Operačný program
Efektívna verejná správa

Európska únia
Európsky sociálny fond

Výstup č. 1

Koncept manažmentu osobných údajov vo verejnej správe

Zmluva o dielo č. 334/2018 Návrh štandardov pre službu Moje dáta a manažment osobných údajov

Projekt:

Zlepšenie využívania údajov vo verejnej správe

ITMS kód projektu:

314011S979

Tento projekt je podporený z Európskeho sociálneho fondu.

Operačný program
Efektívna verejná správa

Európska únia
Európsky sociálny fond

Moje dáta

"Koncept manažmentu osobných údajov vo verejnej správe"

Tento projekt je podporený z Európskeho sociálneho fondu.

Obsah

1 Manažérske zhrnutie ... 4
2 Úvod ... 6
2.1 Dátovo orientovaná organizácia ... 6
3 Vízia služby Moje dáta ... 8
3.1 Dátová doba a osobné údaje ... 8
3.2 Princípy služby Moje dáta ... 12
3.3 Prehľad technických riešení ... 13
3.3.1 MyData.org ... 13
3.3.2 OpenPDS ... 14
3.3.3 Aplikácie pre Moje dáta ... 15
3.4 Skúsenosti so zavádzaním v zahraničí ... 18
3.4.1 Identita a osobné údaje ... 18
3.4.2 Personálni asistenti ... 21
3.4.3 Adresné služby ... 22
3.5 Verejná správa a osobné údaje ... 23
3.6 Odporúčania pre SR ... 24
4 Architektúra služby Moje dáta ... 26
4.1 Základné definície ... 26
4.2 Služby ... 29
4.3 Aplikačné komponenty ... 31
4.4 Scenáre použitia služby Moje dáta ... 36
4.5 Popis spracovania ... 37
4.6 Platforma Talend a manažment osobných údajov ... 39
5 Adresné služby ... 40
5.1 Princípy adresných verejných služieb ... 40
5.2 Scenáre využitia ... 41
5.2.1 Kontextuálne využitie dát pre prístup k službám ... 42
5.2.2 Služby na základe preferencie ... 43
5.2.3 Služby na základe potrieb – proaktívne služby ... 43
5.2.4 Vzťahy medzi subjektami ... 44
5.2.5 Zdieľanie údajov ... 45
5.2.6 Využitie identity ... 45
5.2.7 Použitie osobného asistenta ... 45
5.2.8 „Smart contracts“ - inteligentné zmluvy ... 46
5.3 Služby tretích strán ... 47
6 Implementačná príručka ... 48
6.1 Požiadavky na procesy a organizáciu ... 48
6.1.1 Moje dáta checklist ... 48
6.1.2 Manažment osobných údajov ... 48
6.1.3 Dôležité otázky ... 49
6.2 Požiadavky na informačné systémy ... 50
7 Plán sprístupňovania osobných údajov ... 52
7.1 Kľúčové objekty evidencie ... 52
7.2 Plán sprístupňovania ... 65

1 Manažérske zhrnutie

Dokument popisuje konceptuálny návrh prístupu k manažmentu osobných údajov a k službe Moje dáta v Slovenskej Republike. V prvej časti je predstavená vízia služby Moje dáta. Zaoberáme sa trendami vo svete vo vzťahu k osobným dátam a k ich využívaniu. Opisujeme ekonomiku založenú na osobných údajoch. Vysvetľujeme tiež GDPR ako dôležitý krok k ochrane osobných dát a poukazujeme na dôležitosť osobných dát. V digitálnej ekonomike je potrebné zaviesť nový spôsob nazerania na identitu, súhlasy a splnomocnenia ako spôsob poskytovania prístupu k osobným dátam.

V tomto dokumente predstavujeme princípy konceptu Moje dáta. Ide o reakciu na trendy vo svete, keď sa dáta stali jedným z najvýznamnejších zdrojov v ekonomike. Aktéri, ktorí majú pod kontrolou dátové toky, sa stávajú najvýznamnejšími hráčmi v ekonomike. Z dát dokážu vyťažiť obrovskú hodnotu, ktorá sa dá využiť na vývoj algoritmov umelej inteligencie, na ďalšiu optimalizáciu procesu, na reklamné účely. Biznis model takzvaných internetových obrov, akými sú Amazon, Google, Facebook či Apple, ale i čínskych spoločností Alibaba, Baidu a Tencent je založený na konštantnom zbere dát o používateľoch a modelovaní ich túžob a preferencií z cieľom ich komerčného využitia výmenou za služby zadarmo. Koncept Moje dáta sa snaží zmeniť tento model a posunúť kontrolu nad dátami do rúk ľudí a zvýšiť tak úlohu občana. Ide o ďalšie pokračovanie cesty, ktorá začala schválením GDPR ako regulácie, ktorá jasne pomenováva práva jednotlivca v dátovej ekonomike. Koncept Moje dáta predstavuje zaujímavý spôsob implementácie týchto práv v praxi. Koncept Moje dáta sa využiť v rôznych oblastiach digitálnej ekonomiky. V tomto dokumente sa venujeme otázke, akým spôsobom zabezpečiť jeho realizáciu v podmienkach verejnej správy na Slovensku.

Dôraz je pritom kladený na praktické otázky a ukazujeme možnosti prístupu k technickej implementácii. Jednou z možností je cesta MyData.org, ktorá je postavená na definovaní "operátorov", ktorý zabezpečia prístup k dátam a kontrolu nad ich spracovaním. Druhým možným filozofickým prístupom je OpenPDS, ktorý bol navrhnutý profesorom Pentlandom na MIT. Tento prístup je založený na poskytovaní odpovedí na otázky zapojeným systémom, namiesto poskytovania celých dát. Samozrejme, ďalšou alternatívou je návrh vlastného riešenia manažmentu osobných údajov. Na základe preskúmaných možností bol zvolený prístup MyData.org, ponúka jednoduchú implementáciu a prísľub využitia rozšíreného štandardu, ktorý môže určiť budúcu interoperabilitu medzinárodných riešení.

Venujeme sa tiež prieskumu reálnych implementácie predstavených princípov Moje dáta. Predstavujeme najzaujímavejšie riešenia systémov pre manažment osobných údajov (známych ako PIMS - Personal Information Management Systems), ako napríklad Digi.me. Táto služba sa dokáže napojiť na zdroje dát, ako sú sociálne siete používateľa a zákaznícke informačné systémy (zdravotníctvo, banky, telekomunikácie a podobne) a vytvorí mu na jednom mieste prehľad informácii, ktoré používateľ poskytol s možnosťou ich editovať či prípadne vymazať. Druhou skupinou riešení založených na myšlienkach Moje dáta sú aplikácie na správu identity používateľov. Dôležitou súčasťou vízie Moje dáta je snaha o hľadanie globálnych riešení, ktoré by mohli byť použité v rámci digitálnej ekonomiky. Hľadáme preto inšpiráciu a poučenia v príkladoch zo zahraničia. Popisujeme skúsenosti so zavádzaním virtuálnej identity, personálnych asistentov a adresných služieb. Do hĺbky sa venujeme implementácii konceptu Moje dáta, ktorá je momentálne najďalej, a to je Singapurské MyInfo.

Na záver vízie sa pozeráme na situáciu na Slovensku. Na spôsob narábania verejnej správy s osobnými údajmi a na možnosti, kam sa môže ďalej posunúť. Formulujeme odporúčania pre Slovenskú Republiku v rámci snahy o posun v téme Moje dáta:

- V oblasti legislatívy je dôležité definovať práva a povinnosti jednotlivých sttrán pre službu Moje dáta v pripravovanom zákone o údajoch a legislatívne podmieniť používanie služby vo verejnej správe, ako i v súkromnom sektore. Dôležité tiež bude podporiť pripravovanú legislatívu pre definovanie

služby Moje dáta na úrovni EÚ. Netreba tiež zabúdať na možnosť využiť novelizáciu zákona o e-Governmente, aby sa postupne koncept služby Moje dáta dostal do povedomia a umožnil riešiť reálne problémy.

- Prioritne je však potrebné sa sústrediť na reálne použitie v praxi. Sužbu Moje dáta je perako nástroj na riešenie problémov pri znižovaní byrokratickej a administratívnej záťaže, napríklad pri potvrdení o návšteve školy. Čím skôr je tiež potrebné využiť už v súčasnosti dostupné dáta ako prvý vstup pre službu Moje dáta. Navrhujeme tiež realizáciu experimentov a "proof-of-concepts v nových oblastiach, ako je využitie mobilnej identity, AI asistenti pre riešenie životných situácií, "smart contracts"a podobne. Služba Moje dáta môže byť dôležitým motorom inovácií verejných služieb, ktoré sa môžu stať adresné a personalizované.
- V oblasti architektúry je dôležité nadviazať na medzinárodné snahy využiť architektonický rámec MyData.org a rozšíriť ho pre potreby verejného sektora. Odporúčame tiež stavať službu Moje dáta ako nadstavbu nad Centrálnou integračnou platformou a zabezpečiť dôveryhodné prepojenie služby Moje dáta s identitou používateľa.
- V neposlednom rade je dôležité zabezpečiť dostatočné zdroje financovania pre prístup inštitúcií k službe Moje dáta a pre návrh adresných služieb, napríklad prostredníctvom dopytových výziev z operačného programu integrovaná infraštruktúra (OPII).

Ďalšia časť dokumentu sa venuje prenosu odporúčaní do praxe. Navrhuje architektúru služby Moje dáta. Popisuje základné definície pojmov, s ktorými sa v rámci konceptu ďalej pracuje, ako napríklad identita, objekt evidencie, súhlas na prístup/spracovanie údajov, kontrakt (zmluva) alebo log. Vysvetľujeme základnú koncepciu: poskytovatelia údajov dokážu cez definované rozhranie (API Moje dáta) sprístupniť autentifikovanému operátorovi údaje, ktoré sa týkajú daného používateľa. Konzumenti údajov môžu pristupovať cez operátora na základe súhlasov. Celé riadenie týchto procesov je realizované v osobnom účte. V rámci popisu definujeme relevantné scenáre použitia, na základe ktorých bude následne vytvorený štandard pre Moje dáta vo verejnej správe na Slovensku. Keďže základnou platformou pre výmenu dát vo verejnej správe je Centrálna integračná platforma, ktorá je postavená na technológii Talend, je vhodné zakomponovať systém pre manažment osobných údajov ako jedno z rozhraní tejto platformy.

Sprístupnenie osobných údajov z jednotlivých informačných systémov verejnej správy cez aplikačné rozhranie vytvára priestor na revolučné inovácie verejných služieb vďaka možnosti adresných služieb. Moje dáta umožňujú zmeniť spôsob, ako štát poskytuje služby občanom a podnikateľom. V súčasnosti je vo verejnej správe aplikovaný model, že jedna služba musí sedieť všetkým. Adresné služby znamenajú návrh služieb čo najviac na mieru pre každého občana. Úspešnou implementáciou konceptu adresných služieb sa môže stať Slovensko inšpiráciou pre ostatné krajiny v reformách štátnej správy. Dokument tiež predstavuje zoznam praktických tipov, akým spôsobom implementovať službu Moje dáta. Zameriavame sa najmä na popis postupu implementácie pre inštitúcie verejnej správy. Je vysvetlené, ako musia upraviť svoje procesy a tiež definované, akým spôsobom je potrebné upraviť informačné systémy verejnej správy. Vysvetľujeme, ako je možné identifikovať objekty evidencie, ktoré sú použité v službe Moje dáta, ako zabezpečiť ochranu osobných údajov a ako naplánovať ochranu osobných údajov a GDPR. V oblasti IT sa venuje otázkam, ako volať službu Moje dáta v praxi, ako vytvoriť API, ako nastaviť systém identifikátorov ako registrovať službu Moje dáta.

Záverečná časť sa zaoberá návrhom ďalších krokov. Popisuje kľúčové objekty evidencie, to znamená základné údaje o občanoch a firmách, ktoré sa budú dostupné ako Moje dáta. Na zoznam objektov evidencie sa dá pozerať ako na prípady použitia. Zároveň navrhujeme plán, v akom poradí sa budú objekty evidencie sprístupňovať.

2 Úvod

2.1 Dátovo orientovaná organizácia

Manažmentu osobných údajov je dôležitou témou pre inštitúcie, ktoré chcú zmeniť spôsob svojho fungovania a lepšie využiť potenciál dát pre návrh lepších služieb a v konečnom dôsledku aj verejných politík. Aplikácia princípov Moje dáta je tak súčasťou širšieho programu o systémovú zmenu inštitúcií verejnej správy smerom k lepšiemu využívaniu dát. Ide o jeden z krokov na ceste smerom k transformácií inštitúcií na dátovo orientované organizácie. Tento postup sa nemusí podariť každému rovnako a očakávame rôznu snahu aj rôzne výsledky. Dátová kancelária bude fungovať ako priestor na zdieľanie najlepších skúseností a šírenie dobrej praxe.

Čo je potrebné, aby sa inštitúcia verejnej správy stala Dátovo orientovanou organizáciou? Oveľa viac ako moderné technológie alebo tím dátových vedcov. Vyžaduje si to vytvorenie efektívnej, hlboko zakorenenej kultúry orientovanej na lepšie využitie údajov, čo zahŕňa:

- začať zdola nahor: naučiť sa správne zhromažďovať správne údaje,
- najímať analytikov s potrebnými zručnosťami a organizovať ich do akčných tímov,
- používať štatistické a vizualizačné nástroje a metódy vychádzajúce z faktov pri návrhu politík a pri rozhodovaní,
- zhromažďovať a analyzovať údaje a rešpektovať pri tom súkromie a etiku; k čomu najlepšie pomáha práve služba Moje dáta,
- pochopiť, ako môžu jednotlivý úradníci pomôcť podnietiť kultúru založenú na údajoch,
- pochopiť dôležitosť pozícií, ako sú dátoví kurátori (v zahraničí známi ako chief data officers) a vedúci analytickej jednotky (chief analytics officer).

Predstavujeme základné predpoklady, ktoré je potrebné zabezpečiť, aby sa organizácia posunula smerom k Dátovo riadenej organizácií. Všetky tieto predpoklady budú podporované Dátovou kanceláriou.

Predpoklad #1: Organizácia musí zbierať údaje a starať sa o ich kvalitu

Kľúčovou zložkou sú nepochybne údaje. Samozrejme, musia to byť správne údaje. Súbor údajov musí byť relevantný, včasný, presný, čistý, objektívny; a čo je najdôležitejšie, musí byť dôveryhodný. Niektorí veľkí predajcovia údajov a poskytovatelia služieb inzerujú veľké údaje ako všeliek: ak zbierate všetko, niekde tam sú aj diamanty, ktoré urobia každú spoločnosť úspešnou. Pravdou je, že samotné údaje nestačia. Malé množstvo čistých, dôveryhodných údajov môžu byť oveľa cennejšie ako nespočet nezmyslov.

Predpoklad #2: Údaje musia byť pripojiteľné, zdieľateľné a vyhľadateľné

Presné, včasné a relevantné údaje však nie sú dostatočné. Musia byť tiež:

- Pripojiteľné – údaje musia byť v takej forme, aby sa mohli v prípade potreby pripojiť k iným údajom. Existuje mnoho možností na správu neštruktúrovaných a distribuovaných dát, ako sú relačné databázy, NoSQL alebo Hadoop. Lepšie nástroje vám umožňujú vytvárať hlbšie a bohatšie analýzy.
- Zdieľateľné – v rámci organizácie musí existovať kultúra zdieľania údajov. Údaje v silách vždy obmedzujú rozsah toho, čo sa dá dosiahnuť.

- Vyhľadateľné – všetky prehľady a analýzy vyžadujú filtrovanie, zoskupovanie a zhromažďovanie údajov, aby sa veľké množstvá nespracovaných údajov zmenšili na menšiu množinu údajov vyššej úrovne, ktoré nám pomáhajú pochopiť, čo sa deje. Analytici musia mať nástroje, ktoré im umožňujú relatívne ľahko vypočítať tieto metriky.

Predpoklad #3: Potrebujete ľudí so správnymi schopnosťami na používanie údajov

Stručne povedané, údaje samotné nezachránia vašu organizáciu. Aby organizácia bola riadená údajmi, musia existovať ľudia, ktorí kladú správne otázky týkajúce sa údajov, ktorí majú zručnosti na získanie správnych údajov a metrík.

Predpoklad #4: Špecifické činnosti pre dátami riadené organizácie:

- Dátami riadené organizácie neustále testujú. Môže to byť testovanie A / B, tok na webovej stránke alebo testovanie vplyvu v kampani. LinkedIn napríklad vykonáva 200 experimentov za deň. Testy môžu tiež zahŕňať testovanie priamo s užívateľmi s cieľom získať priamu spätnú väzbu o možných nových funkciách alebo službách.
- Dátami riadené organizácie sú zapojené do prediktívneho modelovania, prognózovania, ale čo je najdôležitejšie, kŕmia predikčné chyby a iné učenia späť do modelov, aby sa zlepšili.
- Dátami riadené organizácie takmer určite budú vyberať medzi budúcimi možnosťami alebo akciami na základe údajov. Analytici musí informovať a ovplyvňovať tých, ktorí rozhodujú. Technológia a školenia môžu urobiť prvú časť: umožniť analytikom vykonávať analýzy a zverejňovať svoje zistenia. Je to však kultúra, ktorá vytvára spôsob myslenia, v ktorom môžu byť údaje dôverované a použité na určenie ďalších krokov.

Transformácia na dátovú orientovanú organizáciu si vyžaduje čas a trpezlivosť

Dôležitým krokom môže byť práve oslobodenie dát zo síl a systémov organizácie:

- všetky dáta s výnimkou citlivých údajov by mali byť sprístupnené vo forme otvorených dát v strojovo-čitateľnom formáte,
- a rovnako, všetky dáta, ktoré sa týkajú danej osoby by mali byť sprístupnené rovnako v strojovo-čitateľnom formáte na spracovanie aplikáciám, ktoré majú príslušné oprávnenie od tejto osoby.

Takýto prístup vytvára predpoklady pre inováciu verejných služieb a môže výrazne posilniť postavenie jedinca v systéme, jeho možnosti a zabezpečuje implementáciu práv z GDPR v praxi.

Nasledujúci dokument predstavuje koncepčný úvod do témy praktickej implementácie služby Moje dáta a riešenie témy Manažmentu osobných údajov v podmienkach verejnej správy na Slovensku. Vychádza pri tom zo schválenej Národnej koncepcie informatizácie verejnej správy 2016 a rozpracováva tézy Strategickej priority Manažment údajov.

3 Vízia služby Moje dáta

3.1 Dátová doba a osobné údaje

"Surveilance capitalizmus": Ekonomika založená na spracovaní osobných dát

Internet a digitálne služby nám prinášajú možnosti o akých sa nám ešte pred 50 rokmi ani nezdalo. Môžeme telefonovať na druhú stranu zemegule, nájsť informáciu takmer o čomkoľvek, hľadať výhodné letenky, ubytovanie, prípadne byť v kontakte so svojimi známymi. A najlepšie je, že to je všetko takmer zadarmo. Problém je, že ono to až tak zadarmo nie je. Všetky firmy potrebujú zarábať ale z čoho mať zisk, keď používateľ používa ich produkt bez platenia? Ako najlepší spôsob sa ukazuje zarábať na samotnom používateľovi. Najjednoduchšie riešenie je ponúkať mu reklamu. Firmy si uvedomili, že čím viac ho moja reklama zaujme, tým viac na nej zarobia. Začali teda o používateľoch zhromažďovať dáta, aby im vedeli ponúknuť reklamu, čo najviac na mieru. Spôsobilo to rast dát, ktoré bolo potrebné efektívne a čo najlepšie analyzovať. Analytické systémy a algoritmy založené na umelej inteligencii sú mimoriadne schopné poradiť si s touto úlohou. Hromadením množstva dát a čoraz dokonalejších nástrojov vzniká skupina spoločností, ktoré o nás v niektorých prípadoch vedia viac, ako my sami. Jedná sa o veľké technologické firmy ako Google, Facebook, Amazon a ďalšie. Zhromažďujú o nás obrovské množstvo informácii. Výsledok súdneho sporu z roku 2012 nariadil Facebooku poskytnúť používateľovi z Európskej únie všetky dáta, čo o ňom má. Zaslali mu na CD dokument s 1200 stranami. Okrem fotiek a statusov, ktoré sám zverejnil na sociálnu sieť, sa tam nachádzali informácie o každej fotke, odkaze a reklame, na ktoré kedy na sieti klikol. Množstvo dát, ktoré Google o nás má a ako ich vie spracovávať môžeme sami vidieť pri používaní ich produktov. Na Google disku odhaduje, aký súbor chcem poslať. Pri písaní emailu odhaduje akú odpoveď by som chcel napísať, pri navigácií ponúka našu pravdepodobnú destináciu. Kedy chcel, tak by mohol odhadnúť aj oveľa viac osobné záležitosti, ako napríklad, či mám nejakú chorobu, prípadne, či chcem podviesť štát na daniach. Všetko toto je možné na základe našich informácií, ktoré spoločnosti zbierajú. Z dát sa stáva komodita. A keďže platí, že čím viac a kvalitnejších dát mám, o to dokážem robiť lepšie predpovede, tak spoločnosti čoraz viac sledujú používateľov. Tento rozvoj sledovania a ekonomiky založenej na ňom už dostal aj pomenovanie a volá sa "Surveilance capitalizmus"[1]. Spoločnosti ale nezostávajú len pri sledovaní, ale skúšajú využitím získaných informácií ovplyvniť naše životy. Facebook napríklad experimentoval so spokojnosťou používateľa, tým, že niektorým ukazoval pozitívne príspevky a ďalším zas negatívne. Sledoval, ako je schopný ovplyvniť jeho náladu. Známy je aj škandál počas prezidentských volieb v USA, kedy firma Cambridge Analytica bez súhlasu ľudí získala ich informácie a na základe toho zacielila reklamnú kampaň s cieľom ovplyvniť výsledok volieb. Spoločnosť si začína uvedomovať, že občan je oproti technologickým firmám v nevýhode a podniká kroky na jeho ochranu. Príkladom sú hnutia ako napríklad Moje dáta alebo zákony, ako nedávno prijaté Naradenie o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej ako GDPR - General Data Protection Regulation).

GDPR[2] je krok správnym smerom, čo však chýba?

GDPR je krokom Európskej Komisie k poskytnutiu väčšej kontroly nad dátami do rúk občanov. Vstúpila do platnosti v máji 2018 a obsahuje práva ako:

[1] https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

[2] https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A32016R0679

- právo na prístup k údajom,
- právo na opravu,
- právo na obmedzenie spracúvania,
- oznamovacia povinnosť pri oprave, vymazaní os. údajov alebo obmedzením spracúvania,
- právo na prenosnosť údajov.

Implementácie tejto smernice prináša výsledky, jedným z nich je, že sa spoločnosti a organizácie začali zaoberať otázkou súkromia používateľov. Používatelia si môžu všimnúť zmeny napríklad pri prehliadaní webových stránok, kde majú možnosť nesúhlasiť s využívaním ich údajov pre cielenú reklamu. Je to dobrý úvodný výsledok, ale je potrebné využiť základ, ktorý GDPR poskytuje a pokračovať[3]:

- Prvou príležitosťou je otázka, ako sa postavia autority k GDPR. Jednou vecou je schválenie smernice, druhou, ako je uvedená do praxe. Štátne orgány ako orgány štátnej moci majú príležitosť vyžadovaním pravidiel z GDPR, zlepšiť postavenie používateľov. Ďalšia šanca sa skrýva pri prípravách budúcej legislatívy.
- Druhou rozvojovou oblasťou vyplývajúcou z GDPR, je otázka akým spôsobom zaručiť, že dáta boli skutočné zmazané. Bude potrebné vybudovať skupina pracovníkov, ktorí budú schopný byť zodpovední za správne nakladanie s dátami.
- Treťou oblasťou je prenesenie práv do rúk používateľov, ktoré GDPR prinieslo a ďalšia aktivita používateľov povzbudená týmto posilnením ich role.
- Poslednou oblasťou, ktorá prináša príležitosti sú rožne iniciatívy, konferencie a aktivity ako napríklad mydata.org. Prinášajú inovatívne myšlienky, ktoré môžu byť potom prenesené do praxe.

Osobné dáta v centre záujmu

GPDR pracuje s pojmom osobné dáta. Používa tento pojem nie len na identifikátory ako je meno, adresa alebo vek, ale tiež aj na "online identifikátory" akými sú napríklad cookies. V GDPR sa výslovne uvádza, že on-line identifikátory, aj keď sa jedná o pseudoanonymné údaje, budú považované za osobné dáta, ak existuje možnosť identifikácie alebo vyčlenenia jednotlivca.

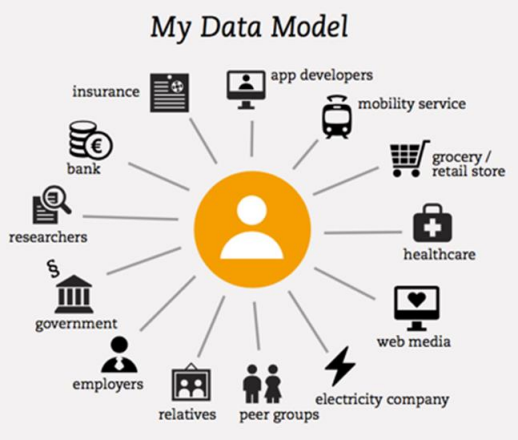
Osobné dáta v kontexte GDPR sa týkajú aj spoločností, ktoré nie sú aktívne v online oblasti. Príkladom je zamestnávateľ s elektronickou databázou zamestnancov, ktorý bude musieť dodržiavať pravidlá GDPR v prípade, ak ich databáza obsahuje citlivé osobné údaje, ako napríklad rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie a ďalšie.[4]

Ukážka skupín dát, ktoré môžeme považovať za osobné, ponúka nasledujúci obrázok: ide o dáta o dopravných presunoch osôb a využívaní dopravných služieb ako je Uber; dáta o poistení; dáta o životnom štýle, aktivitách a záujmoch; dáta o využívaných finančných službách, finančných transakciách a účtoch; dáta o záznamoch a evidenciách vo verejných registroch; dáta o súdnych konaniach; dáta o zamestnávateľoch a zamestnaniach; dáta o príbuzných a vzťahoch s nimi; dáta o používaní utilitných služieb, akými sú elektrina, voda, plyn, kanalizácia; dáta o aktivite na sociálnych sieťach; dáta o zdravotnom stave a využívaní zdravotníckych služieb; dáta o realizovaných nákupoch a podobne.

[3] https://www.youtube.com/watch?v=CsnniK7Ff08

[4] https://www.titanhq.com/blog/what-is-gdpr?utm_source=Facebook&utm_medium=Hootsuite&utm_campaign=Organic_Hootsuite

Obrázok 1: Kategórie osobných dát



Na právach jedinca vzhľadom k jeho osobných dát stojí myšlienka Moje dáta. Táto hovorí, že by používateľ mal mať praktické prostriedky na prístup, získavanie a používanie osobných dát. Práva, ktoré ma za cieľ jedincom poskytnúť hnutie Moje dáta:

- Právo vedieť, aké osobné údaje existujú v evidencii,
- Právo vidieť skutočný obsah osobných údajov,
- Právo na opravu chybných osobných údajov,
- Právo na kontrolu, kto pristupuje a spracováva osobné údaje a za akým účelom,
- Právo získavať osobné údaje a slobodne ich používať,
- Právo zdieľať alebo predávať osobné údaje tretím stranám,
- Právo na odstránenie alebo vymazanie osobných údajov.

Zdroj: https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/2e9b4eb0-68d7-463b-9460-821493449a63?version=1.0

Nový spôsob nazerania na identitu

Jednou z podmienkou možnosti vykonávať transakcie v digitálnom priestore je dôveryhodné preukázanie identity jednotlivých aktérov. Poskytovanie a staranie sa o identitu svojich občanov je jednou zo základných funkcií štátu. Človek potrebuje dokumentáciu k preukázaniu svojej identity a ak ju nemá, tak nemá prístup k službám regulovaným štátom ako financie, bývanie, zamestnanie, svadba. V 19. a 20. storočí sa poskytovanie identity, podobne ako tlač peňazí, stalo výlučným monopolom štátu. Niekedy sa stáva, že to nefunguje a je to problém. Napríklad ako uvádza The Economist vo svojom článku[5], v Rumunsku bol jeden muž prehlásený za mŕtveho, napriek tomu, že žije. Súd povedal, že žiadosť o zrušenie úmrtného listu bola podaná neskoro. Alebo jeden čínsky novinár sa nemôže objednať k lekárovi, pretože jeho meno nie je v oficiálnej databáze čínskych znakov a tak nie je vo formulároch na online objednávanie. Štát v ich prípadoch nezvládol svoju funkciu a spôsobil tak značné problémy dotknutým subjektom. Príchod digitálneho sveta priniesol nový pojem a to elektronickú identifikáciu. Na prístup k službám nepoužívame identifikačný preukaz vydaný štátom, ale prístupové meno a heslo. Ďalšou možnosťou je využiť služby internetových gigantov ako Google a Facebook. Vypĺňať meno a heslo

[5] https://www.economist.com/christmas-specials/2018/12/18/establishing-identity-is-a-vital-risky-and-changing-business

pri prihlasovaní nie je potrebné, človek sa jednoducho prihlási cez svoj účet. Vznikla tak digitálne identita, ktorá nie je v rukách štátov. Pri jej používaní spoločnosti, ktoré identitu sprostredkovávajú, zbierajú o používateľovi množstvo informácií. Tento zber nemá používateľ pod kontrolou. Ako alternatíva začínajú vznikať nové služby poskytovanie identity, napríklad služby, ktoré zabezpečia poskytnutie iba tých informácií, ktoré sú potrebné pre danú situáciu. Príkladom je overenie a garancia veku aplikáciou. Aplikácia potvrdí, že užívateľ má 18 rokov, bez toho aby on musel ukazovať občiansky preukaz s osobnými údajmi. Ďalším trendom je odpojenie identity od štátu - napríklad použitím technológie blockchain. Digitálnu identitu majú záujem poskytovať aj finančné a telekomunikačné firmy. Vlády dnes nezaostávajú. Mnohé z nich sa inšpirujú v Estónsku, ktorému sa podarilo spustiť zabezpečenú a užitočnú e-identitu. Na Slovensku je štátom garantovaná digitálna identita momentálne dostupná len pre verejné služby a je potrebné jej otvorenie pre ďalšie prípady využitia. Nie vždy však tieto systémy prinesú iba pozitíva, napríklad nový venezuelský identifikátor je používaný na sledovanie hlasov pri voľbách. Digitálna identita sa vyvíja a ak chce Slovensko poskytovať občanom dobré služby, musí aktívne sledovať a prinášať trendy, napríklad využiť spojenie digitálnej identity a manažmentu osobných údajov.

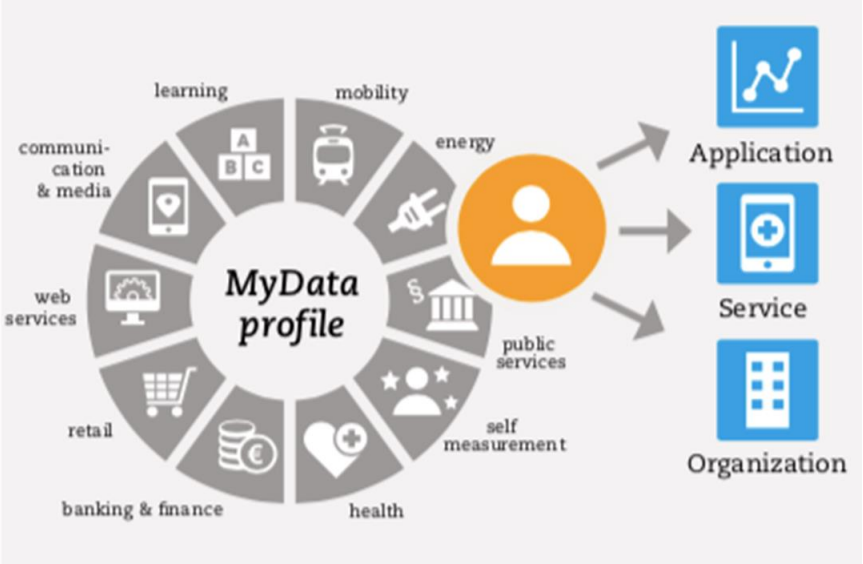
Súhlasy na prístup k údajom

Pokrok vo využívaní a ochrane osobných údajov je možné dosiahnuť, ak sú k dispozícii praktické nástroje pre jednotlivých aktérov digitálnej ekonomiky. Jedinec by mal mať možnosť a nástroje na správu svojich osobných dát, ako rozšírenie svojho práva na slobodu myslenia a vyjadrovania. Organizácie by zároveň mali mať spôsob, ako praktický získavať súhlasy jednotlivcov na prácu s ich osobnými údajmi, ak objavia nový spôsob ich využitia.

Súhlas na používanie je v súčasnosti vyjadrovaný súhlasom s podmienkami spoločnosti. Toto vo väčšine prípadov prebieha bez toho, aby si užívateľ tieto podmienky vôbec pozrel. Súčasná legislatíva neposkytuje spoločnostiam príliš iných spôsobov, ako súhlas od občana získať.

Služba Moje dáta ponúka možnosť, ako chrániť digitálnu identitu a zároveň organizácie získajú nástroje, ako využívať dáta. Užívateľ získa možnosť zhromažďovať si svoje údaje z viacerých miest. Časti zhromaždených dát môže následne použitím súhlasov a splnomocnení poskytovať vybraným konzumentom údajov, aplikáciám a organizáciám za účelom získania kvalitnejších, viac na mieru prispôsobených služieb, ako je znázornené na nasledujúcom obrázku.

Obrázok 2: Možnosti využitia osobných dát[6]



Zdroj: https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/2e9b4eb0-68d7-463b-9460-821493449a63?version=1.0

Využitie blockchain

Snaha o nezávislosť a prenositeľnosť dát sa v internetovom svete objavila už v 90. rokoch a na začiatku prvého desaťročia 21. storočia. Problémom, ktorý vo svojej dobe nebolo známe ako prekonať, bola otázka, ako vytvoriť nezávislú databázu, kde by mohli byť tieto dáta uložené. Nezávislosťou je myslená nezávislosť od centrálnej entity. Nájsť odpoveď sa podarilo osobe vystupujúcej pod identitou Satoshi Nakamoto, ktorý prišiel s myšlienkou distribouvanej databázy, známej aj pod názvom blockchain. Dôveryhodnosť tejto databázy nie je zabezpečovaná jednou centrálnou entitou, ale množstvom drobných účastníkov. Informácie uložené v databáze vďaka tomu nie sú závislé na jednej entite a používatelia môžu voľne interagovať medzi sebou navzájom.[7]

Technológia blockchain je možná pre technickú realizáciu myšlienok hnutia Moje dáta, ktorá je založená na digitálnej identite ako centrálnom prvku a pracuje s univerzálnym riešením, nezávislým na infraštruktúre alebo jedinej centrálnej organizácii. Technológia blockchain tiež dokáže zabezpečiť dôveryhodnosť údajov zdieľaných na základe princípov hnutia Moje dáta.[8]

3.2 Princípy služby Moje dáta

Služba Moje dáta je postavená na týchto základných princípoch:[9]

[6] https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/2e9b4eb0-68d7-463b-9460-821493449a63?version=1.0

[7] https://www.economist.com/special-report/2018/06/30/blockchain-technology-may-offer-a-way-to-re-decentralise-the-internet

[8] http://www.sytyke.org/ilmiot/mydata-and-blockchain-lead-to-a-smarter-society/

[9] https://mydata.org/declaration/

Osobné dáta pod kontrolou ľudí

Ľudia by mali byť pánmi nad svojimi údajmi ako v offline tak aj v online svete. Mali by mať k dispozícii praktické nástroje na kontrolovanie, kto má prístup k údajom o nich a ako sú tieto informácie používané a zdieľané.

Občan v centre diania

Občania by sa mali stať uzlami, cez ktoré sa bude dať dostať k dátam. Budú tak mať prehľad o všetkých súvisiacich dátach.

Posilnenie úlohy jednotlivca

Každý jeden občan by mal mať k dispozícii bezpečný nástroj na slobodné narábanie a spravovanie svojich dát.

Prenositeľnosť: Prístupnosť a znovu-použitie

Používateľ by mal mať praktické možnosti ako získať a znovu použiť svoje dáta v inej službe.

Transparencia a zodpovednosť

Organizácie by mali deklarovať na aký účel používajú dáta. Chovajú sa tiež zodpovedne k dôsledkom držania a používania osobných dát.

Interoperabilita

Používanie otvorených protokolov, API, technických štandardov, tak aby boli dáta prenositeľné a použiteľné medzi službami navzájom.

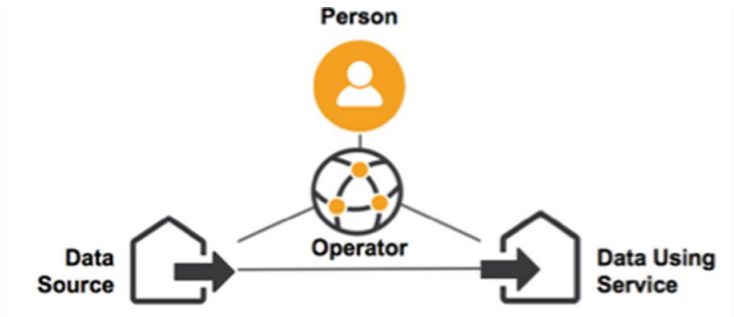
3.3 Prehľad technických riešení

Existuje viacero technických riešení pre manažment osobných údajov. V nasledujúcej časti predstavíme dva v súčasnosti najpokročilejšie prístupy k implementácii služby Moje dáta. Podrobnejšie sa tiež budeme venovať aplikáciám pre správu osobných údajov a pre správu digitálnych identít.

3.3.1 MyData.org

Organizácia MyData.org je centrálnym propagátorom myšlienky Mojich dát. Ich technické riešenie umožňuje používateľovi z jedného miesta pristupovať, spravovať a kontrolovať svoje osobné dáta. Používateľ má svojho operátora, ktorý realizuje prepojenie a zabezpečuje zdieľanie údajov medzi ostatnými hráčmi v ekosystéme (poskytovateľmi osobných dát a ich konzumentami).

Obrázok 3: Základné role v koncepte MyData.org



Základným komponentom tohto riešenia sú osobné účty MyData. Tieto účty sú štandardizované a prenositeľné medzi operátormi. Účet umožňuje jednotlivcovi ľahko kontrolovať svoje dáta z jedného miesta, nech sú vytvárané kdekoľvek. Účty MyData sú štandardne poskytované operátormi Moje dáta.

V koncepte MyData je oddelený prenos dát od prenosu súhlasov. Účelom MyData je hlavne sprostredkovať tok súhlasov, nie je nutné, aby boli osobné dáta uložené na serveroch operátorov. Komunikácia v systéme prebieha prostredníctvom štandardizovaných API. Toto umožňuje službám pracovať s dátami a používateľovi spravovať svoje dáta z jedného miesta. Cieľom je tiež umožniť preniesť si svoj účet od jedného operátora k druhému.

Výhody:

- Možnosť voľby, ktoré dáta, akej službe používateľ poskytne.
- Komplexné riešenie pre službu Moje dáta, vrátane navrhnutého štandardu API.
- Spravuje vitálna medzinárodná komunita, združená v MyData.org.

Nevýhody:

- Nie je otestované v masovom meradle.
- Vyžaduje aktívnu účasť používateľa na správe svojich dát.

3.3.2 OpenPDS

Ďalším spôsobom prístupu k technickému riešeniu služby Moje Dáta je model OpenPDS. Základným princípom tohto modelu je poskytovanie odpovedí. Mechanizmus SafeAnswers umožňuje aplikáciám klásť otázky, ktoré sú zodpovedané pomocou osobných údajov používateľa. Osobné dáta nie sú zdieľané, služba poskytne iba kód obsahujúci odpoveď na zadanú otázku.

Aplikácia, napríklad Fitness tracker, zašle otázku na Personal Data Store (PDS). Ten využije systém SafeAnswers na to, aby spravil výpočet nutný k získaniu odpovede. Dáta používateľa sú využité vo výpočte, ale prostredie PDS neopustia. Správa zaslaná od PDS obsahuje odpoveď na položenú otázku, ale nie dáta používateľa. Fitness aplikácia sa tak napríklad dozvie, či sa používateľ vyskytuje v určitej oblasti, ale nezíska všetky údaje z jeho GPS modulu. Tento prístup umožní používateľovi využívať personalizované služby aplikácie, ale zároveň zdieľať iba nutne potrebné informácie.

Zdroj: http://openpds.media.mit.edu

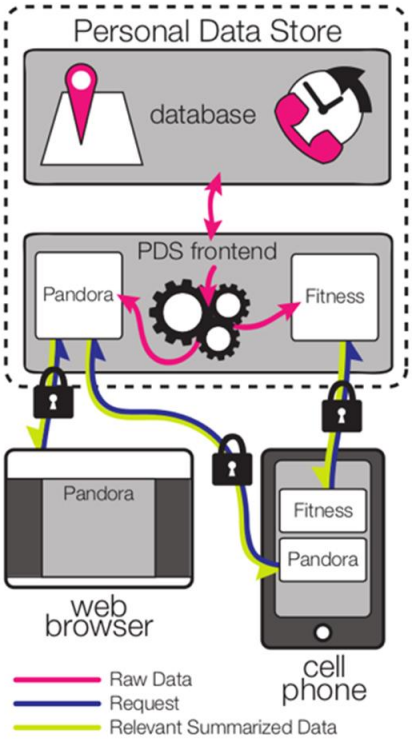
Výhody:

- Nie náročné na starostlivosť zo strany používateľa, služba sama minimalizuje zásahy do súkromia
- Množstvo poskytovaných dát je redukované, nie je poskytovaný celý dátový set používateľa

Nevýhody:

- Obmedzené na otázky a odpovede, limituje analýzy a činnosti, ktoré by cieľová služba mohla ponúknuť
- Náročnejšia technická implementácia, ktorá vyžaduje predefinovanie architektúry

Obrázok 4: Architektúra OpenPDS



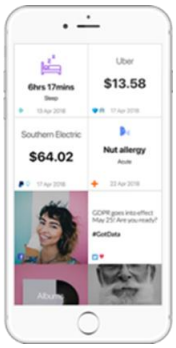
3.3.3 Aplikácie pre Moje dáta

V nasledujúcej časti sú predstavené najzaujímavejšie súčasné riešenia postavené na princípoch Moje dáta, ktoré slúžia ako systémy pre manažment osobných údajov alebo ako systémy pre manažment identít.

3.3.3.1 Systémy pre manažment osobných údajov (PIMS – Personal Information Management Systems)

Digi.me

https://digi.me/



Digi.me je aplikácia, ktorá dokáže zhromaždiť dáta používateľa zo sociálnych sietí, finančných, zdravotných, verejných, zábavným a ďalších služieb na jednom mieste. Aplikácia neukladá osobné dáta, ale funguje ako prostredník medzi používateľom a službami. Používateľ môže prostredníctvom tejto aplikácie pracovať so svojimi osobnými dátami v iných službám. Môže vo svojich dátach vyhľadávať a do budúcna ich bude môcť aj upravovať. Digi.me tiež umožňoje používateľovi preniesť svoje dáta medzi jednotlivými službami a tiež ponúkne možnosť vymieňať dáta s firmami za výhody.

CitizenMe

https://www.citizenme.com/

Aplikácia CitizenMe je založená na presvedčení, že používateľ by mal získať odmenu za zdieľanie svojich údajov. Aplikácia sa pripája k sociálnym účtom používateľa, získané informácie mu uloží do profilu a

potom mu umožňuje zdieľať svoje informácie ďalším stranám za odmenu. Zdieľanie prebieha prostredníctvom kvízov, kde používateľ poskytne časť svojich údajov a zodpovie kvízové otázky. V budúcnosti je plánovaný priamy predaj vlastných dát reklamným spoločnostiam a ďalším firmám.

PersonalData.IO

http://personaldata.io/

Personaldata.io je platforma, ktorá umožňuje občanom pristupovať k svojim dátam a pochopiť, ako sú využívané veľkými spoločnosťami. PersonalData.IO je súčasťou hnutia MyData a umožňuje občanom získať dáta od spoločností, ktoré spravujú ich dáta. Poskytuje návody ušité na mieru týmto spoločnostiam a ich predpisom a prevedie používateľa procesom, ako získať svoje dáta. Medzi spoločnosťami, od ktorých pomôže používateľovi získať dáta cez PersonalData.IO sú už teraz napríklad Facebook alebo Google.

3.3.3.2 Identita

Mooti

https://mooti.co/

Spoločnosť Mooti vytvorila nový štandard pre kryptografickú identifikáciu a validáciu. Na základe technológie blockchain, dokáže Mooti poskytovať digitálnu identitu, ktorá nebude závislá na centrálnej entite a bude zároveň zachovávať súkromie, bude bezpečná a použiteľná v rôznych oblastiach. Spoločnosti, ktoré potrebujú identifikovať svojich používateľov, môžu využiť služby Mooti a ponúknuť im digitálnu identitu so spomínanými výhodami.

https://www.crunchbase.com/organization/mooti#section-overview

Civic

https://www.civic.com/

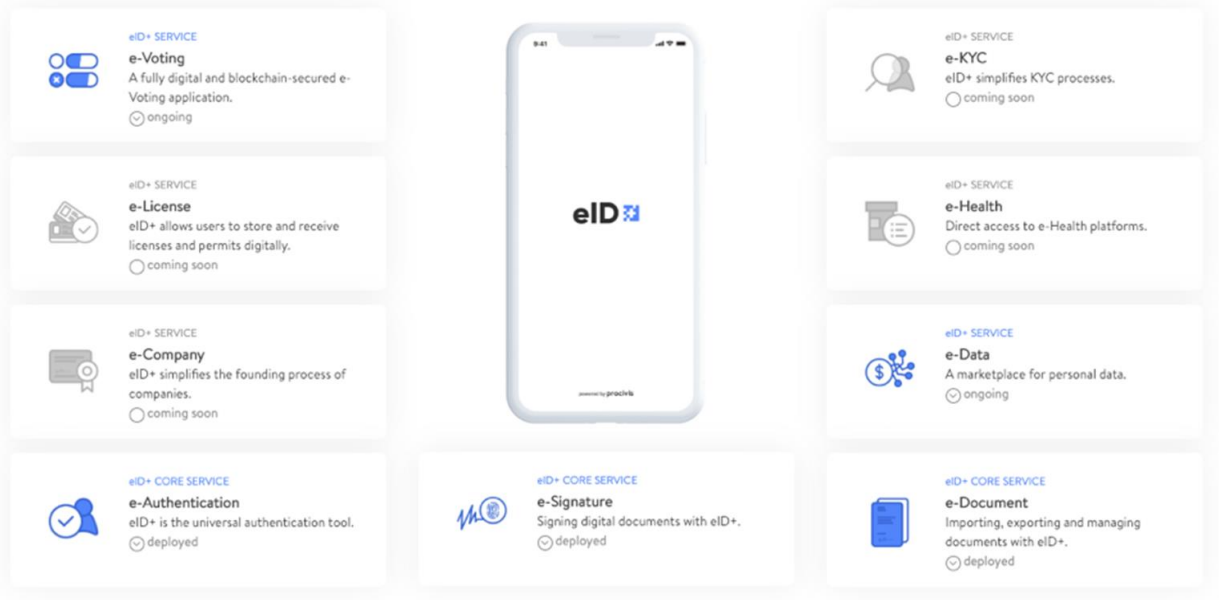
Civic je ďalšia služba, ktorá poskytuje používateľovi digitálnu identitu. Používateľ si do nej uloží svoje údaje a potom ich môže využiť na prístup k rôznym službám, kde nebude musieť znovu udávať a potvrdzovať svoje údaje. Príkladom je nákup letenky, používateľ svoje údaje poskytne prostredníctvom aplikácie a nebude ich musieť vypĺňať. Aplikáciu znovu využije pri check in na letisku, kde sa opäť prostredníctvom nej preukáže. Potvrdzovanie identity je postavené na technológii blockchain, čo umožňuje identitu a informácie o používateľovi mať uložené iba na používateľom zariadení.

Procivis

https://procivis.ch/

Procivis poskytuje digitálnu identitu obyvateľom švajčiarskeho kantónu Schaffhausen. Obyvatelia si môžu vytvoriť digitálnu identitu eID+, ktorá im prostredníctvom aplikácie umožňuje prístup k rôznym službám štátnej správy ale aj súkromných firiem. Prostredníctvom eID+ môže občan napríklad voliť na diaľku alebo podpisovať dokumenty. Ďalšie služby, ako založenie spoločnosti sú plánované. **Chyba! N enašiel sa žiaden zdroj odkazov.** ponúka prehľad služieb eID+.

Obrázok 5: Poskytované a plánované služby Procivis:



Tradle

https://tradle.io/

Tradle

Tradle buduje globálnu sieť, ktorá posilňuje dôveru medzi finančnými inštitúciami a ich klientami. V sieti na základe blockchain budú uložené informácie o klientoch a banky budú môcť pracovať s týmito informáciami ako overenými. Informácie budú zároveň uložené v podobe, v ktorej budú ľahko auditovateľné. Toto riešenie umožní bankám zamerať sa na svoje hlavné aktivity, namiesto trávenia času zisťovaním a overovaním informácií o svojom klientovi.

Banqu

https://banqu.co/

BanQu

Banqu poskytuje ekonomickú identitu ľuďom ktorý nemajú prístup k bankovým službám. Týchto je v súčasnosti 2,7 miliardy a napriek tomu, že sú ekonomický aktívny, vďaka ich nepriaznivej situácii, ako napríklad v prípade utečencov, nemôžu využívať bankové služby. Banqu im chce na základe blockchain poskytnúť ekonomickú digitálnu identitu, ktorá by zaznamenávala a ukladala informácie o ich ekonomickej aktivite v svetovom hospodárstve. Ekonomická identita poskytne týmto používateľom možnosť priamo sa zúčastniť vzťahov s globálnymi značkami, pre ktorých sú subdodávatelia. Umožní im

to tiež prístup k pôžičkám, pretože aj napriek tomu, že nemali bankové účty, budú mať preukázateľnú a overiteľnú hospodársku históriu.

Solid

https://solid.mit.edu

Projekt profesora Tim Berners-Leeho, ktorý chce zmeniť spôsob, ako fungujú webové aplikácie. Jeho cieľom je umožniť používateľom skutočne vlastniť svoje dáta. Solid je skratkou od Social Linked Data a svoje riešenie zakladá práve na princípoch prepojených údajov. Solid bude poskytovať:

- skutočné vlastníctvo dát. Táto vlastnosť je dosiahnutá oddelením dát od aplikácie, ktorá ich využíva,
- modulárny dizajn. Oddelenie aplikácií a dát, ktoré produkujú, zamedzí takzvanému uzamknutiu používateľov na platformách a umožní im voľne prechádzať medzi aplikáciami a osobnými úložiskami bez toho, aby stratili svoje dáta alebo kontakty,
- znovu požitie existujúcich dát. Dáta produkované jednou aplikáciou, budú môcť používať aj ďalšie aplikácie, čo poskytne priestor pre rozvoj nových inovatívnych služieb.

3.4 Skúsenosti so zavádzaním v zahraničí

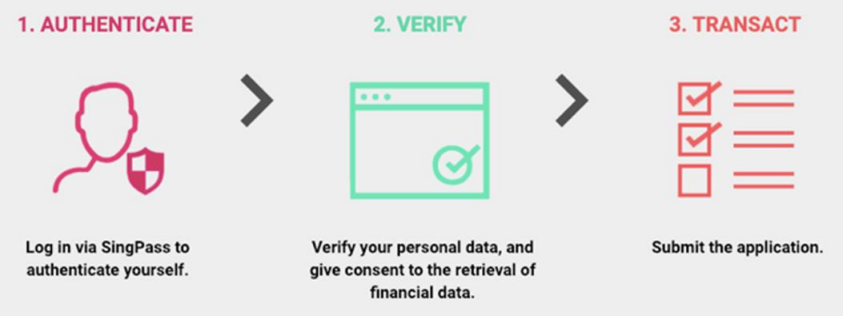
Dôležitým aktérom pri zavádzaní nových riešení na správu identity a manažment osobných údajov sú najmä vlády. Nasledujúci prehľad predstavuje najzaujímavejšie skúsenosti zahraničných vlád pri poskytovaní osobných údajov, zavádzaní personálnych asistentov ale aj skúsenosti s adresnými verejnými službami.

3.4.1 Identita a osobné údaje

Singapur MyInfo

Singapurské MyInfo je služba, ktorá šetrí čas rezidentov tím, že automatický vypĺňa vládne online e-formuláre. Služba je prístupná pre 3,3 milióna rezidentov, ktorý majú účet v prihlasovacom rozhraní SignPass.

Obrázok 6: Postup použitia singapurského MyInfo[10]



[10] https://www.singpass.gov.sg/myinfo/intro

V MyInfo účte sa vyskytujú vládou overené informácie ako napríklad meno, NRIC číslo a adresa, získané z rôznych inštitúcií. Keď užívateľ potrebuje vyplniť online formulár pre použitie egovernment služby, ako napríklad žiadosť o nový byť ale o príspevok na dieťa, môžu na formulári kliknúť na tlačidlo "získať informácie z MyInfo" a požadované informácie z profilu občana sa automaticky vyplnia do formulára.

Používateľ tak poskytne svoje osobné údaje vláde iba jedenkrát a tie sa potom používajú miesto toho, aby ich musel opakovane poskytovať pri každom ďalšom online kontakte so štátnou správou.

MyData je otvorený aj pre súkromný sektor. V pilote, ktorý sa realizoval v roku 2018 umožnili 4 banky automatické vypĺňanie žiadostí o nové účty a žiadosti o úvery pomocou MyData. V súčasnosti majú súkromné spoločnosti k dispozícii rozhranie, pomocou ktorého môžu zasielať požiadavky na MyData. Aby bolo ochránené súkromie občana, je každé zdieľanie údajov tretím stranám nutné potvrdiť jeho súhlasom. Ak súhlas neudelia, môžu pokračovať vo vypĺňaní žiadosti, akurát musia potrebné údaje vyplniť ručne.

Obrázok 7: Prehľad dát, ktoré sú k dispozícii v singapurskom MyData:[11]

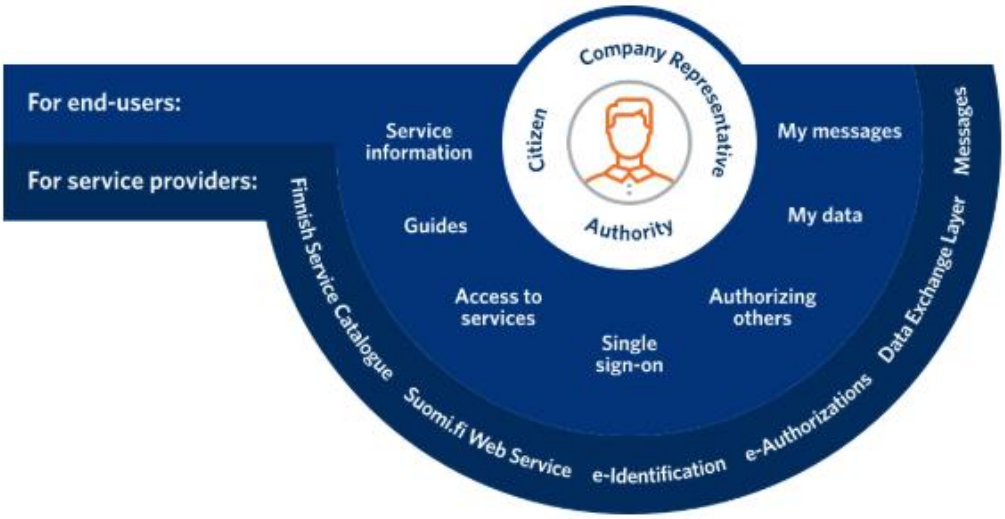
SUOMI.FI

https://esuomi.fi/?lang=en

[11] https://www.singpass.gov.sg/myinfo/intro

Suomi.fi je aktivita fínskej vlády, ktorá vytvára pre občana, verejný a súkromný sektor spoločnú platformu pre digitálne služby. Pomocou jedného prihlásenia a teda jednej digitálnej identity bude mať používateľ prístup do všetkých služieb na tejto platforme. Používateľom môže byť ako občan, tak aj súkromná alebo verejná organizácia. Platforma tiež umožní delegovať právomoci pri využívaní poskytovaných služieb na iných používateľov, napríklad pri podaní daňového priznania. Všetky tieto kroky prispejú k tomu, že komunikácia so štátnou správou sa výrazne zjednoduší. Súčasťou riešenia sú aj služba Moje dáta, ktoré umožňujú občanovi správu jeho osobných dát. Riešenie je práve v priebehu implementácie, po jej skončení bude hlavným kanálom pre občanov na získavanie informácii a komunikáciu so štátnou správou. Obrázok 8 poskytuje prehľad komponentov, ktoré Suimi.fi obsahuje.

Obrázok 8: Moje dáta ako súčasť Suomi.fi[12]



Data Exchange Layer X-tee

https://www.ria.ee/en/state-information-system/x-tee.html

X-tee je aktivita estónskej vlády. Ide o systém výmeny údajov, ktorý zabezpečuje, že úrady sú schopné medzi sebou zdieľať potrebné informácie. Nie je teda potrebné, aby tieto informácie poskytoval občan. Napríklad pri narodení dieťaťa zašle informačný systém nemocnice informáciu do registra obyvateľov, ktorý udelí občianstvo novonarodenému dieťaťu. Register obyvateľov následne informuje poisťovňu a dieťaťu je pridelené poistenie. Systém nie je závislý na tom, aký informačný systém je používaný v danej inštitúcii.

Základné vlastnosťami systému sú:

- Dáta sú ľahko prístupné tomu, kto ich potrebuje.
- Dáta môže zmeniť iba ten, kto má na to oprávnenie.
- Dáta sú počas svojho prenosu chránené pred neoprávneným použitím.

[12] https://esuomi.fi/?lang=en

Aadhaar

Pred rokom 2009 neexistoval spôsob, ako by bolo možné zaručene overiť identitu indických občanov. Jedným z dôsledkov bola vysoká korupcia, nebolo napríklad možné zistiť, kto má nárok na dávky, kto ich už dostal, kto ich ešte nedostal. Ako reakcia na tento stav bol vytvorený systém Aadhaar. Systém, ktorý každému záujemcovi poskytne identitu. Identita je poskytnuté ako reťazec 16 znakov a zahŕňa tiež fotku tváre, otlačky prstov a scany zorničiek. Systém slúži na overenie totožnosti občanov pre štátne inštitúcie a tiež má otvorené API, ktoré umožňujú oprávneným poskytovateľom služieb overiť totožnosť používateľa. Pomocou Aadhaaru môžu občania otvoriť získať príspevok v nezamestnanosti, otvoriť si bankový účet, požičať si bicykel, ale aj elektronicky podpisovať dokumenty. V súčasnosti je v ňom registrovaných 1,2 mld. ľudí a otvorené API na overenie identity mesačne využíva 500 000 používateľov.

Na základe, ktorý postavil systém Aadhaar, sú budované ďalšie systémy pracujúce s osobnými dátami. Jedným z nich je systém "Know your customer" fungujúci od roku 2012. Môžu ho používať banky a telefónne spoločnosti na overenie svojich zákazníkov. Platforma poskytuje jednoduchý, štandardizovaný a bezpapierový systém na overenie. V roku 2017 bolo na tejto platforme realizovaných 3,4 mld. overení. Ďalším súvisiacim systémom je rozhranie na jednoduché a zasielanie bankových platieb.

Všetky tieto služby produkujú dáta, ktoré je možné následne využívať. India je presvedčená, že poskytované systémy a v nich produkované dáta by mali slúžiť občanom. Aby mohli ľudia profitovať z dát, musia k nim mať prístup a možnosť kontrolovať ich. V Indii sú realizované 2 prístupy, ktoré poskytujú kontrolu používateľom:

- Prvým z nich je štandard na poskytovanie súhlasov s použitím dát. Jednoduchý, štandardizovaný digitálny formulár, ktorým používateľ dá súhlas k použitiu svojich dát a tiež môže rozhodnúť o ich šírení ďalej. Tiež môže kedykoľvek tento súhlas jednoducho odvolať.
- Druhým je vytvorenie role osobných správcov súhlasov, ktorých môže občan využiť pri aktivitách, ktoré vyžadujú zdieľanie dát. Správca sa postará o to, že dáta, ktoré občan potrebuje budú dostupné a poskytnuté s jeho súhlasom. V minulosti mali Indovia problém získať výpis z banky. Toto spôsobovalo komplikácie pri žiadosti o pôžičku, kedy boli na overenie svojej bonity nútení poskytnúť prihlasovacie údaje do internetového bankovníctva. Nemali kontrolu, čo sa tam potom s nimi deje. Vznikol preto systém, ktorý zbiera informácie o účtoch používateľa a na jeho požiadanie ich poskytne. Údaje, ktoré neboli dostupné, sú teraz dostupné pre všetkých a idú ľahko a kontrolovane zdieľať. Súkromie používateľa je zabezpečený tým, že správca dát má zakázané pristupovať k údajom používateľ a okrem toho je za každú transakciu zaplatený. Ďalší systém, ktorý vzniká, bude poskytovať overené informácie o pracovných skúsenostiach používateľa. Toto poskytne občanom lepšie podmienky pri vyjednávaní budúcej mzdy.[13]

3.4.2 Personálni asistenti

Prístup k osobným údajom z rôznych systémov umožňuje navrhovať nové typy adresných služieb. Jeden z hlavných spôsobov, ako ich využiť je prostredníctvom personálnych asistentov, ktorí dokážu riešiť životné situácie používateľov vďaka algoritmom umelej inteligencie.

[13] https://www.foreignaffairs.com/articles/asia/2018-08-13/data-people

Aurora – AI asistent pre verejný sektor

Aurora je projekt fínskeho digitálneho asistenta pre verejný sektor. Ten na základe umelej inteligencie, pochopenia situácie a potrieb občana navrhne používateľovi najvhodnejšiu službu. Pokroková je v tomto prípade snaha o pochopenie a analýzu potrieb používateľa.[14] Projekt je v súlade s heslom Fínska, že chcú vybudovať najlepšie verejné služby na svete.

Pilotný projekt Aurora začal v septembri 2018 a zameriava sa na tri špecifické scenáre: sťahovanie sa za štúdiom, zúčastnenie sa kurzov na zlepšenie šancí na nájdenie zamestnania a podpora detí a rodičov v zmenách rodinných vzťahov.[15]

Program AI osobný asistenta US Federálnej vlády

S virtuálnym asistentom experimentujú aj v USA. Tu sa v roku 2017 uskutočnil pilot na prepojenie virtuálnych asistentov ako Alexa, Siri, Cortana a ďalších s vládnymi službami, tak aby vedeli poskytovať informácie o verejných službách.[16]

3.4.3 Adresné služby

Midata v Spojenom Kráľovstve

Midata je iniciatíva v Spojenom Kráľovstve, ktorá umožňuje občanom získať informácie o ich spotrebe a finančných transakciách v strojovo čitateľnom formáte. Na ich základe dokážu napríklad aplikácie ponúkať spotrebiteľom tarify, ktoré sa im najviac hodia na základe vzorov ich spotreby. Iniciatíva spája súkromné spoločnosti, spotrebiteľské organizácie a vládu v roli regulátora (uvedený koncept sa nazýva Smart Disclosure).

Občan má od zapojených organizácií možnosť stiahnuť si prehľad svojej finančnej histórie a spotrebiteľských zvykov. Tento prehľad je generovaný v štandardnom formáte, ktorý bol odsúhlasený zúčastnenými stranami iniciatívy. Občan môže následne prehľad nahrať do aplikácií (porovnávačov), ktoré mú na základe jeho histórie odporučia najlepší produkt.[17] Služba, ktorá spotrebiteľovi odporučí pre neho najvýhodnejší účet bola spustený v roku 2015.[18] Ďalšie služby, ako napríklad výber najvhodnejšieho mobilného operátora budú nasledovať.

Built for Zero v USA

Built for Zero je program v USA, ktorý využitím dát pomáha štátu určiť, komu a aké presne služby štátu poskytnúť. V troch amerických mestách sa vďaka nemu podarilo výrazným spôsobom znížiť počet ľudí bez domova. V meste Abilene v Texase vďaka nemu zredukovali problém bezdomovectva z radov vojnových veteránov. Prvým krokom bolo získanie podrobných údajov o každom jednom občanovi, ktorého sa tento problém týka. Následne bola vytvorená pracovná skupina, ktorá pracovala so získanými dátami a hľadala nápady na riešenie problému. Riešenia sa hľadali obecné pre celú skupinu, ale aj na

---

[14] https://medium.com/@ODSC/meet-aurora-finlands-ai-assistant-answer-to-siri-and-alexa-f82b3f14b553

[15] https://www.zdnet.com/article/meet-aurora-finlands-ai-assistant-aims-to-give-each-citizen-tailored-advice/

[16] https://digital.gov/2017/04/24/federal-pilot-to-integrate-public-services-into-intelligent-personal-assistants/

[17] http://www.pcamidata.co.uk

[18] https://www.finextra.com/news/fullstory.aspx?newsitemid=27168

úrovni jednotlivcov na základe získaných dát. Jedným z riešení bola dohoda s prenajímateľmi bytov, že ľudia z tejto skupiny bude mať prednosť pri hľadaní ubytovania. Pracovná skupina na základe dát sledovala výsledky svojej snahy a upravovala svoj prístup. Po 10 mesiacoch sa im podarilo skrátiť čas, ktorý trvalo nájdenie ubytovanie veteránovi zo 40 dní na 26.[19]

3.5 Verejná správa a osobné údaje

Ako s údajmi narába štát dnes

Súčasný stav narábania štátu s dátami:

- Manažment údajov funguje len obmedzene pre inštitúcie, ktoré sú zapojené do CSRÚ a pre vybrané objekty evidencie ktoré sú prístupné všetkým inštitúciám verejnej správy cez portál over.si. Výsledkom je, že princíp "jeden krát a dosť" obmedzene v praxi funguje.
- Občan nevie, ako sú jeho osobné údaje zdieľané a kto mal k ním prístup. Vo všeobecnosti je prístup k vlastným údajom problematický (formálne, na základe GDPR). Implementácia všeobecného nariadenia o ochrane údajov prebehla, ale používateľom chýbajú technické nástroje pre uplatňovanie svojich práv.
- Absencia znalostí a expertov v oblasti dátovej vedy vo verejnej správe je výrazným limitujúcim faktorom pre prebiehajúci dátovú transformáciu organizácií. Najväčší analytický talent vo verejnej správe je momentálne na analytických útvaroch ako IFP, IZP, ISA, či UHP.
- Vyhlasovanie referenčných údajov je pomalé a prakticky sa zastavilo. Bude potrebné venovať zvýšenú pozornosť k rozbehnutiu tohto procesu.
- Procesy v inštitúciách nie sú nastavené pre využívanie možností „veľkých údajov“
- Nie sú definované jasné dátové štandardy. Kvalita údajov bola dlhodobo zanedbávaná.

Analytické spracovanie údajov vo verejnej správe nie je systematické. Kam sa môžeme posunúť

Zavedenie princípov služby Moje dáta a inšpirácia príkladmi zo zahraničia môže mať významné prínosy:

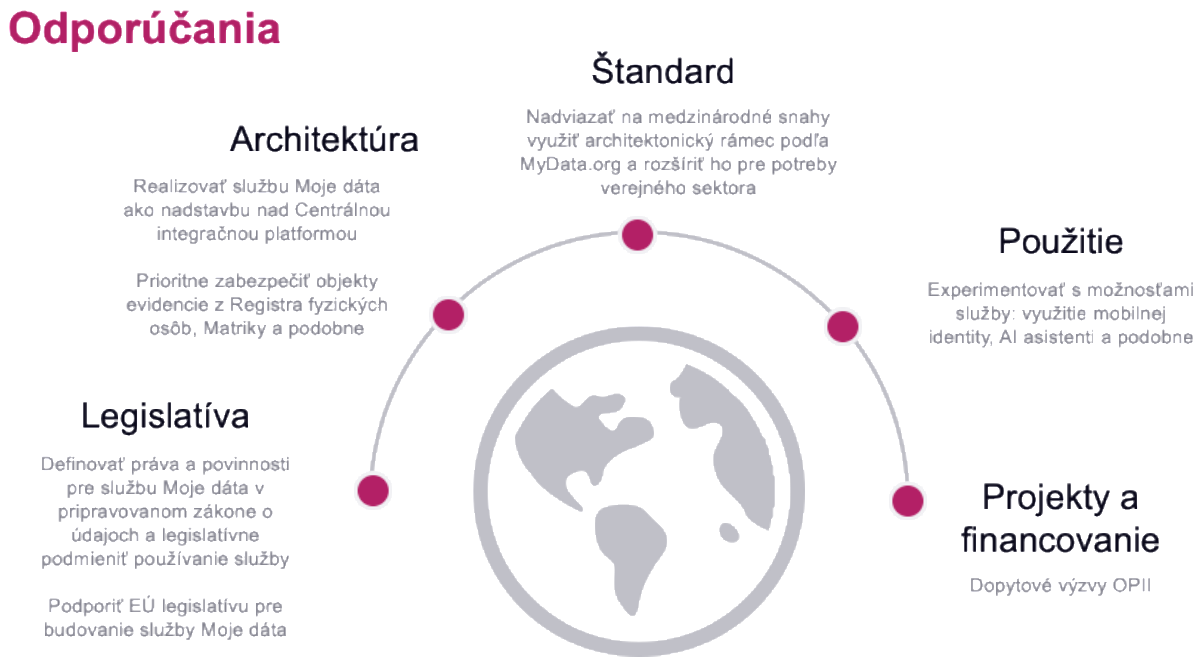
- Vytvorenie podmienok na elimináciu oznamovacích povinností a zavedenie proaktívnych služieb (vrátane implementácie pilotných riešení, čo povedie k výraznej debyrokratizácii štátu),
- Výrazne vyššia adopcia systémov pre manažment osobných údajov v populácií a s tým súvisiaci rast dátovej ekonomiky,
- Lepšia orientácia občanov vo svojich právach a povinnostiach,
- Vyriešenie kľúčových požiadaviek nariadenia GDPR v informačnom prostredí verejnej správy v rámci poskytovania a konzumácie údajov prostredníctvom CIP a MOU (pre zapojené inštitúcie do projektu),
- Výrazné zlepšenie prístupu k údajom pre inštitúcie verejnej správy a umožnenie systémového prístupu k dátam verejnej správy zo strany strategických neštátnych inštitúcií (finančný sektor, utilitné spoločnosti a podobne).

[19] https://www.fastcompany.com/90316607/3-cities-in-the-u-s-have-ended-chronic-homelessness-heres-how-they-did-it

3.6 Odporúčania pre SR

Formulácia odporúčaní pre potreby Slovenskej Republiky, aby sme dokázali implementovať navrhnutý koncept v praxi.

Obrázok 9: Prehľad odporúčaní



Legislatíva

- Definovať práva a povinnosti pre službu Moje dáta v pripravovanom zákone o údajoch a legislatívne podmieniť používanie služby vo verejnej správe, ako i v súkromnom sektore,
- Podporiť pripravovanú EÚ legislatívu pre budovanie služby Moje dáta,
- Využiť novelizácie zákona o eGovernmente, aby sa postupne koncept služby Moje dáta dostal do povedomia a umožnil riešiť reálne problémy.

Architektúra

- Nadviazať na medzinárodné snahy využiť architektonický rámec podľa MyData.org a rozšíriť ho pre potreby verejného sektora,
- Realizovať službu Moje dáta ako nadstavbu nad Centrálnou integračnou platformou,
- Prioritne zabezpečiť objekty evidencie z Registra fyzických osôb, Matriky a podobne, aby bolo jasné prepojenie s Identitou používateľa.

Použitie

- Použiť službu Moje dáta ako nástroj na riešenie problémov pri znižovaní byrokratickej a administratívnej záťaže, napríklad pri potvrdení o návšteve školy,
- Využiť už v súčasnosti dostupné dáta ako vstup pre službu Moje dáta a orientovať sa na vhodné prípady použitia.

- Experimentovať s možnosťami služby: využitie mobilnej identity, AI asistenti a podobne.

Projekty a financovanie

- Zabezpečiť dostatočné zdroje financovania pre prístup inštitúcií k službe Moje dáta a pre návrh adresných služieb, napríklad prostredníctvom dopytových výziev z OPII.

4 Architektúra služby Moje dáta

Architektúra služby Moje dáta je navrhnutá tak, aby umožnila:

- splnenie legislatívnych požiadaviek na prácu s osobnými dátami a teda zabránila nechcenému a nevhodnému nakladaniu s osobnými dátami používateľa,
- používateľovi ľahko poskytovať a odoberať súhlas na spracovávanie jeho osobných dát,
- upozornila používateľa formou notifikácie na spracovávanie jeho osobných dát,
- prinesenie transparencie pre používateľa o využívaní jeho dát.

Kapitola začína základnými definíciami, kde sú stanované pojmy ako súhlas a osobný účet služby moje dáta. Ďalej je spracovaný popis business pohľadu na funkcie služby Moje dáta, na ktorý následnej popis aplikačných komponentov. Sú vysvetlené scenáre použitia a tiež procesný pohľad na funkcionalitu služby.

4.1 Základné definície

Identita

Identitou používateľa je súbor atribútov, ktoré sú zaznamenané v elektronickej podobe a ktoré jednoznačne odlišujú jednu osobu od inej osoby na účely prístupu k službe Moje dáta. Identita osoby sa preukazuje identifikáciou osoby a overuje sa autentifikáciou osoby.

Objekt evidencie

V zákone o e-Govermente je objekt evidencie definovaný ako množina údajov o subjekte evidencie, ktorá je predmetom evidovania orgánom verejnej moci v rámci jeho pôsobnosti podľa osobitných predpisov a ktorá je jednoznačne identifikovaná identifikátorom objektu evidencie. Subjektom evidencie môže byť osoba, vec, právo, povinnosť alebo skutočnosť. Príkladmi subjektov evidencie sú Partnerský vzťah, dieťa, vozidlo, dom, zamestnanie, bankové údaje, vodičské oprávnenie. Vlastnosti týchto objektov (evidované údaje), ako napríklad miesto vydania vodičského oprávnenia alebo dátum jeho platnosti sú atribútmi objektu evidencie. Objekt evidencie je tvorený množinou všetkých jeho atribútov. Súhlas používateľa na prístup k jeho osobným dátam je udeľovaný na úrovni objektov evidencie.

Súhlas

Manažment súhlasov je hlavným mechanizmom povoľovania zákonného používania údajov. Prostredníctvom osobného účtu služby Moje dáta môže používateľ udeľovať súhlasy, na základe ktorých potom môžu služby spracovávať sprístupnené objekty evidencie. Súhlasy sú dynamické, jednoducho pochopiteľné pre používateľov, strojovo čitateľné, štandardizované a riadené koordinovaným spôsobom.

Súhlas obsahuje minimálne informácie o:

- Objektu evidencie ku ktorému je viazaný
- Časovej platnosti
- Adresátovi súhlasu - komu bol súhlas udelený
- Účel využitia dát

Užívateľ bude môcť udeliť súhlasy aj podľa účelu. Napríklad bude môcť poskytnúť svoj objekt evidencie na výskumné účely.

Bude existovať množina objektov evidencií, ktorá bude štandardne prístupná všetkým inštitúciám štátnej správy. Sem bude patriť napríklad meno, priezvisko a adresa trvalého bydliska. Pre ostatné informácie, ako napríklad daňové priznanie, bude občan udeľovať súhlasy. Súkromné inštitúcie nebudú mať štandardne prístup k žiadnym informáciám, na všetky im bude potrebné udeliť súhlasy.

Kontrakt

Predstavuje formu garancie prístupu k údajom, ktorá je udelená konzumentovi dát na základe jeho zákonného nároku. V prípade ak ma inštitúcia zákonný nárok na určite osobné údaje občana, nebude občan dávať súhlas na takého spracovávanie, ale prČostup bude umožnený automaticky v podobe kontraktu. Občan bude o každom takomto prístupe k údajom informovaný a bude môcť tiež môcť vzniesť námietku voči spracovávaniu.

Správu kontraktov bude vykonávať Úrad podpredsedu vlády SR pre investície a informatizáciu.

Log (záznam o prístupe)

Pri každom prístupe k objektom evidencie bude vytvorený záznam o tomto prístupe a používateľ si bude môcť si tieto prístupy prehliadať.

Log bude obsahovať informácie o:

- Osobe pristupujúcej k údajom
- Inštitúcie, súkromnej spoločnosti, do ktorej osoba pristupujúca k údajom patrí
- Dátume prístupu

Vzťah k údajom

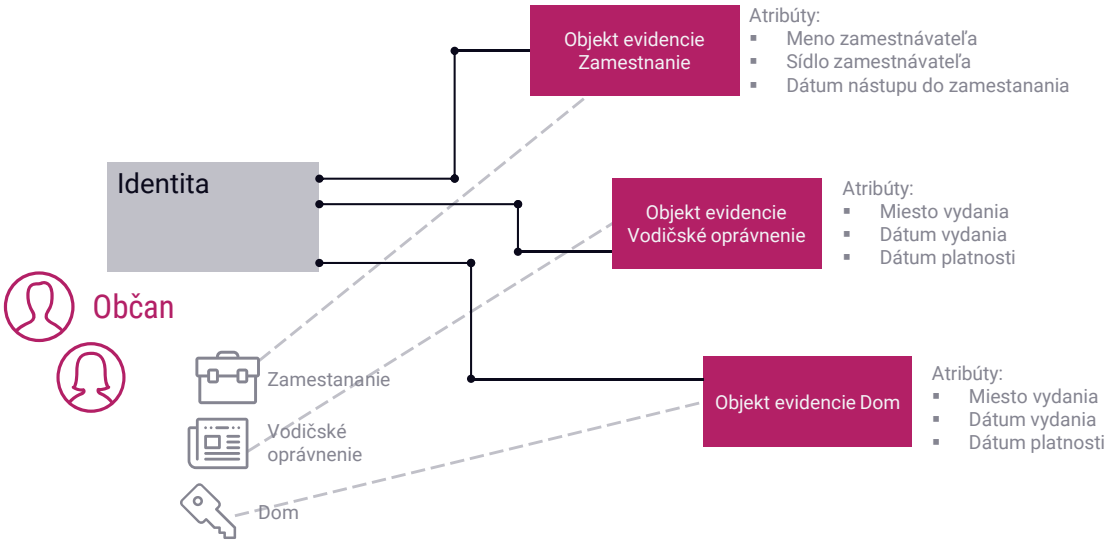
Vzťah medzi subjektom evidencie a objektom evidencie určuje úroveň, na základe ktorej môže používateľ pristupovať k dátam. Základným vzťahom k objektom evidencie je "môj", ide o údaje, ktoré sú o osobe, ktoré sa jej týkajú, ktoré sú o objektoch, ktoré sú jej vlastníctvom a podobne. Koncept Moje dáta počíta aj s ďalšími vzťahmi pre prípady použitia, ktoré vyplývajú najmä z legislatívy (napríklad zoznam parciel, pre ktoré som účastník stavebného konania). Pre možnosť prístupu k objektom evidencie, s ktorým používateľa spája určitý vzťah, ako definované v business službe Prístup k údajom je potrebná funkčnosť Registru vzťahov.

Tabuľka 1: Popis rolí v službe Moje dáta

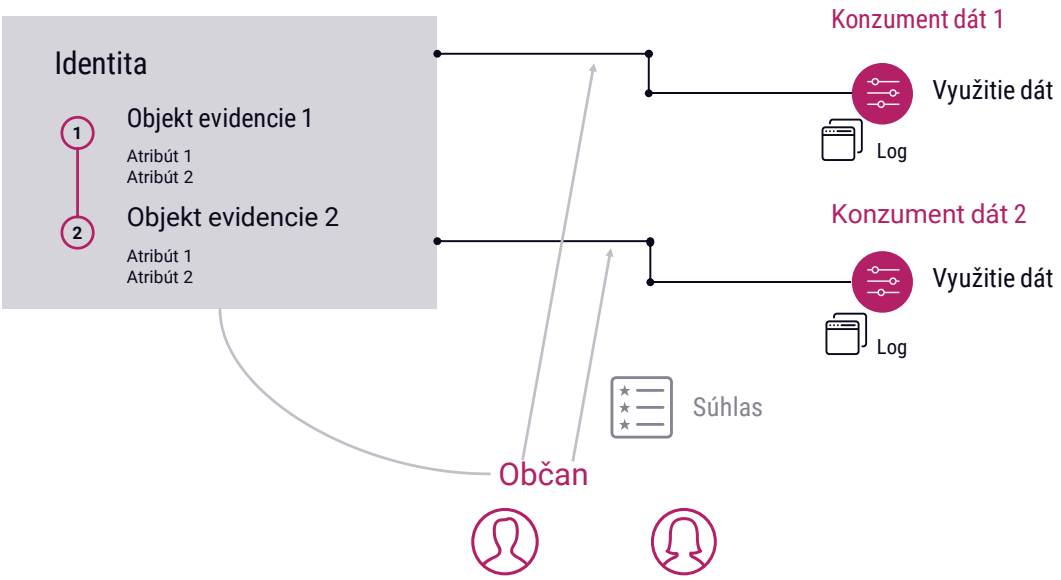
	Používateľ / Vlastník osobného účtu / Občan Osoba, ktorá používa Osobný účet služby Moje dáta na správu svojich osobných údajov
	Osobný účet Osobný účet obsahuje informácie o identite používateľa, pripojených službách a umožňuje mu správu prístupov k osobným údajom
	Operátor služby Moje dáta Hostí osobné účty používateľov, vykonáva požiadavky používateľa na služby, spravuje register služieb

	Služba Pristupuje k osobnými dátami používateľa
	Poskytovateľ dát Zdrojová služba, ktorá obsahuje osobné dáta používateľa a môže ich poskytnúť pre ďalšie služby
	Konzument dát (synonymom je aj spracovávateľ alebo spotrebiteľ dát) Spotrebiteľská služba, ktorá spracováva osobné dáta používateľa vzniknuté v iných službách
	Poskytovateľ a zároveň konzument dát Služba, ktorá zároveň vystupuje ako poskytovateľ a konzument dát

Obrázok 10: Identita a objekt evidencie

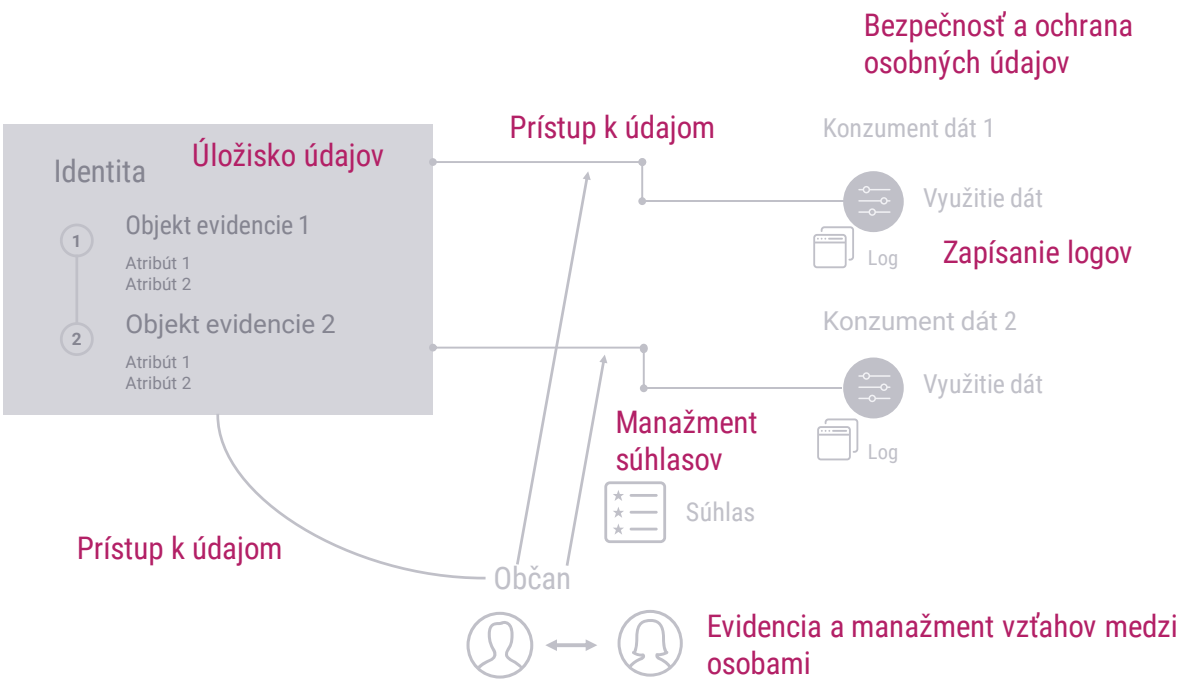


Obrázok 11: Súhlasy a logy



4.2 Služby

Obrázok 12: Business služby



Prístup k údajom

Občan, ako používateľ, má prístup k všetkým svojim dátam, ktoré sú v službe Moje dáta prepojené s jeho identitou. Môže si zobraziť všetky elektronické údaje, ktoré o ňom eviduje štát, prípadne prepojené tretie strany, a prehľadným spôsobom v nich vyhľadávať.

Štátnym úradom služba umožňuje pristupovať k osobným informáciám občana, ktoré potrebujú na realizáciu svojich agiend. Prístup k údajom sa deje na základe udeleného súhlasu alebo kontraktu. Inštitúcie verejnej správy na základe kontraktu získavajú prístup k údajom, na ktorý majú zákonný nárok a na prístup k údajom, na ktorý tento zákonný nárok nemajú, potrebujú získať súhlas občana. Občan tak vďaka službe Moje dáta nemusí absolvovať cestu na úrad.

Služba Moje dáta bude slúžiť aj pre zdieľanie osobným údajov s tretími stranami zo súkromného sektora, ako sú napríklad banky, energetické spoločnosti a ďalšie. Zdieľanie mu umožní, že nebude musieť spoločnostiam poskytovať informácie, ktoré už sú o ňom evidované v službe Moje dáta a tiež na základe dát, ktoré poskytne získavať služby prispôsobené mu na mieru. Poslednou možnosťou občana bude zdieľanie dát spoločnosti, aby ich bude môcť využiť na svoje účely. Toto zdieľanie bude prebiehať za poplatok, občan dostane zaplatené.

Ďalším vývojom služby Moje dáta bude možnosť zahrnutia osobných analytických funkcií. Občan tak bude môcť prostredníctvom tejto služby vidieť aj to, čo o ňom jeho údaje hovoria.

Primárne informácie, ku ktorým bude občan pristupovať sú jeho osobné dáta. Služba Moje dáta mu umožní pristupovať aj k dátam, ku ktorým má určitý vzťah. Sú to tieto dáta:

- Dáta osoby, ktorej je používateľ zákonným zástupcom
- Dátach rodinných príslušníkov
- Dátach registrovaných partnerov
- Objekty evidencie, ku ktorým ma občan prístup z titulu účastníka konania

Vyššie uvedené dáta budú sprístupnené na základe zákonného nároku, alebo na základe prístupov definovaných prostredníctvom business služby Evidencia a manažment vzťahov medzi osobami.

Služba Moje dáta bude obsahovať aj informácie právnických osôb. K týmto údajom bude mať prístup oprávnená osoba.

Manažment súhlasov

Manažment súhlasov zabezpečuje kontrolu občana nad osobnými údajmi. Manažment súhlasov slúži na správu súhlasov k prístupom k dátam v systéme. Umožňuje udeľovať a odoberať súhlasy a tiež zobraziť aktuálne udelené súhlasy. Poskytnuté súhlasy umožňujú konzumentom údajov pristupovať k osobným dátam používateľa. Služba tiež umožňuje konzumentovi údajov požiadať o prístup k osobným údajom občana, úrad tak môže učiniť ako reakciu na určitú udalosť alebo životnú situáciu občana.

Nesprávne nastavenie súhlasov so sebou prináša riziko pre používateľa a je preto dôležité, aby bol systém efektívny a užívateľsky prívetivý. Ak je udelený súhlas alebo spracovávanie údajov podozrivé, dôjde k upozorneniu používateľa, prípadne bude spustený ľudský zásah na strane systému.

Evidencia a manažment vzťahov medzi osobami

Riešenie umožní evidovanie vzťahov medzi fyzickými osobami a umožní tak podporiť napríklad evidenciu zákonného zastupovania pre občanov SR (v rámci projektu sa overí takáto funkcionalita a jej možnosti, samotné riešenie zákonného zastupovania je mimo rozsahu projektu). Ďalšou funkciou tejto business služby je udelenie splnomocnenia na ďalšie osoby na prístup k objektom evidencie.

Úložisko údajov

Používatelia, ktorí budú mať záujem si budú môcť svoje dáta ukladať v osobnom úložisku. Budú môcť použiť niektorú z cloudových služieb ako Google drive, Dropbox, Onedrive a podobne. Využitím

vlastného úložiska budú mať používatelia dáta k dispozícii podľa potreby a nebudú musieť čakať na vstupy z informačných systémov, ktoré sú poskytovateľmi údajov. Tieto dáta budú z osobného úložiska k dispozícii aj konzumentom údajov.

Občan si bude môcť na úložisku ukladať okrem objektov evidencie aj rozhodnutia štátu, osobné doklady a ďalšie údaje.

Zapísanie logov

Účelom služby zapísanie logov je transparentnosť a sledovateľnosť osobných údajov. Služba Moje dáta bude poskytovať informácie o prístupoch k dátam občana. Bude sa tak diať v prípade keď sa dáta nebudú nachádzať v informačnom systéme konzumenta dát a ten k nim bude pristupovať prostredníctvom služby Moje dáta. Evidované bude, kto, prečo a za akým účelom k objektom evidencie pristupoval. Systém bude zobrazovať informácie o prístupoch v prehľadnej forme a bude používateľovi poskytovať možnosť vyhľadávania.

Používateľ bude tiež informovaný v prípade podozrivej aktivity dejúcej sa s jeho dátami. Jednou z takýchto podozrivých aktivít je využitie dát na iný účel, než na aký boli poskytnuté.

Bezpečnosť a ochrana osobných údajov

Služba bude zabezpečovať integritu, pravosť a dôveryhodnosť poskytovaných údajov. Je dôležité, aby dáta získané a spracovávané prostredníctvom služby Moje dáta zodpovedali zdrojovým dátam v príslušných informačných systémoch.

Na ochranu údajov bude využitá šifrovanie a kryptografia. Šifrovane zabezpečí, aby dáta mohla čítať iba oprávnená osoba. Systém zabezpečí overenie totožnosti konzumenta a taktiež zhodu s povoleným a deklarovaným účelom využitia dát. Kryptografické metódy zabezpečia integritu a dôveryhodnosť údajov v systéme.

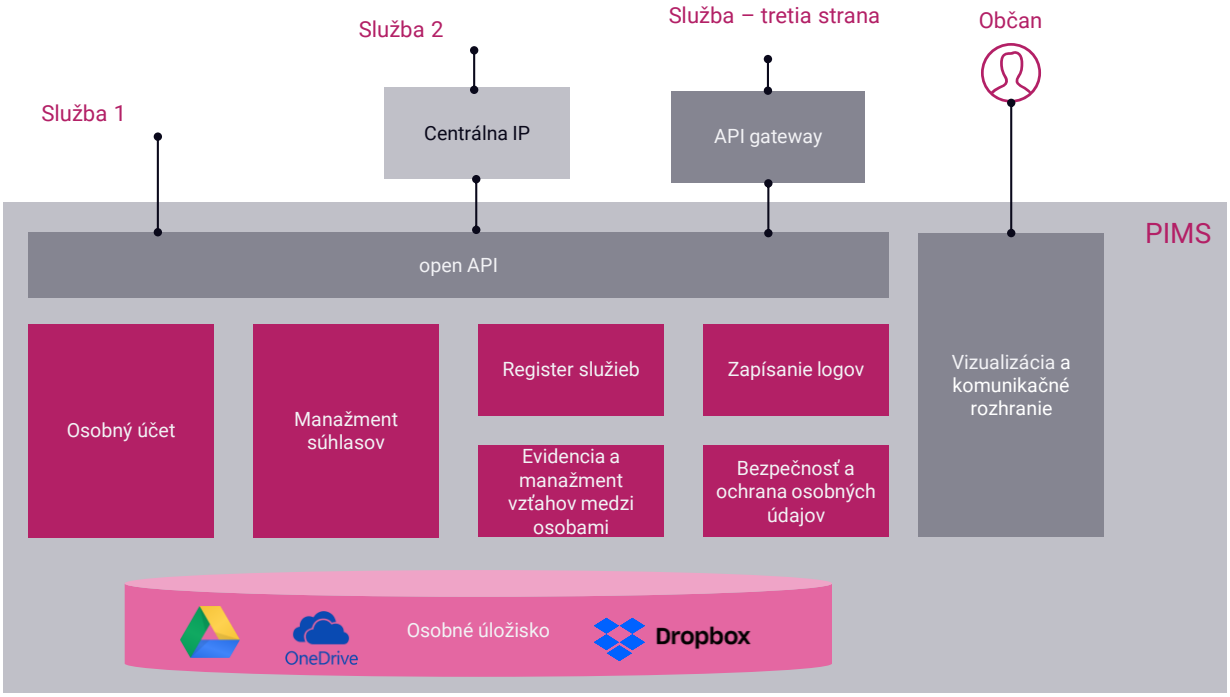
4.3 Aplikačné komponenty

Aplikačná architektúra predstavuje technický pohľad na riešenie. Riešenie pre Manažment osobných údajov je postavené na princípoch referenčnej architektúry pre Moje dáta[20][21]. Riešenie je otvorené a umožňuje cez otvorené API pripojiť ľubovoľný Systém pre manažment osobných údajov (PIMS), ktorý spĺňa požiadavky tejto architektúry. PIMS sú prevádzkované operátormi a jeden z operátorov bude vybudovaný nad Centrálnou integračnou platformou.

[20] https://hiit.github.io/mydata-stack/stack.html

[21] https://research.aalto.fi/files/17076008/MyData_Architecture_Framework_2.0.pdf

Obrázok 13: Architektonický rámec pre Moje dáta



Samotná aplikácia PIMS (nazývaná aj My data operation stack) umožňuje obsluhovať identitu používateľa, riadiť prezeranie údajov a riadiť ukladanie údajov. Identita používateľa je manažovaná v osobnom učte, kde je prepojená so všetkými objektami evidencie a súhlasmi, ktoré sa jej týkajú. Osobný účet tak obsahuje informácie o poskytovateľoch údajov prepojených k identite používateľa, to znamená kde (v ktorom informačnom systéme (IS)) sa nachádzajú súvisiace objekty evidencie. Register služieb obsahuje aktuálne definície služieb (poskytovateľov aj konzumentov údajov), umožňuje objavovanie nových služieb a registráciu takýchto služieb. Manažment súhlasov umožňuje riadiť prístup k objektom evidencie pre konzumentov dát (informačné systémy verejnej správy, aplikácie tretích strán) na základe súhlasov používateľa a je to kľúčový modul v tomto kontexte. Zabezpečuje pridávanie a odoberanie súhlasov pre používateľa - vlastníka osobného účtu. Obsahuje tiež rozhranie, pomocou ktorého môže potencionálny konzument dát požiadať o pridelenie súhlasu. Prístupy k objektom evidencie používateľa sú evidované v module Zapísanie logov. Tento modul tiež notifikuje používateľa v prípade rizikových alebo podozrivých prístupov k jeho údajom. Modul evidencie vzťahov medzi osobami umožňuje evidovať vzťahy medzi rôznymi používateľmi a ich identitami prostredníctvom definovaných rolí. Používateľ používa Moje dáta cez Modulu vizualizácia a komunikačné rozhranie, ktorý tiež slúži na zobrazenie dát. Všetky operácie, ako napríklad prístup k objektom evidencie, sú zabezpečené prostredníctvom Open API. Ak konzument dát získa súhlas od používateľa osobného účtu, môže sa prostredníctvom Open API pripojiť do zdrojového IS systému a tieto informácie ďalej použiť. Táto udalosť sa zapíše do transparentného logu. V prípade, ak má používateľ záujem, môže si svoje dáta uložiť do osobného úložiska, kde budú k dispozícií pre ďalšie použitie. Takéto riešenie zvyšuje rýchlosť prenosu informácií a znižuje záťaž na zdrojový informačný systém. Dôveryhodnosť identity a údajov bude zabezpečovať modul Bezpečnosť a ochrana osobných údajov.

Pre Informačné systémy verejnej správy bude komunikačný kanál a dátovú integráciu zabezpečovať Centrálna integračná platforma.

Open API

Koncept Mojich dát je postavený na otvorenom API (Open API) a sú definované presné funkcie (respektíve webové služby v aplikačnej architektúre) pre jednotlivé operácie. API poskytne údaje vo strojovo čitateľnom formáte a tiež umožní poskytovateľom údajov a konzumentom údajov vymieňať si informácie s osobným účtom.

Štandard Open API pre Moje dáta bude postavený na nasledujúcich štandardoch:

- MyData (https://github.com/mydata-sdk/mydata-docs/tree/master/architecture_specs)
- Identifikácia: OpenID Connect (https://openid.net/connect/)
- Autentifikácia: UMA – User Managed Access (https://kantarainitiative.org/confluence/display/uma/Home)
- API: Oauth 2.0 (https://oauth.net/2/)

API pre moje dáta bude dostupné cez platformu dátovej integrácie (rovnaké pre všetky typy údajov) a bude slúžiť ako proxy pre pripojené informačné systémy verejnej správy. API budú mať rovnakú funkčnosť pre všetky typy údajov. API môžu implementovať:

- zdrojové informačné systémy,
- konzumenti údajov,
- Centrálna integračná platforma (ktorá zabezpečí prístup k údajom jednotným spôsobom),
- A v najširšej podobe jednotlivé PIMS (pričom sa počíta s vytvorením PIMS ako nadstavbou nad CIP).

Cez navrhnuté Open API budú komunikovať jednotlivé systémy a PIMS a bude tak možné implementovať jednotlivé scenáre použitia (vyžiadanie prístupu k dátam, overovanie súhlasov, udeľovanie súhlasov, vyžadovanie súhlasov, prístup na základe zmluvy, notifikácia použitia dát, zápis údajov o prístupe do transparentného logu).

Za základný scenár je možné považovať prístup konzumenta k objektu evidencie. Konzument pristupuje k API a pýta si objekt evidencie. V module osobný účet sa musí overiť nárok takéhoto prístupu, či už na základe kontraktu, udeleného súhlasu alebo sú údaje verejne dostupné. V prípade, že súhlas neexistuje, generuje sa notifikácia, na ktorú môže reagovať používateľ osobného účtu.

Osobný účet

Osobný účet je základným modulom systému. Ide o kľúčový nástroj pre používateľa, ktorým môže byť informovaný o svojich osobných údajoch a riadiť ich spracovanie, ako i prístup, logovanie a súhlasy medzi rôznymi poskytovateľmi a konzumentami údajov. Osobný účet udržuje záznam o používateľových súhlasoch, notifikáciách, námietkach a ďalších relevantných informáciách. Znamená to, že osobný účet predstavuje jednotný pohľad nad transakciami spracovania osobných dát.

Osobný účet obsahuje:

- základné informácie o používateľovi,
- digitálnu identitu, prostriedky autentifikácie a autorizácie, verejné a privátne kľúče,
- a odkazy na pripojené objekty evidencie (cez registrované služby).

Cez odkazy na pripojené objekty evidencie je možné vedieť adresu služby v rozhraní dátovej integrácie. Znamená to, že osobný účet zabezpečí mechanizmus výmeny informácií medzi konzumentom a poskytovateľovom spôsobom, aby bolo možné bezpečne zdieľať osobné údaje. Osobný účet tak dokáže rozhodnúť, ktorí konzumenti majú prístup k daným objektom evidencie. V prípade, ak konzument

údajov nemá udelený súhlas na požadovaný objekt evidencie, môže tento získať prostredníctvom modulu Manažment súhlasov. Samotné dáta z objektov evidencie sa v osobnom účte nenachádzajú. Dôležitá požiadavka na osobný účet je, aby boli informácie uložené vo formáte, ktorý umožňuje ľahkú prenositeľnosť medzi rôznymi operátormi služby Moje dáta.

Manažment súhlasov

Modul manažment súhlasov slúži na správu súhlasov, ktoré predstavujú explicitné pravidlá, na základe ktorých môže užívateľ povoliť respektíve obmedziť prístup konzumentov dát k svojim údajom. Obsahuje funkcionalitu, potrebnú pre tvorbu súhlasu, ako i jeho modifikáciu, respektíve zrušenie. Užívateľ si môže robiť prehľady svojich súhlasov prostredníctvom nadhľadov. Môže udelené súhlasy meniť, prípadne odoberať. Tiež mu modul umožňuje prideľovať nové prístupy. V prípade ak konzument potrebuje pristúpiť k objektu evidencie, ku ktorému nemá prístup alebo za iným účelom, než má odsúhlasený, užívateľ je o tomto používateľ notifikovaný a má možnosť potrebný súhlas udeliť alebo zamietnuť. Manažment súhlasov tiež umožňuje udeliť súhlas, ktorý nie je viazaný na konkrétnu službu, ale umožňuje pristupovať k anonymizovaným dátam napríklad za účelom vedeckého využitia. Súhlasy je tiež možné používať ako splnomocnenia.

Súhlasy sú definované ako dynamické, ľahko pochopiteľné, strojovo čitateľné a štandardizované. Spoločný formát umožní každému jednotlivcovi delegovať spracovanie údajov na tretie strany.

Register služieb

Služby, ktoré sa týkajú identity sú spracované v registri služieb. Nachádzajú sa tu definície rozhraní poskytovateľov dát pre prístup k objektom evidencie. Register služieb tiež obsahuje zoznam konzumentov údajov, ktoré majú právo pristupovať a pracovať v systéme Moje dáta.

Register služieb obsahuje funkcionalitu:

- Pre popis služieb (konfigurácia služby, popis v čitateľnom formáte, popis účelu, popis spracovania, popis notifikácií),
- Registrácia služieb (jednoznačný identifikátor URI),
- Pre objavovanie služieb (Service Discovery).

Zapísanie logov

V momente, keď dôjde konzumentom dát k prístupu k objektu evidencie, ktorý sa nenachádza v jeho informačnom systéme, je o tomto prístupe vytvorený auditovateľný záznam. Tieto záznamy sú vytvárané v module zapísanie logov. Log sa bude vytvárať pri každom čítaní, alebo zmene daného objektu evidencie. Formát logu a pravidlá jeho tvorbu budú rovnaké v celej verejnej správe. Log bude uložený lokálne v IS systéme poskytovateľa a tiež konzumenta dát a bude službe Moje dáta k nemu umožnený prístup alebo bude ukladaný v službe moje dáta prostredníctvom služby zapísanie logov. Budú evidované aj také prístupy k objektom evidencie, pre ktoré nie je potrebný súhlas používateľa, čiže na základe kontraktu.

Prístupy je možné prehľadne zobraziť a modul upozorňuje používateľa na podozrivé aktivity.

Evidencia a manažment vzťahov medzi osobami

Modul zabezpečuje evidenciu vzťahov medzi identitami v službe Moje dáta. Jednotlivé vzťahy sú tvorené:

- súvisiacou identitou,

- rolou, v akej sa súvisiaca identita nachádza a časovým rámcom platnosti,
- súborom oprávnení vo vzťahu k súvisiacej identite (splnomocnenia).

Evidencia a manažment vzťahov medzi osobami umožňuje realizáciu zákonného zastupovania osôb.

Vizualizácia a komunikačné rozhranie

Modul slúžiaci ako komunikačné rozhranie pre používateľa. Prostredníctvom komunikačného rozhrania je možné ovládať ostatné komponenty a vizualizácia zobrazuje a interpretuje objekty evidencie prehľadným ľudsky čitateľným spôsobom. Modul tiež poskytuje nástroje na vizualizáciu informácií uložených v ostatných moduloch.

Osobné úložisko

Osobné úložisko ponúka používateľovi možnosť uložiť si svoje dáta (obsah objektov evidencie) na osobnom externom úložisku. Môže tak mať na jednom mieste uložené objekty evidencie, ktoré sa nachádzajú v rôznych informačných systémoch a stadiaľto môžu byť poskytované konzumentom údajov, ktoré k nim majú schválený prístup. Údaje ukladané v úložisku údajov budú spracovávané v interoperabilnom, strojovo čitateľnom formáte, umožňujúcom interakcie bez zásahu človeka. Komponent osobné úložisko sa tiež postará o to, že uložené dáta budú aktuálne. Dôveryhodnosť uloženým a následne poskytovaným dátam zabezpečí komponent bezpečnosť a ochrana osobných údajov.

Jednou zo základných požiadaviek na riešenie služby „Moje dáta“ je, že systém musí byť vhodne navrhnutý systém tak, aby neobmedzoval záťaž ostatných zdrojových informačných systémov verejnej správy. Využitie osobných úložísk môže výrazne pomôcť naplneniu tejto požiadavky.

Bezpečnosť a ochrana osobných údajov

V službe moje dáta sa bude vyskytovať množstvo dôverných informácií, ktoré je potrebné ochrániť proti zneužitiu. O túto funkcionalitu sa bude starať komponent bezpečnosť a ochrana osobných údajov. Bude overovať identitu používateľov, služieb a operátorov. Bude tiež garantovať dôveryhodnosť a konzistentnosť dát poskytovaných konzumentov údajov a tiež tých uložených v osobnom úložisku používateľa, tak aby dáta zodpovedali dátam v zdrojovom systéme a nebolo možné ich svojvoľne meniť.

Centrálna integračná platforma

Pre IS zapojené do Centrálnej IP to bude táto platforma, ktorá bude sprostredkovávať pripojenie do služby Moje dáta. Bude slúžiť ako rozhranie medzi Open API a informačnými systémami služieb a poskytne systémom rovnaké možnosti, ako keby sa napájali prostredníctvom Open API. Pre funkčnosť mojich dát je dôležité, aby poskytovatelia údajov rozšírili svoju integráciu tak, aby bola schopná využívať službu Moje dáta.

API gateway

API gateway sprostredkúva pripojenie do služby Moje dáta pre tretie strany, ktoré nie sú orgány štátnej správy. Služby budú môcť pristupovať do služby Moje dáta na základe registrácií u operátorov služby Moje dáta.

Systémy tretích strán

Štandardizované API poskytované prostredníctvom API Gateway môžu riadeným spôsobom používať aplikácie tretích strán. Dá sa predpokladať, že veľké množstvo benefitov manažmentu osobných údajov

zabezpečí použitie osobných dát v aplikáciách tretích strán, ktoré tak dokážu priniesť výraznú hodnotu pre používateľov a personalizované služby

4.4 Scenáre použitia služby Moje dáta

Prístup konzumenta dát k údajom používateľa, ku ktorým nemám prístup

Udelenie súhlasu, zamietnutie prístupu

Konzument dát (Úrad, 3. strana) potrebuje získať informácie, ktoré ma poskytovateľ dát a zatiaľ k nim nemá prístup. Konzument dát pošle požiadavku na používateľa. Uvedie do nej aké dáta potrebuje, za akým účelom, v akej dobe a či jednorazovo alebo kontinuálne. V prípadoch, ktoré to nutne nevyžadujú je preferovaný jednorazový prístup k dátam. Používateľ môže s použitím súhlasiť alebo ho zamietnuť. V prípade, ak používateľ udelí službe súhlas, tento je zaevidovaný v osobnom účte používateľa a operátor umožní konzumentovi dát za daných podmienok pristupovať k údajom produkovaným poskytovateľom dát. V prípade, ak používateľ neudelí súhlas, konzument dát nebude môcť pristúpiť k osobným údajom Občana prostredníctvom služby moje dáta. Buď k poskytnutiu dát nedôjde vôbec, alebo prebehne inou cestou.

Konzument dát chce zmeniť svoje oprávnenie

Zmena súhlasu, nesúhlas

Konzument dát má prístup k údajom používateľa, ale chce zmeniť niektorý z parametrov tohto prístupu. Chce napríklad dáta využiť za iným účelom alebo zmeniť množinu dát, ku ktorým má prístup. V takomto prípade príde používateľovi žiadosť o udelenie súhlasu so zmeneným použitím dát. Používateľ má znovu možnosť súhlasiť, prípadne zmenu zamietnuť.

Konzument dát pristúpil k dátam

Notifikácia

V momente, keď konzument dát pristúpil k dátam, ku ktorým má udelený súhlas, je generovaný log o tomto prístupe. Používateľ ma možnosť zobraziť si notifikácie o prístupoch k jeho osobným dátam.

Objavovanie, pridávanie konzumentov dá používateľom

Pridanie 3. strany

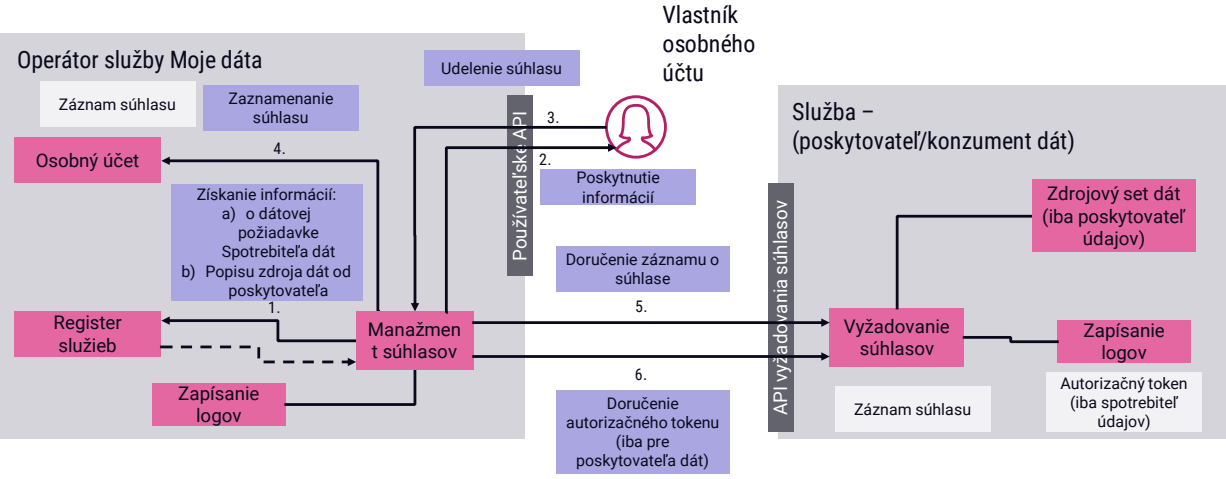
Občan má možnosť sprístupniť svoje dáta aj konzumentom dát, ktorý nie sú zo štátnej správy. Používateľ

môže tieto služby objaviť prostredníctvom Registra služieb, ku ktorému má prístup cez PIMS, prípadne môže služby tretích strán nájsť na iných miestach, napríklad v médiách. V prípade, ak ma záujem poskytnúť svoje informácie tejto službe, skontaktuje sa s ňou spôsobom uvedenom v registri služieb. Jedným zo spôsobov môže byť napríklad aplikácia. Tu si zvolí o aký produkt ma záujem a na základe neho, mu služba prostredníctvom služby Moje dáta zašle žiadosť o udelenie súhlasu na použitie dát.

4.5 Popis spracovania

Spracovanie súhlasu so spracovaním dát

Obrázok 14: Súhlas so spracovaním dát konzumentom údajov



Súhlas so spracovávaním prebieha v 6. krokoch:

1. Zistenie informácií, ktoré potrebuje konzument dát, popisu zdroja informácií

2. Predstavenie informácií používateľovi

3. Používateľ určí pravidla spracovania dát, udelený súhlas musí splniť minimálne požiadavky konzumenta dát inak nebude prebiehať spracovanie

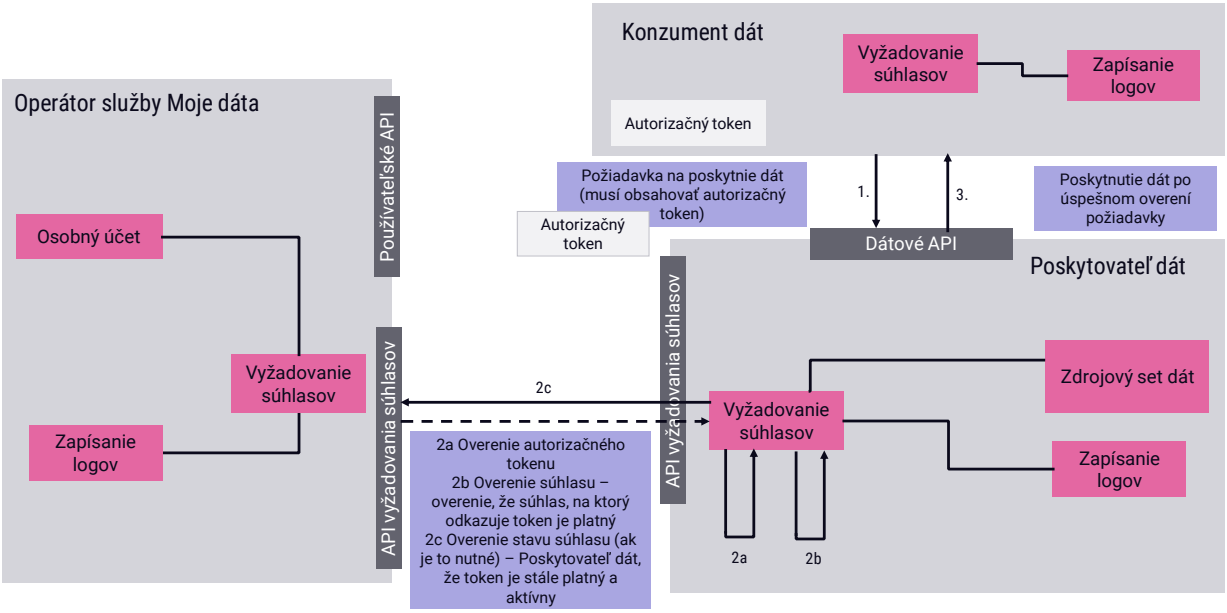
4. Záznam súhlasu je uložený v osobnom účte používateľa

5. Záznam súhlasu je doručený obom službám

6. Konzumentovi dát sú doručené relevantné autorizačné dáta (token)

Proces prenosu dát

Obrázok 15: Proces prenosu dát



Prenos dát prebieha v 3 krokoch:

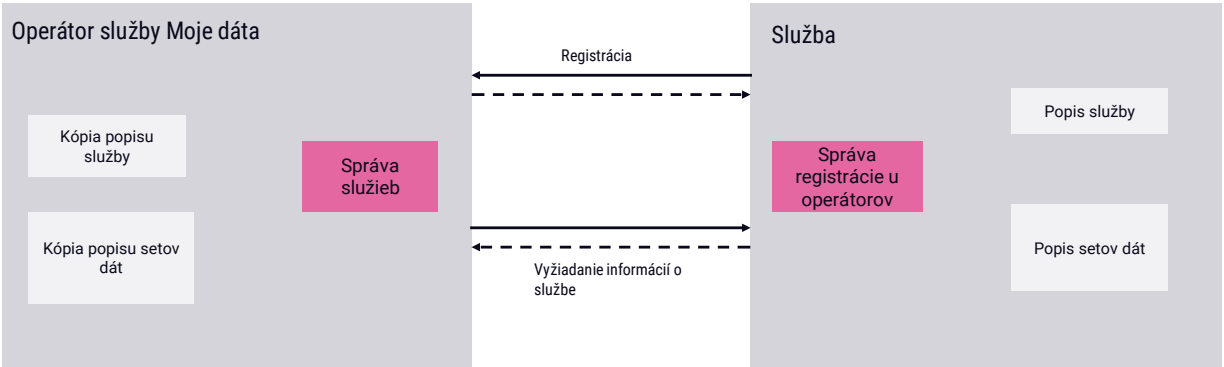
1. Konzument dát odošle požiadavku poskytovateľovi dát. Požiadavka obsahuje autorizačné dáta (autorizačný token) získané pri udelení súhlasu. Pred zaslaním požiadavky konzument tiež overí aktuálnosť a platnosť udeleného súhlasu.

2. Poskytovateľ dát v prvom kroku overí autorizačný token a v druhom platnosť s ním spojeného súhlasu. V prípade ak sa jedná o rizikové dáta alebo ak má poskytovateľ dát podozrenie, môže overiť súhlas s operátorom služby moje dáta.

3. V závislosti na výsledku overenie sú buď poskytnuté dáta alebo je požiadavka zamietnutá. V momente udelenia súhlasu dochádza tiež uloženiu informácie o sete dát, ktorého sa tento súhlas týka. Rovnaký set dát, je v prípade overenia požiadavky, poskytnutý konzumentovi dát.

Proces registrácie služby

Obrázok 16: Registrácia služby



Registrácia služby prebieha v nasledovných krokoch:

1. Služba požiada o registráciu u operátora služby Moje dáta. Ten ju zaregistruje a pridelí jej unikátne ID. Toto ID je unikátne pre registre služieb u daného operátora. Množstvo operácií realizovaných v rámci služby Moje dáta vyžadujú ID na svoj priebeh.

2. Služba poskytne svoj popis služby a popis setov dát vrátane technického popisu rozhrania, ako sa k týmto setom možno pripojiť. Poskytovateľ dát popisuje sety dát, ktoré vie dodať, konzument tie, ktoré vie spracovávať.

3. Popis služby a technické popisy rozhraní sú pridané do operátorovho registru služieb.

4.6 Platforma Talend a manažment osobných údajov

Centrálna integračná platforma štátu je postavená na module dátovej integrácie. Momentálne je do platformy zapojených viac ako 20 inštitúcii verejnej správy a v rámci pripravovaného projektu Dátová integrácia sa zapojí ďalších viac ako 50 inštitúcií. IS CSRÚ je postavený na open-source riešení Talend a jeho funkcionalita je primárne určená pre obsluhu dátového toku od registra do konania ("jeden-krát a dosť") a stotožnenia údajov pre účel referencovania.

Talend poskytuje nástroje pre dátovú integráciu, manažment dátovej kvality a správu kmeňových dát (MDM). Riešenie podporuje správnu implementáciu GDPR vďaka kontrolu tokov údajov, správy meta-údajov a maskovaniu údajov. Platforma je v našich podmienkach nastavená spôsobom, aby neuchovávala informácie centrálne, ale slúžila ako prostriedok pre zdieľanie a výmenu informácií.

Keďže cez integračnú platformu sú realizované jednotlivé väzby, ako vhodné riešenie konceptu moje dáta sa javí implementovať MyData API ako službu platformy, ku ktorej sa budú môcť pripájať jednotlivé PIMS.

5 Adresné služby

Moje dáta nezvyšujú len transparentnosť, ale môžu zásadne zmeniť zážitok a pridanú hodnotu služieb, keďže k dispozícii je veľké množstvo dát, ktoré sa môžu využiť. Súkromný sektor má z veľkej časti bohaté skúsenosti s využívaním osobných údajov pri návrhu služieb a mnohé spoločnosti, napríklad Amazon pri odporúčaní kníh, ktoré by sa nám mohli páčiť, Netflix pri odporúčaní filmov a seriálov, ktoré by sme si chceli práve pozrieť alebo Google, ktoré dokáže ponúknuť reklamu na výrobky na základe hľadaných výrazov a záujmov. Tieto spoločnosti majú na základe personalizácie postavený svoj biznis model a vďaka personalizácii dokážu ponúknuť svojim používateľom jedinečnú pridanú hodnotu. Prvé spoločnosti, ktoré začínajú systematicky využívať princípy hnutia moje dáta[22] sú poisťovne, pretože rizikové modely dokážu byť po zahrnutí osobných skúseností a vzorov omnoho presnejšie. Hlavná otázka je, či dokáže tento trend využiť aj verejná správa tak, aby dokázala využiť možnosti adresných služieb a zároveň nediskriminovala určité skupiny obyvateľstva.

Adresné služby využívajú personalizáciu a zabezpečujú pre používateľa obsah, skúsenosť, funkcionalitu, potvrdenie na základe potrieb používateľa bez jeho vedomého úsilia (na základe dát, ktoré sú o ňom pre službu k dispozícii).

Technologické spoločnosti vo svojich štúdiách navrhujú (ako napríklad Microsoft[23]) adresné služby ako novú veľkú vec v digitálnej verejnej správe. Skutočných prípadov použitia a princípov je však k dispozícii veľmi limitovaný počet. V tejto kapitole preto navrhujeme základné princípy pre návrh adresných služieb a zároveň predstavujeme základné scenáre využitia.

Adresné služby, ktoré fungujú transparentne a dokážu priniesť výhodu všetkým používateľom na základe ich súhlasu by mali byť postavené na myšlienkach Moje dáta. Ak sa adresné služby zavedú do praxe, bude to znamenať: 1) lacnejšie a efektívnejšie poskytovanie verejnej služby, 2) možnosť vytvárať zaujímavejšie a kvalitnejšie verejné služby pre používateľom a 3) lepšie zamerať verejnú službu na skupiny, ktoré ju naozaj potrebujú.

5.1 Princípy adresných verejných služieb

Návrh princípov nového typu verejných služieb, ktoré dokážu využívať osobné údaje klienta na vytváranie novej pridanej hodnoty. Znamená to, že digitálnej skúsenosti je potrebné venovať omnoho vyššiu pozornosť, služby je potrebné navrhovať z pohľadu architektúry voľby, podľa princípov behaviorálnych vied.

Moje dáta a adresná služba:

Vďaka Mojim dátam sú v čase riešenia služby alebo životnej situácie k dispozícii (za podmienky, že k tomu dal používateľ súhlas): 1) informácie o všetkom, čo verejná správa o danom používateľovi eviduje, 2) informácie o aktuálnych konaniach a histórií interakcií s verejnou správou, ako i 3) jeho demografické údaje a 4) osobne nastavené preferencie. Znamená to, že logika služby môže tieto informácie využiť a ponúknuť:

- predvyplniť všetky informácie, ktoré je možné získať z prístupných objektov evidencie (napríklad meno, priezvisko, dátum narodenia, korešpondenčnú adresu a podobne),

[22] http://mesinfos.fing.org/mesinfos-mydata-everything-you-need-to-know-about-the-project/

[23] https://enterprise.microsoft.com/en-gb/articles/industries/public-sector/the-next-phase-in-public-sector-digital-transformation/

- overiť platné skutočnosti a zamietnuť respektíve pokračovať v službe (napríklad overiť podmienku návštevy v škole pre žiaka, overiť dosiahnutý príjem),
- ponúknuť zabezpečenie špeciálnych potrieb (napríklad rezervovať parkovanie pre zdravotne ťažko postihnutých, dohodnúť prednostné vybavenie pre rodinu s malými deťmi),
- odporučiť nasledovné kroky a ďalšie súvisiace služby, ktoré by občan alebo podnikateľ mohol chcieť využiť alebo na ktoré má nárok.

Adresné služby sú z princípu založené na zdieľaní veľkého množstva údajov medzi inštitúciami navzájom ako i s používateľom. Je preto veľmi dôležité, aby boli dodržané zásady transparentnosti a aby služba korektne využívala logovanie, to znamená, aby používateľovi bolo jasné, kto počas spracovania ku ktorým jeho údajom pristúpil respektíve ktoré údaje sa vyhodnotili automaticky bez zásahu tretej osoby.

Ako by mala vyzerať adresná služba:

- Informácie by mali byť prispôsobené záujmom, veku, lokalite používateľa.
- Služba by mala predikovať potreby používateľa.
- Služba by mala pomáhať používateľovi z jeho rozhodovaním a voľbou.
- Adresnosť služby by mala byť voliteľná a ku každej službe by mala existovať jej "štandardná verzia" alebo "default".
- K službe by malo byť naviazané odporúčanie ďalších vhodných služieb, aby občan získal maximálny komfort (na základe jeho veku, stavu, životnej situácie, lokalite).
- Služba by mala transparentne uvádzať, ku ktorým údajom bude pristupovať a po spustení služby korektne v logoch uviesť, ku ktorým údajom sa pristupovalo.
- Využitie spätnej väzby od používateľov na ďalšie zlepšovanie služby.

Vhodnosť využitia adresných služieb:

- Adresné služby je vhodné implementovať, keď je štandardná digitálna služba plne funkčná a funguje monitorovanie jej výkonnosti. Máme tak k dispozícii dostatok údajov pre správny návrh služby.
- Digitálna služba je/môže byť súčasťou komplexnejšej životnej situácie. Je preto potrebné zanalyzovať architektúru voľby pre celú životnú situáciu.
- Digitálna služba realizuje politiku, ktorá ma jasne nastavené ciele a meranie výkonnosti.
- Je možné očakávať iné preferencie pre rôzne skupiny obyvateľstva. Nastavenie adresných služieb je preto potrebné

5.2 Scenáre využitia

V nasledujúcej časti je predstavený návrh možných scenárov využitia adresných služieb. Adresné služby sú postavené na využití možností prístupu k osobným dátam a iným údajom počas realizácie verejnej služby.

Podrobnejšie sa venujeme scenárom:

- Kontextuálna navigácia na základe objektov evidencie - môžem narábať s objektom evidencie,
- Služby je možné nastaviť na základe osobných preferencií, evidovaných cez Moje dáta,
- Služby je možné nastaviť na základe identifikovaných potrieb,

- Definované vzťahy medzi inými používateľmi umožňujú udeľovanie splnomocnení a oprávnení,
- Cez službu Moje dáta sa dá riadiť zdieľanie údajov a ich následné použitie,
- Aplikáciu Moje dáta je možné využiť ako alternatívny identifikátor,
- Použitie digitálnych služieb prostredníctvom inteligentného osobného asistenta, ktorý má prístup k údajom o subjekte,
- Aplikáciu Moje dáta je možné využiť ako priestor na ukladanie a interpretáciu "smart contracts".

Obrázok 17: Prehľad scenárov využitia pre adresné služby

5.2.1 Kontextuálne využitie dát pre prístup k službám

Cez službu Moje dáta je možné sprístupniť jednotlivé objekty evidencie, ktoré sa týkajú danej osoby, používateľa, ktoré sa viažu k danej identite. Ak máme k dispozícii prehľad objektov evidencie, sme len krok k volaniu ďalších služieb, ktoré sa daného objektu evidencie týkajú. Kontext daný objektom evidencie je možné považovať za výborný navigačný prostriedok pre prístup k digitálnym službám a k elegantnejší spôsob ako použitie klasických formulárov (keďže služba dopredu vie o ktorý objekt evidencie sa jedná).

Služby môžu byť:

- Špecifické - viažuce sa k danému konkrétnemu objektu evidencie. Napríklad naplánovanie očkovania pre môjho psa, odhlásenie psa z evidencie, ak môj pes nešťastnou náhodou zomrel alebo vysporiadanie daňovej povinnosti za psa. Volanie špecifickej služby je možné chápať ako volanie formuláru, pričom objekt evidencie je vstupom. Služby k objektu evidencie môže registrovať správca objektu (napríklad MV SR pri služby týkajúcich sa "mojich" vozidiel) alebo dokonca i tretia inštitúcia, ktorá dokáže takýto objekt ďalej spracovať (v príklade vozidla havarijná poisťovňa),
- Všeobecné - vhodné pre objekty evidencie ako také: stiahnutie objektu evidencie, preposlanie objektu evidencie cez dostupné aplikácie, archivácia objektu evidencie, elektronické podpísanie objektu evidencie, nahlásenie sťažnosti na obsah dátového objektu a podobne. Všeobecné služby

sú súčasťou architektúry Moje dáta a pre každý objekt evidencie bude možné nastaviť, ktoré všeobecné služby budú k dispozícií.

Vďaka kontextuálnemu využitiu dát sa výrazne zvýši užívateľská prívetivosť digitálnych verejných služieb a rozhranie služby Moje dáta sa môže stať navigačným priestorom pre orientáciu sa v ponuke služieb.

Z pohľadu implementácie to znamená, že prevádzkovateľ služby moje dáta vytvorí vhodný mechanizmus pre registráciu služieb, ktoré je možné volať z kontextu vylistovaných objektov evidencie a prevádzkovatelia digitálnych služieb zaregistrujú svoje služby. Dá sa očakávať, že takéto riešenie bude podporovať "single sign-on" a prechod medzi objektom evidencie a službou by mal byť čo najjednoduchší.

Dá sa však predpokladať, že kontextuálne využitie dát pre prístup službám bude rásť postupne, ako prvé by mali pribúdať služby, ktoré sú najžiadanejšie.

5.2.2 Služby na základe preferencie

Používateľ cez službu Moje dáta dokáže zadať všeobecné aj konkrétne preferencie. Napríklad údaje o preferovaných kanáloch komunikácie, korešpondenčnej adrese, preferovanom spôsobe platby alebo potreby notifikácií o udalostiach vo verejnej správe. Vďaka konkrétnym preferenciám pre jednotlivé služby je možné meniť "defaultné" východiská a riešiť "opt-out" alebo "opt-in" prístupy k službe. Napríklad na základe preferencií je možné určovať výber dôchodkového poistenia a rôzne doplnkové služby, ako i preferencie v politických otázkach na lokálnej úrovni. Digitálna služba na základe prístupu k týmto dátam dokáže navrhnúť formu a obsah služby podľa deklarovaných potrieb používateľa.

Využívať možnosti optimalizovať služby na základe preferencií je vhodné najmä pre služby, ktoré sa opakujú. Používateľ má možnosť nastaviť si službu na mieru a získať tak vyššiu pridanú hodnotu na základe svojich potrieb. Celková informácia o preferenciách umožní inštitúcii lepšie plánovať ponuku služieb a získava tiež dôležitú spätnú väzbu od občanov (ako chcú získavať výsledky svojej digitálnej služby, čo vlastne chcú od inštitúcii a podobne). V konečnom dôsledku tak je možné optimalizovať efekt služieb. Prieskum preferencií je tiež možné využiť aj ako podklad pri nastavovaní politík a uvažovaní o budúcom rozvoji služby.

Poskytovať služby na základe preferencií je vhodné aj pri využívaní behaviorálneho prístupu. Ak má služba jasnú architektúru voľby, je možné určiť jednotlivé módy poskytovania tejto služby, určiť východiskovú ("default") možnosť a umožniť používateľom následný výber. Túto vlastnosť aplikácie Moje dáta je možné využiť aj pri

Ak chce inštitúcia využívať možnosť sledovať preferencie, okrem všeobecných preferencií, ktoré budú nastavené na centrálnej úrovni, bude potrebné, aby si definovala takzvané "preferenčné objekty evidencie" pre svoje služby, pričom kľúčové je správne nastavenie atribútov. Pre jednoduchosť sa odporúča, aby v prvom kroku išlo o atribúty typu áno/nie alebo o výber zo zoznamu.

5.2.3 Služby na základe potrieb – proaktívne služby

Služby na základe preferencií umožňujú používateľom vybrať mód služby. Analýzou dostupných údajov o používateľovi však môže poskytovateľov služby identifikovať jeho potreby automatizovane a zaviesť tak takzvané proaktívne služby:

- Nárok na adresné sociálne služby: napríklad ponuka sociálnych služieb pre seniorov pri odchode do dôchodku, ponuka rekvalifikačných kurzov pre nezamestnaných a podobne.

- Nárok na dávky alebo príspevky na základe stavu alebo zmeny stavu: napríklad nárok na príspevok na bývanie pre ZŤP, cestovanie vlakom zadarmo pre dôchodcov, príspevok pri narodení dieťaťa a podobne.
- Odporúčanie súvisiacich služieb a vhodných krokov pre životnú situáciu používateľa: napríklad ponuka registrácie daňové subjektu pri založení obchodnej spoločnosti.
- Odporúčanie na riešenie povinností, ktoré vyplývajú z aktuálne detekovaných udalostí, napríklad výpočet daňovej povinnosti.

Výhody návrhu služieb na základe potrieb je, že tvorca verejnej politiky získa omnoho lepší prehľad o situácií používateľa a môže navrhnúť politiku spôsobom, ktorá umožní personalizované riešenie konkrétneho problému a zacielenie intervencie. Znamená to možnosť efektívnejšieho využitia zdrojov v danej politike spôsobom, ktorý najviac pomáha cieľovej skupine respektíve ktorý najlepšie pomáha dosiahnuť daný cieľ. Návrh digitálnych služieb na základe potrieb tak podporí hodnotu za peniaze a celkovo podporí lepší návrh politík.

Pre používateľa digitálne služby na základe potrieb znamenajú omnoho lepšiu orientáciu v jeho nárokoch a povinnostiach. Používateľ sa tak nestratí v byrokracii, ale dozvie sa, čo sa ho týka a čo si môže jednoduchým spôsobom vybaviť. Znamená to, že prístup k verejným výhodám bude jednoduchší a priamočiarejší. Zvýši sa úspešnosť domáhania nárokov a zníži sa miera nestíhania povinností, čo v konečnom dôsledku znamená vyššiu mieru spravodlivosti. Služby na základe potrieb s využitím služby Moje dáta tak môžu v praxi realizovať víziu takzvaných "proaktívnych" služieb, ktoré boli časti vyžadované v NKIVS a iný ch strategických dokumentoch e-Governmentu.

Implementácia služieb na základe potrieb pre inštitúcie znamená: že je potrebné pochopiť dátový model súvislostí, ktoré sa viažu k nároku, povinnosti resp. odporúčaní a na základe nich identifikovať kľúčové skutočnosti, ktoré je možné v osobných dátach používateľa identifikovať. Tento koncept je následne potrebné preniesť do biznis logiky služby. Takýto dátový prístup povedie k redizajnu služby, ale dá sa očakávať, že výsledná služba bude kvalitnejšia a lepšie poslúži svojmu účelu. V každom prípade sa odporúča evolučný prístup, postupné zlepšovanie možností a počtu dátových objektov, ktoré sú automaticky analyzované.

5.2.4 Vzťahy medzi subjektami

Moje dáta umožňujú "tvorbu" sociálnej siete s ostatnými užívateľmi platformy pomocou rolí. Cez službu je tak možné zabezpečiť prístup k údajom pre špecifické osoby:

- zákonne definovaným osobám (manžel/ka, otec, matka, deti, zákonný zástupca a podobne),
- užívateľsky zvoleným osobám, ktoré majú práva na prístup k údajom (splnomocnenec, kapitujúci lekár, právnik a podobne).

Systémy tretích strán sa cez aplikáciu Moje dáta môžu dozvedieť, kto má súhlas na prístup a ďalšie činnosti od používateľa. Riešenie je tak možné využiť pre riešenie splnomocnení (na čo je koncept súhlasov veľmi vhodný). Výhodou je, že transparentný log pre Moje dáta umožní používateľovi sledovať, akým spôsobom jeho poverené osoby s dátami narábali. Aplikácia Moje dáta tak získava ďalšie možnosti použitia v reálnom úradnom fungovaní.

Implementácia vzťahov medzi subjektami do procesov na strane inštitúcií si okrem klasickej integrácie s API pre Moje dáta vyžaduje aj definovanie a nastavenie typov rolí, ktoré sa v informačnom systéme inštitúcie vyskytujú a môžu na základe špeciálnych práv k dátam pristupovať, ako i podporiť rôzne role používateľov z externého prostredia a správne zadefinovať používanie digitálnych služieb zástupcami a splnomocnencami.

5.2.5 Zdieľanie údajov

Mnohé verejné služby dokážu pracovať lepšie, keď dokážu využiť údaje od občanov a podnikateľov. Nie všetky údaje však môžu byť štátom spracovávané priamo (napríklad vďaka obave z "veľkého brata"), niekedy však pomôže, ak má inštitúcia možnosť získať prístup k špecifickým dátam na základe súhlasu používateľa služby.

Zdieľanie údajov má zmysel:

- pri výmene personalizovaných záznamov o histórií prípadov, napríklad pri zdravotnej starostlivosti (zdieľanie zdravotných záznamov medzi poskytovateľmi zdravotnej starostlivosti),
- pri zabezpečení prístupu k dokumentom pre inštitúciu v konaní (napríklad pri stavebnom konaní),
- pseudo-anonymizované zdieľanie veľkého množstva údajov pre výskumné účely (čo bude mať čím ďalej väčší význam ako vstupné dáta pre návrh algoritmov umelej inteligencie).

Takýto koncept výrazne pomôže zvýšiť dôveru používateľov v zdieľanie svojich údajov na dobré ale i komerčné účely a podporiť tak rozvoj dátového hospodárstva. Využitie Mojich dát na zdieľanie údajov rieši aj rozpor medzi potrebou spracovania čím ďalej väčšieho množstva údajov, aby sme dokázali navrhovať presnejšie algoritmy a individuálnymi právami na ochranu osobných údajov. Hlavnými výhodami je tak vyššia transparentnosť, ako i efektivita zberu údajov a zvýšenie rozsahu údajov pre potreby štatistického spracovania.

Inštitúcie, ktoré poskytujú služby klientom by sa mali pripraviť na možnosti, že dokážu cez Moje dáta získať prístup ku kvalitným údajom a nastaviť si podľa toho svoje procesy, najmä vstupné spracovanie dokumentov.

5.2.6 Využitie identity

Mechanizmus autentifikácie pre Moje dáta bude postavený na protokoloch UMA (User-Managed Access) - používatelia môžu rozhodovať a autorizovať prístup k dátam a manažovať, ako sa ich dáta zdieľajú medzi online službami. Mechanizmus identifikácie je postavený na protokole OpenID Connect, ktorý umožní federalizovaný "single sign-on". UMA aj OpenID sú pritom postavené ako profily OAath 2.0. Aplikácia tak podporuje asynchrónne súhlasí a centralizovaný manažment súhlasov.

Aplikácia Moje dáta tak môže slúžiť ako alternatívny identifikátor a výrazne podporiť služby mobilného governmentu.

Výhody: Keďže zmysluplné riešenie mobilnej identity stále chýba aplikácia Moje dáta s vyriešeným identifikačným a autentifikačným mechanizmom je ideálnym nástrojom, ako priniesť digitálne služby do mobilných zariadení, najmä pri využití kontextovej navigácie.

Implementácia: V prvom rade je dôležité, aby jednotlivé informačné systémy verejnej správy implementovali Open API pre Moje dáta a dokázali tak akceptovať a pracovať s identifikačným a autentifikačným mechanizmom, ktoré budú aplikácie Moje dáta používať. Zmeny a vylepšenie architektúry sa očakávajú najmä od MV SR a NASES.

5.2.7 Použitie osobného asistenta

Chatboty a virtuálny asistenti otvárajú nové možnosti a nové komunikačné kanály medzi používateľmi a verejnými inštitúciami. Z pohľadu nových možností je zaujímavá najmä hlasová asistencia, ktorá znamená intuitívny spôsob komunikácie pre čo najširšie množstvo používateľov (aj napríklad seniorov a osoby s nižšou digitálnou gramotnosťou). Úspech virtuálnych asistentov ako Siri, Alexa, Cortana alebo

Google Asistent pri riešení komerčných požiadaviek (nákup) alebo vybavovanie životných situácií (plánovanie schôdzok, objednanie reštaurácie, navigácia). V budúcnosti sa očakáva ďalší rozdiel podobných služieb a očakáva sa, že budúcnosť e-Governmentu sa bude uberať práve týmto smerom. Na to, aby osobný asistent správne fungoval, potrebuje v prvom rade prístup k dátam, aby chápal situáciu používateľa a aby sa mohol učiť zo skúseností a z minulých situácií; ako i prístup k biznis logike digitálnych služieb a znalostiam o nich (procesné mapy). Osobný asistent je preto ideálna nadstavba nad rozhraním Moje dáta.

Osobný asistent môže byť použitý všade na riešenie nasledujúcich problémov:

- Analýza práv a povinností používateľa vo vzťahu k inštitúciám verejnej správy,
- Odporúčania a rady, čo by mal používateľ spraviť a kedy,
- Príprava dokumentov a podkladov na základe dostupných informácií z Mojich dát,
- Navigácia a orientácia v komplexných životných situáciách.

Inteligentní asistenti predstavujú budúcnosť e-Governmentu. Ich zavedením sa, vďaka intuitívnemu a interaktívnemu štýlu komunikácie a kognitívnej podpore v rozhodovaní, výrazne zníži administratívna záťaž pre používateľov, zvýši sa spravodlivosť, vybavovanie nárokov bude úspešnejšie a povinnosti sa budú plniť ľahšie a prehľadnejšie, čo zníži riziko budúcich problémov a súdnych sporov. Z pohľadu verejnej správy inteligentní asistenti znížia potrebu po lacnej administratívnej sile a inštitúcie sa tak môžu venovať dôležitejším činnostiam.

Implementácia: Podpora zavádzania AI asistenta si vyžaduje snahu aj na strane inštitúcií: okrem sprístupnenia objektov evidencie cez aplikáciu Moje dáta je vhodným a žiadaným doplnkom príprava a zverejnenie biznis logiky digitálnych služieb v strojovo spracovateľnom formáte, napríklad vo forme vývojových diagramov alebo procesných máp. Pomôže i úprava legislatívy spôsobom, aby bola jasne vyjadriteľná ako algoritmus. V konečnom dôsledku sa ako optimálne riešenie javí i implementácia vlastnej AI, ktorá dokáže efektívne komunikovať s AI asistentami občanov.

Inštitúcie si môžu zavádzať aj vlastných chatbotov a AI asistentov, najmä ak existuje reálna potreba pre riešenie vzťahov s klientami, ako je to v prípade Finančnej správy, Sociálnej poisťovne, zdravotných poisťovní, alebo pri vybavovaní evidenčnej a registračnej agendy na okresných úradoch (MV SR).

5.2.8 „Smart contracts“ - inteligentné zmluvy

Myšlienky Moje dáta do veľkej miery súvisia so sľubnou víziou decentralizovanej vrstvy dôvery, ktorá môže byť postavená na technológii "blockchain": Za dôležitú aplikáciu sa považujú, ktorá súvisí s administratívnymi procesmi sa považujú takzvané "Smart contracts" alebo inteligentné zmluvy sú dohody, ktoré po splnení podmienok dokážu automatizovane realizovať predmetnú transakciu. Podmienky v inteligentných zmluvách sa môžu týkať osobných údajov dostupných cez Moje dáta.

Architektúra Moje dáta predstavuje ideálny priestor na ukladanie, interpretáciu a spúšťanie inteligentných zmlúv.

Výhody: Hlavnou nevýhodou bežných zmlúv je možnosť manipulovať s výkladom a zmyslom slov, pomocou právnej interpretácie. Inteligentné zmluvy sú naopak presné a jednoznačné, je ich možné popísať jasným algoritmom. Zavedenie inteligentných zmlúv do procesov verejnej správy môže výrazne redukovať administratívnu záťaž a ďalej vylepšiť adresné služby, kde po naplnení podmienok môže dochádzať k automatickým plneniam, napríklad prevodu peňažných prostriedkov a podobne. Inteligentné zmluvy sú výhodné aj v občianskom a obchodnom práve a pomocou nich je možné riešiť najmä

Implementácia: Dôležitým krokom pre zavedenie inteligentných zmlúv do praxe je najmä prijatie legislatívnej úpravy, ktorá ich použitie umožní, reguluje a nastaví správne podmienky používania inteligentných kontraktov. Tejto téme sa bude venovať pripravovaný zákon o dátach.

5.3 Služby tretích strán

Architektúra Moje dáta je navrhnutá spôsobom, aby umožnila používateľovi kontrolovať svoje dáta a zároveň mu ponechala voľbu nad spôsobom ich použitia. Každá aplikácia, ktorá naplní architektonické princípy a dôveryhodne implementuje definovaný štandard Open API pre Moje dáta môže slúžiť ako:

- Konzument údajov, napríklad pri využití konceptu "Smart disclosure" je možné na základe osobných údajov poskytovať konkrétne odporúčania pre používateľa,
- Samotný PIMS, ktorý implementuje funkcionality na manažment osobných údajov. Očakávame konkurenciu takýchto riešení, aby občania mali možnosť voľby.

Smart disclosure

Politika "Smart Disclosure[24]" alebo inteligentné odhalenie informácií je inovatívny nástroj, ktorý pomáha spotrebiteľom a používateľom prijímať lepšie informované rozhodnutia a využívať nové produkty a služby postavené na dátach. Ide o rozšírenie prístupu k údajom v strojovo čitateľných formátoch o osobné údaje, aby inovátori mohli vytvárať interaktívne služby a nástroje, ktoré spotrebiteľom umožnia robiť dôležité rozhodnutia v sektoroch, ako sú zdravotníctvo, vzdelávanie, financie, energetika, doprava a telekomunikácie. Realizáciu Smart Disclosure v praxi je možné podporiť práve využitím služby Moje dáta.

Použitie OpenAPI

OpenAPI je aplikačné rozhranie, ktoré je verejne dostupné. Využitie princípov OpenAPI pre zabezpečenie Smart Disclosure a realizáciu adresných verejných služieb je dôležité najmä z pohľadu podpory inovácie.

[24] https://www.data.gov/consumer/smart-disclosure-policy

6 Implementačná príručka

Implementačná príručka pre manažment osobných údajov, ktorá bude obsahovať:

- Požiadavky na procesy a organizáciu,
- Požiadavky na informačné systémy verejnej správy.

6.1 Požiadavky na procesy a organizáciu

6.1.1 Moje dáta checklist

Aby mohla organizácie povedať, že pracuje s osobnými údajmi evidovanými o občanovi v súlade s požiadavkami služba Moje dáta, musia byť splnené nasledujúce podmienky:

- Občan má prístup k svojím dátam (vidí ich a môže s nimi pracovať),
- Občan vidí, kto k dátam pristupoval a za akým účelom,
- Občan môže svoje dáta sprístupniť tretej strane,
- Občan môže tretej strane zakázať prístup k svojim dátam, okrem zákonom opodstatnených dôvodov
- Občan môže k svojim dátam spravovať pomocou API definovanej v službe Moje dáta

Aby boli dáta kompatibilné so službou Dáta organizácie musia splniť nasledovné požiadavky:

6.1.2 Manažment osobných údajov

Manažment osobných údajov sa musí stať súčasťou rutinného výkonu činnosti organizácie. Implementácia smernice GDPR v praxi výrazne zvýšila povedomie organizácií o dôležitosti manažmentu osobných údajov a mnohé inštitúcie verejnej správy preto zaviedli základné organizačné predpoklady potrebné pre manažment osobných údajov v praxi. Tento postup je pre potreby Moje dáta potrebné systematizovať.

Definovanie potrebných procesov, aby bolo možné realizovať manažment osobných údajov:

- Zber dát - pri zbere nových dát je vhodné vytvoriť referenčný dátový model, ktorý jasne definuje spracované objekty evidencie a rozhodne, ktoré budú vstupovať do služby Moje dáta,
- Popisovanie dát - je potrebné zabezpečiť, aby všetky vznikajúce objekty evidencie mali správne priradený identifikátor,
- Správa kmeňových a referenčných údajov,
- Manažment kvality dát,
- Riadenie prístupu k dátam,
- Uchovávanie dát a archivácia.

Zoznam zmien v manažmente dát, ktoré je potrebné zaviesť do praxe v inštitúcií:

- Podpora role dátového kurátora v riadení organizácie,
- Zriadenie rezortnej dátovej kancelárie,
- Nastavenie správy rezortného modelu údajov, ktorý bude kompatibilný z Centrálnym modelom údajom (resp. jeho súčasťou),

- Manažment kvality údajov musí počítať so spätnou väzbou od evidovaných subjektov. Príslušný proces je potrebné upraviť spôsobom, aby bolo možné rýchlo upraviť príslušné údaje a zvýšiť tak ich kvalitu.
- Je potrebné zaviesť monitoring prístupov k osobným údajom.

6.1.3 Dôležité otázky

Ako identifikujem objekty evidencie, pre ktoré je možné použiť službu Moje dáta?

- Odporúčame realizáciu Dátovej analýzy, ktorej výstupom bude Model údajov (kompatibilný s Metodikou dátového modelovania, ktorú vydáva Dátová kancelária verejnej správy). Dátová analýza by mala identifikovať objekty evidencie, ktoré sú evidované v jednotlivých informačných systémoch organizácie. Pre každý objekt je možné posúdiť:
  - či obsahuje osobné údaje,
  - aké možné vzťahy má daný objekt evidencie k subjektom (občanom, právnickým osobám) v zákonom definovaných rolách,
  - relevancia.
- Ako prvé by mali byť cez službu Moje dáta sprístupnené:
  - objekty evidencie, ktoré sa viažu na výpisy, ktoré sú výstupmi súčasných e-government služieb;
  - doklady, ktoré vydáva inštitúcia,
  - povolenia,
  - licencie a certifikáty.
- Medzi objekty evidencie pre Moje dáta je potrebné zaradiť aj spisy v rámci konaní, ktoré sa týkajú subjektu, vrátane informácie o stave konania,
- Pri identifikácií objektov evidencie je vhodné komunikovať s Dátovou kanceláriou verejnej správy, ktorá spravuje plán zavádzania služby Moje dáta.

Ako naplánujem zavedenie služby Moje dáta?

- Zavedenie služby Moje dáta je vhodné riadiť projektovo, pričom je potrebné realizovať organizačné, procesné, technické a prevádzkové opatrenia. Rozsah projektu závisí od komplexnosti informačného prostredia danej inštitúcie.
- Dôležitým bodom rozhodnutia je výber, akým spôsobom bude služba Moje dáta realizovaná:
  - či sa využije centrálne API, ktoré bude k dispozícii v rámci Centrálnej integračnej platformy,
  - či sa implementuje API pre Moje dáta lokálne.
- Odporúčame sprístupňovať objekty evidencie do služby postupne a zosúladiť projekt Moje dáta s celkovým procesom
- Zavedenie služby Moje dáta do praxe nie je finančne náročne, k dispozícii sú momentálne nasledovné zdroje:
  - štrukturálne fondy: Dopytová výzva pre Manažment údajov má ako oprávnenú aktivitu zavedenie služby Moje dáta.

  - štátny rozpočet: prechod na Moje dáta je možné riešiť v rámci zmenových konaní.

Ako zabezpečím ochranu osobných údajov a GDPR?

- Architektúra služby Moje dáta je navrhnutá spôsobom, aby zabezpečovala podporu GDPR a poskytovala nástroje. Ak sa do služby Moje dáta zaradia všetky objekty evidencie, ktoré obsahujú osobné údaje a nachádzajú sa v danom informačnom systéme, služba Moje dáta umožní oboznámiť sa s nimi a podávať elektronický súhlas na ich spracovanie.
- Výstupy služby Moje dáta je možné použiť ako podklad v audite GDPR.

Ako riešiť sťažnosti na kvalitu dát?

- Cez službu Moje dáta je možné reklamovať kvalitu údajov, ktoré sa týkajú danej osoby. Znamená to, že inštitúcia si musí nastaviť proces, ako takéto sťažnosti riešiť. Ideálnym riešením by bolo vytvoriť automatizovaný workflow pre dátových kurátorov. Zároveň je potrebné, aby sa vyriešil spôsob, ako overiť reklamáciu, napríklad priamym kontaktom so sťažovateľom. V niektorých prípadoch bude potrebné upraviť legislatívu, aby proces zmeny na základe digitálnej požiadavky.

6.2 Požiadavky na informačné systémy

Definovanie požiadaviek na informačné systémy verejnej správy, aby boli schopné implementovať službu Moje dáta. Zoznam požiadaviek na zmeny v informačných systémoch, aby dokázali podporovať službu Moje dáta:

- Objekty evidencie v systéme majú pridelený identifikátor, ktorý ich dokáže priradiť k subjektom evidencie (občanom alebo podnikateľom).
- Riešenie implementuje systém pre definovanie vzťahov medzi subjektami evidencie a objektami evidencie a obsahuje služby, ktorá umožňuje vyhľadávať tieto vzťahy.
- Riešenie využíva službu pre evidenciu a sprístupnenie logov (pre prístup k osobným údajom).
- K osobným údajom môžu pristupovať iba registrovaní používatelia.
- Prístup k objektom evidencie je zabezpečený cez MyData API, ktoré môže byť:
  - Implementované v rámci Centrálnej integračnej platformy (známej aj ako Modul dátovej integrácie),
  - Implementované v rámci informačného systému inštitúcie. V takomto prípade je potrebné, aby API bolo registrované v Metainformačnom systéme a oznámene Dátovej kancelárii verejnej správy.
- Pre vybrané objekty evidencie je k dispozícii webová služba, ktorá overuje ich platnosť.
- Pre vybrané objekty evidencie je k dispozícii definícia vizuálnej podoby (najmä doklady, licencie a podobne).
- Ak je informačný systém konzumentom osobných údajov z iných informačných systémov (v našom prípade mimo verejnej správy), riešenie implementuje MyData API pre konzumentov údajov.

Ako volať službu Moje dáta?

V prípade, že inštitúcia chce využívať dáta o používateľov nad rámec možností zdieľania referenčných údajov, dokáže sa dostať k ďalším dátam o používateľovi na základe jeho explicitného súhlasu. V takom

prípade je možné použiť štandardizované API MyData, ktoré implementuje operátor. Znamená to vytvorenie nového modulu pre konzumovanie osobných údajov z iných systémov.

Ako vytvoriť API pre Moje dáta?

API pre Moje dáta, cez ktoré budú poskytované údaje je možné vytvoriť dvoma spôsobmi:

- buď sa využije centrálne riešenie, ktoré implementuje Centrálna integračná platforma. V takom prípade je v rámci modulu Centrálnej integračnej platformy nastaviť mapovanie na objekty evidencie cez príslušný identifikátor. V takomto prípade je možné využiť existujúcu integračnú väzbu.
- alebo sa vytvorí vlastné rozhranie podľa dohodnutého štandardu MyData API SK, ktorý sa momentálne pripravuje. Štandard by mal byť schválený počas leta 2019. Štandard popíše jednotlivé rozhrania a spôsob ich použitia. V rámci Dátovej kancelárie sa pripraví balíček otvoreného zdrojového kódu, ktorý implementuje tieto rozhrania a bude ho možné používať. Vlastné API je možné v budúcnosti posilniť cez pripravovanú API Gateway.

Aké nastaviť identifikátory pre objekty evidencie?

- Objekty evidencie zaradené a dostupné cez službu Moje dáta musia mať jednoznačnú možnosť identifikácie.
- Ak sa nevyužíva štandardný identifikátor povinnej osoby, logiku prevodu identifikácie realizuje Centrálna integračná platforma alebo vlastné MyData API (v prípade, že sa pre potreby Moje dáta).

Ako registrovať služby Moje dáta?

- Register všetkých služieb, ktoré poskytujú Moje dáta bude súčasťou Modulu Manažment osobných údajov v rámci Metainformačného systému verejnej správy. Pri každom novom objekte evidencie bude potrebné vykonať registračný záznam. Proces registrácie bude koordinovaný Dátovou kanceláriou. Na začiatku začne proces ako manuálny a postupne bude automatizovaný (ako sa bude budovať infraštruktúra pre Manažment osobných údajov).

Ako monitorovať prevádzku?

Súčasťou štandardu MyData API SK je aj formát monitorovacieho súboru. Dodržanie tohto formátu umožní reportovať reálne používanie služby Moje dáta rovnakým spôsobom.

7 Plán sprístupňovania osobných údajov

7.1 Kľúčové objekty evidencie

Obrázok 18: Prehľad objektov evidencie pre fyzickú osobu

Osobné informácie	
Meno a priezvisko	
Základné osobné informácie	a. Pohlavie
	b. Národnosť
	c. Dátum narodenia
	d. Miesto narodenia
Identifikácia	a. Rodné číslo
	b. IFO
Doklad	a. Občiansky preukaz
	b. Cestovný pas
	c. Vodičský preukaz
Rodný list	
Zdravotná dokumentácia	

Zamestnanie	
Práca a zamestnanie	
Príjem	
Osobité postavenie	a. Súdna prax
	b. Advokátska prax -
	c. Exekútorská prax -
	d. Notárska prax
	e. Znalecká prax
	f. Prax ako štátny zamestnanec
Kvalifikácia	a. Kvalifikácia v doprave
	b. Diskvalifikácia

Ďalšie
Súdny proces
Zviera
Patent
Vedecká publikácia
Vojenská služba
Exekúcia
Úpadok - Register úpadcov
Trest - Register trestov

Kontakt
Trvalé bydlisko
Prechodné bydlisko
Kontaktná adresa
Emailová adresa
Datová schránka
Telefónne číslo

Majetok
Auto
Nehnuteľnosť

Vzdelanie
Vzdelanie
Diplom
Certifikát

Podnikanie	
Identifikátory	a. IČO
	b. IČ DPH
Firma	
Živnosť	
Investícia	

Rodina
Rodinný príslušník
Sobáš
Rozvod

Dane, poistenie, dôchodok
Zdravotné poistenie
Sociálne dávky
Dôchodok
Dane

Tabuľka 1: Detail objektov evidencie Fyzickej osoby

ID	Vzťah	Objekt evidencie		Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
								Cez portál	API	Moje dáta API	Moje dáta aplikácia
Osobné informácie											
1	Môj	Meno a priezvisko		Krstné meno, Priezvisko, Titul		MV SR	RFO				
2	Osoba, ktorej som zákonný zástupca	Meno a priezvisko		Krstné meno, Priezvisko, Titul		MV SR	RFO				
3	Môj	Základné osobné informácie	a. Pohlavie	Pohlavie		MV SR	RFO				
4	Osoba, ktorej som zákonný zástupca		a. Pohlavie	Pohlavie		MV SR	RFO				
5	Môj		b. Národnosť	Národnosť		MV SR	RFO				
6	Osoba, ktorej som zákonný zástupca		b. Národnosť	Národnosť		MV SR	RFO				
7	Môj		c. Dátum narodenia	Dátum narodenia		MV SR	RFO				

ID	Vzťah	Objekt evidencie		Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
								Cez portál	API	Moje dáta API	Moje dáta aplikácia
8	Osoba, ktorej som zákonný zástupca		c. Dátum narodenia	Dátum narodenia		MV SR	RFO				
9	Môj		d. Miesto narodenia	Miesto narodenia		MV SR	RFO				
10	Osoba, ktorej som zákonný zástupca		d. Miesto narodenia	Miesto narodenia		MV SR	RFO				
11	Môj	Identifikácia	a. Rodné číslo	Rodné číslo		MV SR	RFO				
12	Osoba, ktorej som zákonný zástupca		a. Rodné číslo	Rodné číslo		MV SR	RFO				
13	Môj		b. IFO	IFO		MV SR	RFO				
14	Osoba, ktorej som zákonný zástupca		b. IFO	IFO		MV SR	RFO				
15	Môj	Doklad	a. Občiansky preukaz	Občiansky preukaz, číslo OP, miesto vydania, dátum		MV SR	RFO				

ID	Vzťah	Objekt evidencie		Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
								Cez portál	API	Moje dáta API	Moje dáta aplikácia
				vydania, dátum platnosti							
16	Môj		b. Cestovný pas	Cestovný pas, číslo cestovného pasu, miesto vydania, dátum vydania, dátum platnosti		MV SR	RFO				
17	Môj		c. Vodičský preukaz	Vodičský preukaz, ID, platnosť, oprávnenie		MV SR	RFO				
18	Môj	Rodný list		meno a priezvisko, miesto narodenia, dátum narodenia, miesto vydania, Otec, Matka		MV SR	RFO				
19	Môj	Zdravotná dokumentácia		Zdravotná dokumentácia		NCZI	NZIS IS PZS				
Kontakt											
20	Môj	Trvalé bydlisko		Adresa trvalého bydliska		MV SR	RFO				
21	Môj	Prechodné bydlisko		Adresa prechodného bydliska		MV SR	RFO				

ID	Vzťah	Objekt evidencie	Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
							Cez portál	API	Moje dáta API	Moje dáta aplikácia
22	Môj	Kontaktná adresa	Kontaktná adresa							
23	Môj	Emailová adresa	Emailová adresa							
24	Môj	Dátová schránka	Dátová schránka		NASES	EDESK				
25	Môj	Telefónne číslo	Telefónne číslo							
Majetok										
26	Môj	Auto	Značka, číslo VIN, rok výroby, ŠPZ, držiteľ vozidla - priezvisko/obchodné meno, držiteľ vozidla - krstné meno, držiteľ vozidla - adresa, vlastník vozidla - priezvisko/obchodné meno		MV SR	NEV				
27	Môj	Nehnuteľnosť	List vlastníctva		ÚGKK	Kataster				
Vzdelanie										
28	Môj	Vzdelanie	Najvyššie dosiahnuté vzdelanie, dátum, názov školy		MŠ SR					
29	Môj	Diplom	Diplom		Univerzity					

ID	Vzťah	Objekt evidencie		Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
								Cez portál	API	Moje dáta API	Moje dáta aplikácia
30	Môj	Certifikát		Certifikát		Oprávnená autorita					
Moje zamestnanie											
31	Môj	Práca a zamestnanie		Názov zamestnávateľa, sídlo zamesnávateľa, dátum začiatku pracovného pomeru							
32	Môj	Príjem		Posledný ročný príjem							
33	Môj	Osobité postavenie	a. Súdna prax	Záznam v Registri sudcov		MS SR					
34	Môj		b. Advokátska prax	Záznam v Registri advokátskej komory		Slovenská advokátska komora					
35	Môj		c. Exekútorská prax	Záznam v Zozname exekútorov		Slovenská komora exekútorov					
36	Môj		d. Notárska prax	Záznam v Zozname notárov		Notárska komora Slovenskej republiky					
37	Môj		e. Znalecká prax	Záznam v Zozname znalcov		MS SR					

ID	Vzťah	Objekt evidencie		Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
								Cez portál	API	Moje dáta API	Moje dáta aplikácia
38	Môj		f. Prax ako štátny zamestnanec	Záznam v Registri štátnych zamestnancov		Úrad vlády Slovenskej republiky	Register štátnych zamestnancov				
39	Môj	Kvalifikácia	a. Kvalifikácia v doprave	Záznam v Registri odborne spôsobilých osôb v doprave		MDVRR SR					
40	Môj		b. Diskvalifikácia	Záznam v Registri diskvalifikácií		MS SR					
Podnikanie											
41	Môj	Identifikátor	a. IČO	IČO		MS SR					
42	Môj		b. IČ DPH	IČ DPH		MS SR					
43	Môj	Firma		Názov spoločnosti, sídlo spoločnosti, vlastnícky vzťah		MS SR	Obchodný register				
44	Môj	Živnosť		Výpis zo živnostenského registra, sídlo, predmet podnikania, odbory činnosti, dátum vzniku oprávnenia, platnosť, príslušný úrad		MV SR	Živnostenský register SR				

ID	Vzťah	Objekt evidencie	Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
							Cez portál	API	Moje dáta API	Moje dáta aplikácia
45	Môj	Investícia	Cenný papier							
46	Môj	Osoba, ktorej som zákonný zástupca	Meno, dátum narodenia, miesto narodenia							
Rodina										
47	Môj	Rodinný príslušník	Atribúty fyzickej osoby							
48	Môj	Sobáš	Sobášny list, dátum svadby		Matrika					
49	Môj	Rozvod	Dátum rozvodu		Matrika					
Dane, poistenie, dôchodok										
50	Môj	Zdravotné poistenie	Názov poisťovne, odvedená čiastka, dlh na poistnom		Zdravotné poisťovne					
51	Môj	Sociálne dávky	Poberaná sociálna dávka		Sociálna poisťovňa					
52	Môj	Dôchodok	Výška vyplácaného dôchodku		Sociálna poisťovňa					
53	Môj	Dane	Typ dane, výška dane, dlh na dani		Finančná správa SR					

ID	Vzťah	Objekt evidencie	Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
							Cez portál	API	Moje dáta API	Moje dáta aplikácia
Ďalšie										
54	Môj	Súdny proces	Číslo súdneho procesu, názov súdu		Súdy					
55	Môj	Zviera	Registrácia zvieraťa		Komora veterinárnych lekárov Slovenskej republiky	Centrálny register spoločenských zvierat				
56	Môj	Patent	Názov patentu, číslo patentu		Úrad priemyselného vlastníctva Slovenskej republiky					
57	Môj	Vedecká publikácia	Názov publikácie, miesto publikácie, autori publikácie							
58	Môj	Vojenská služba	Dátum začiatku vojenskej služby, dátum konca vojenskej služby		MO SR					
59	Môj	Exekúcia	Číslo exekúcie, meno exekútora		Slovenská komora exekútorov	Centrálny register exekúcií				

ID	Vzťah	Objekt evidencie	Atribúty		Inštitúcia	Informačný systém	Dostupnosť			
							Cez portál	API	Moje dáta API	Moje dáta aplikácia
60	Môj	Úpadok - Register úpadcov	Záznam v Registri úpadcov		MS SR	Register úpadcov				
61	Môj	Trest - Register trestov	Záznam v Registri trestov		Generálna prokuratúra SR	Register trestov				

Tabuľka 2: Navrhované prípady použitia

ID	Prípad použitia	Objekty evidencie	Vzťah	Inštitúcia	Informačný systém	Dostupnosť			
						Cez portál	API	Moje dáta API	Moje dáta aplikácia
P.1	Susedné (súvisiace) pozemky v stavebnom konaní	▪ List vlastníctva	▪ Pozemok v stavebnom konaní susedí s pozemkom, ktorého som vlastníkom, alebo ak moje vlastnícke alebo iné právo k môjmu pozemku môže byť dotknuté na základe staveného konania na danom pozemku						
P.2									
P.3									

Tabuľka 3: Detail objektov evidencie

ID	Objekt evidencie	Atribúty	Inštitúcia	Informačný systém	Dostupnosť			
					Cez portál	API	Moje dáta API	Moje dáta aplikácia
1	Základné informácie	Názov, adresa, právna forma		Register právnických osôb, Obchodný register				
2	Zoznam vlastníkov	Meno, priezvisko, obchodné meno						
3	Zoznam konateľov	Meno, priezvisko						
4	Vlastník	Meno, priezvisko, miesto narodenia, dátum narodenia / obchodné meno						
5	Konateľ	Meno, priezvisko, miesto narodenia, dátum narodenia						
6	Predmet činnosti	Predmet činnosti						
7	Identifikátory a. IČO	IČO						
8	Identifikátory b. IČ DPH	IČ DPH						
9	Kontaktná adresa	Kontaktná adresa						
10	Emailová adresa	Emailová adresa						
11	Dátová schránka	Dátová schránka						

12	Telefónne číslo	Telefónne číslo						
13	Certifikáty	Certifikát						
14	Normy	Norma						
15	Súdny proces	Číslo súdneho procesu, názov súdu						
16	Exekúcia	Číslo exekúcie, meno exekútora						
17	Dane	Typ dane, výška dane, dlh na dani						
18	Auto	Značka, číslo VIN, rok výroby, ŠPZ, držiteľ vozidla - priezvisko/obchodné meno, držiteľ vozidla - krstné meno, držiteľ vozidla - adresa, vlastník vozidla - priezvisko/obchodné meno						
19	Nehnuteľnosť	List vlastníctva						
20	Účtovná uzávierka	Účtovná uzávierka						
21	Moji zamestnanci a) Sociálna poisťovňa	Zoznam zamestnancov						
22	Moji zamestnanci b) Zdravotná poisťovňa	Zoznam zamestnancov						
23	Môj súdny proces	Číslo súdneho procesu, názov súdu						

24	Môj patent	Názov patentu, číslo patentu						
25	Zmluva so štátom	Číslo zmluvy, názov zmluvy, zmluvní partneri						

7.2 Plán sprístupňovania

Na základe predchádzajúcich tabuliek bude vytvorený verejný plán sprístupňovania objektov evidencie cez službu Moje dáta (ďalej len plán sprístupňovania). Plán sprístupňovania bude manažovaný Dátovou kanceláriou verejnej správy a dostupný na jej webovej stránky.

Na základe spôsobu dostupnosti evidujeme nasledujúce typy sprístupnenia:

1. Cez portál povinnej osoby,
2. Cez API, ktoré realizuje povinná osoba,
3. Cez API, ktoré spĺňa štandard MyData API SK,
4. Cez centrálnu aplikáciu Moje dáta, ktorá komunikuje cez MyData API SK.

Konečným cieľom je, aby všetky relevantné objekty evidencie boli sprístupnené cez spôsob 4 a boli dostupné používateľom v rámci aplikácie Moje dáta. Dosiahnutie konečného cieľa však bude náročný a dlhodobý proces.