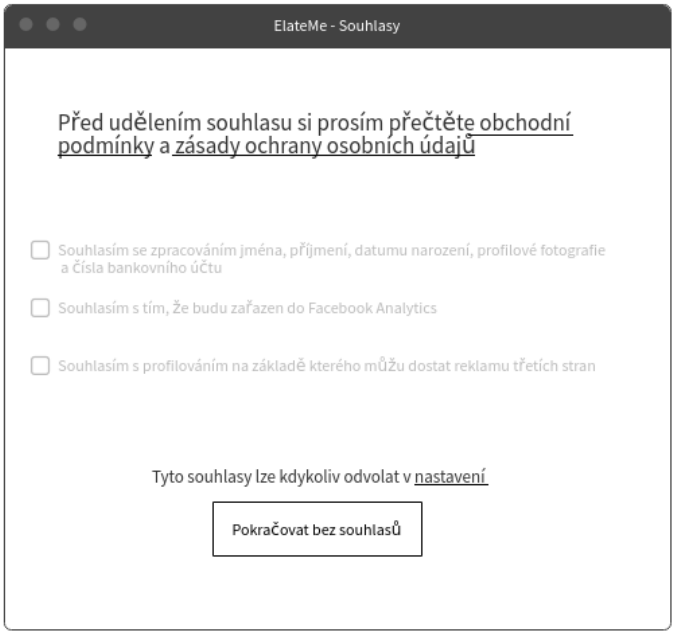
Souhlas se zpracováním by měl být doložitelný (a to i v rámci smlouvy) – navrhuji v tomto případě vytvořit v databázi tabulku souhlasů, kam se uloží, kdo, kdy a co odsouhlasil – může se jednat o další tabulku, kde bude uloženo znění požadavku, viz obrázek 6.7 na straně 57.



Obrázek 6.7: Návrh tabulek pro databázi, pro uchování souhlasů

Samotné udělení souhlasu se zpracováním osobních údajů (nebo se smlouvou) by mohlo začít zobrazením okna zobrazeného na obrázku 6.8 na straně 58. Zaškrtávací políčka by byla neaktivní, dokud si uživatel neprojde obchodní podmínky a zásady ochrany osobních údajů (resp. smlouvu). Po té, co by si je zobrazil, by se okno proměnilo na 6.9 na straně 59. Samotné čtení těchto dokumentů by pak mělo probíhat minimálně tak, že bude nutné „doscrollo-

vat“ až úplně dolů na konec textu a až po něm bude možné souhlas udělit. V případě smlouvy by se nejednalo o zaškrtávací políčka, ale o text, kde by bylo podrobně popsáno pro jaké účely údaje potřebujeme (a ostatní náležitosti). Taktéž by bylo nutné projít smlouvu až do konce a teprve po té souhlasit s jejím zněním. Ve všech případech musí být popsáno zpracování odděleně od obchodních podmínek a dostatečně srozumitelně popsáno uživateli. Dále zde musí být informace o tom, že je možné souhlasy odvolat.



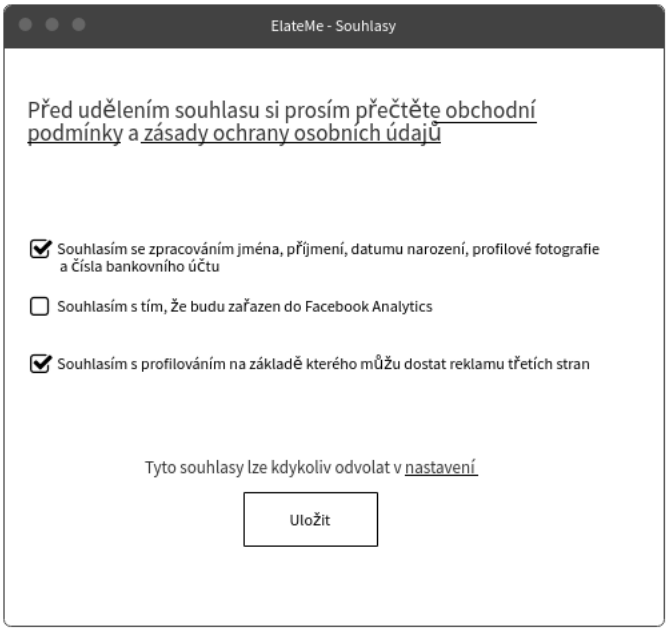
Obrázek 6.8: Takto by mohlo vypadat dialogové okno na vyžádání souhlasu před přečtením podmínek

UC04,UC05,UC08 – Zadání profilových informací

Všechny tyto případy se týkají informací o uživateli resp. jeho profilu v případě, kdy nejsou získány ze sociální sítě Facebook.

Řešení vzhledem k GDPR

V případě, že se jedná o vyplnění informací na profilu a uživatel již souhlasil se zpracováním v rámci smlouvy a nebo k tomu dal souhlas po prvním přihlášení (ať už smluvně nebo souhlasem se zpracováním), není nutné vyžadovat souhlas. Tento souhlas lze dle současných zásad o ochraně osobních údajů zrušit e-mailem, dle mého názoru by byla vzhledem k GDPR vhodná nějaká z automatizovaných cest v rámci aplikace – třeba po kliku na tlačítko nebo



Obrázek 6.9: Takto by mohlo vypadat dialogové okno na vyžádání souhlasu po přečtení obou dokumentů

podobný způsob (viz 6.2.2 na straně 65). V případě, že souhlas ještě udělen nebyl, navrhuji si ho vyžádat při pokusu vyplnit tyto údaje na profilu.

UC06 – Zadání bankovních údajů při přispění

Pojmenování tohoto případu užití je poněkud nešťastné, protože proces příspěvků je komplexnější a stejný postup bude i v případě, že uživatel vytvoří přání sám pro sebe. V případě přispění(resp. vytvoření přání) na přání jako takového je zde povinností je zde celá řada – od předávání IP adresy bance, přes evidenci kdo komu na jaké přání přispěl, až k povinnostem, které určují jiné zákony (ale jiné zákony jsou již nad rozsah této práce).

Řešení vzhledem k GDPR

Povinnost předání IP adresy je popsána v UC10. Další je zmíněná evidence kdo komu na co přispěl, přičemž z databáze lze vyčíst i například jak často – tato informace se hodí, v případě potírání trestné činnosti (praní špinavých peněz) a takové zpracování by mělo být **oprávněným zájmem v kombinaci povinností ostatních zákonů**.

V případě, že nebude použito zpracování na základě smlouvy a uživatel nepovolil zpracování osobních údajů ihned po prvním přihlášení (nebo tak

neučinil později v nastavení), údaje nemohly být předvyplněny a bude nutné informace vyplnit zde. Jedná se o údaje jméno, příjmení a číslo účtu (včetně kódu banky), tyto údaje nebude možné spojit s uživatelem, protože jsou získány za rozdílným účelem, kterým je přispění nebo vytvoření přání.

UC07 – Uložení geoIP údajů a nastavení jazyka

V tomto případě mne napadají dvě varianty řešení.

První varianta: Zvolit režim opt-in. A to například ve formě lišty podobné té, která upozorňuje na používání souborů cookies. Pokud by uživatel souhlas nedal, použil bych nějaký výchozí jazyk, ale zároveň ponechal možnost uživateli, že si jazyk může sám vybrat ze snadno přístupného seznamu i bez lokačních údajů. Tato varianta mi přijde uživatelsky nepřívětivá.

Druhá varianta: Využít **oprávněného zájmu** provozovatele služeb, protože je to nezbytné vzhledem k tomu, aby uživatel rozuměl obsahu ve webové aplikaci. Navíc samotná IP adresa se nikam neukládá, dále se nezpracovává a jen je „přeložena“ na jazyk. **Osobně bych šel touto cestou**.

UC09, UC10 – Logování a předávání IP adresy bance při platbě

IP adresa je považována jako osobní údaj, ale vzhledem k tomu, že se jedná o webovou aplikaci, lze kvůli zabezpečení zaznamenávat adresy na základě **oprávněného zájmu z důvodu bezpečnosti a ochrany aplikace**. Stejný důvod spatřuji i v druhém případě, kdy banka může například **zamezit zneužití bankovních údajů** např. jedná-li se o IP adresu z nějakého jejich interního black listu nebo o několik plateb z míst (resp. ze zemí) za krátkou dobu, kde se za normálních okolností vlastník účtu nevyskytuje.

UC11 – Předání cookies eshopu na základě interakcí mezi uživateli

Mapování interakcí uživatelů mezi sebou, by dle mého názoru, mělo spadat do profilace, z těchto dat totiž lze snadno vyčíst další chování. Z předchozího tvrzení tedy vyplývá, že by uživatel před samotným začátkem profilování měl udělit souhlas (viz kapitola 3.5 na straně 25), navíc se jedná o případy, kdy profilování může mít dopad na subjekty údajů v důsledku jejich přání (a dle skupiny WP29 se v takovém případě jedná o tzv. obdobné důsledky jako důsledky právní). Vzhledem k tomu, že souhlasy musí být jasné a musí být jasné jejich důsledky, navrhoval bych v tomto případě řešení, že při prvním přihlášení se uživateli zobrazí dialog (nebo do dialogu, který se zobrazí bude přidána možnost), kde budou požadované informace a možnost souhlas udělit.

V případě, že by udělit souhlas nechtěl, mohl by ho udělit kdykoliv později v nastavení, nebo mu to může být průběžně připomínáno (nikoliv však na úkor funkčnosti aplikace) –např. ve formě lišty podobné té, která informuje o využívání souborů cookies.

V případě, že data budou skutečně předána, nesmíme zapomenout na povinnost v případě žádosti o výmaz nebo odebrání souhlasu o **informování ostatních správců, kterým byla data předána** a dále případně vypracovat DPIA.

UC12 – Přihlášení pomocí e-mailu a hesla

Přihlášení resp. registrace pomocí e-mailu a hesla by samozřejmě, co se týká osobních údajů, měla být mnohem méně „komplikovaná“ a náchylná na případné úniky dat – bohužel právě zde můžeme narazit na problém vzhledem ke stanovisku WP136 skupiny WP29 (jak již bylo napsáno v úvodním odstavci této kapitoly, v případě, že nejsme schopni rozlišit, že jde nebo nejde o osobní údaje, ale existuje možnost, že to osobní údaje být mohou, měli bychom vyžadovat souhlas v případě, že nemáme jiný právní důvod). V případě, že by tento způsob měl sloužit jako úplně anonymizování uživatele, volil bych spíše použití kombinace přezdívky a hesla, nicméně vzhledem k povaze projektu toto není žádoucí. E-mailové adresy obecně bych osobně rozdělil na dvě kategorie:

- e-mail, který si založí uživatel na nějaké volné službě,
- e-mail, který je přidělen v zaměstnání či podobném vztahu.

V případě, že se jedná o **druhou kategorii** e-mailu, bude se jednat o osobní údaj, protože uživatele lze jednoznačně identifikovat (např. petr.novak@firma.cz). V případě prvním pak záleží na tom, jaké uživatelské jméno si uživatel při registraci zvolil – tato situace je poněkud složitá, protože dle mého názoru nelze kontrolovat zda uživatel, který bude mít e-mail např. petr.novak@sluzba.cz ještě neznamená, že se skutečně jedná o Petra Nováka, ale může se jednat o úplně někoho jiného (to je zásadní rozdíl proti firemnímu e-mailu). Nastává otázka jak tento případ řešit a bude záležet k jakým účelům e-mail potřebujeme.

Řešení vzhledem k GDPR

Řešení může být informovat uživatele při registraci, že se nemá registrovat s takovým e-mailem u kterého je jasné, že jde právě o něj a v příkladu zmínit právě firemní variantu, společně s touto informací bych využil oprávněného

Obrázek 6.10: Jedna možnost z navrhovaných řešení registrace s e-mailem

zájmu, kdy e-mail slouží jen ke kontaktu a verifikaci, že uživatel s tímto e-mailem se chtěl skutečně registrovat (obrázek 6.10 na straně 62). Nepracuje se s ním dále jako se jmény a daty narození. Navíc není v silách provozovatele služby rozpoznat o jaký typ e-mailu se jedná, nebo jak ho „rozparsovat“, tak aby získal například zmíněné jméno a příjmení – takových variant je mnoho. Tuto variantu by bylo samozřejmě nutné popsat v zásadách o ochraně osobních údajů.

Dále tento případ užití je vhodný jako alternativa a možnost volby v případě, kdy uživatel nechce využívat, resp. sdělovat své osobní údaje sociální síti Facebook. V případě profilu, který vidí ostatní nebo komentářů by bylo nutné uvést e-mail nebo ideálně „Anonym“ místo jména, příjmení nebo e-mailu.

UC13,UC14,UC15 – Přihlášení pomocí účtu ze sítí Instagram, Google a vKontakte

Postup v těchto případech shledávám identický jako v případě přihlašování pomocí účtu na sociální síti Facebook na straně 54. Navíc v případě Instagramu se jedná o stejného správce dat, a to společnost Facebook. Data jsou předány od sociální sítě projektu ElateMe, a tedy uživatel by nějakou interakcí schvaloval přístup ElateMe k požadovaným údajům. ElateMe je tedy ve všech těchto případech příjemce dat a v případě dalšího zpracování by s ním uživatel měl souhlasit po přihlášení. To je již popsáno v předchozím případě přihlášení viz UC3 na straně 54.

UC16 – Zálohování dat v databázi

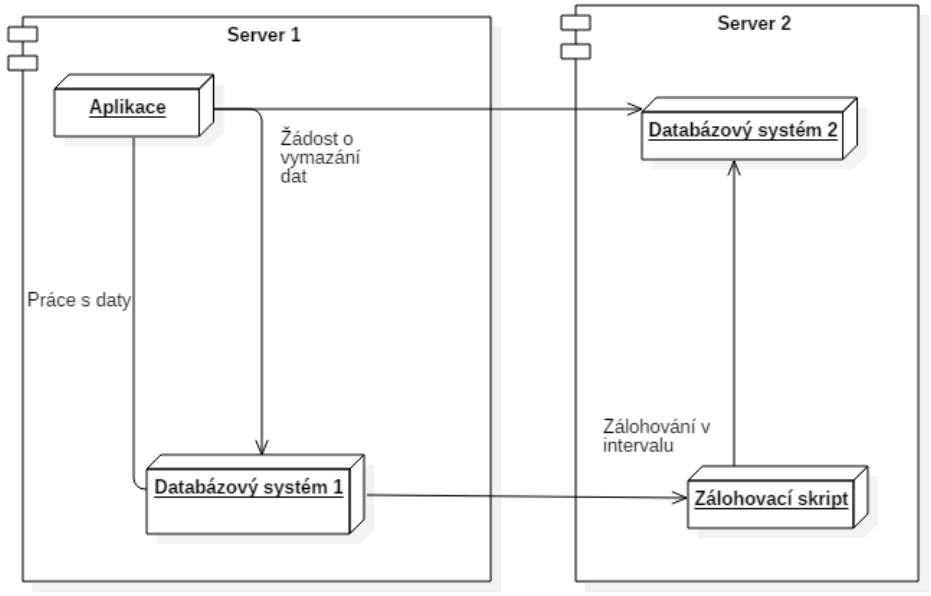
Zálohování dat je zajímavé v případě, že nějaký ze subjektů údajů požádá o vymazání a nebo vznese námitku proti zpracování. Kdybychom GDPR brali doslovně, bylo by nutné vymazat uživatelská data i ze všech záloh, nezáleží na exportovaném formátu a mělo by to být na správci, jak si s implementací poradí. Na druhou stranu **GDPR ukládá povinnost schopnost obnovit dostupnost** osobních údajů v případě incidentů. V této souvislosti mě napadají tři možnosti řešení:

První varianta: Jednodušší a přívětivější k GDPR by byla varianta, kde by existovaly dvě instance databáze a data by se v nějakých intervalech přesouvala z jedné do druhé. Odpadl by tak problém při exportování dat resp. mazání uživatelských dat z onoho exportu. Naopak slabá stránka řešení je, že v případě selhání celého databázového systému nebo systémů nemáme jak data obnovit, další slabou stránkou je vyšší náročnost na hardware resp. služby hostingu viz obrázek 6.11 na straně 64 a s tím je samozřejmě spojena vyšší cena.

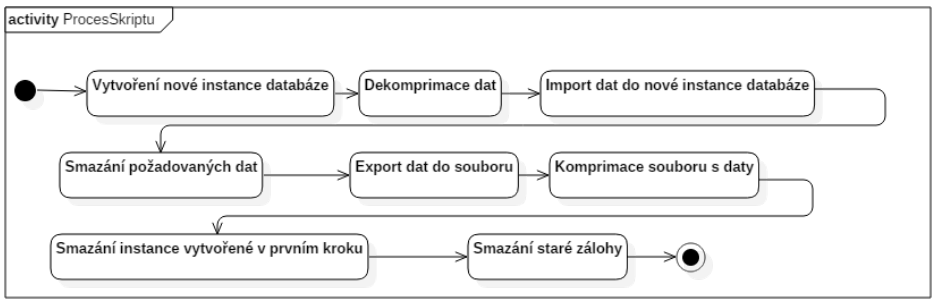
Druhá varianta: Tato varianta je méně přívětivější k GDPR, nicméně je alespoň z pohledu IT jednodušší na implementaci a zároveň lidsky pochopitelná. V tomto případě, bychom zachovali zálohování dat v podobě exportu a volitelného využití nějaké kompresní metody, nicméně periodicita záloh by měla mít nějakou delší dobu a tyto skutečnosti by samozřejmě měly být uvedeny v zásadách o ochraně osobních údajů.

Třetí varianta: Tato varianta je časově nejspíše nejnáročnější na implementaci, ale finančně výhodnější. **Jedná se o kombinaci dvou předchozích řešení**. Zálohy by probíhaly exportem a následnou komprimací a v případě, že by přišla žádost o výmaz dat, spustil by se skript. Ten by vytvořil novou instanci databázového systému, dekomprimoval data, následně je naimportoval do nové instance databázového systému (nebo do nové databáze). Dále by v předposledním kroku požadované údaje smazal a v posledním kroku by po těchto akcích uklidil (obrázek 6.12 na straně 64) a udělal export dat z nové instance DS resp. DB (a tedy již bez onoho nechtěného záznamu).

Dvě malé poznámky na závěr: GDPR nařizuje mít korektní data a v případě záloh se může stát, že se data objeví starší a tedy v přítomnosti nekorektní. V takovém případě navrhuji **uživatele upozornit na skutečnost, že data jsou obnovena ze zálohy a vyžádat úpravy, které provedl, znovu**. Dále v případě žádosti o vymazání (nebo odebrání souhlasu) je nutné informovat správce, kterým byla data předána (pokud takoví správci existují) viz UC11 na straně 60.



Obrázek 6.11: První možnost z navrhovaných řešení zálohování



Obrázek 6.12: Průběh navrhovaného skriptu

Poznámky: Výše zmíněné případy užití se týkají zpracování v rámci aplikace a navrhují dle autora nejlepší možná řešení. Tato práce nabízí rozšíření o případy, kdy zpracování, resp. uchování dat, je nařízeno zákonem – například v situaci, kdy se jedná o daňové doklady apod. Dále je nutné všechny navržené operace důkladně popsat v zásadách ochrany osobních údajů či ve smlouvě s uživatelem. Je nutné dbát na formu, která musí být zvolena tak, aby ji uživatel pochopil. Dále je nutné dát si pozor na používání souborů cookies, kde je třeba uživatele upozornit na jejich využívání.

6.2 Ostatní změny

6.2.1 Věková hranice, kdy je subjekt údajů považován za dítě

Věková hranice, kdy je subjekt údajů považován ještě za dítě, je v současné době v ČR do dovršení 15ti let. GDPR pohlíží ve výchozím stavu jako na děti na všechny osoby mladší 16ti let – členské státy mohou hranici posunout směrem dolů právním předpisem (článek 8).

V obchodních podmínkách aplikace ElateMe je podmínka dovršení alespoň 15ti let a osobně si myslím, že by tato hranice měla zůstat stejná vzhledem k platným zákonům ČR. V případě, že se aplikace **rozšíří za hranice České republiky po Evropské unii**, je vhodné hranici **stanovit na 16 let**.

Dále, vzhledem k přihlášení skrze profil na sociální síti Facebook a následnému předání dat do aplikace, navrhuji v případě zjištění nižšího věku, než je právě 15 (resp. 16) let, uživatele do aplikace vůbec nepustit, ale zobrazit například dialogové okno s informací „Je nám líto, ale bohužel nedosahujete požadovaného věku“ a samozřejmě veškeré údaje o takové osobě odstranit a nezpracovávat. Toto zpracování věku považuji za **oprávněný zájem** správce, neb **nechce zpracovávat osobní údaje subjektů, které jsou považovány za děti**.

6.2.2 Odebírání souhlasu a odstranění účtu

Odebrání souhlasu by mělo být tak snadné jako jeho poskytnutí. V případě aplikace tedy automatizované, bez nutnosti nějakých velkých komunikací.

Vzhledem k tomu, že zpracování údajů je navrhováno na základě smlouvy nebo souhlasu se zpracováním uživatele, který proběhne nějakou akcí – zaškrtnutím či podobným způsobem, lze rozdělit i odebrání souhlasu ke zpracování těchto údajů resp. smazání účtu na dva případy. V případě, že se údaje zpracovávají na základě smlouvy, tak odebrání souhlasu a smazání účtu bude tatáž operace – bez dat nelze službu poskytovat. V případě, že se budou data zpracovávat na základě souhlasu uživatele se zpracováním bez uzavření smlouvy, bude se jednat o dvě různé operace. Možnost smazání dat již teď existuje, avšak v obchodních podmínkách se můžeme dočíst, že data zde mohou být ještě 5 let uložena – toto uložení by mělo dle mého názoru skončit ihned po odebrání souhlasu nebo smazání účtu.

Řešení vzhledem k GDPR

V případě, že si uživatel bude přát účet odstranit, zvolil bych cestu dvojího potvrzení. První krok je kliknutí na tlačítko v profilu, po kterém by se zobrazilo okno, upozorňující na to, o co všechno uživatel přijde v případě zrušení účtu a volbou mezi potvrzením a zrušením odstranění (resp. data nemusí být

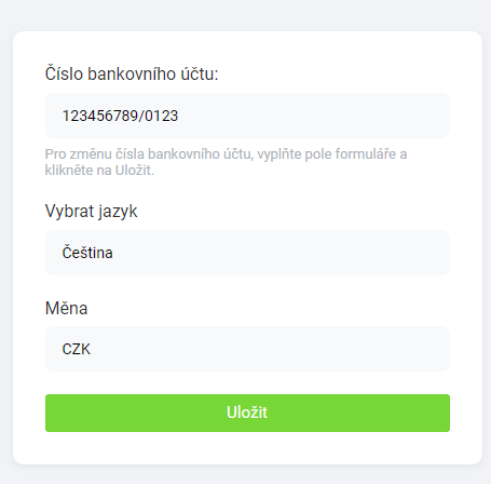
odstraněna, ale například anonymizována pro statistiku). V našem případě by to mohlo vypadat například takto: „Zrušením účtu přijdete o probíhající sbírky, peníze budou navráceny přispěvatelům, ale na dárky již nevybereme a to by mohlo někoho udělat smutným - opravdu chcete smazat účet?“, lze předpokládat, že by si uživatel rozhodnutí na poslední chvíli rozmyslel.

V případě, že se data začnou předávat dalším správcům (například UC11 na straně 60), je nutné je o této skutečnosti informovat.

V případě, že jsou data zpracována ne na základě smlouvy, ale samotného souhlasu subjektu údajů, musí mít možnost (například v nastavení) tento souhlas odvolat – opět může jít například o zaškrtávací políčka. V případě, že souhlas odvolá, je nutné odstranit (anonymizovat) data, která se týkají konkrétního zpracování se kterým uživatel nesouhlasí, jinými slovy, v případě odebrání souhlasu se zpracováním k účelu zobrazení profilových informací údaje, které se týkají přihlášení mohou zůstat. Obdobně to platí pro všechna ostatní zpracování ke kterým dal uživatel souhlas.

6.2.3 Právo na korektnost

Jedním z dalších práv uživatele je právo na korektnost osobních údajů – v případě ElateMe se jedná především o profilové údaje a bankovní účet. V případě, že uživatel chce své údaje změnit má tuto možnost v případě bankovního účtu již v současnosti. Může tak učinit v nastavení svého profilu (viz 6.13 na straně 67). Pokud uživatel provede změny, dojde k uložení do databáze. Pokud bude využita registrace přímo do aplikace, bude nutné podobně umožnit editaci jména, příjmení a data narození. V případě, že by z nějakého důvodu **byla data obnovena ze zálohy, doporučuji o tom informovat uživatele** dialogovým oknem či jinou notifikací s žádostí o kontrolu a případně opravu údajů.



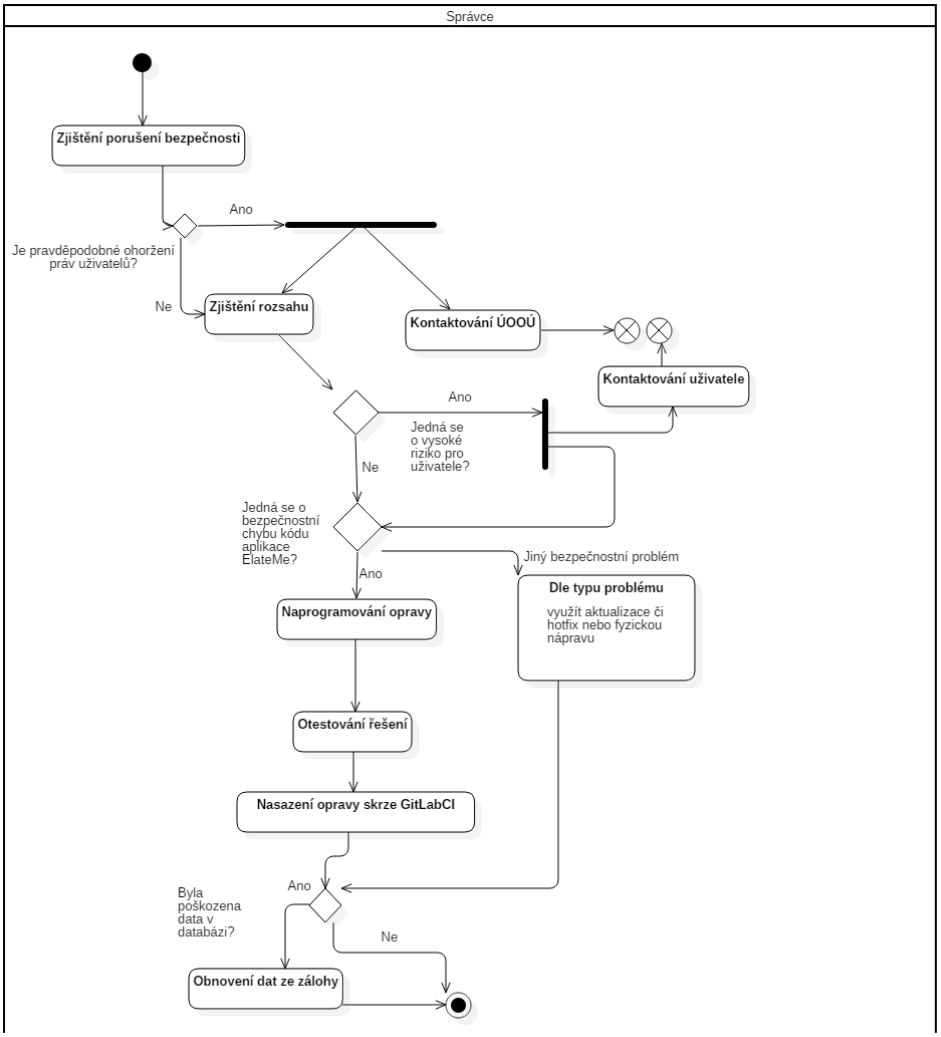
Obrázek 6.13: Změna uloženého bankovního účtu, zdroj[10]

6.2.4 Ohlašování porušení bezpečnosti

Obecné nařízení nařizuje v případě, že by mohlo hrozit porušení práv a svobod subjektu údajů nahlásit porušení zabezpečení do 72 hodin příslušnému úřadu (a v případě velkého rizika i samotnému subjektu údajů) - viz kapitola 3.1.2 na straně 17.

Vzhledem k plánovanému počtu uživatelů a celkové povaze aplikace navrhuji proces (viz obrázek 6.14 na straně 68), pro tento případ. V případě, že bylo zabezpečení porušeno a skutečně se jedná o případ, kdy se to dotkne uživatelů podle odstavce výše, je třeba zjistit rozsah škod a kontaktovat Úřad pro ochranu osobních údajů, dále zjistit zda-li je to vysoké riziko pro samotné uživatele a zjistit příčinu a zdroj chyby. V případě chyby implementační se nabízí naprogramovat hotfix, otestovat zda je chyba opravena a pomocí Continous Integration ho zakomponovat na produkci. V případě, že se nejedná o chybu na straně vývoje samotné aplikace, bude nutné posoudit konkrétní případ a dle toho postupovat dále - např. aktualizací operačního systému nebo jeho části. V případě, že se zjistí úpravy nebo zmizení dat, bude nutné obnovit data z pravidelných záloh.

[10] ElateMe s. r. o. *Wowee* [online] [cit. 2018-05-09]. Dostupné z: `https://wowee.cz`.



Obrázek 6.14: Proces v případě porušení zabezpečení

Kapitola 7

Posouzení vlivu na ochranu osobních údajů – DPIA

7.1 Klasifikace podle dokumentu ÚOOÚ

Ke zjištění zda-li je nutné vypracovat DPIA využívá práce návrhu klasifikace ÚOOÚ (viz kapitola 3.7 na straně 30). Na základě schůzek a zjištěných procesů byly zjištěny skutečnosti v tabulkách 7.1 na straně 70 a 7.2 na straně 71.

Poznámka: U některých ohodnocení se vyskytuje znak * – v takto označených případech se jedná o stav, který bude přibližně následující rok a v budoucnu je plánováno rozšíření.

7.2 Zdůvodnění ohodnocení

Kritérium č. 1 – Určení míry monitorování subjektů údajů

Projekt ukládá údaje o subjektech jako jsou jméno a příjmení, datum narození, profilová fotografie; neukládají se však žádné polohy, které by monitorovaly pohyb jak zmiňuje dokument. Jedná se tedy o žlutou kategorii, kdy jsou subjekty rozpoznatelné.

Kritérium č. 2 – Údaje shromažďované o subjektech údajů

V současné době projekt nevyužívá žádné profilování nebo automatizované rozhodování, ale je v plánu tyto praktiky využít v budoucnosti. Samozřejmostí je používání logů. Dále se zpracovávají údaje jako jsou jméno, příjmení, datum narození, profilová fotografie a číslo účtu s kódem banky. Výsledkem je tedy červená kategorie.

Tabulka 7.1: Klasifikace na základě návrhu dokumentu ÚOOÚ pro vypracování DPIA

Kritérium č.	Název	Ohodnocení
1	Určení míry monitorování subjektů údajů	Subjekty údajů jsou identifikovatelné/identifikované a rozpoznatelné
2	Údaje shromažďované o subjektech údajů	Provozní a další údaje využitelné pro vytváření profilů uživatelů nebo automatizovaného rozhodování + další údaje
3	Míra zranitelnosti subjektů údajů	Bez zvláštní zranitelnosti
4	Dostupnost osobních údajů	Určitá nedostupnost je přijatelná
5	Rozsah zpracování osobních údajů	Velký rozsah zpracování osobních údajů (nad 10 001 a/nebo nad 20 přistupujících osob)
6	K zasaženému území z hlediska subjektů údajů	Nadnárodní úroveň

Kritérium č. 3 – Míra zranitelnosti subjektů údajů

Vzhledem ke zranitelnosti subjektů údajů zde není žádná „selekce“, na všechny se nahlíží stejně a možnost nějaké diskriminace či podobného chování je minimální. Výsledkem je tedy zelená kategorie – bez zvláštní zranitelnosti.

Kritérium č. 4 – Dostupnost osobních údajů

Dostupnost osobních údajů uložených v rámci tohoto projektu není nijak zásadní pro práva uživatelů a ani jinak omezující jejich život. Dále se provádí pravidelné zálohy a tedy dlouhým výpadkům přístupnosti dat se ElateMe snaží předejít. Výsledkem tedy je, že určitě nedostupnost je přijatelná – zelená kategorie.

Kritérium č. 5 – Rozsah zpracování osobních údajů

Kritérium vzhledem k rozsahu považuji v dokumentu za velice netolerantní a podhodnocené; hranici 10 001 uživatelů překročí většina větších projektů. Stejně tomu tak je i u ElateMe – minimální rozsah je počítán na celorepublikový a v budoucnu celoevropský – jedná se tedy dle klasifikace o nejrizikovější případ, a tedy červenou variantu.

Tabulka 7.2: Pokračování tabulky klasifikace ze strany 70

Kritérium č.	Název	Ohodnocení
7	K uplatnění práv subjektů údajů ke zpracování osobních údajů	Subjektem údajů ovlivnitelné zpracování a předání
8	Přístupnost osobních údajů	Údaje jsou veřejně přístupné
9	Soustavnost zpracování osobních údajů	Dlouhodobé, soustavné, systematické zpracování
10	K předávání	Nepředává se nebo se předává do zemí EU (*)
11	K působnosti správce / zpracovatele	Národní úroveň
12	K rozložení správce / zpracovatele v území	Omezeně v území rozložený
13	Ke složitosti systému zpracovávajícího osobní údaje u správce	Systém s propojením na jiná zpracování prováděná stejným správcem/zpracovatelem
14	Vazby na jiné subjekty	Bez vazeb na jiné správce/zpracovatele
15	Inovativnost řešení	První nasazení řešení

Kritérium č. 6 – K zasaženému území z hlediska subjektů údajů

Rozsah vzhledem k území je již popsán v kritériu číslo 5 – je počítáno s národní nebo s celoevropským rozsahem – žlutá kategorie.

Kritérium č. 7 – K uplatnění práv subjektů údajů ke zpracování osobních údajů

Uplatnění práv subjektu údajů vzhledem k zpracování jejich dat lze provést e-mailem na specifikovanou adresu, která je na webu projektu nebo účet smazat či odebrat souhlas se zpracováním. Není tedy žádná zábrana tomu vyřešit případné spory (změny) o zpracování osobních údajů, dále se v současné době žádná data nepředávají – zelená kategorie.

Kritérium č. 8 – Přístupnost osobních údajů

Údaje subjektů údajů (jméno, příjmení, datum narození) jsou vzhledem k povaze projektu přístupné všem, kdo se registrují (nikoliv pouze správci či zpracovateli) a výsledkem je tedy červená kategorie.

Kritérium č. 9 – Soustavnost zpracování osobních údajů

Projekt drží údaje subjektů, dokud existuje jejich profil a uživatelé mají tak možnost aplikaci stále používat – jedná se tedy o dlouhodobé zpracování údajů. Výsledkem je žlutá kategorie.

Kritérium č. 10 – K předávání

Předávání údajů třetím stranám prozatím neprobíhá a pokud nějaké bude, bude se jednat o státy EU – jedná se tedy o ohodnocení, že předávání neprobíhá nebo probíhá jen na území EU – zelená kategorie. V budoucnosti se počítá s předáním dat do zemí, které mají zajištěnu adekvátní ochranu dat a pak by se jednalo o kategorii žlutou.

Kritérium č. 11 – K působnosti správce

Působnost správce je prozatím omezena na národní úroveň – zelená kategorie.

Kritérium č. 12 – K rozložení správce

Rozložení správce je také minimální možné: 1 – 4 místa zpracování a tedy zelená kategorie.

Kritérium č. 13 – Ke složitosti systému zpracování

Data jsou zpracovávány algoritmy pouze u správce – jedná se tedy u žlutou kategorii.

Kritérium č. 14 – Vazby na jiné subjekty

Vazby na jiné subjekty jsou jednoznačně vymezené – data o uživatelích pochází ze sociální sítě Facebook, která splňuje a hlásí se k Privacy Shield. V případě předávání dat dalším správcům, bude jasné o které správce půjde např. konkrétní internetové obchody apod. – zelená kategorie.

Kritérium č. 15 – Inovativnost řešení

Inovativnost řešení – projekt na bázi crowdfundingu a bussiness modelem není na trhu ničím novým, novým je pouze „formát“ ke kterému se přispívání používá – jedná se tedy o žlutou kategorii – první nasazení.

7.2.1 Resumé klasifikace

Podle dokumentu je nutné DPIA vypracovat v případě, že v klasifikaci dosáhneme dvou červených ohodnocení nebo jednoho červeného a minimálně

pěti žlutých. Ohodnocení projektu ElateMe dosahuje v současné podobně ohodnocení třech červených a pěti žlutých, je tedy nutné vypracovat DPIA. V případě, že se v budoucnosti přistoupí k některým změnám zmíněných u některých případů užití, budou změny znamenat už pouze zhoršení klasifikace a tedy DPIA bude nutné vypracovat taktéž.

7.3 Popis a posouzení nezbytnosti zpracování

Posouzení je dle klasifikace ÚOOÚ z předešlé kapitoly 7.2.1 nutné vypracovat. Tato kapitola pojednává o nezbytnosti osobních údajů a účelech za kterými jsou zpracovávány v případech vysokého rizika pro práva subjektů údajů. Dále jsou posouzena rizika a zmíněna opatření, která by měla rizika, co nejvíce eliminovat.

7.3.1 Profilové údaje

Aplikace potřebuje **jméno a příjmení, datum narození a profilovou fotografii** pro vytvoření přání (resp. sbírky), na které se následně bude vybírat finanční obnos. Dále pro profil uživatele a možnost přidávání komentářů.

Popsání samotného procesu: Po odsouhlasení přístupu (a tedy předání dat) aplikace k datům z profilu na Facebooku budou přihlašovací data synchronizována do databáze aplikace. Po udělení souhlasu se smlouvou nebo se zpracováním osobních údajů, jsou dále zpracovány jméno, příjmení, datum narození a profilová fotografie. Jméno a příjmení je použito pro identifikaci osoby společně s profilovou fotografií pro ostatní uživatele – lze tak například vyloučit možnost záměny (případ, kdy se dva uživatelé jmenují stejně a jeden z nich založí sbírku). Dále tyto údaje umožňují psát komentáře k vytvořeným sbírkám. Datum narození je pak nezbytný pro určení, kdy má uživatel narozeniny, používá se k upozornění ostatních uživatelů, že toto výročí nastává a nabízení vytvoření sbírky. E-mailová adresa v případě využitých dat z Facebooku slouží jako kontaktní možnost pro projekt (například v případě porušení bezpečnosti), případně i jako přihlašovací údaj. Je skrze ni možnost upozornit na přání nebo blížící se výročí. V případě, že by se jednalo o registraci přímo do aplikace (a tedy bez využití účtu na sociální síti Facebook), jedná se mimo předešlé možnosti také o způsob verifikace uživatele a omezení zneužití e-mailové adresy – zasláním odkazu uživatel potvrdí, že si účet skutečně přeje vytvořit. Údaje o uživatelích jsou dle navrženého řešení odebrány, jakmile svou žádost potvrdí. Dále jsou údaje (jméno a příjmení) použity v případě, že si uživatel přeje přispět na sbírku.

7.3.2 IP adresa a číslo bankovního účtu včetně kódu banky

Dalším osobním údajem je IP adresa, ta je zpracovávána ve třech případech. Prvním je zaznamenávání přístupů do logovacího souboru – zde se neděje žádné další spojování s konkrétním uživatelem, ale jedná se o prostředek, jak se bránit kybernetickým útokům (například DDoS nebo snaze odcizení dat) a je zde využíváno oprávněného zájmu správce.

Druhým případem, kdy již lze spojit uživatele s IP adresou je případ, kdy uživatel posílá platbu na nějakou sbírku a zároveň povolil zpracování OÚ – lze tak například předvyplnit platební údaje. V případě, že zpracování uživatel nepovolil, musí vyplnit své osobní údaje při platbě, kde je využito oprávněného zájmu v kombinaci s právní povinností. Tato data slouží jen k platbám. Správce je dále **povinen bance sdělit IP adresu** odkud je platba posílána a opět se využívá oprávněného zájmu kvůli bezpečnosti – banka může v případě nesrovnalostí (např. časté platby z míst, kde se subjekt údajů běžně nevyskytuje) tyto údaje využít a zamezit tak ztrátě financí subjektu.

Dalším osobním údajem, který je zpracováván je číslo bankovního účtu a kód banky, tyto údaje jsou využívány k výše zmíněným platbám na jednotlivé sbírky, na které si subjekt přeje přispět nebo v případě refundování sbírky vráceny na tento účet. Údaje jsou uchovávány kvůli usnadnění budoucích plateb (jak směrem od uživatele, tak směrem k uživateli) a podléhají souhlasu subjektu údajů se zpracováním stejně jako profilové údaje.

Dalším zpracováním IP adresy je zjištění země, kde se subjekt nachází a následné nastavení jazyka aplikace. Dle mého názoru jde o oprávněný zájem správce – subjekt údajů díky lokalizaci snáze porozumí jeho obsahu a v důsledku nejde o nijak přesná či obsáhlá data, která by byla spojována. IP adresa jako taková se neukládá, jen se „přeloží“ na jazyk a uloží se právě ten.

7.3.3 Zálohování databáze

Pro proces zálohování jsou navrženy tři varianty (viz UC16 na straně 63), každá varianta umožňuje, v případě odebrání souhlasu (resp. při smazání účtu), smazání profilových informací o uživateli v zálohách. Zálohy jsou uloženy na VPS jejíž zabezpečení je popsáno dále v kapitole 7.3.4 na straně 74. Stejně jako platí přístupy pro VPS i do produkční databáze má přístup pouze vedení projektu (dvě osoby).

7.3.4 Zabezpečení

Veškerá komunikace mezi uživatelem a aplikací probíhá přes HTTPS – certifikát je vydán autoritou Let's Encrypt. V případě odchycení samotných dat při

přenosu tedy útočníkovi k ničemu nejsou. Fyzické zabezpečení samotných serverů je na provozovateli služeb VPS, které aplikace využívá - jsou zde kódové dveře, kamerový systém a fyzická ostraha. Co se týká zabezpečení samotného produkčního systému je zde přístup jen omezeného počtu zainteresovaných osob – jedná se pouze o vedení projektu, čítající dvě osoby. Vzdálený přístup do systému využívá šifrované komunikace pomocí SSH, které nabízí šifrovaný přenos dat. Autentizace uživatelů do operačního systému je pomocí RSA certifikátů. Dále neexistuje možnost přihlásit se vzdáleně pouze s uživatelským jménem a heslem. Na VPS nejsou nainstalovány rizikové nástroje pro přístup do databáze jako je je phpMyAdmin, který nabízí úpravy databáze z webového prohlížeče. Projekt má svoji webovou administraci, která je chráněna kombinací přihlašovacího jména a hesla, navíc je zde dvoufázové ověření - využívá se služeb Google Authenticator.

7.3.5 Profilování a předávání dat třetím stranám

GDPR nařizuje jakékoliv profilování, které se může nějak výrazněji dotknout uživatele v režimu opt-in. V případě, že projekt bude profilování na základě přání a interakcí využívat, je tedy **nutný souhlas subjektu údajů**. Data o které se jedná v tomto projektu se týkají interakcí mezi jednotlivými uživateli resp. subjekty. Jedná se například o

- kdo dal komu přání,
- o jaké přání šlo,
- jak často.

Tyto informace by mohly být zajímavé pro internetové obchody, se kterými se také počítá jako s budoucími třetími stranami, kam se údaje mohou předat. Internetové obchody dále data mohou využít k nabízení slev, reklam na produkty a jiné podobné akce. Jednotlivé případy zatím nejsou známy.

7.4 Hodnocení a eliminace rizik

Pro hodnocení rizik jsem vybral postup uvedený v [11]. Jedná se o techniku ohodnocení 1 – 5 (stejné jako ve škole, 1 nejlepší případ, 5 nejhorší). Dále je zde rozdělení na tři pohledy na jednotlivá rizika: pravděpodobnost (P), závažnost (Z) a ohodnocení hodnotitelů (H). Pro každé riziko ohodnotíme všechny tři kategorie a na závěr je vynásobíme mezi sebou. Výsledná hodnota (R) pak sděluje o jak závažný stupeň rizika se jedná. Čím je výsledná hodnota vyšší, tím je riziko závažnější, hodnoty od 51 výš jsou již nežádoucí a hodnoty nad 100 jsou nepřijatelné. Rizika s opatřeními jsou rozdělena do tabulek 7.3 na straně 76 a 7.4 na straně 77.

Tabulka 7.3: Tabulka rizik

Druh činnosti	Zdroj rizika	Identifikace nebezpečí	Hodnocení rizika				Bezpečnostní opatření
			P	Z	H	R	
Analýza přístupů na webovou stránku	Hacker	Proniknutí do analytických služeb	1	1	1	1	**Organizační**: Přístup má jen členové vedení projektu **Technické**: Dostatečně složitá hesla a dlouhá hesla
Zpracování OÚ pro profil, sbírky, komentáře	Hacker	Plný přístup k OS, včetně dat v DB	1	4	5	20	**Organizační**: Na produkční systém má přístup jen vedení **Technické**: Vzdálené přihlášení do OS je možné pouze s certifikátem, spojení je šifrované a používá se princip „fail to ban“
	Uživatel, který přišel k přihl. účtu	Zneužití profilu na Facebooku a registrace do aplikace	2	2	1	4	**Technické**: Uživatel má v aplikaci možnost zrušit účet
	Hacker	Webová administrace systémových entit	3	4	5	60	**Organizační**: Do produkční administrace má opět přístup jen vedení **Technické**: Pro přihlášení je třeba e-mail a heslo, které je netriviální a použití dvoufázové autentizace služby Google Authenticator

Tabulka 7.4: Pokračování tabulky rizik

Zpracování OÚ pro profil, sbírky, komentáře	Hacker	Uhádnutí nebo prolomení uživatelského hesla a e-mailu	3	3	2	18	**Technické**: Vyžadována netriviální kombinace znaků a dostatečná délka, v databázi je uložen jen hash otisk hesla (algoritmus Argon)
	Lupiči, kteří nevědí kam se vloupali	Vloupání do serverovny, kde je VPS a následná ztráta dat	1	1	2	4	**Organizační**: VPS umístěna v externím datacentru s ostrahou **Technické**: Datacentrum umožňuje vstup pouze přes kódové dveře, kamerový systém
	Lupiči, kteří vědí kam se vloupali	Vloupání do serverovny, kde je VPS a následné zneužití dat	1	4	5	20	Stejné jako v předchozím řádku
	Bezpečnostní díry software	Zneužití uživatelských dat	3	4	5	60	**Technické**: Použití GitLab Continuous Integration, testování API a pravidelné aktualizace
Profilování uživatelů na základě interakcí, které provádějí mezi sebou	Někdo z vývojového týmu	Použití vytvořených profilů uživatelů jinou než smluvní třetí stranou	1	4	5	20	**Organizační**: Vývojáři nemají na produkci přímý přístup **Technické**: Používá se GitLab Continuous Integration

Kapitola 8

Shrnutí procesů zpracování

Shrnutí zpracování ilustruje tabulka 8.1 na straně 81. ElateMe s.r.o. je správcem osobních údajů. Přístup ke skutečným datům subjektů údajů mají jen dvě osoby – CEO a CTO projektu. Data jsou uložena na zabezpečeném serveru, ke kterému je možný vzdálený přístup jen skrze SSH s certifikátem RSA.

E-mail a přihlašovací informace jsou zpracovány na základě oprávněných zájmů, uživatel se chce do aplikace přihlásit a e-mail je např. nutné verifikovat.

Jméno, příjmení a datum narození jsou zpracovávány ve dvou případech a za splnění podmínky, je subjekt starší 15 resp. 16ti let:

1. Jako profilové informace (zde je navíc ještě profilová fotografie)
   – k tomuto je žádán souhlas se smlouvou nebo souhlas se zpracováním subjektu údajů.
2. V případě vytvoření nebo přispění na přání – zde je využit oprávněný zájem a jiné právní povinnosti.

IP adresa je zpracována ve třech případech:

1. Zaznamenávání přístupů do logovacích souborů
2. Při platbě, kdy se IP adresa předává bance
3. Nastavení jazyka celé služby

Všechna tato zpracování jsou na základě **oprávněných zájmů**, první dva z důvodu bezpečnosti a třetí je **nutný k tomu aby uživatel vůbec porozuměl obsahu**.

Předávání dat a profilování je plánováno do budoucna. Dle mého názoru by s takovým zpracováním osobních údajů měl souhlasit subjekt údajů – toto zpracování je nad rámec smlouvy o poskytnutí služby.

Analytické nástroje jsou dva. Prvním z nich je Google Analytics, který lze při dodržení postupu použít v rámci oprávněného zájmu. Druhým zástupcem je Facebook Analytics, který lze použít až po souhlasu subjektu údajů se zpracováním (je to opět nad rámec zpracování, nutných k poskytnutí služby v rámci smlouvy).

Zálohování je navrženo tak, aby v případě žádosti o odstranění dat nebo odebrání souhlasu nebyl problém žádosti vyhovět.

Tabulka 8.1: Shrnutí zpracování

	Oprávněný zájem	Souhlas se smlouvou	Souhlas se zpracováním	Doba uchování
Předání přihlašovacích informací do ElateMe				Do zrušení účtu
Odmítnutí vpuštění do aplikace (zpracování věku)				Milisekundy
Profilové informace				Do odebrání souhlasu nebo zrušení účtu (podle zvolené implementace)
Bankovní údaje a informace				V závislosti na ostatních zákonech (daňové dokumenty 10 let)
Logování IP adresy				Přibližně měsíc
Předávání IP adresy				Nelze určit, jedná se o třetí stranu
Přeložení IP adresy na jazyk				Milisekundy, jazyk je uchován do zrušení účtu
Google Analytics				V závislosti na nastavení
Facebook Analytics				Nekonečno, resp. dokud bude služba využívána
E-mail v případě registrace				Do zrušení účtu
Profilování a předávání těchto informací				Nelze určit, nejsou známy zatím třetí strany

Kapitola 9

Pověřenec pro ochranu osobních údajů (DPO)

Jmenování DPO je povinné v případě, že zpracování OÚ je hlavní činnost, je rozsáhlé a soustavné – viz kapitola 3.6 na straně 29.

Vzhledem k povaze projektu, kdy principem je vlastně sociální síť, kde jednotlivé příspěvky jednotlivých uživatelů (kde se můžeme dozvědět jejich osobní údaje v kombinaci jméno, příjmení a datum narozen) tvoří sbírky na dárky pro nějakého uživatele a plánované rozšíření o profilaci, nadnárodní rozsáhlost a předpokladu, že projekt bude fungovat několik let, navrhuji DPO jmenovat.

Práce DPO je dokumentovat zpracování OÚ projektu, přičemž tato práce by mu měla poskytnout dostatečný základ. Bude se tedy jednat o dokumentaci budoucích změn a případných řešení sporů ať už s uživateli, nebo samotným úřadem. Samozřejmostí jsou konzultace nabízených řešení ze strany vedení projektu.

9.1 Shrnutí

Tato pozice bude pro projekt znamenat další finanční výdaje, nicméně osobně ji považuji v tomto případě za přínosnou, protože se z pohledu projektového řízení bude jednat o lepší dělení práce. Každý z členů vývojového týmu se tak bude moci věnovat svému zaměření a neztrácet čas studiem něčeho, co v důsledku vlastně nepotřebuje.

Kapitola 10

Finanční kalkulace

10.1 Cena změn implementace

Průměrná hrubá mzda programátora v hlavním městě s dosaženým bakalářským vzděláním s nulovou praxí (tedy téměř po škole) se dle portálu platy.cz pohybuje kolem 44 829,- Kč. Uvážíme-li, že měsíc je cca 20 pracovních dní, které mají 8 pracovních hodin, znamená to, že takový pracovník má příjem cca 280,- / hodinu. Skutečné náklady zaměstnavatele však tvoří superhrubá mzda (a náklady na dovolenou), která se skládá z hrubé mzdy a poplatků za sociální a zdravotní pojištění. Zdravotní pojištění 9 % z hrubé mzdy a sociální 15 %, ve výsledku se tedy dostaneme k 34 %. Co se týká mzdy je tedy skutečný náklad 44 829,- Kč + 34 % = 60 100,- Kč (zaokrouhleno na stokoruny). Přepočítáno opět na hodinovou taxu je to pak 376,- / hodina. Zaměstnanec má však ze zákona nárok na 4 týdny dovolené a po tuto dobu mu jde i mzda, kdyby byl zaměstnaný celý rok - tedy 12 měsíců a z toho si 4 týdny vybral dovolenou, bude pracovat 11 měsíců, ale zaměstnavatel mu zaplatí oněch 12. K měsíčním nákladům je tedy vhodné přičíst i ten to fakt, zaokrouhleně je to cca 10 % z hrubé mzdy. Skutečné celkové náklady tedy budou 44 829,- Kč + 34 % (pojištění) + 10 % (dovolená) = 63 800,- Kč (zaokrouhleno na stokoruny), tím se dostáváme na konečnou hodinovou taxu cca 400,- Kč / hodina. Časové odhady jednotlivých změn odpovídajícím případům z kapitoly 6.1 na straně 52, lze nalézt v tabulce 10.1 na straně 87.

K výsledné ceně je nutné připočítat ještě čas strávený vypracováním této praktické části, případných technických změn a v případě jmenování i na DPO.

V době psaní této kapitoly bylo na této praktické části stráveno 32,5 hodiny a odhadem přibližně dalších 20 hodin ještě stráveno bude. S rezervou tedy lze říci, že jen praktická část zabrala cca 53 hodin. V případě, že budeme uvažovat stejnou hodinovou taxu, bude se jednat o částku cca 21 200,- Kč. **Náklady na**

vypracování analýzy změn, dokumentů a změn implementace tedy v součtu vycházejí na 36 200,- Kč.

10.2 Náklady na DPO

Dlouhodobé náklady na DPO se snažím odhadnout podle pozice účetních, kteří jsou často externisté a jejich práce je často nárazová. Průměrná mzda na této pozici je 30 338,- Kč, k této částce opět musíme přičíst povinné poplatky pro zaměstnavatele zmíněné výše, abychom se dostali na reálné náklady - 30 338,- Kč + 44 % = 43 700,- Kč (hrubého a zaokrouhleno na stokoruny) a tedy cca 274,- / hodina. Vzhledem k tomu, že náplň práce DPO je dokumentace zpracování v rámci projektu bude záležet, jak moc se projekt bude měnit. V případě, že by se jednalo například o 20 hodin týdně (poloviční úvazek) by částka byla poloviční - 21 850,- / měsíc.

10.3 Shrnutí

Shrnutí nákladů je popsáno v tabulce 10.2 na straně 87. Náklady potřebné na provedení změn a funkci pověřence nejsou v případě start-up zanedbatelné, v obecném měřítku to takový extrém není. Náklady a časové odhady zde uvedené jsou středním odhadem a v případě pověřence mohou být ještě mnohem nižší než je uvedeno v závislosti na vývoji projektu, v případě implementace změn tomu může být naopak.

Tabulka 10.1: Časový odhad navržených řešení

Use-case	**Odhadnutý čas v hodinách**	**Vypočítaná cena ze mzdy v korunách**
Využívání služeb Google Analytics	1	280
Facebook Analytics	0,5	140
Přihlášení pomocí Facebooku	0,5	140
Zadání profilových informací	1	280
Předání IP adresy bance	0	0
Zadání bankovních údajů při přispění	0,5	140
Geografické údaje a nastavení jazyka	1	280
Nahrání profilové fotografie (*)	1	280
Profilování uživatelů na základě interakce	10	2 800
Přihlášení pomocí e-mailu a hesla	1	280
Přihlášení pomocí účtu na sociálních sítích	1	280
Zálohování dat v databázi	20	5 600
Součet	**37,5**	**15 000**

Tabulka 10.2: Shrnutí finančních nákladů

Aktivita	**Potřebný čas v hodinách**	**Náklady v korunách**
Čas strávený s praktickou částí této práce	53	21 200
Implementace změn	37,5	15 000
Náklady na DPO	20	21 850
Celkem	**110,5**	**58 050**

Část III

Závěr

Kapitola 11

Závěr

Obecné nařízení není tak revoluční, jak se občas někteří snaží prezentovat. Cílem práce bylo poukázat na stav před příchodem GDPR a na změny, které GDPR přinese. Změny jsou především v nových povinnostech vést záznamy, dokumentaci, jmenovat pověřence (pokud je to nutné) a nebo vypracování DPIA. Většina základních definic zůstala stejná. Z mého pohledu je sjednocení ochrany osobních údajů v rámci EU správným krokem, avšak je nutno přiznat, že některé části by si zasloužily větší konkrétnost ve specifických odvětvích. Je zřejmé, že nařízení a zákony musí být obecné a nemohou pokrýt vše konkrétně, v případě GDPR však narážíme například v internetové reklamě na to, jak technicky věci fungují, nebo jak je vůbec lze technicky realizovat.

V případě, že správci osobních údajů dodržují (resp. dodržovali) současný zákon č. 101/2000 Sb. o ochraně osobních údajů, neměli by se příchodu nařízení bát. Správcům samozřejmě vznikají nové povinnosti, problémy mohou nastávat v případě nových procesů, jako je kontaktovat v případě narušení bezpečnosti Úřad pro ochranu osobních údajů (a případně i samotné subjekty údajů) nebo uživatelovo právo na odebrání souhlasu ke zpracování, které má právo uplatnit kdykoliv. Tato skutečnost se i odráží v praktické části.

Většina procesů v projektu ElateMe, které jsou mnohdy přirozené a zjevné nacházejí právní základ pro zpracování v podobě oprávněného zájmu. Zpracování, která podléhají souhlasu uživatele se smlouvou nebo samotným zpracováním, se týkají zpracování osobních údajů pro účely aplikace, profilování nebo v případě Facebook Analytics kroků, které uživatel nemůže běžně očekávat. Dále bylo vypracováno posouzení vlivu na ochranu osobních údajů, jehož vypracování vyplývá z návrhu klasifikace ÚOOÚ. Vypracování se nevyhne nikdo, kdo používá profilaci uživatelů dle mého názoru a i přes výjimky stále zbytečně zatěžuje některé správce administrativou.

Finanční náklady související s příchodem GDPR nevycházejí nikterak velké a mohou se lišit v závislosti na zvolené implementaci, a nebo budoucího vývoje projektu a legislativy.

Cíle práce byly naplněny a návrhy pro projekt ElateMe jsou připraveny k implementaci.

Bibliografie

1. SAGIT. *Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR - obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 28.8.2017.* Ostrava: Sagit, 2017. ISBN 978-80-7488-241-8.
2. ŽŮREK, Jiří. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. Právo (ANAG)., 2017. ISBN 978-80-7554-097-3.
3. KALINOVÁ, Jana. *Zákon o ochraně osobních údaju a právní vztahy.* Vysoká škola ekonomická v Praze, nám. W. Churchilla 4, 130 67 Praha 3, http://www.vse.cz, 2011. Dostupné také z: http://www.nusl.cz/ntk/nusl-114423. Diplomová práce. Vysoká škola ekonomická v Praze.
4. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.
5. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Aplikace Úmluvy Rady Evropy č. 108 ve vztahu k povinnosti žádat Úřad o povolení k předání osobních údajů do zahraničí* [online] [cit. 2018-02-24]. Dostupné z: https://www.uoou.cz/aplikace-umluvy-rady-evropy-c-108-ve-vztahu-k-povinnosti-zadat-urad-o-povoleni-k-predani-osobnich-udaju-do-zahranici/ds-1657/p1=1657.
6. ECONOMIA. *Cookies na službách Economia a.s.* 2018. Dostupné také z: http://napoveda.centrum.cz/index.php?/Knowledgebase/Article/View/145/7/cookies-na-sluzbach-economia-as.
7. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Vodítka k souhlasu podle Nařízení 2016/079* [online] [cit. 2018-04-26]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29162.
8. EVROPSKÁ KOMISE. *Druhy právních předpisů EU* [online] [cit. 2018-03-06]. Dostupné z: https://ec.europa.eu/info/law/law-making-process/types-eu-law_cs.

9. KUČERA, Zdeněk. *Prezentace k přednášce na FIT ČVUT - Úvod do předmětu, právo a IT* [online] [cit. 2018-03-25]. Dostupné z: https://edux.fit.cvut.cz/courses/BI-PAI/_media/lectures/1-2017.ppt.

10. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *S účinností GDPR končí oznamovací povinnost správců* [online] [cit. 2018-03-10]. Dostupné z: https://www.uoou.cz/s-nbsp-ucinnosti-gdpr-konci-oznamovaci-povinnost-spravcu/d-28855.

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

12. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Tisková zpráva: Nařízení o ePrivacy jako doplněk k GDPR* [online] [cit. 2018-02-25]. Dostupné z: https://www.uoou.cz/tiskova-zprava-narizeni-o-nbsp-eprivacy-jako-doplnek-k-nbsp-gdpr/d-27454/p1=1017.

13. EVROPSKÁ KOMISE. *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES* [online] [cit. 2018-04-27]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017PC0010&from=EN.

14. COUNCIL OF THE EUROPEAN UNION. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text* [online] [cit. 2018-04-27]. Dostupné z: http://data.consilium.europa.eu/doc/document/ST-15333-2017-INIT/en/pdf.

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

16. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Základní příručka* [online] [cit. 2018-03-04]. Dostupné z: https://www.uoou.cz/zakladni-prirucka/ds-4744/archiv=0&p1=3938.

17. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Desatero omylů* [online] [cit. 2018-03-06]. Dostupné z: https://www.uoou.cz/desatero-omylu/ds-4818/archiv=0&p1=3938.

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

19. KUČERA, Zdeněk. *Prezentace k přednášce na FIT ČVUT - Úvod do smluvního práva, typické smlouvy v IT* [online] [cit. 2018-04-25]. Dostupné z: https://edux.fit.cvut.cz/courses/BI-PAI/_media/lectures/2-2017.pdf.

20. NULÍČEK, Michal; KOVAŘÍKOVÁ, Kristýna; TOMÍŠEK, Jan; ŠVOLÍK, Oliver. *GDPR v otázkách a odpovědích* [online] [cit. 2018-04-28]. Dostupné z: http://www.bulletin-advokacie.cz/gdpr-v-otazkach-a-odpovedich.

21. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Schválené pokyny* [online] [cit. 2018-03-14]. Dostupné z: https://www.uoou.cz/schvalene-pokyny/d-28603.

22. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679* [online] [cit. 2018-04-27]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29170.

23. VODAFONE CZECH REPUBLIC A.S. *Můj Vodafone* [online]. Verze 3.1 [cit. 2018-05-10]. Dostupné z: https://play.google.com/store/apps/details?id=com.zentity.vodafone&hl=cs.

24. ČESKÁ SPOŘITELNA, A. S. *SERVIS 24* [online] [cit. 2018-05-10]. Dostupné z: https://www.servis24.cz.

25. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online] [cit. 2018-04-27]. Dostupné z: https://www.uoou.cz/k-nbsp-povinnosti-provadet-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/d-28385.

26. STUCHLÍK, Petr; PEGNER, Martin; DVOŘÁČEK, Martin. *Marketing a reklama na internetu*. Praha: Grada, 1998. ISBN 80-7169-630-7.

27. ELMER, Greg. *Profiling machines: mapping the personal information economy*. Cambridge, Mass.: MIT Press, c2004. ISBN 0-262-05073-0.

28. VIKRAM, Anudit; JOHN WILEY & SONS, Inc. The Ad Tech Ecosystem: Special Contributor: Anudit Vikram. In: *The Rise of the Platform Marketer*. John Wiley & Sons, Inc., 2015, s. 21–38. ISBN 9781119153863. Dostupné z DOI: 10.1002/9781119153863.ch02.

29. BARANYK, Jan. *Monetizace internetového obsahu*. Vysoká skola ekonomická v Praze, nám. W. Churchilla 4, 130 67 Praha 3, http://www.vse.cz, 2009. Dostupné také z: http://www.vse.cz/vskp/eid/14021. Bakalářská práce.

30. CPEX. *Jak nakupovat na CPEXU – DSP* [online] [cit. 2018-05-03]. Dostupné z: https://www.cpex.cz/info/jak-nakupovat-dsp/.

31. GOOGLE. *Doporučené postupy, které zabrání odesílání údajů umožňujících zjištění totožnosti* [online] [cit. 2018-03-29]. Dostupné z: https://support.google.com/analytics/answer/6366371?hl=cs&ref_topic=2919631.

32. GOOGLE. *Uchovávání údajů* [online] [cit. 2018-05-12]. Dostupné z: https://support.google.com/analytics/answer/7667196?hl=cs.

33. AUTORITEIT PERSOONSGEGEVENS. *Handleiding privacyvriendelijk instellen van Google Analytics* [online] [cit. 2018-03-31]. Dostupné z: `https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics_mrt_2018.pdf`.

34. FACEBOOK. *Průvodce získáním souhlasu s používáním souborů cookie na webech a v aplikacích* [online] [cit. 2018-04-28]. Dostupné z: `https://developers.facebook.com/docs/privacy`.

35. FACEBOOK. *Soubory cookie a další technologie úložiště* [online] [cit. 2018-04-28]. Dostupné z: `https://www.facebook.com/policies/cookies/`.

36. ELATEME S. R. O. *Wowee* [online] [cit. 2018-05-09]. Dostupné z: `https://wowee.cz`.

Příloha **A**

Seznam použitých zkratek

DB Databáze

DMP Data Management Platform

DPIA Data Protection Impact Assessment (Posouzení vlivu na ochranu osobních údajů)

DPO Data Protection Officer (Pověřenec pro ochranu osobních údajů)

DSP Demand Side Platform

DS Databázový systém

EU Evropská unie

GDPR General Data Protection Regulation

HTTP(S) Hypertext Transfer Protocol (Secure)

IP Internet Protocol

NAT Network address translation

NOZ Nový občanský zákoník

OMP Open Market Place

OÚ Osobní údaje

PMP Private Market Place

PPC Pay Per Click

RSA Asymetrický šifrovací algoritmus

RTB Real Time Bidding

SSP Supply Side Platform

UC Use Case

URL Uniform Resource Locator

VPS Virtuální privátní server

WP136 Stanovisko č. 4/2007 k pojmu osobní údaje skupiny WP29

WP29 Pracovní skupina pro ochranu údajů zřízená podle článku 29

ZOÚ Zákon o ochraně osobních údajů

opt-in Dobrovolné povolení nebo souhlas

opt-out Možnost zakázání zpracování, které ve výchozím stavu již probíhá

ÚOOÚ Úřad pro ochranu osobních údajů

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `BP_Šanda_Michal_2018.pdf` ..... text práce ve formátu PDF