ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra veřejné správy

DIPLOMOVÁ PRÁCE

Elektronizace veřejné správy v ČR - e-Goverment.

Plzeň, 2021 Mgr. Kateřina WÜRZOVÁ

ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PRÁVNICKÁ

Katedra veřejné správy

DIPLOMOVÁ PRÁCE

Elektronizace veřejné správy v ČR - e-Goverment.

Předkládá: Mgr. Kateřina Würzová

Vedoucí diplomové práce: JUDr. Tomáš Louda, CSc.

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta právnická

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Mgr. Kateřina WÜRZOVÁ**
Osobní číslo:	**R19N0058P**
Studijní program:	**N0421A220001 Veřejná správa**
Studijní obor:	**Veřejná správa**
Téma práce:	**Elektronizace veřejné správy v ČR- e-Goverment**
Zadávající katedra:	**Katedra veřejné správy**

Zásady pro vypracování

I) Úvod
II) eGovernment
III) Symboly eGovernmentu
IV) Vybrané pilíře eGovernmentu
V) Zhodnocení eGovernmentu
VI) Závěr

Rozsah diplomové práce:
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná**

Seznam doporučené literatury:

viz zvláštní seznam

Vedoucí diplomové práce: **JUDr. Tomáš Louda, CSc.**
Katedra veřejné správy

Datum zadání diplomové práce: **29. března 2020**
Termín odevzdání diplomové práce: **31. března 2021**

JUDr. Petra HRUBÁ SMRŽOVÁ, Ph.D. (v.z.)

L.S.

Západočeská univerzita v Plzni * Fakulta právnická *

JUDr. et PhDr. Stanislav Balík, Ph.D.
děkan

JUDr. Tomáš Louda, CSc.
vedoucí katedry

V Plzni dne 25. srpna 2020

Prohlášení

„Prohlašuji, že jsem tuto diplomovou práci na téma Elektronizace veřejné správy v ČR - eGoverment vypracovala samostatně a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.“

V Plzni, březen 2021

Kateřina Würzová, v.r.

Obsah

Úvod

Když se podíváme kolem sebe, uvědomíme si, že jsme obklopeni moderní technologií, která zasahuje do života každého z nás. Využíváme ji v rámci běžných činností našeho života, od nákupů, studia, práce, používání internetového bankovnictví či placení pomocí chytrého telefonu, tak třeba i v rámci komunikace. Díky elektronice a jejím možnostem můžeme vykonávat všechny výše zmíněné činnosti jednoduše, rychle a leckdy z pohodlí domova. Stejný přístup a výsledek si slibuje i stát, když podstupuje elektronizaci veřejné správy. Budovaný český eGovernment má za cíl sloužit občanům a podnikatelům jako uživatelsky přívětivé a nápomocné on-line prostředí. Proto aby toto prostředí bylo efektivní, je hlavní strategií státu zaměřit se na online služby, legislativu, vytvoření vhodného prostředí podporující digitální technologie, vytvořit centrální řízení všech dostupných informačních technologií a podporovat vzdělávání úředníků. Cílem je samozřejmě spokojený občan a úspora času nejen občanům ale i státu. Právě elektronizace veřejné správy neboli eGovernment je tématem této diplomové práce.

Tato diplomová práce je zpracovaná popisnou metodou, když dvě z kapitol práce reflektují subjektivní názor autorky vzhledem k její osobní zkušenosti s využíváním služeb eGovernmentu.

Diplomová práce jako taková má pak za cíl přiblížit problematiku digitalizace veřejné správy na území České republiky. Téma je rozděleno do pěti hlavních kapitol, jež mají čtenáři poskytnout ucelený přehled stěžejních informací spojených s elektronizací veřejné správy.

První kapitola, která je pro tuto práci stěžejní, je zaměřena na samotný mezinárodně uznávaný pojem eGovernment a jeho stručný vývoj v České republice. Poskytuje čtenáři český i mezinárodní právní rámec elektronizace a rovněž ho seznamuje s některými pojmy, jež s digitalizací úzce souvisí, a které jsou pro celou práci podstatné. Následující dvě kapitoly, které se věnují symbolům a vybraným nástrojům eGovernmentu v České republice. Tyto kapitoly na sebe navazují a jsou defacto propojené, neboť některé z vybraných nástrojů jsou zobrazovány společně jako symbol celého eGovernmentu. Kapitola třetí se proto zabývá těmi nástroji eGovernmentu, které stály v procesu elektronizace veřejné správy od samého počátku, tj. komunikační infrastruktura veřejné správy, datové schránky, CzechPOINT a základní registry, ale dále se zaměřuje také na ty z prvků

eGovernmentu, které jsou v poslední době často tématem diskuse a autorka práce považovala za nebytné je zmínit. Ve čtvrté kapitole je pak čtenáři přiblíženo fungování některých z prvků eGovernmentu v praxi. Autorka diplomové práce je zaměstnaná na pozici notářského koncipienta, díky čemuž má přístup do určitých uživatelských rozhraní a s elektronickou formou veřejné správy přichází do styku každý den. V poslední kapitole pak čtenář nalezne zhodnocení elektronizace v České republice, její pozitiva, negativa a rizika, která jsou s ní spojená.

1. eGovernment

Veřejná správa jako taková slouží lidem. Vzhledem k objemu činností, jež je nutné v rámci moderní a demokratické veřejné správy vykonat, je nezbytné, aby tato správa byla efektivní a hlavně účinná. K tomu je třeba zohlednit potřebu neustálé aktualizace odpovídající dané moderní době. Proto, se zohledněním veškerých ovlivňujících faktorů, je jediným východiskem využít informační a komunikační technologie, jež způsobí rovněž zjednodušení a urychlení samotného výkonu veřejné správy. Tento proces integrace informačních a komunikačních technologií do činnosti veřejné správy, jímž veřejná správa přechází do elektronické formy, při němž dochází k zajištění výměny informací s veřejností a zjednodušení komunikace mezi občany, soukromými organizacemi a jiným veřejnými institucemi, je mezinárodně označován jako tzv. eGovernment.[1]

I přesto, že tento termín je všeobecně mezinárodně uznávaným, neznamená to, že by byl jeho obsah literaturou jednotně chápán a přijímán. Definice eGovernmentu se liší dle různých autorů a jsou jich desítky. Žádná definice však nedokáže plně vystihnout rozsah tohoto pojmu. Samotná jednotná definice eGovernmentu sice není nikde vymezena, avšak jsou určité definice, které jsou známější než ostatní. Jednou z nich je definice, jenž eGovernment definuje jako sérii procesů, jež vedou k výkonu státní správy a samosprávy a k uplatnění občanských práv a povinností fyzických a právnických osob, realizovaných elektronickými prostředky.[2] Dále např. Lidinský ve své publikaci eGovernment bezpečně cituje definici OSN, která eGovernment vymezuje tak, že představuje „*trvalou povinnost veřejné správy zlepšovat vztah mezi občany a veřejným sektorem poskytováním levných a efektivních služeb, informací a znalostí. Je to praktická realizace toho nejlepšího, co může veřejná správa nabídnout*.“ Ve stejné publikaci pak uvádí definici vlastní, a to takto: „*eGovernment je využívání informačních technologií veřejnými institucemi i pro zajištění výměny informací s občany, soukromými organizacemi a jinými veřejnými institucemi za účelem zvyšování efektivity vnitřního fungování a poskytování rychlých, dostupných a kvalitních*

[1] POMAHAČ, Richard a kol. *Veřejná správa*. 1. vydání. Praha: C. H. Beck, 2013. ISBN: 978-80-7400-447-6. s. 183
[2] ŠTĚDROŇ, B., *Úvod do eGovernmentu v České republice: právní a technický průvodce.* 1. vyd. Praha: Úřad vlády České republiky, 2007. ISBN 978-808-7041-253 , s. 9

informačních služeb.“ [3] Autoři Mates a Smejkal pak uvádí, že pojem eGovernment je vhodnější chápat spíše obsahově, než jeho popisem. Uvádí, že „… *smyslem je poskytnout všem soukromým subjektům větší komfort při realizaci kontaktů se státem a jinými subjekty veřejné moci tím, že zrychlí a zjednoduší komunikaci s nimi, zefektivní vnitřní procesy orgánů veřejné moci a povede k větší transparentnosti v jejich činnosti vůči veřejnosti. Lze také říci, že eGovernment přispívá k vytváření toho, co je označováno jako dobrá správa (Good Governance), tj. proces vládnutí a jeho kontrola a participace občanů na tomto procesu a je spojován s přechodem od vrchnostenského pojetí správy k veřejné správě, jakožto službě občanům, coby zákazníkům*.“[4] Jak je vidno, ani v mezinárodním měřítku ani v českém právním řádu není žádná jednotná definice. V České republice ani Ministerstvo vnitra ČR, jakožto kompetentní a zaštiťující orgán, nenabízí jasnou definici. Na svých webových stránkách lze však najít popis eGovernmentu, kdy „*jde o proces transformace vnitřních a vnějších vztahů veřejné správy pomocí informačních technologií s cílem optimalizovat interní procesy.*[5] *Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.“*[6]

S ohledem na výše uvedené definice můžeme obecně shrnout, že mezi autory panuje shoda, že jde o takové úkoly různého druhu, jež se zabývají elektronizací institucí veřejné správy a veřejné moci jako takové, když hlavním cílem je poskytovat subjektům větší pohodlí při jednání se státem a jeho orgány, a rovněž také posílení demokratizace veřejné správy.

V literatuře se často setkáme také s jednotlivými odvětvími eGovernmentu, které jsou zaměřeny na specifický úsek své činnosti. Jedná se převážně o služby poskytované ve zdravotnictví, které jsou obecně nazývány jako eHealth (e-zdravotnictví), kam můžeme zařadit např. nově uvedený eRecept či eNeschopenku.

---

[3] LIDINSKÝ, V. et al. *EGovernment bezpečně*. 1. vyd. Praha: Grada. 2008, ISBN 978-80-247-2462-1. s. 7

[4] MATES, P., SMEJKAL, V., *E-government v České republice. Právní a technologické aspekty.* Praha, Leges. 2012. ISBN 978-80-87576-36-6

[5] MATES, P., SMEJKAL, V. *E-government v českém právu*. Praha: Linde Praha, 2006, ISBN 80-7201-614-8. s. 9.

[6] MINISTERSTVO VNITRA. Indikátory Prioritní osy 1a,1b: Oblasti intervence: 1.1A, 1.1B - Rozvoj informační společnosti ve veřejné správě. [online]. Dostupné z: www.mvcr.cz/soubor/indikatory-prioritnich-os-1a-a-1b-pdf.aspx

Dále se jedná také např. o justici, která se samostatně nazývá e-justice či dále oddělení eEnviroment, a další specifická oddělení.[7]

1.1. Stručný vývoj eGovernmentu v České republice

První myšlenka, že by se využívalo IT služeb ve státní správě se objevila již zpočátku devadesátých let.[8] Tato myšlenka měla za cíl vytvoření jednoho konkrétního místa, které by se stalo univerzálním pro komunikaci se státem a které by bylo občanům garantované, věrohodné a bezpečné. Primárním cílem tedy bylo vytvoření jednotné infrastruktury, přes kterou by se dalo spojit se všemi existujícími informačními systémy.[9] K šíření této myšlenky elektronizace veřejné správy přispěly jak politické a sociální změny nastalé v tehdejším listopadovém Československu, tak nesporně k ní přispěl také rozmach využívání osobních počítačů v českých domácnostech, využívání informačních technologií a internetu obecně. K realizaci této vidiny však došlo až o téměř dekádu později.

V literatuře jsou uváděna celkem čtyři vývojová stádia eGovernmentu. První stadium je označované jako „Webová prezentace“, kdy jednotlivé organizace veřejné správy poskytují pasivně elektronické informace. Další stadium je tzv. stadium „Omezená interakce“, v němž dochází ke komunikaci zejména prostřednictvím běžných e-mailů. Pro třetí stupeň, označovaný jako „Transakční přístup“, je pak typické vytváření specifických aplikací jejích zaměření je důvěryhodné elektronické doručování a realizace podání, tzn. vláda se snaží postoupit veřejnosti snazší přístup k veřejným službám, ale nepoužívá internet jakožto nástroj systémové transformace. Poslední stádium je nazýváno „Interaktivní demokracií“ a představuje integrované elektronické služby zahrnující všechny elektronické transakce včetně elektronických plateb, vybudované portály poskytující různé elektronické služby s posílenou odpovědností a prvky přímé demokracie.[10]

[7] POMAHAČ, Richard a kol. *Veřejná správa*. 1. vydání. Praha: C. H. Beck, 2013. ISBN: 978-80-7400-447-6., s. 184.
[8] VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6. s. 25
[9] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1. str. 17.
[10] LECHNER, T., MATES, P. *E-Government v evropském prostředí*. Správní právo. Praha: Ministerstvo vnitra ČR, 2012, roč. 45, č. 4, ISSN 0139-6005. s. 249

Podle JUDr. Bohumíra Štědroně, LL.M., autora publikace Úvod do eGovernmentu: právní a technický průvodce, byl počátek eGovernmentu v roce 1999, kdy první elektronickou službou, kterou mohli občané využívat, bylo podávání žádostí o informace podle zákona o svobodném přístupu k informacím, prostřednictvím elektronické pošty. Z publikací věnujících se vývoji eGovenmentu se lze však domnívat, že úplný počátek se datuje od r. 1996, kdy vznikl Úřad pro státní informační systém, k němuž byla jmenována jako konzultativní orgán v oblasti záležitostí informační instituce Rada vlády pro státní informační politiku. Společně pak předložili první českou koncepci rozvoje elektronizace zvanou „Státní informační politika – cesta k informační společnosti“, jež byla v roce 1999 schválena a s ní o rok později i tzv. akční plán, jímž byl stanoven postup, jak dosáhnout transparentního, ekonomicky vhodného prostředí a zároveň vytvoření bezpečné a stálé informační společnosti.[11] Tyto cíle vybudování a fungování sjednocené národní komunikační infrastruktury měly zabezpečit propojení individuálních oddělení a informačních systémů tak, aby mohly vzájemně komunikovat a vyměňovat si mezi sebou data. V roce 2000 tak byl založen Úřad pro veřejné informační systémy, jež nahrazoval předešlý Úřad státních informačních systémů, jehož úkolem bylo odpovídat právě za strategické plánování v oblasti informačních systémů ve veřejné správě tak, aby to bylo v souladu se státní informační politikou.[12]

Obecně lze říct, že rok 2000 byl významným ve vývoji elektronizace veřejné správy v České republice. V roce 2000 nabyli účinnosti dva zákony, tj. zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, což představovalo první větší krok ve vývoji eGovernmentu. Díky tomuto zákonu došlo k vymezení jednotlivých pojmů jako je elektronický podpis, datová zpráva, akreditovaný poskytovatel certifikačních služeb, aj. Dále tento zákon stanovil povinnost pro orgány veřejné správy přijímat taková podání v elektronické formě, jež budou opatřena elektronickým podpisem. Všechny tyto povinnosti ohledně elektronických podání byla nadále upravena vyhláškou č. 496/2004 Sb., o elektronických podatelnách. Kromě tohoto převratného zákona nabyl účinnosti rovněž zákon. č. 365/2000 Sb., o informačních systémech veřejné správy a o změně

[11] Vláda České republiky. Státní informační politika – cesta k informační společnosti. [online]. Dostupné z: https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/

[12] ŠTĚDROŇ, B., *Úvod do eGovernmentu v České republice: právní a technický průvodce.* 1. vyd. Praha: Úřad vlády České republiky, 2007. ISBN 978-808-7041-253, s. 20

některých dalších zákonů, často užívaný pod zkratkou „zákon o ISVS“, jež byl vydán hlavně v souvislosti s nově zřízeným Úřadem pro veřejné informační systémy.

K roku 2003 zanikl Úřad pro veřejné informační systémy a bylo zřízeno nové Ministerstvo informatiky. Podle ust. § 18 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky (kompetenční zákon) bylo Ministerstvo informatiky „*ústředním orgánem státní správy pro informační a komunikační technologie, pro telekomunikace a poštovní služby*.“[13] Vzhledem k tomu, že Česká republika přistoupila k Evropské unii, musela se vytvořit nová strategie, jež by se přizpůsobila změnám nastalým v důsledku stáním se právoplatným členem. Po vzniku Ministerstva informatiky tedy došlo k výraznému odklonu od původních strategických dokumentů a byla vypracována nová Státní informační a komunikační politika, jež byla schválena v roce 2004, známá pod názvem e-Česko 2006. Tímto dokumentem, jež měl představovat obdobnou strategii eEurope 2005, mělo Česko dostát závazkům vůči Evropské unii, ke kterým se v rámci oblasti eGovernmentu zavázalo. Záměry a požadavky eEurope 2005 byly do české koncepce přijaty na základě posouzení tehdejšího stavu v ČR a to tak, aby bylo vyhověno evropským prioritám v měřítkách specifických potřeb České republiky.[14] Česko však celkem podstatné části stanovených cílů nedosáhlo.

K další velké změně došlo v oblasti eGovernmentu v České republice v roce 2006, kdy došlo s účinností od 1. 6. 2007 ke zrušení Ministerstva informatiky a většina jeho kompetencí přešla na Ministerstvo vnitra ČR. Pomocným orgánem pro Ministerstvo vnitra byla poté na základě usnesení č. 293 z 28. 6. 2007 ustanovena Rada pro informační společnost. Jednotlivé podobory byly rozděleny mezi ostatní ministerstva, např. působnost týkající se elektronických komunikací a poštovních služeb převzalo ministerstvo průmyslu a obchodu a působnost ve věcech veřejných dražeb přešla na Ministerstvo pro místní rozvoj.[15] S přechodem kompetencí na nová ministerstva byly stanoveny nové cíle a vytvářeny nové strategie. Jedna z nových strategií byla strategie se zaměřením na jiné cíle

[13] Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

[14] Culturenet. Státní komunikační a informační politika. [online]. Dostupné z: http://www.culturenet.cz/res/data/002/000269.pdf

[15] Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů

zvaná „Efektivní veřejná správa a přátelské veřejné služby – Strategie realizace Smart Administration v období 2007 – 2015“, k níž byly dodatečně vydány dokumenty jako „Strategie rozvoje služeb pro informační společnost“ a „Strategie implementace e- Governmentu v území.“ Prostřednictvím strategie realizace Smart Administration mělo dojít k zapojení informačních a komunikačních technologií do činností úřadů tak, aby došlo k efektivnější komunikaci občanů s úřady, a aby bylo regulováno přílišné papírování.[16] Strategie Smart Administration je zobrazována také jako tzv. hexagon, kdy každý vrchol hexagonu představuje klíčové prvky veřejné správy, a spolu v rámci vzájemného propojení tvoří symbol efektivní veřejné správy[17] (viz následující obrázek č. 1).

Obrázek č. 1: Hexagon efektivní veřejné správy, Smart Administration[18]

Vrcholy hexagonu představují organizaci, legislativu, občana, finance, technologii a úředníka. Organizace je jeden z nejdůležitějších prvků, neboť organizace činností veřejné správy je důležitá, aby bylo správně nakládáno s veřejnými prostředky a poskytovaly se kvalitní služby občanům. Legislativa je tady pro ochranu společenských hodnot a regulaci chování občanů. Dalším

[16] POMAHAČ, Richard a kol. Veřejná správa. 1. vydání. Praha: C. H. Beck, 2013. s. 216
[17] SMART ADMINISTRATION: Hexagon efektivní veřejné správy. [online]. Dostupné z: http://www.smartadministration.cz/clanek/hexagon-efektivni-verejne-spravy.aspx
[18] Hexagon efektivní veřejné správy, Smart Administration. [online]. Dostupné z: http://www.smartadministration.cz/clanek/hexa gon-efektivni- verejne-spravy.aspx

prvkem je samotný občan, na kterého je touto strategií zacíleno, kdy výsledkem by mělo být usnadnění komunikace občanů s orgány veřejné správy, umožnit jim kontrolovat činnosti veřejné správy a participaci na rozhodnutích veřejné správy. Občan jako klient veřejné správy představuje nejdůležitější prvek hexagonu. Dalším vrcholem hexagonu je úředník, který představuje velmi důležitý předpoklad k fungování veřejné správy, proto je na něj kladena vysoká odpovědnost za kvalitu výkonu a řízení. Velký důraz v rámci strategie je kladen také na rozpočtování, alokaci zdrojů a provázání veřejných rozpočtů. K tomu, aby vše bylo zajištěno a finance byly vynakládány efektivně slouží vrchol hexagonu zvaný finance. A celé je to propojeno moderní technologií, díky které je možné usnadnit komunikaci občana s úřady či komunikaci úřadů mezi sebou. [19]

Na základě této strategie také došlo k největším legislativním změnám od roku 2000, a to hlavně k přijetí průlomového zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který nabyl účinnosti k 1. 7. 2009 (někdy nazývaného jako zákon o eGovernmentu) a k přijetí zákona č. 111/2009 Sb., o základních registrech, který nabyl účinnosti k 1. 7. 2012. Stejně tak se do roku 2007 začalo využívat několika specializovaných komunikačních kanálů informačních systémů veřejné správy, jako jsou katastr nemovitostí, obchodní rejstřík, registr ekonomických subjektů (tzv. ARES), centrální registr vozidel či rejstřík politických stran a hnutí, a spousty dalších. [20]

V červenci roku 2013 Ministerstvo vnitra aktualizovalo dokument s názvem Strategický rámec rozvoje eGovernmentu 2014+. Tento dokument hodnotí dosavadní průběh elektronizace veřejné správy, stanoví cíle pro období 2014 až 2020 a vymezuje podmínky jak těchto cílů. dosáhnout. Mezi základní cíle tohoto předělávaného dokumentu patří umožnit v roce 2020 nejméně 85% podání vůči veřejné správě podat kompletně elektronicky či realizovat úplná elektronická podání bez nutnosti uvádět a ověřovat údaje doložitelné z propojeného datového fondu veřejné správy. [21]

---

[19] MINISTERSTVO VNITRA ČR. Efektivní veřejná správa a přátelské veřejné služby: Strategie realizace Smart Administration v období 2007-2015. 2007, http://www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx, 25. 2. 2013, s. 55-57

[20] ŠTĚDROŇ, B., *Úvod do eGovernmentu v České republice: právní a technický průvodce.* 1. vyd. Praha: Úřad vlády České republiky, 2007. ISBN 978-808-7041-253, s. 38-41.

[21] VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6., s. 25

[21] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1. str. 26

V roce 2018 přijala Vláda České republiky svým usnesením Strategii koordinované a komplexní digitalizace České republiky 2018+ zvanou také jako „Digitální Česko“. Tato strategie rozlišuje vládní priority do třech provázaných pilířů, tj. Česko v digitální Evropě, Digitální ekonomika a společnost a Informační koncepce ČR.[22] Právě pilíř Informační koncepce ČR se zabývá rozvojem eGovernmentu a zaměřuje se na splnění pěti hlavních cílů, tj. na naplnění uživatelsky přívětivé a efektivní on-line služby pro občany a firmy, digitálně přívětivou legislativu, rozvoj prostředí podporujícího digitální technologie, zvýšení profesionality veřejné správy, efektivní a centrálně koordinované ICT státu a efektivní a pružný digitální úřad.[23] V oblasti digitálních služeb se strategie zaměřuje na naplnění zejména rozvoje Portálu veřejné správy, jakožto centrálního webu státu, který bude jediným rozcestníkem pro všechny služby občanům. Tento program si ale dává za cíl i profesionalizaci veřejné správy v oblasti ICT, zajištění dostatečných financí na digitalizaci a posilování centrální digitální autority. Digitalizace se smí pohybovat v mezích obecných principů eGovernmentu a to způsobem, jak uvádí Akční plán EU. Mezi tyto zásady řadíme především digitalizaci služeb jako standardní položka v běžném životě, poskytování informací občanů veřejné správy pouze jednou, transparentnost a otevřenost, zajištění bezpečnosti a ochrany soukromí, a především uživatelská přívětivost. Digitální Česko krom jiného slibuje též zlepšení kvalty a zvýšení kvantity otevřených dat. Celý program digitalizace služeb by tak měl proběhnout do pěti let.[24]

1.2. Důležité pojmy

Celá práce je doprovázena dvěma důležitými termíny, a to pojmem služba, převážně ta elektronická, a informační systémy. Pro lepší pochopení slouží tato kapitola k objasnění těchto termínů, bez kterých by se tato práce neobešla.

[22] Ministerstvo vnitra České republiky. Rada vlády pro informační společnost. Program Digitální Česko. [online]. Dostupné z: https://www.mvcr.cz/webpm/clanek/rada-vlady-pro-informacni-spolecnost.aspx?q=Y2hudW09Ng%3D%3D

[23] Digitální Česko. Základní informace o programu. [online]. Dostupné z: https://www.digitalnicesko.cz/zakladni-informace/

[24] [Ne]digitální Česko. Zpráva o plnění vládních slibů v oblasti digitalizace. Rekonstrukce státu. [online]. Dostupné z: https://www.rekonstrukcestatu.cz/download/3nQoIg/nedigitalni_cesko.pdf

1.2.1. Elektronické služby

Pro oblast eGovernmentu jsou elektronické veřejné služby (e-služby) důležitou kategorií. Služba obecně představuje takovou činnost, jež uspokojuje lidské potřeby. Tyto služby je možné rozdělit dle způsobu jejich hrazení. Prvním dělením jsou služby, které uspokojují zájmy jednotlivce, a které si jednotlivec sám i hradí z vlastních soukromých zdrojů. Druhým dělením jsou služby uspokojující kolektiv, veřejnost, a jsou proto hrazeny veřejnou správou veřejnými zdroji. Jednou z těchto kolektivních potřeb, jež jsou hrazeny z veřejných zdrojů, jsou právě elektronické služby.

E-služba je informační službou. Nové technologie jsou považovány za nástroj, který snižuje nejistotu a riziko v kvalitě informací. Právě vyhledávání informací a jejich získávání a rovněž obsah webových umístění hraje roli v hodnocení kvality služeb jejich uživatelem.

Jak již bylo řečeno výše, elektronické služby poskytují hlavně jejich uživatelům větší pohodlí. Jedná se hlavně o snížení byrokratické zátěže pro veřejnost a podnikatele, kdy např. díky elektronizaci veřejné správy už nemusí subjekty opakovaně dávat různým orgánům stejné údaje, mohou značnou část svých povinností vyřešit dálkovým přístupem, tedy bez nákladů na dojíždění a čas, a mohou těchto služeb využívat i mimo pracovní hodiny úřadů. Jde tedy o službu, kdy většinou neprobíhá přímá asistence interakce s člověkem, jakožto agentem služby.[25] Je však nutno přiznat, že tato výhoda může být rovněž nevýhodou, neboť kontakt občana s úřadem je mnohdy pro řešení dílčích problémů nezbytný.[26]

Elektronické služby též dopomáhají k demokratizaci veřejné správy, tj. k participaci občanů na veřejné správě. eParticipaci si pak lze představit v tom nejširším slova smyslu, tj. jako možnost volit zastupitele v elektronických volbách (e-voting), možnost elektronických referend či elektronických petic, možnost různých internetových diskusních skupin, fór, kde by bylo možné klást elektronickou cestou dotazy úřadům a voleným zástupcům. Tento princip eParticipace také umožňuje kontrolu transparentnosti rozhodování veřejné správy prostřednictvím tzv. otevřených dat, a díky tomu omezení často zmiňovaného korupčního jednání.

---

[25] ŠPAČEK, David. *Public management. V teorii a praxi*. 1. vydání. Praha: C. H. Beck, 2016, ISBN: 978-80-7400-621-0. s. 289

[26] MINISTERSTVO VNITRA: Elektronické služby eGovernmentu [online]. Dostupné z: https://www.mvcr.cz/clanek/elektronicke-sluzby-egovernmentu.aspx

EGovernment není ale pouze výhoda pro koncové uživatele, ale také pro samotné zaměstnance veřejné správy, neboť tímto zjednodušením celého procesu získají více času věnovat se jednotlivým adresátům bez nutnosti zdlouhavého papírování.[27] Toto zvýhodnění na straně orgánů veřejné moci představuje personální, materiální a finanční úspory při výkonu činnosti veřejné správy. Konkrétně může jít o hromadné zpracovávání standardizovaných elektronických žádostí a o automatizaci rutinních činností díky dálkovému přístupu do sdílených elektronických databází, s čímž úzce souvisí zvýšení rychlosti rozhodování a snižování nákladů v důsledku snižování počtu zaměstnanců orgánů veřejné správy.

1.2.1.1. Kategorie služeb eGovernmentu

Elektronické služby, které eGovenrment poskytuje, lze též rozdělit do kategoriií. Nejčastěji se v literatuře setkáme s popisem jednotlivých kategorií pomocí zkratek, tj. G2C, G2B a G2G.

Zkratka G2C představuje pojem „Government to Citizen“ nebo také „Government to consumer“. Tato kategorie se zabývá zdokonalováním služeb s koncovými zákazníky z hlediska poskytování informací, zpracování žádostí, transakčních služeb a participace v rámci demokratizace veřejné správy. G2C tedy usnadňuje občanům komunikaci s úřady tím, že např. zprovozní internetové či elektronické portály konkrétních úřadů, které budou obsahovat informace pro řešení různých životních situací. V České republice tento koncept splňuje např. Portál veřejné správy. Příkladem mohou být také služby občanům, které poskytuje Czech POINT, např. výpis z rejstříku trestů.

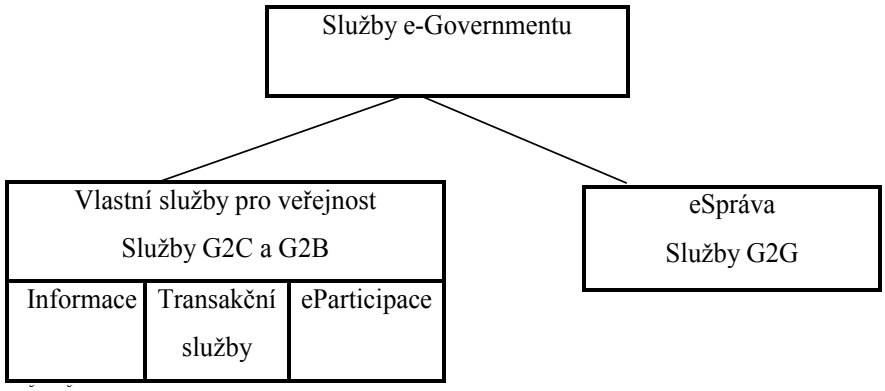
G2B nebo-li „Government to Business“ vyjadřuje vztah a komunikaci mezi subjekty veřejné správy a různými organizacemi, včetně podniků a neziskových organizací. Cílem je zjednodušení komunikace mezi úřady a odnky. Příkladem může být opět elektronický portál, např. v rámci zadávání veřejných zakázek.

Význam zkratky G2G je „Government to government“, tj. zdokonalování a modernizace vládních procesů z hlediska interních pracovních a řídících procesů institucí a systému veřejné správy se zapojením informačních technologií. [28]

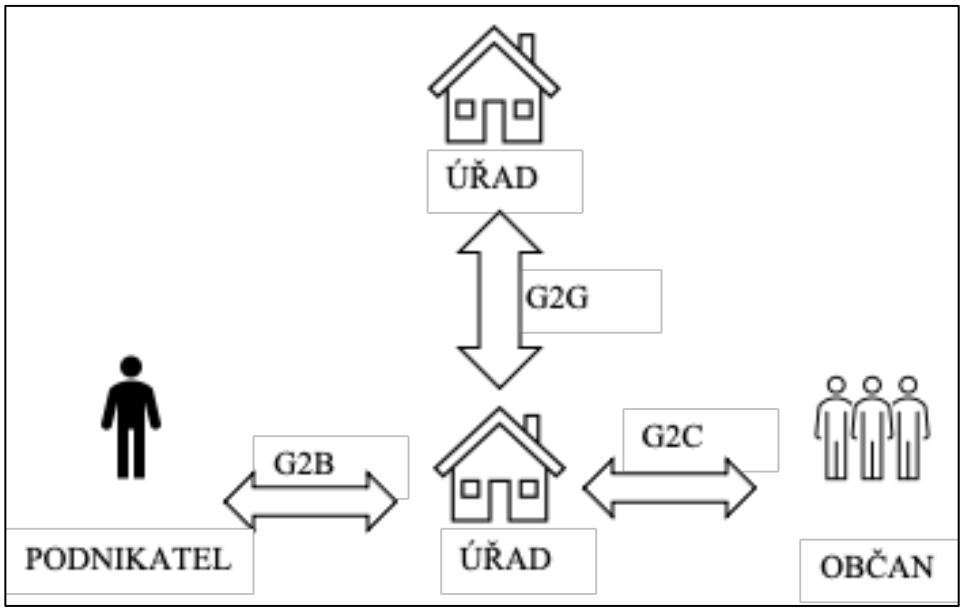
[27] MATES, P., SMEJKAL, V. *E-government v českém právu*. Praha: Linde Praha, 2006, ISBN 80-7201-614-8, s. 9.
[28] POMAHAČ, Richard a kol. *Veřejná správa*. 1. vydání. Praha: C. H. Beck, 2013. ISBN: 978-80-7400-447-6, s. 187.

Příkladem můžeme uvést např. data zveřejněná katastrem nemovitostí či různé registry veřejné správy (např. centrální evidence obyvatel).

Názorné rozdělení služeb eGovernmentu popisuje následující obrázek.



Obrázek č. 2: Členění e-Governmentu [29]



Obrázek č. 3: Komunikační služby e-Governmentu[30]

[29] ŠPAČEK, David. Kategorie služeb e-governmentu in: EGovernment: cíle, trendy a přístupy k jeho hodnocení. 1. vydání. Praha: C.H. Beck, 2012, ISBN 978-80-7400-261-8, s. 6
[30] Vlastní zdroj.

1.2.2. Informační systémy veřejné správy

„*Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy*.“[31]

Informační systémy (dále též jen ISVS) představují jeden ze základních pojmů eGovernmentu. Jsou upraveny zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „zákon o ISVS“) a jejich cílem je ucelený a uspořádaný, pro uživatele přívětivý systém, díky kterému mohou komunikovat občané s orgány veřejné správy a orgány veřejné správy navzájem bez jakýchkoliv potíží. Rozvoj, výstavbu a metodické řízení ISVS zajišťuje Ministerstvo vnitra. To je také kontrolním orgánem ISVS a správcem Centrálního místa služeb[32], prostřednictvím kterého orgány veřejné správy využívají sítě elektronických komunikací v rámci ISVS.[33]

Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností“[34]. Slouží tedy k bezpečné výměně dat mezi subjekty komunikace a informace, které ISVS poskytují, jsou důležitým prvkem pro rozhodování správních orgánů o právech a povinnostech adresátů veřejné správy.[35]

ISVS mají, jak je řečeno ve výše uvedené definici, sloužit veřejné správě, respektive jejímu výkonu. Informační činnost zahrnuje nejen získávání a poskytování informací, ale také jejich shromažďování, hodnocení, ukládání a uchovávání, vyhledávání a úpravu dat, jejich předávání, šíření, zpřístupňování, aj. Všechny tyto činnosti vykonávají subjekty, jako jsou správci, provozovatelé a uživatelé ISVS pomocí informačních a komunikačních technologií. Práva a povinnosti správců ISVS jsou upraveny zákonem o ISVS. Podle tohoto zákona je

[31] Ministerstvo vnitra České republiky. Informační systémy veřejné správy. [online]. Dostupné z: https://www.mvcr.cz/clanek/informacni-systemy-verejne-spravy.aspx

[32] „Centrálním místem služeb se rozumí soubor technického a programového vybavení, jehož prostřednictvím jsou poskytovány služby informačních systémů veřejné správy a jehož prostřednictvím jsou využívány a propojovány sítě elektronických komunikací.“ in §6 h odst. 1 ZZákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

[33] Ministerstvo vnitra České republiky. Informační systémy veřejné správy. [online]. Dostupné z: https://www.mvcr.cz/clanek/informacni-systemy-verejne-spravy.aspx

[34] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. § 2 písm. b)

[35] SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů: právní a technologické aspekty*. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004. ISBN 80-7179-765-0.s. 225

správcem ISVS „*osoba nebo její součást, která poskytuje služby informačního systému veřejné správy a za informační systém veřejné správy odpovídá*“.[36] Jedná se vždy o orgány veřejné správy, konkrétně ministerstva, jiné ústřední orgány státní správy a jejich územní pracoviště (např. katastrální úřady), veřejné ozbrojené i neozbrojené sbory a územní samosprávné celky.[37] Provozovatelem ISVS se rozumí osoba nebo její součást, která zaručuje funkčnost technických a programových prostředků, které tvoří ISVS. Provozovatelem však může být i jiná osoba, která bude správcem ISVS pověřena.[38] Uživatelem ISVS je taková osoba, která data do systému zapisuje či je využívá. Uživatelem tak může být správce i provozovatel, využívají-li ISVS při výkonu veřejné správy.[39]

Mezi základní ISVS řadíme především základní registry veřejné správy, ale spadají sem také různé evidence, seznamy, katalogy, katastry či rejstříky. Mezi ISVS naopak nepatří informační systémy, které jsou vedené za účelem potřeby zajišťování obrany státu, nakládání s utajovanými informacemi, informační systémy vedené bezpečnostními sbory a další tomu podobné.[40]

1.2.2.1. Portál veřejné správy

Jedním z nejvýznamnějších informačních systémů veřejné správy je Portál veřejné správy. Jedná se o jeden z nástrojů eGovernmentu a považuje se za klíčový prvek z hlediska vývoje eGovernmentu v České republice. Právně je portál veřejné správy upraven zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o jeho správu se stará Ministerstvo vnitra. Ke spuštění portálu došlo v roce 2003 na webovém serveru www.portal.gov.cz.

Portál veřejné správy představuje „*informační systém veřejné správy zajišťující přístup k informacím veřejných orgánů a komunikaci s veřejnými orgány.*“[41] Jedná se o univerzální portál, který je zaměřen na jednoduchost a využitelnost širokou veřejností. Cílovými subjekty jsou tedy jak občané, orgány státní správy i samosprávy či podnikatelé či živnostníci České republiky ale rovněž

[36] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. § 2 písm. c)
[37] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 54
[38] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. § 2 písm. d)
[39] Tamtéž. § 2 písm. e)
[40] Tamtéž. § 1
[41] Tamtéž. § 6g odst. 1

cizinci. Proto je přehledně rozdělen do čtyř sekcí podle cílových skupin na Občan, Podnikatel, Cizinec a Úředník. Systém není uživatelsky náročný, neboť má reprezentovat nejjednodušší cestu k informacím a službám celé veřejné správy, což umožňuje využívat jeho služeb i počítačově negramotné populaci. Na jednom místě lze nalézt zveřejňované a veřejně přístupné informace veřejné správy včetně zákonů, různých druhů formulářů elektronického podání, návodů na řešení všech životních situací ve vztahu k orgánům veřejné moci aj. Součástí portálu je rovněž přímý přístup do uživatelského rozhraní datových schránek a na informační stránky Czech POINTu. [42]

Součástí portálu je rovněž tzv. portál občana, který od roku 2018 nabízí mimo jiné přihlášení občanů prostřednictvím elektronického občanského průkazu. Občané, jež využijí těchto služeb mají možnost nastavit si v portálu svůj osobní profil a využívat tak přímo služeb jež portál poskytuje, jako např. podání žádostí ale třeba i možnost kontrolovat své údaje jakožto občana České republiky, které jsou evidovány v základních registrech nebo například podávat svá daňová přiznání fyzických osob. [43]

1.3. Legislativa

Současná právní úprava eGoverenmentu se opírá o několik stěžejních zákonů, které jsou rovněž doplněny o značné množství podzákonných doprovodných předpisů. Bezpochyby se opírá o ústavní základy v Ústavě ČR a Listině základních práv a svobod, jakožto právních předpisech s nejvyšší právní silou. Legislativa umožňuje jednotlivým složkám eGovernmentu legálně fungovat a umožňuje veřejné správě i veřejnosti plnit a využívat jejich funkcí i služeb. Otázka právního zakotvení problematiky elektronizace do právního řádu jako celku vyžaduje vytvoření právního rámce, jenž by upravoval každý jednotlivý prvek eGovernmentu a stejně tak by reagoval na neustále se vyvíjející výpočetní techniku a schopnosti jejích uživatelů. Vzhledem k faktu, že k elektronizaci veřejné správy a s ní spojenou bezpečností se váže velké množství předpisů, kterým není možné věnovat pouze jednu kapitolu, je zde uveden pouze základní rámec právních

[42] Portál veřejné správy, © 2018. Ministerstvo vnitra České republiky. [online]. Dostupné z: https://www.mvcr.cz/clanek/portal-verejne-spravy.aspx
[43] Ministerstvo vnitra ČR. Přes Portál občana zjistíte stav bodového konta řidiče a jednoduše podáte i daňové přiznání. [online]. Dostupné z: https://www.mvcr.cz/clanek/pres-portal- obcana-zjistite-stav-bodoveho-konta-ridice-a-jednoduse-podate-i-danove-priznani.aspx

předpisů. Mezi stěžejní zákonné normy upravující současný rozsah eGovernmentu v České republice, lze zařadit:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.
- Zákon č. 111/2009 Sb., o základních registrech,
- Zákon č. 634/2004 Sb., o správních poplatcích
- Vyhláška č. 496/2004 Sb., o elektronických podatelnách
- Vyhláška č. 364/2009 Sb., o seznamu obecních úřadů a zastupitelských úřadů, které jsou kontaktními místy veřejné správy
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů,
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých zákonů.

Tyto základní právní předpisy v oblasti eGovernmentu rovněž dopadají na velké množství jiných právních předpisů, které bylo nezbytné novelizovat tak, aby byly s těmito zákony v souladu. Jako příklad lze uvést zákon č. 99/1963 Sb., občanský soudní řád, zákon č. 141/1961 Sb., o trestním řízení soudním, zákon č. 150/2002 Sb., soudní řád správní či zákon č. 500/2004 Sb., správní řád a řadu dalších jiných předpisů, např. zákon č. 325/1999 Sb., o azylu, zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky, zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů a spousty dalších.

Jedním z nejdůležitějších zákonů, kterým byl ovlivněn chod eGovernmentu je zákon č. 101/2000 Sb. o ochraně osobních údajů. Tato právní norma se vztahuje na zpracování osobních údajů státními orgány, orgány územní samosprávy, jinými orgány veřejné moci, jakožto i fyzickými a právnickými osobami, kdy přenáší

odpovědnost za ochranu osobních údajů na samotného občana, který sám určí, zda udělí či neudělí souhlas se zpracováním svých osobních údajů. S tímto zákonem také úzce souvisí zákon č. 106/1999 Sb., o svobodném přístupu k informacím, kdy zásadním východiskem svobody informací je tzv. publicita veřejné správy, který upravuje, jaké údaje může veřejná správa poskytnout. Před přijetím tohoto zákona bylo stanoveno, že orgán veřené správy, úřad, může poskytnou pouze informace, na které má žadatel o ně nárok (např. účastník stavebního řízení). V současné době, díky přijetí tohoto zákona platí, že se poskytne jakákoliv informace z veřejné správy, s výjimkami zákonem stanovenými (např. ochrana osobních údajů či utajované skutečnosti).[44]

Využívání internetu a různé výpočetní techniky a elektronických zařízení sebou přináší hrozbu narušení bezpečnosti přenášených dat a hrozbu narušení celé informační infrastruktury. Proto další legislativou, která sice netvoří samotný eGovernment, ale je s ní velice úzce spjata, jsou legislativní rámce ochrany osobních údajů při jejich zpracování, kyberbezpečnosti a důvěryhodnost elektronických transakcí.

1.3.1. Nařízení GDPR

Nařízení Evropského parlamentu a Rady EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“) přineslo spousty změn v ochraně osobních údajů. Toto nařízení upravuje legislativní rámec ochrany osobních údajů v rámci celého území EU, přičemž hájí práva občanů při neoprávněnému zacházení s jejich daty a osobními údaji. Úprava GDPR se dotýká veškerých subjektů, jež různým způsobem pracují s daty jednotlivých fyzických osob, a vznikla jako reakce na pokrok v oblasti komunikačních a informačních technologií, kdy bylo důležité zamezit obchodování s osobními údaji, které se stávalo stále častějším.[45] GDPR se týká všech firem a institucí, a stejně tak jednotlivců a online služeb, jejichž činností je zpracovávání dat uživatelů. GDPR je striktním nařízením, které zavedlo astronomické pokuty za porušování pravidel a nařizuje některým správcům nebo zpracovatelům osobních údajů zřídit

[44] VAVROCHOVÁ, S., ČEJP, V., ŠTĚPÁNKOVÁ, M., SAMKOVÁ, B., PŘICHYSTAL, A. *Vzdělávání v eGovernmentu*. 1. vyd. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, a.s. 2014. ISBN 978-80-86847-74-0. s. 13

[45] GDPR (obecné nařízení). [online]. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938.

nezávislou kontrolní funkci zvanou DPO (Data Protection Officer), neboli pověřence pro ochranu osobních údajů.

GDPR vymezuje principy práce s osobními a citlivými údaji, a to v oblasti práv a možností fyzických osob, resp. vlastníků osobních údajů, tak v oblasti povinností jejich zpracovatelů, jež jsou povinni veškerý proces zpracování údajů evidovat. Do široké škály práv občanů v rámci GDPR patří zejména práva na přístup, opravu, výmaz, právo být zapomenut, právo na omezení zpracování, přenositelnost údajů a v neposlední řadě právo vznést námitku. Jako občané máme tato práva ke všem údajům, které o nás jsou vedeni správcem a jsou mu k dispozici, tj. i k tzv. nestrukturovaným údajům, jež mohou tvořit přílohy e-mailů nebo které jsou uloženy na různých interních a externích úložištích. Občan má také možnost větší kontroly nad svými údaji, proto v případě, že se jeho osobní údaje zpracovávají automatizovaně, má právo získat tyto osobní údaje o jeho osobě ve strukturovaném a strojově čitelném formátu a může je dále předat jinému správci. Toto právo by vzhledem ke své povaze nemělo být uplatňováno vůči správcům, jež zpracovávají osobní údaje v rámci výkonu veřejné moci.[46]

1.3.2. Kyberbezpečnost

Problematika kyberbezpečnosti veřejné správy je stále důležitejší úměrně tomu, jaké množství citlivých dat veřejná správa začíná sdílet. Významným právním předpisem upravujícím oblast ochrany a bezpečnosti eGovernmentu je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů. Tento zákon již prošel dvěma novelami, oběma v roce 2017, jako reakce na stále větší pokrokovost v informačních a komunikačních technologií, a to tzv. Malou novelou a Velkou novelou. Malá novela pouze přidala k povinným osobám provozovatele informačních či komunikačních systémů a vymezila vztahy mezi nimi a správci těchto systémů. O dost větší a rozsáhlejší změny však přinesla tzv. Velká novela, která vznikla o měsíc později po Malé novele, jako reakce na přijetí přijetí evropské směrnice č. 2016/1148, o síťové bezpečnosti (NIS). V rámci této novely opět došlo k rozšíření okruhu povinných osob, které se nově staly zákonu o kybernetické bezpečnosti podřízeny, a nově byly uloženy určité povinnosti poskytovatelům

[46] GDPR. Obecné nařízení o ochraně osobních údajů prakticky. [online]. Dostupné z: https://www.gdpr.cz/gdpr/prava/

digitálních služeb. Tato směrnice rovněž zavádí nová bezpečnostní pravidla a pravidla pro hlášení bezpečnostních incidentů a má snahu o prohloubení mezinárodní spolupráce, především mezi jednotlivými členskými zeměmi v oblasti kybernetické bezpečnosti. Tato směrnice NIS zřizuje členským státům Evropské Unie povinnost zřídit státní orgán, jenž bude spravovat a zajišťovat kybernetickou bezpečnost. Proto bylo kromě jiného Velkou novelou vytvořen Národní úřad pro kybernetickou a informační bezpečnost (dále také jen „NÚKIB“). Jeho hlavní povinností je kontrola dodržování zákona o kybernetické bezpečnosti. Tato kontrola probíhá v případě, existuje-li podezření na porušení některých ze zákona stanovených povinností provozovatelů informačních a komunikačních systémů, nebo je-li podezření na bezpečnostní narušení. [47]

[47] CO JE NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB [online]. Brno, 2017. Dostupné z: https://www.govcert.cz/

2. Symboly eGovernmentu

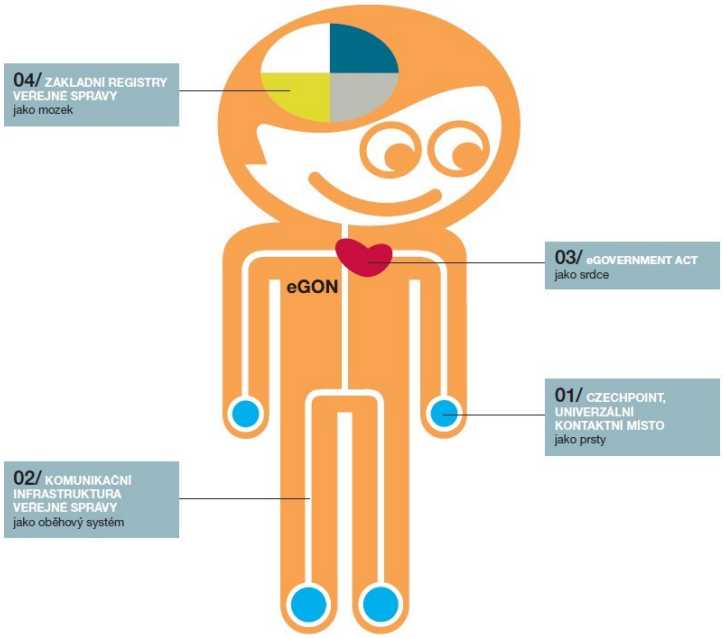
Je zvykem, že každý projekt něco symbolizuje. Něco, co se vybaví vždy, když se zmíní daný název, místo či služba, aj. I eGovenrment má takové symboly, které sice vznikaly postupně, avšak do podvědomí občanů se dostaly poměrně rychle. Jedná se o symboly, které symbolizují nejen postupný vývoj eGovernmentu v České republice, ale které symbolizují i občana samotného, neboť eGovernment představují „panáčci“, kteří jsou prezentováni jako živé organismy. Bylo samozřejmě důležité brát ohled i na genderovou vyváženost, proto symboly českého eGovernmentu jsou muž a žena, **eGON a Klaudie.**

2.1. eGON a Klaudie

Nejznámější složkou a symbolem celé elektronizace veřejné správy je schéma eGovernmentu – postavička eGONa. Tato postavička se zrodila v roce 2006 a představuje komplexní projekt, který řeší elektronizaci veřejné správy. Jeho cílem a snahou bylo vytvoření vhodného prostředí pro efektivní sdílení dat ve veřejné správě, které do té doby neexistovalo, a zefektivnění tak veřejné správy a usnadnění života občanů pomocí informačních a komunikačních technologií. Název eGON vznikl spojením tří začátečních písmen ze slova eGovernmentu – „eGO“ a anglické zkratky pro slovo zapnuto - „ON“. Doslovně lze tedy název tohoto symbolu přeložit jako „eGovernment zapnut“.

eGon je vyobrazován jako živý organismus, jehož životní funkce zabezpečují propojený fungující systém čtyř základních projektů českého eGovernmentu a umožňuje efektivně a bezpečně sdílet data uvnitř veřejné správy, přičemž se řídí heslem „Obíhat úřady mají doklady nebo data, ne občan“.[48] Základní projekty českého eGovernmentu jsou znázorněny v obrázku.

[48] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1. s. 15



Obrázek č. 4: Symbol eGovernmentu - postavička eGona[49]

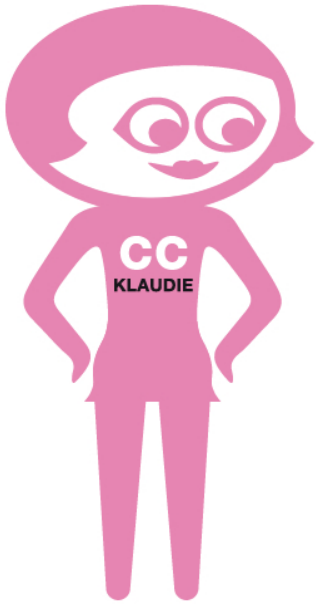
eGONovo srdce tvoří Zákon o eGovernmentu (eGovernment Act), který má za cíl zrovnoprávnění elektronických a papírových dokumentů a vytvoření vhodných podmínek pro elektronickou komunikaci. Mozek eGONa je znázorněn čtyřmi různě barevnými části, které symboluzují jednotlivé základní registry veřejné správy. Tyto registry jsou tzv. pamětí eGovernmentu, neboť obsahují data o občanech, státních a nestátních subjektech a zajišťují jejich propojení. Snadný kontakt občanů s veřejnou správou zajišťují kontaktní místa veřejné správy, tj. Czech POINT, znázorněný jako eGonovy prsty. Důležitou funkcí pak je Komunikační infrastruktura veřejné správy, znázorňující oběhovou soustavu, jejímž cílem je propojení všech eGonových orgánů.[50] Postavička je svým způsobem propagací eGovernmentu v České republice a má za úkol zviditelnit všechny jeho součásti a služby, kterých mohou občané využívat.

Projekty eGovernmentu se postupně stávaly finančně neudržitelnými pro další roky provozu, neboť náklady na provoz nových komplikovanějších a více provázaných systémů narůstaly a možnosti kde náklady snížit naopak klesaly. Z toho důvodu v roce 2011 se k eGONu přidala Klaudie, jakožto další ze symbolů

[49] Ministerstvo vnitra. [online]. Dostupné z http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu- moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx
[50] Ministerstvo vnitra. [online]. Dostupné z http://www.mvcr.cz/clanek/egon-jako-symbol-egovernmentu- moderniho-pratelskeho-a-efektivniho-uradu-252052.aspx

elektronizace. Klaudie představuje tzv. cloud computing[51], který má umožnit, aby ICT projekty nebyly pouze efektivnější a levnější, ale aby došlo k nákupu a využívání služeb v prostředí více transparentním, lépe měřitelným a snáze předvídatelným. Smysl projektu je tedy vyšší užitečnost a účelnost. Klaudie má za cíl poskytovat služby pro orgány veřejné moci a jejich klienty, a to nepřetržitě a celoplošně.

Stejně jako eGON, i Klaudie je vyobrazována jako živý organismus. Její životní funkce tvoří hlavně srdce Klaudie - CMS 2.0, nebo-li nová verze Centrálního místa služeb, které zabezpečují spolehlivé propojení sítí orgánů veřejné správy, a které poskytují společné technické, softwarové a bezpečnostní služby. Tato nová verze byla plně integrována do komunikační infrastruktury veřejné správy a zajistila tak možnost komunikace se systémy EU a standardy poskytovaných služeb a jejich rozhraní. Součástí Klaudie jsou dále tzv. eGON centra, která se podílejí na spolehlivém a bezpečném spojení služeb a eGON služby poskytované orgány veřejné moci, a to na všech úrovních veřejné správy.[52]



Obrázek č. 5: Symbol eGovernmentu - postavička Klaudie[53]

[51] *„Cloud computing je doručování výpočetních služeb, včetně serverů, úložišť, databází, sítí, softwaru, analytických nástrojů a inteligentních funkcí, přes internet („cloud“) a nabízí rychlejší inovace, flexibilitu prostředků a cenové výhody. Obvykle platíte jenom za cloudové služby, které skutečně využijete, což pomáhá snižovat provozní náklady, efektivněji provozovat infrastrukturu a škálovat s ohledem na měnící se obchodní potřeby.*“ Zdroj: Microsoft Azure. Co je cloud computing? Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/

[52] Egovernment: Klaudie – spadla z oblak a kulhá? [online]. 2011. ISSN 1801-9420. Dostupné z: https://www.egovernment.cz/soubor/2011-2/

[53] Ministerstvo vnitra. [online]. Dostupné z: https://www.mvcr.cz/clanek/ministerstvo-vnitra-predstavilo-klaudii-novy-symbol-egovernmentu.aspx

3. Vybrané pilíře eGovernmentu

V následujících podkapitolách budou podrobněji popsány jednotlivé projekty eGovernmentu. Vzhledem k množství projektů, které již existují, a i k těm, které budou v brzké budoucnosti realizovány, není možné aby byly všechny obsažené v jedné kapitole, ba i v celé práci. Proto je tato kapitola zaměřena pouze na některé vybrané nástroje eGovernmentu, a to především na ty základní.

3.1. Komunikační infrastruktura veřejné správy (KIVS)

Devadesátá léta znamenaly velký vývoj v oblasti informačních systémů ve veřejné správy. Právě v této době začaly jednotlivé instituce veřejné správy budovat své vlastní informační systémy. Vzhledem k rychlému rozvoji technologií a legislativy bylo nezbytné tyto systémy spojit v jeden, a to propojením všech stávajících systémů. Díky tomu vznikla první koncepce KIVS, na které stojí celý chod eGovernmentu. KIVS je prvním ze základních pilířů, k jehož realizaci nebylo potřeba legislativních změn. Je součástí těla eGONa, resp. je jeho oběhovou soustavou, což znamená, že protíná všechny důležité orgány eGONa, tj. zajišťuje přenos dat mezi jednotlivými informačními systémy veřejné správy.

Vývoj projektu KIVS začal v roce 2001, kdy byla uzavřena Rámcová smlouva na poskytování služeb KIVS mezi státem a společností ČESKÝ TELECOM a.s., a to na dobu pěti let. Důležitým milníkem byl rok 2004, kdy byl schválen program Státní informační a komunikační politiky. V následujících letech pak byly vypracovány nové koncepce KIVS a byly uzavírány nové rámcové smlouvy o poskytování datových či hlasových služeb. Ty následně upravovaly povinnosti a jiné aspekty součinnosti mezi Centrálním místem služeb, jakožto centrálním zadavatelem, a příslušnými poskytovateli. KIVS je tedy realizována prováděcími smlouvami mezi provozovatelem, jednotlivými orgány veřejné moci a Centrálním místem služeb.

Centrální místo služeb (dále též jen „CMS“) je podstatnou součástí KIVS, neboť umožňuje úředníkům veřejné správy získat prostřednictvím služeb CMS bezpečný a efektivní přístup k informacím. CMS vytváří logické místo, které slouží

k propojení elektronických komunikací a operátorů telekomunikačních infrastruktur, jejichž úkolem je především poskytování služeb pro KIVS.[54]

V současné době je KIVS nedílnou součástí eGovernmentu. Zajišťuje „*poskytování služeb pro ústřední orgány veřejné správy, organizační složky státu a jejich příspěvkové organizace, případně i jiné subjekty veřejné správy, které o zajištění takové činnosti Ministerstvo vnitra (předtím Ministerstvo informatiky) požádaly a uzavřely s ministerstvem za tím účelem příslušnou smlouvu.“* [55] Z toho výplývá, že se nejedná o službu přímo poskytovanou občanům, ale pouze o služby poskytované v rámci státní správy.

3.2. CzechPOINT

CzechPOINT, celým názvem Český Podací Ověřovací Informační Národní Terminál, neboli kontaktní místo asistovaného výkonu veřejné správy, je jeden z nejvýznamnějších milníků v rámci vývoje českého eGovernmentu. Cíl tohoto projektu byl založen na zjednodušení komunikace občana s úřady a upuštění od zbytečné byrokracie tím, že se vybuduje síť kontaktních míst veřejné správy, kde bude možné občanům poskytnout data z různých informačních systémů na jednom místě. Než byl projekt spuštěn, byla vždy pro komunikaci s úřadem nezbytná osobní přítomnost občana a leckdy pro získání potřebných dokumentů občanem bylo nutné být přítomen na více než jednom úřadě. Občan tak ztrácel čas čekáním na jednotlivé úkony na různých úřadech, které kolikrát nejsou ani v nějaké dostupné vzdálenosti mezi sebou a úřadům tak vznikala vysoká míra administrativních úkonů. Základní myšlenkou informačního systému CzechPOINT je „Konec běhání po úřadech“, proto úkolem bylo vybudovat síť kontaktních míst veřejné správy, kde budou schopni občanům na jednom místě poskytnout data z různých informačních systémů a zjednodušit tak jejich komunikaci s příslušnými úřady. To se podařilo a CzechPOINT je jedním ze systémů českého eGovernmentu, který už 14 let naplňuje heslo: "obíhat mají data, ne občan" a je plně funkční.[56]

[54] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1. str. 147
[55] Tamtéž. str. 144
[56] ŠPAČEK, David. *EGovernment: cíle, trendy a přístupy k jeho hodnocení.* 1. vydání. Praha: C.H. Beck, 2012, ISBN 978-80-7400-261-8. s. 86.

Vznik projektu je spojeno se vznikem projektu eGON a ostatními projekty, jež vedly k rozšíření služeb eGovernmentu. Prvně byl CzechPOINT spuštěn roku 2007, jako jeho pilotní verze, kdy bylo zprovozněno první kontaktní místo veřejné správy, a mělo otestovat všechny potřebné úkony spojené s provozováním kontaktního místa. Postupně bylo spuštěno dalších 37 kontaktních míst a do provozu se zapojilo i desítky pracovišť České pošty. V roce 2008 byl projekt CzechPOINT oficiálně spuštěn na území celé České republiky.[57]

V rámci postavičky eGONa je CzechPOINT znázorňován jako prsty, jež symbolicky představují pomocnou ruku při zpracovávání požadavků klienta veřejné správy. Pomocná ruka znázorňuje rovněž na kontaktních místech vždy přítomného asistenta, jenž zpracovává požadavky klienta CzechPOINT. Tyto požadavky klientů lze vyřídit buď tzv. „na počkání“ nebo v zákonných lhůtách. Výstupy z činností těchto kontaktních míst mohou mít jak papírovou podobu, tak rovněž podobu elektronickou, která může být doručena přímo příslušným adresátům pomocí elektronické pošty.[58] Těmito výstupy se rozumí ověřené výpisy z centrálních registrů. Ověřený výstup, který kontaktní místo veřejné správy vydá, je vždy veřejnou listinou. Vždy je nezbytné, aby výpis byl označen ověřovací doložkou.[59] Subjekt, jenž ověřené výpisy vydává, je povinen vést rovněž jejich evidenci. [60]

V současné době poskytují kontaktní místa celkem 19 různých služeb, které lze rozdělit do kategorií:

- *výpisy z informačních systémů veřejné správy* (výpis z rejstříku trestů fyzických i právnických osob, výpis z obchodního rejstříku, výpisy z katastru nemovitostí, aj.),
- *podání vůči státní správě* (ohlášení živnosti do registru živnostenského podnikání),
- *základní registry* (výpisy ze základních registrů či podání žádosti o změnu údajů),
- *datové schránky* (žádost o zřízení datové schránky či úkony spojené s datovým schránkami),

[57] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1. s. 43-50
[58] Tamtéž. str. 24-26
[59] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. § 9a odst. 1
[60] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 75

- *konverze na žádost a související služby* (konverze dokumentů z listinné do elektronické podoby a naopak, úschovna systému CzechPOINT a Centrální úložiště ověřovacích doložek),
- *zprostředkovaná identifikace osoby* (vydání veřejné listiny o identifikaci osoby).[61]

V České republice je vysoký počet kontaktních míst, takže každý občan si najde své kontaktní místo v okolí svého bydliště, které si lze snadno zjistit na webových stránkách vč. otvírací doby. Ustanovení §8a odst. 2 zákona o ISVS říká, že kontaktním místem veřejné správy jsou notáři, krajské úřady, matriční úřady, obecní úřady, úřady městských částí nebo městských obvodů územně členěných. statutárních měst a úřady městských částí hlavního města Prahy, jejichž seznam stanoví prováděcí právní předpis, dále zastupitelské úřady určené ministrem zahraničních věcí, držitelé poštovní licence, Hospodářská komora České republiky, banka, pojišťovna, zdravotní pojišťovna a poskytovatel univerzální služby podle zákona o elektronických komunikacích, kterým byla ministerstvem udělena autorizace k výkonu působnosti kontaktního místa veřejné správy.[62]

Informační systém Czech POINT poskytuje 2 uživatelská rozhraní:

a) *rozhraní CzechPOINT@home*,
b) *rozhraní CzechPOINT@office*.

CzechPOINT@home je kontaktní místo pro občany, jež upřednostňují styk s orgány veřejné moci čistě elektronickou formou. Jedná se o podpůrnou online službu, jež je určená pro fyzické osoby, které mají zřízenou datovou schránku. Díky tomu se mohou přihlásit do rozhraní CzechPOINTU a komunikovat tak s orgány veřejné moc prostřednictvím internetu a žádat tak online prostřednictvím elektronických formulářů o vydání výpisu ze základních registrů. Přihlásit se do tohoto rozhraní skrze datové schránky slouží k odesílání žádostí a přijímání doručených dokumentů jejím prostřednictvím. Poskytování elektronických originálů listin skrze tento portál je pro občany bezplatné, oproti poskytování listinných výpisů na jednotlivých kontaktních místech. [63] CzechPOINT@offce je

[61]CzechPOINT. Jaké služby poskytuje Czech POINT? [online]. Dostupné z: https://www.czechpoint.cz/public/verejnost/sluzby/
[62] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. §8a odst. 2
[63]Czech POINT: CzechPOINT@home. [online]. Dostupné z: https://www.czechpoint.cz/public/verejnost/czechpointhome/

naopak neveřejným rozhraním, určeným pouze pro úředníky orgánů veřejné moci. Funguje na stejném principu jako CzechPOINT@home, avšak výstupy lze užít pouze pro vnitřní potřeby úřadů. Úředník zde zpracovává, ověřuje a předkládá podání v rámci eGovernmentu z úřední moci. Využívá dálkových přístupů, díky nimž lze získávat informace z agendy matrik, soudů či ohlašoven a provádět autorizovanou konverzi dokumentů z moci úřední.[64]

3.3. Datové schránky

Dalším prvkem eGovernmentu jsou datové schránky, znázorňované jako srdce celého eGovernmentu. Informační systém datových schránek byl poprvé spuštěn dne 1. 9. 2009. Datová schránka představuje elektronické úložiště, které je určeno k doručování orgánům veřejné moci, k provádění úkonů vůči orgánům veřejné moci a k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Jedná se tedy o komunikační nástroj, garantovaný státem, pomocí kterého je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a rovněž je takto od nich přijímat. Všechny úřady jsou povinni upřednostnit komunikaci prostřednictvím datových schránek s každým subjektem, jenž ji má zřízenou. Jsou zřizovány a rovněž i spravovány Ministerstvem vnitra, avšak provozovatelem je státní podnik Česká pošta.[65] Cílem datových schránek je efektivnější, rychlejší, levnější a spolehlivější veřejná správa. Samotný název už napovídá, že primárním účelem systému je příjem datových zpráv takovým způsobem, že budou prokazatelně doručené správnému příjemci, a to za dodržení bezpečnosti v rámci jejich zneužití nebo neoprávněného užití. Druhým úkolem je pak zaručit vyzvednutí zprávy pouze oprávněnou osobou nebo osobou, která k tomu byla pověřena.[66]

Výhody datových schránek jsou spatřovány kromě v rychlejší a efektivnější komunikaci, také v tom, že je možné činit jejím prostřednictvím podání i mimo úřední hodiny úřadů a zdarma. Dále poskytují datové zprávy lepší průkaznost, vzhledem k možnosti jejího uložení, lépe se kontroluje, zda zpráva byla svému adresátovi doručená, či nikoli. Např. zpráva odeslaná úřadu se považuje za

[64] Czech POINT: Agendy CzechPOINT@office. [online]. Dostupné z: https://www.czechpoint.cz/public/urednik/agendy-czechpointoffice/
[65] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 2
[66] VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6. s. 76

doručenou již v okamžiku dodání do datové schránky orgánu veřejné moci, a to i přesto, že to zákon výslovně nestanoví, neboť je nezbytné brát zřetel na zásadu kontinuity veřejné správy, resp. orgánů veřejné moci. V ostatních případech je dokument, který byl dodán do datové schránky doručený v okamžiku, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu[67]. V případě, že nedojde k přihlášení do datové schránky ve lhůtě 10 dnů ode dne dodání do datové schránky, považuje se dokument za doručený posledním dnem této lhůty – tzv. fikce doručení.[68] Doručení dokumentu do datové schránky (i v případě uplatnění fikce doručení) má stejné právní účinky jako doručení do vlastních rukou. Podle ustanovení § 20 odst. 1 písm. e) zákona č. 300/2008 Sb. Ministerstvo vnitra oznámí odesílateli, že jeho odeslaná datová zpráva byla doručena jejímu adresátovi a toto oznámení označí uznávanou elektronickou značkou ministerstva. Toto oznámení tedy představuje doklad o doručení písemnosti.

Kromě toho je možné využít přístupu do datové schránky také v rámci přihlašování do různých informačních systémů veřejné správy, např. portál občana či využívat tak službu CzechPOINT@home.[69] Komunikace skrze datové schránky nahrazuje klasický způsob doručování v listinné podobě, neboť zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů byla zrovnoprávněna papírová a elektronická verze zasílaných dokumentů.[70]

Datové schránky jsou rozděleny do čtyř skupin, a to podle jejich uživatelů. Dělí se na datové schránky pro fyzické osoby, pro fyzické osoby podnikající, pro právnické osoby a pro orgány veřejné moci. Orgánům veřejné moci a určitým skupinám právnických a podnikajících fyzických osob jsou datové schránky zřízeny automaticky ze zákona, všem ostatním na základě jejich žádosti. Datová schránka pro fyzické osoby je zřízena pouze na žádost fyzické osoby a bezúplatně. Fyzická osoba nemá prozatím povinnost mít zřízenou datovou schránku. Pokud si ji však zřídí, může mít pouze jednu. V případě, že by stejná osoba začala podnikat, bylo by nezbytné zřídit si další jakožto pro podnikající fyzickou osobu. Ta je rovněž

[67] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 17 odst. 3.
[68] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 17 odst. 4.
[69] Datové schránky. O datových schránkách. Výhody datových schránek. [online]. Dostupné z: https://www.datoveschranky.info/o-datovych-schrankach/vyhody-datovych-schranek
[70] Datové schránky. Základní informace. Informační systém datových schránek. [online]. Dostupné z: https://www.datoveschranky.info/o-datovych-schrankach/zakladni-informace

zřizována na základě žádosti. Výjimkou jsou určité skupiny, jako jsou např. advokáti, notáři či insolvenční správci, neboť těm je datová schránka zřizována ze zákona automaticky. Povinnost založit si datovou schránku mají však kromě orgánů veřejné moci rovněž právnické osoby, které jsou zapsané v obchodním rejstříku a samozřejmě ty zřízené zákonem.[71]

K tomu, aby mohly subjekty zřízenou datovou schránku užívat je nezbytné ji zpřístupnit. K tomu je zapotřebí přihlašovacích údajů, jež zasílá Ministerstvo vnitra ihned po zřízení datové schránky s tím, že klient se musí do datové schránky pomocí těchto údajů přihlásit, aby ji zaktivoval. Na první přihlášení do datové schránky mají subjekty lhůtu 15ti dnů. Pokud však subjekt lhůtu nedodrží, nic se neděje a po uplynutí posledního dne lhůty se datová schránka zpřístupní automaticky.[72] Každá datová schránka má svůj identifikační kód (ID) jež je tvořen pomocí číslic a písmen, díky kterému je možné datovou schránku konkrétního adresáta najít. Tyto údaje jsou pak nadále přístupové, pomocí nichž se uživatel může spolu s bezpečnostním heslem do datové schránky přihlásit. Bezpečnostní heslo je tvořeno nejméně osm znaky, obsahující písmena, číslice a speciální znaky jako velká písmena, závorky, pomlčky, aj. Nejvíce může mít heslo až třicet dva znaků. Heslo do datové schránky by mělo být měněno každé tři měsíce, nicméně lze v systému nastavit platnost hesla jako neomezenou.

Přístup do datové schránky je tedy vždy umožněn osobě oprávněné (tj. osobě, pro kterou byla datová schránka zřízena), ale je umožněn i tzv. pověřeným osobám. Systém datových schránek umožňuje tzv. přidat uživatele datové schránky s tím, že této osobě je možné určit rozsah oprávnění ve smyslu čtení zpráv, jejich posílání, odmazávání apod. Je možné rovněž zřídit přístup pouze pro zobrazování seznamů a dodejek. Pokud má ověřená osoba udělený pouze tento přístup, může vidět jaké datové zprávy a od koho byly do schránky dodány, avšak nenastává účinek jejich doručení, tj. nezapočne běh lhůt odvislých od doručení. Kromě pověřených osob je možné určit datové schránce tzv. administrátora, který bude zprvu datových schránek zajišťovat, tzn. on bude udělovat přístupy pověřeným osobám a bude zajišťovat komunikaci s Ministerstvem vnitra.[73]

---

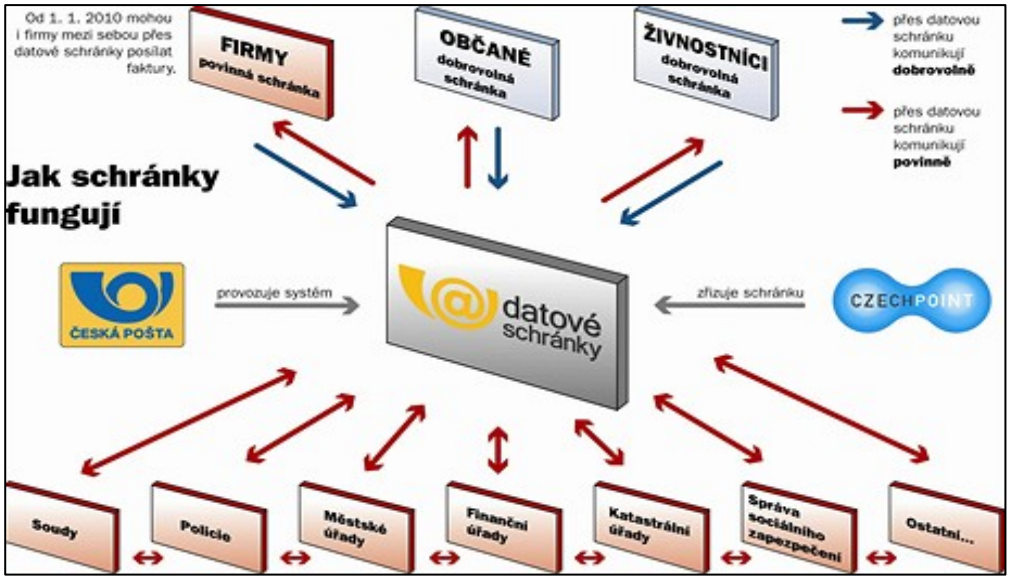
[71] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1. s. 101

[72] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 10

[73] VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6. s. 76

Ministerstvo vnitra datové schránky rovněž může znepřístupnit, případně zrušit. Ministerstvo zruší datovou schránku fyzické osoby po uplynutí tří let ode dne úmrtí fyzické osoby, případně po prohlášení za mrtvého. Fyzické podnikající osobě zruší ministerstvo datovou schránku též po 3 letech ale od výmazu ze zákonem stanovené evidence. Právnické osobě se zruší datová schránka opět po 3 letech od zániku právnické osoby zapsané v obchodním rejstříku. Po zrušení datových stránek ministerstvo vnitra zneplatní přístupové údaje.[74]

Datové schránky dnes už představují nedílnou součást komunikační struktury orgánů veřejné moci. Kromě účelu, pro který byl založen datová schránka plní i další úlohy, např. při získávání údajů z elektronických rejstříků prostřednictvím Portálu veřejné správy, tak přihlašovací údaje z datových schránek lze využít jako metodu tzv. autentizace, tj. identifikace i v ostatních IT systémech státní správy (např. Daňový portál či ePortál České správy sociálního zabezpečení).



Obrázek č. 6: Schéma subjektů zapojených do systému datových schránek[75]

[74] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 13
[75] Zdroj: Datové schránky. Informace o datových schránkách. [online]. Dostupné z: https://www.datoveschranky.eu/info-o-datovych-schrankach/komunikace-pomoci-datovych-schranek/komu-budu-ja-zasilat-a-naopak-kdo-mne

3.4. Autorizovaná konverze dokumentů

Na využívání služeb v oblasti CzechPOINTu a datových schránek navazuje nástroj eGovernmentu upravený zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, tj. autorizovaná konverze dokumentů. Jedná se o nástroj, jehož prostřednictvím dochází k úplnému převedení dokumentu z listinné podoby do podoby elektronické a naopak.[76] Jedná se o výjimečný institut, který umožňuje zpracování dokumentů v digitální i analogové podobě a jeho následné doručení prostřednictvím datové schránky. Výsledek konverze, tzv. výstup, má stejné právní účinky jako dokument, jehož převedením vznikl. Subjekt, jenž provádí autorizovanou konverzi dokumentů nemá za úkol kontrolovat soulad údajů uvedených ve výstupu konverze a rovněž nekontroluje ani jejich správnost či pravdivost, neboť provedením konverze dokumentů se nepotvrzuje správnost údajů ani jejich soulad s právními předpisy. Je důležité ověřit pouze shodu obou dokumentů, tedy převáděného dokumentu (tzv. vstupu konverze) s převedeným dokumentem (tzv. výstupem konverze).[77]

Autorizovanou konverzi dokumentů lze provést jak *na žádost*, tak *z moci úřední*. Konverze dokumentů na žádost je prováděna prostřednictvím kontaktních míst veřejné správy v rozhraní tzv. úschovny[78], nebo jiných subjektů k tomu oprávněných, jako jsou např. advokáti. Za tento úkon je však žadatelům účtován správní poplatek. Autorizovaná konverze prováděná z moci úřední je prováděna pouze orgány veřejné moci, a to v rozsahu, jenž je nezbytně nutný pro výkon jejich vlastní působnosti.[79] Subjekty provádějící autorizované konverze jsou povinni vést evidenci všech provedených konverzí. Každá konverze musí být označena tzv. ověřovací doložkou. Náležitosti ověřovací doložky jsou stanoveny v ustanovení §25 zákona o elektronických úkonech a autorizované konverzi dokumentů a liší se podle toho, jakým směrem byla konverze provedena. Společnými znaky ověřovacích doložek jsou název subjektu, který konverzi provedl, pořadové číslo, pod kterým je konverze vedena v evidenci provedených

[76] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 22
[77] BUDIŠ, P., HŘEBÍKOVÁ, I. Datové schránky. 1. vyd., Olomouc: Anag. 2010. ISBN 978-80-7263-617-4. s. 41
[78] Úschovna je podpůrný systém pro konverzi dokumentů, jenž je využíván pro dočasné uložení dokumentů v rámci prováděné konverze na kontaktním místě CzechPOINT. Zde si mohou občané vyzvednout vzniklý elektronický dokument, případně prostřednictvím tohoto portálu zažádat o jeho převedení do listinné podoby. Dostupné z: https://www.czechpoint.cz/uschovna/info
[79] BUDIŠ, Petr, HŘEBÍKOVÁ, Iva. Datové schránky: fungování, doručování, bezpečnost, návody. Olomouc: ANAG, 2010, ISBN 978-80-7263-617-4. s. 210-211

konverzí, sdělení, že obsah výstupu odpovídá obsahu vstupu, údaj o tom, z kolika listů se vstup skládá, datum vyhotovení doložky.[80]

Ustanovení §24 zákona o elektronický úkonech a autorizované konverzi dokumentů rovněž stanoví, v jakých případech není možné konverzi provést. Jedná se např. o dokumenty, které nelze konverzí nahradit (občanský průkaz, řidičský průkaz, směnky či geometrický plán), o dokumenty, jež obsahují různé škrty či doplňky zeslabující věrohodnost dokumentu, nebo např. dokumenty obsahující zvukový či audiovizuální záznam, a další.[81]

3.5. Základní registry

Primárním zdrojem informací pro ISVS jsou základní registry veřejné správy. Jsou jedním ze základních projektů eGONa a v rámci živého organismu symbolizují mozek, jakožto paměť celého eGovernmentu. Koncepce základních registrů je založena na moderních technologiích a online přístupu, což veřejné správě umožňuje využívat ke své činnosti základní registry odkudkoli a kdykoli. Jejich prostřednictvím jsou shromážděny a sjednoceny údaje o občanech a ostatních státních i nestátních subjektech.[82] Stejně jako datové schránky popsané v podkapitole výše, mají i základní registry svůj vlastní informační systém, který spravuje zvláštní úřad zřízený zákonem o základních registrech, tj. Správa základních registrů, jenž je odpovědný Ministerstvu vnitra. Ten obstarává bezpečné uchovávání dat a jejich sdílení řízeným přístupem, a to mezi základními registry a jednotlivými agendovými informačními systémy či mezi agendovými informačními systémy navzájem.[83] Vytvořil se tak jednotný provázaný systém, z něhož oprávněné subjekty mohou bezpečně čerpat aktualizovaná a zaručená data v takovém rozsahu oprávnění, jež uvádí registr práv a povinností.[84] Tyto data uváděná v základních registrech se označují jako referenční údaje, když „*...referenčním údajem míníme jedinečný a důvěryhodný údaj vedený v jednom ze základních registrů, který je určen ke sdílení v příslušných informačních systémech veřejné správy podle jasně vymezených pravidel*, ...“[85]

[80] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 25 – 26.
[81] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. § 24.
[82] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015. ISBN 978-80-87125-28-1. s. 137
[83] Zákon č. 111/2009 Sb., o základních registrech. § 2 písm. g)
[84] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 97-98
[85] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1. s. 28.

Tyto údaje se považují za důvěryhodné a státem garantované, proto je úřady nemusí dále nijak prověřovat. V případě změny některého z údajů (např. nové trvalé bydliště občana, stav, či příjmení), jsou tyto údaje automaticky zaktualizovány ve všech registrech. Záměr celého systému základních registrů bylo naplnění odlehčení byrokracie občanům, tj. aby orgány veřejné správy nevyžadovaly od občanů údaje, které jsou již jednou v základních registrech vedené.

Jak již bylo uvedeno výše, mozek panáčka eGONa je znázorněn čtyřmi různě barevnými části, které symbolizují jednotlivé základní registry veřejné správy. To znamená, že jsou celkem čtyři základní registry, tj. registr obyvatel, registr osob, registr územní identifikace, adres a nemovitostí a registr práv a povinností.

3.5.1. Registr obyvatel

Registr obyvatel eviduje údaje o státních občanech České republiky, ale rovněž i o cizincích, kterým bylo vydáno povolení k trvalému pobytu či k přechodnému pobytu na území České republiky, dále o občanech členských států Evropské unie a o občanech států vázaných mezinárodní smlouvou sjednanou s Evropským společenstvím či smlouvou o Evropském hospodářském prostorou, kteří na území České republiky přechodně pobývají po dobu delší 3 měsíců, a v neposlední řadě vede registr obyvatel údaje o osobách, jímž byl udělen azyl na území republiky a o jiných fyzických osobách, u nichž to vyžaduje jiný právní předpis. V tomto registru obyvatel lze dohledat referenční údaje všech výše uvedených fyzických osob, a to jejich jméno, příjmení, adresu místa pobytu (popř. doručovací adresu), datum a místo narození (popř. úmrtí, a v tom případě i místo a stát, na jehož místě k úmrtí došlo), dále státní občanství, rodné číslo, omezení nebo zbavení způsobilosti k právním úkonům, údaj o osvojení, rodinný stav a další. Kromě aktuálních údajů se v registru obyvatel evidují také údaje historické. Celý registr je však veřejnosti nepřístupný, tzn. nejedná se o veřejný seznam. Údaje z registru obyvatel mohou získávat orgány veřejné moci, tj. např. soudy, státní zastupitelství, notáři či Policie České republiky, aj.[86]

Registr obyvatel je spravován Ministerstvem vnitra České republiky. Údaje do registru se zapisují a jsou editovány prostřednictvím několika agendových

[86] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 99 – 101.

systémů. Těmi jsou agendový informační systém evidence obyvatel (aiseo), agendový informační systém cizinců (aisc), agendový informační systém evidence občanských průkazů (aiseop), agendový informační systém evidence cestovních dokladů (aisecd), agendový informační systém datových schránek.[87]

3.5.2. Registr osob

Kromě registru obyvatel máme také registr osob, jež slouží k evidenci právnických a podnikajících fyzických osob a orgánů veřejné moci a jejich referenčních údajů. Registr poskytuje základní identifikační údaje o výše uvedených subjektech, jejichž plný výčet jej vyjmenován v ustanovení §26 zákona č. 111/2009 Sb., o základních registrech. Např. se jedná o referenční údaje o názvu či obchodní firmě, data vzniku a zániku, o právní formě daného subjektu, o ID datové schránky subjektu, o identifikačním čísle provozovny, které je přidělováno editory dle působnosti jimi vykonávané agendy, aj. Registr osob je stejně jako registr obyvatel neveřejným seznamem a přístup do něj mají pouze orgány veřejné správy jež k tomu mají oprávnění z Registru práv a povinností.[88]

Registr osob je vedený Českým statistickým úřadem, který je rovněž editorem jednotlivých identifikátorů. Zajišťuje provoz registru, bezpečné poskytování identifikátorů a referenčních údajů. Český statistický úřad je odpovědný za správnost veškerých údajů v tomto registru uvedených.[89]

3.5.3. Registr územní identifikace, adres a nemovitostí (RÚIAN)

Tento registr byl spuštěn v polovině roku 2012 spolu s ostatními registry a slouží k „*evidenci údajů o územních prvcích, územně evidenčních jednotkách, adresách, územní identifikaci a údajů o účelových územních prvcích*.“[90] Na rozdíl od předešlých registrů představuje tento veřejný seznam, jenž umožňuje všem jeho uživatelům zdarma dálkový přístup přeš internet. Je veřejně přístupný, neboť nevede žádné osobní údaje, nýbrž pouze zprostředkovává údaje o vlastnictví

[87] Správa základních registrů. Editační agendové systémy. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-obyvatel/editacni-agendove-systemy
[88] Správa základních registrů. Registr osob. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-osob
[89] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 103
[90] Správa základních registrů. Registr územní identifikace, adres a nemovitostí. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti

pozemků, staveb aj. z informačního systému katastru nemovitostí. Je to jediný registr, který vede tzv. nereferenční údaje, což představují jednotlivé atributy stavebních objektů jako je např. počet podlaží, způsob vytápění objektu, připojení na plyn, aj.[91]

Správcem RÚIAN je Český úřad zeměměřičský a katastrální. Ke správnému fungování samotného RÚIAN byl vytvořen podpůrný agendový informační systém zvaný Informační systém územní identifikace, který rovněž spadá do správy Českého úřadu zeměměřičského a katastrálního, a který slouží k vedení údajů v databázi registru a k jejich správě. Spravuje veškeré údaje v RÚIAN evidované vyjma těch, jež jsou zapisované prostřednictvím katastru nemovitostí.[92]

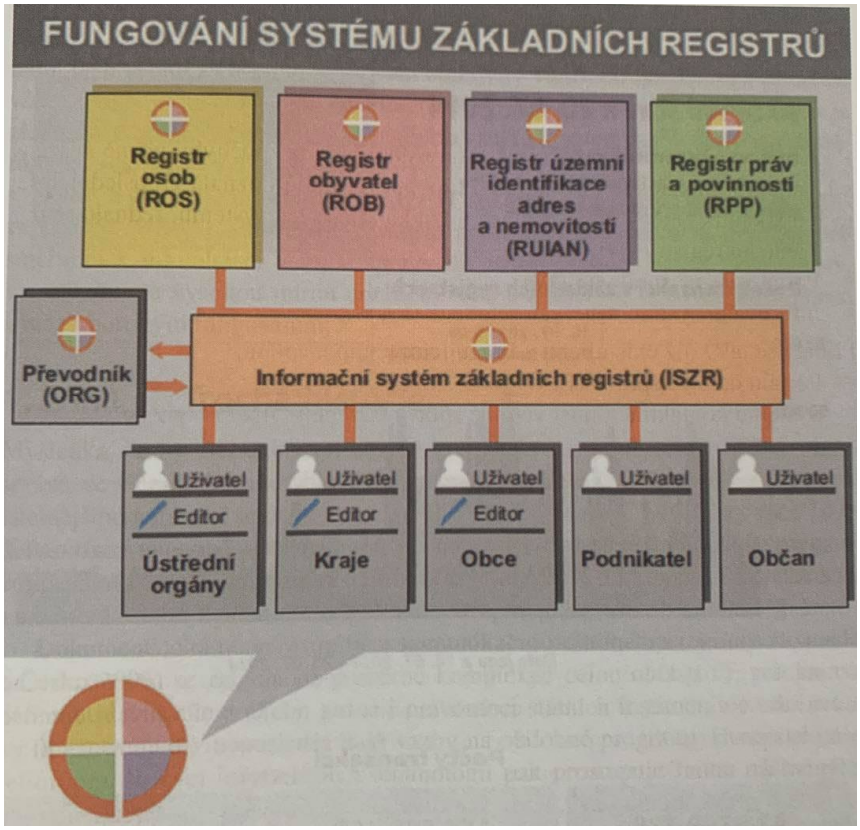
3.5.4. Registr práv a povinností

Čtvrtým a posledním základním registrem veřejné správy je registr práv a povinností, celým názvem Základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností. Vznikl za účelem zajištění přístupu do informačních systémů základních registrů, a to pouze oprávněných orgánů veřejné moci a úředních osob. Slouží tedy ke stanovení oprávnění jednotlivých uživatelů a editorů všech základních registrů (tj. orgánů veřejné moci) k přístupu k referenčním údajům v ostatních registrech a brání neoprávněným osobám ve zpracovávání osobních údajů osob.[93] Díky těmto referenčním záznamům se může každý občan dozvědět kdo a kdy data o něm vedená využíval, kdo je měnil či upravoval, a za jakým účelem. Fyzické osobě, jež má zřízenou datovou schránku tento výpis o užití jeho osobních údajů přijde automaticky jednou ročně, ostatní fyzické osoby, jež datovou schránku zřízené nemají si mohou o tento výpis zažádat na jakémkoli kontaktním místě CzechPOINTu.[94]

Správcem registru práv a povinností je Ministerstvo vnitra. To také registruje jednotlivé agendy vedené v registru práv a povinností a přiděluje jim

[91] Správa základních registrů. Registr územní identifikace, adres a nemovitostí. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti
[92] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 103-104
[93] FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1. str. 28.
[94] Správa základních registrů. Registr práv a povinností. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-prav-a-povinnosti

kódy agendy, které musí být obsažené v číselníku agend. Každá taková registrovaná agenda pak obsahuje informace o zákoně, který je jejím podkladem a informace o tom, který z orgánů veřejné moci mají oprávnění danou agendu vykonávat. Tím získává příslušný orgán veřejné moci oprávnění k využívání jednotlivých registrů.[95]



Obrázek č. 7. Fungování systému základních registrů[96]

3.6. Elektronický podpis

Mezi základní nástroje, které jsou použitelné pro bezpečnou elektronickou komunikaci s (nejen) orgány veřejné moci, patří kromě datové schránky a jiných portálů také elektronický podpis. Ke vzniku elektronických podpisů byla vyžadována spolupráce nejméně tří oborů, tj. *oboru kryptografie*, který měl za úkol vymyslet způsob jejich fungování, *oboru IT*, jenž musel připravit nástroje a postupy pro praktické používání, tj. prostředky a služby pro vytváření a pro ověřování

[95] Správa základních registrů. Registr práv a povinností. [online]. Dostupné z: https://www.szrcr.cz/cs/registr-prav-a-povinnosti
[96] Zdroj: VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6. s. 23

elektronických podpisů a *oboru právo*, který musel připravit právní rámec, jež by umožnil přisuzovat elektronickým podpisům právní účinky. Původní legislativní normou upravující elektronický podpis v České republice byl zákon č. 227/2000 Sb., o elektronickém podpisu, který však pozbyl účinnosti k roku 2016. Současná právní úprava vztahující se k úpravě elektronického podpisu má však základ v unijním právu, konkrétně na základě nařízení eIDAS (definováno níže). V rámci adaptace tohoto nařízení do právního řádu České republiky byl přijat zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „zákon č. 297/2016 Sb.).

3.6.1. Nařízení eIDAS

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (tzv. nařízení eIDAS) ze dne 23. července 2014 a s účinnosti k 1. 7. 2016 bylo vydáno za účelem zvýšit důvěryhodnost elektronických transakcí na vnitřním trhu tím, že poskytne společný základ pro bezpečnou elektronickou komunikaci mezi občany, podniky, orgány veřejné moci, a posílí tak efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a také elektronického obchodu v Unii. Nařízení eIDAS mimo jiné stanoví právní rámec pro elektronickou identifikaci, autentizaci, elektronické podpisy a související důvěryhodné služby, za účelem zvýšení pohodlí a důvěry uživatelů v digitálním světě.[97] Nařízení přineslo oficiální zrovnoprávnění elektronických listin opatřených kvalifikovaným elektronickým podpisem s originály listinných dokumentů. Vyjma toho EU prostřednictvím tohoto nařízení uložila povinnost členským státům vytvořit systém garantované elektronické identifikace občanů, jenž umožní dálkově elektronicky prokázat totožnost občana.[98]

3.6.2. Druhy elektronických podpisů

Elektronický podpis představuje **„***data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena,*

[97] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&from=CS

[98] Ministerstvo vnitra ČR. eIDAS do roka a do dne. [online]. Dostupné z: https://www.mvcr.cz/clanek/eidas-do-roka-a-do-dne.aspx

a která podepisující osoba používá k podepsání.“[99] Slouží k projevu vůle, resp. k projevení souhlasu podepisující soby s daným dokumentem, stejně, jako tomu je v listinné formě. Elektronický podpis je vyhrazen pouze fyzickým osobám. Elektronické podpisy členíme na tři, respektive čtyři typy, když nařízení eIDAS zná 3 druhy elektronických podpisů, tj. elektronické podpisy prosté, zaručené a kvalifikované, kdežto česká právní úprava přidala k výše uvedeným rovněž podpis uznávaný. Druhy elektronických podpisů se od sebe výrazně odlišují svými vlastnostmi a jsou mezi sebou v hierarchickém postavení.[100]

3.6.2.1. Prostý elektronický podpis

Tento elektronický podpis představuje nejjednodušší formu elektronického podpisu. Jedná se o podpisy v různých formách, ke kterým však není vyžadováno speciálních prvků. Mezi metody provedení prostého elektronického podpisu řadíme např. připojení, resp. napsání svého jména a příjmení v e-mailové zprávě, vložení svého naskenovaného vlastnoručního podpisu do obyčejného elektronického dokumentu nebo jím mohou být biometrická data, tj. vzorek sebe sama, např. podpisu vytvořený elektronickou tužkou. Mezi prostý elektronický podpis řadíme rovněž např. jen předání některé informace, např. zadání PINu, jména, či úkon, kterým např. zaškrtneme políčko „souhlasím“ na webové stránce (např. souhlas s obchodními podmínkami). Jedná se však o podpis s nejnižší mírou spolehlivosti a důvěryhodnosti, proto v pomyslné pyramidě elektronických podpisů je na nejnižším stupni.

3.6.2.2. Zaručený elektronický podpis

Zaručený elektronický podpis je v pomyslné pyramidě závaznosti elektronických podpisů na druhém nejnižším místě. I přesto, že se nazývá zaručeným, nezaručuje to podstatné, tj. neověří identitu autora podpisu. Název „zaručený“ vznikl z ne zcela přesného překladu z anglického „Advanced Electronic

[99] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014R0910&from=CS.

[100] Ministerstvo vnitra České republiky. Informace k problematice kvalifikovaných elektronických pečetí. Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce. [online]. Dostupné z: https://www.mvcr.cz/clanek/informace-k-problematice-kvalifikovanych-elektronickych-peceti.aspx?q=Y2hudW09Ng%3D%3D

Signature“. Tento typ podpisu sice nezaručuje identitu autora podpisu, ale zaručuje neměnnost zprávy. To znamená, že zaručuje zjištění jakékoliv změny dat a umožňuje identifikaci podepsané osoby. Proto, aby mohl být podpis označen jako zaručený, musí splnit podmínky, jež jsou určené v Nařízení eIDAS v článku 26. Těmito podmínkami jsou a) jednoznačné spojení s podepisující osobou, b) umožnění identifikaci podepisující osoby, c) vytvoření pomocí dat pro vytváření elektronických podpisů, které osoba, jež podpisem podepisuje může s vysokou úrovní důvěry použít pod svou výhradní kontrolou, d) připojení k datům, které jsou tímto podpisem podepisována takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.[101] Vzhledem k tomu, že pro vytvoření zaručeného podpisu je třeba výhradní kontroly dat podepisující osobou, může si tak podepisující osoba vytvořit nový zaručený elektronický podpis. Tento podpis však uživateli nabídne vytvoření ID, a proto si daná osoba může vytvořit elektronický podpis jakékoliv osoby, tzn. může vytvořit úplně novou osobu, klidně i falešnou (např. na jméno Jára Cimrman).

3.6.2.3. Uznávaný zaručený elektronický podpis

Pojem uznávaný elektronický podpis, jak již bylo naznačeno výše, byl zaveden zákonem č. 297/2016 Sb. Jedná se o podpis, který je svou závazností druhým nejvyšším. K tomu, aby elektronický podpis byl uznávaným, je zapotřebí tzv. kvalifikovaného certifikátu. To znamená, že k použití tohoto podpisu je zapotřebí schválení tzv. certifikační autoritou, čímž dojde k záruce, že elektronický podpis je skutečně podepsán osobou, jež je v něm uvedena, jejím autorem. Mezi certifikační autority řadíme jejich poskytovatele, tj. Česká pošta, s.p., eIdentity a.s. či První certifikační autorita, a.s. a jiné.

Uznávaný elektronický podpis je platnou právní úpravou vyžadován v rámci jednání vůči veřejnoprávním subjektům v elektronické formě.[102]

[101] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Čl. 26

[102] Elektronický podpis pohledem aktuální právní úpravy. [online]. Dostupné z: https://www.epravo.cz/top/clanky/elektronicky-podpis-pohledem-aktualni-pravni-upravy-110560.html

3.6.2.4. Kvalifikovaný elektronický podpis

Tento druh podpisu stojí na úplném vrcholu naší pyramidy. Jde o nejvyšší formu elektronického podpisu, a to především v souvislosti s jeho povinným uznáváním ve všech členských státech Evropské unie.[103] Kvalifikovaný elektronický podpis lze vytvořit pouze pomocí dat pro vytváření elektronických popisů. Tato data představují kvalifikovaný certifikát, který je umístěn na samostatném nosiči, a který nelze žádným způsobem přenést na nosič jiný. Tímto nosičem může být například tzv. USB token, díky němuž daná osoba kvalifikovaný elektronický podpis vytvoří.[104] Jedná se o podpis s nejvyšší mírou spolehlivosti a důvěryhodnosti.

Zákon č. 297/2016 Sb. v určitých případech stanoví, že ke kvalifikovanému elektronickému podpisu je zapotřebí připojit elektronickou kvalifikovanou pečeť a časové razítko. Elektronickou kvalifikovanou pečetí se pak rozumí obdoba úředního razítka. K jejímu vytvoření je rovněž zapotřebí kvalifikovaného prostředku jako je USB token. Tyto pečeti jsouo však poskytovány pouze právnickým osobám. Časové razítko pak slouží k časovém označení elektronických dokumentů. Díky němu je na podepisovaném dokumentu vyznačen čas, který zaručuje, že v daném čase data v uvedeném dokumentu skutečně existovala.[105]

3.7. Elektronická identifikace

Elektronická identifikace neboli eIdentita slouží k prokázání totožnosti. Tento institut je upraven zákonem č. 250/2017 Sb., o elektronické identifikaci, který stanoví, že pokud je vyžadováno právním předpisem nebo výkonem působnosti prokázání totožnosti, je nezbytné umožnění takového úkonu prostřednictvím kvalifikovanému systému elektronické identifikace.[106] K získání přístupu k těmto online službám je zapotřebí provést bezpečné a zaručené vzdálené

[103] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Čl. 25.
[104] Ministerstvo vnitra České republiky. Informace k problematice kvalifikovaných elektronických pečetí. Metodický pokyn k elektronickým podpisům a pečetím pro veřejnoprávní původce. [online]. Dostupné z: https://www.mvcr.cz/clanek/informace-k-problematice-kvalifikovanych-elektronickych-peceti.aspx?q=Y2hudW09Ng%3D%3D
[105] PostSignum. Slovníček pojmů. [online]. Dostupné z: https://www.postsignum.cz/slovnicek_pojmu.html
[106] Zákonem č. 250/2017 Sb., o elektronické identifikaci. §2

ověření Vaší totožnosti. K tomuto ověření totožnosti pak slouží nástroj zvaný „Národní bod“, neboli portál Národního bodu pro identifikaci a autentizaci (tzv. Portál NIA). Ten slouží k tomu, aby veřejná správa měla přehled a zaručenou informaci o tom, komu služby poskytované veřejnou správou poskytuje a kdo se jako klient k těmto službám přihlašuje. Poskytovatelé veřejných služeb získají veškeré údaje o uživateli ale pouze tehdy, udělí-li k tomu v rámci přihlašování se uživatel souhlas.[107] Portál NIA k prokazování totožnosti užívá různé identifikační prostředky. Tyto prostředky pak slouží jako tzv. klíč, a v současné době jsou vydávány jak státem, tak i soukromoprávními poskytovateli. Mezi identifikační prostředky vydávané státem patří občanský průkaz s aktivovaným kontaktním elektronickým čipem, NIA ID a Mobilní klíč eGovernmentu.[108] Identifikační prostředky vydávané soukromoprávními kvalifikovanými poskytovateli jsou např. MojeID, ČSOB Identita či např. Bankovní Identita poskytovaná Českou spořitelnou a.s.

3.7.1. eObčanka

Od 1. 7. 2018 se v České republice začaly vydávat občanské průkazy se strojově čitelnými údaji a elektronickým čipem. Tento občanský průkaz neboli eObčanka, umožňuje, jak již bylo výše zmíněno, aby se jeho držitel bezpečně přihlásil do rozhraní veřejné správy a mohl bezpečně užívat online služeb, které veřejná správa nabízí. Důvěryhodnost eObčanky, používané při online komunikaci s úřadem, je na stejné úrovni, jako je fyzické předložení občanského průkazu při osobní návštěvě úřadu.

K použití eObčanky jako identifikačního prostředku pro přihlášení k výše zmíněným online službám je potřeba, aby držitel občanského průkazu elektronický čip aktivoval. To lze učinit např. rovnou při převzetí občanského průkazu na úřadě obce s rozšířenou působností, či později, a to na kterémkoliv z úřadů vydávajících osobní doklady. Aktivaci lze provést zadáním tzv. přístupových kódů, které jsou tvořeny čtyřmi až deseti znaky. Přístupových kódů je několik, např. PIN (Personal Identification Number), PUK (PIN Unblocking Key), BOK (Bezpečnostní osobní kód), a další. Jedním z nich je rovněž IOK neboli „Identifikační osobní kód“ sloužící jako kód k ověření užívání občanského průkazu, a který se používá

[107] eIdentita. Portál národního bodu pro identifikaci a autentizaci (NIA). [online]. Dostupné z: https://info.eidentita.cz/portal/
[108] eIdentita. Základní informace. [online]. Dostupné z: https://info.eidentita.cz

při každé identifikační operaci. V případě zadání chybného IOKu či jeho zapomenutí, může držitel eObčanky užít tzv. Deblokační osobní kód, který slouží k odblokování občanského průkazu.[109] K plnohodnotnému fungování eObčanky je rovněž nezbytné, aby její držitel vlastnil čtečku čipových karet, která může už být zabudována např. v osobním počítači. Chce-li pak aktivně eObčanku její držitel využívat k online komunikaci s orgány veřejné správy, musí si rovněž stáhnout aplikaci s názvem eObčanka např. do svého chytrého telefonu. V případě, že se držitel občanského průkazu rozhodne přestat těchto služeb využívat, je možné elektronický čip deaktivovat.[110]

eObčanka s aktivovaným elektronickým čipem umožní držiteli kromě jeho identifikace vůči online službám veřejné správy i využívání dalších služeb, např. vytvořit si kvalifikovaný elektronický podpis či provést autentizaci pomocí certifikátu vůči informačním systémům.

3.7.2. NIA ID

Dalším identifikačním prostředkem je tzv. NIA ID. Jedná se o identifikační prostředek, který umožňuje zaručené prokázání totožnosti při přihlašování se k online službám pomocí kombinace jména, hesla a SMS kódu. NIA ID představuje tzv. dvoufaktorové ověření, kdy při přihlášení uživatel zadá přístupové údaje tvořené uživatelským jménem a heslem, které si zvolí během registrace. Poté zadá jednorázově vygenerovaný SMS kód, který mu přijde na jeho mobilní telefon. Právě SMS představuje to druhé ověření.

NIA ID je nejprve potřeba založit, a to prostřednictvím registračního formuláře dostupné na internetové stránce www.eidentita.cz. Před prvním použitím je pak třeba tento identifikační prostředek aktivovat. Aktivaci lze provést buďto prostřednictvím datových schránek, ověřením pomocí eObčanky nebo osobně na jakémkoliv kontaktním místě veřejné správy CzechPOINT.[111]

[109] eIdentita. Kódy pro ochranu občanského průkazu. [online]. Dostupné z: https://info.eidentita.cz/eop/OchranneKody.aspx
[110] eIdentita. eObčanka. [online]. Dostupné z: https://info.eidentita.cz/eop/
[111] eIdentita. NIA ID (Jméno, heslo a SMS kód). [online]. Dostupné z: https://info.eidentita.cz/ups/

3.7.3. Mobilní klíč

Mobilní klíč představuje identifikační prostředek, k němuž v rámci přihlašování není potřeba zadávání dalších ověřovacích kódů. K jeho použití je třeba mít nainstalovanou aplikaci mobilního klíče na mobilním zařízení. Po instalaci aplikace a po aktivaci mobilního klíče se pak uživatel může přihlašovat ke službám využívající elektronickou identifikaci, a to prostřednictvím Národního bodu.[112]

3.7.4. Bankovní identita

Účinnosti k 1. 1. 2021 nabyl jeden z největších digitalizačních projektů českého bankovního sektoru s názvem SONIA neboli Bankovní identita. Díky tomuto projektu se může občan, jenž využívá elektronické bankovnictví, přihlásit k portálům s elektronickými službami státu či soukromých firem a nemusí k tomu užít žádný z identifikačních prostředků zmíněných výše. Bankovní identita je totiž tvořena z přístupových údajů, resp. z údajů, jakými se občan přihlašuje do elektronického bankovnictví. To znamená, že každý, kdo má elektronické bankovnictví již má svoji bankovní identitu a může ji dále využívat jako identifikační prostředek. Nyní se tedy díky projektu SONIA kterákoli banka v České republice může stát tzv. poskytovatelem elektronické identity v souladu se zákonem o elektronické identifikaci, a občan tak může komunikovat z domova s úřady i soukromými společnostmi, jež toto ověření podporují, a to snadno, bezpečně a zdarma.[113]

Bankovní identitu je možné využít rovněž k elektronickému podepisování dokumentů, či její pomocí je možné předvyplnit vaše údaje do příslušných internetových formulářů. Vždy vše proběhne na základě iniciativy občana a jeho souhlasu, bez uchovávání dat.[114] Záměrem tohoto identifikačního prostředku je, aby se bankovní identita stala univerzálním prostředkem pro elektronické ověřování.

[112] eIdentita. Mobilní klíč eGovernmentu. [online]. Dostupné z: https://info.eidentita.cz/mep/
[113] Bankovní identita. O projektu. [online]. Dostupné z: https://bankovni-identita.cz/o-projektu/
[114] Tamtéž.

Obrázek č. 8: Schéma fungování bankovní identity.[115]

3.8. Internetové portály

Tato kapitola byla zaměřena pouze na vybrané insitituty eGovernmentu, které jsou základními prvky neustále se vyvíjející elektronizace veřejné správy. Je však nezbytné alespoň zmínit i podstatu internetových portálů poskytující služby vázané na konkrétní subjekt. Kromě portálu veřejné správy a Portálu občana tedy v České republice existují další portály slouužící občanům, klientům veřejné správy, mezi které patří například:

a) *Portál zdravotních pojišťoven*, který umožňuje komunikaci s pěti zdravotním pojišťovnami ze sedmi, které působí na českém trhu zdravotních pojišťoven. Jedná se o internetovou aplikaci, jejímž prostřednictvím mohou zdravotní pojišťovny přijímat informace od klientů, tj. získávat vyúčtování jejich zdravotní péče, klient (zaměstavatel či osoba samostatně výdělečně činná) může jejím prostřednictvím podat např. hlášení o platbách za zdravotní pojištění, aj. výhodné služby šetřící čas občanům i admnistrativu.[116]

[115] Zdroj: https://bankovni-identita.cz/banky-a-reseni/
[116] Portál ZP. [online]. Dostupné z: https://www.portalzp.cz/aktuality/portal-zp

b) *ePortál ČSSZ*, který nabízí služby, díky nimž klient České správy sociálního zabezpečení (dále jen ČSSZ) může snadněji komunikovat, a to nejen s ČSSZ ale i s okresními správami (OSSZ). Tento portál byl spuštěn v průběhu roku 2014 a mohou využívat nejen pojištěnci, ale rovněž zaměstnavatelé a osoby samostatně výdělečně činné.[117] Díky tomuto portálu mohou nahlížet na své údaje evidované v evidenci ČSSZ ale mohou využívat i jednotlivých interaktivních tiskopisů, v podobě tzv. „samoobsluhy", kdy o autorizaci žadatele se postará Informační systém datových schránek.[118] Nejnovější aplikací poskytovanou ePortálem ČSSZ je aplikace e- Neschopenka. *E-neschopenka je neschopenka (hlášení pracovní neschopnosti) pro zaměstnavatele a správu sociálního zabezpečení, která je vystavena lékařem elektronicky. Účelem eNeschopenky je zjednodušení přenosu informací, protože elektronicky propojuje hned 3 subjekty: lékaře, zaměstnavatele a Českou správu sociálního zabezpečení (ČSSZ).*[119]

c) *Daňový portál*, jakožto další z velmi často využívaných portálů umožňuje snadnější komunikaci občanů s finanční správou. Daňový portál zahrnuje řadu aplikací jako je podání přiznání, žádostí, formulářů či hlášení. Díky intuitivním elektronickým formulářům může uživatel snadno vyplnit daňové přznání a zaslat v příslušné lhůtě. Další službou daňového portálu je např. elektronická evidence tržeb (EET), regstr plátců DPH vč. bankovních spojení a označení (ne)spolehlivosti či tvz. Online finanční úřad (DIS+), který přihlášenému uživateli poskytuje vybrané fnormace z osobního daňového účtu a ze spisu.[120]

d) *eJustice* představuje „*využití informačních technologií a systémů v prostředí justice (resortu spravedlnosti), především pak zavedení elektronické formy komunikace, výměny a zpracování informací mezi subjekty, nacházejícími se v prostředí justice nebo vstupujícími do kontaktů s resortem justice (účastníci řízení, jiné orgány veřejné moci).*"[121] Portál justice přístupný na webových

[117] ePortál ČSSZ. [online]. Dostupné z https://www.cssz.cz/web/cz/zakladni-informace-eportal
[118] VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6. s. 159
[119] COVID portál. eNeschopenka. [online]. Dostupné z: https://covid.gov.cz/situace/zamestnani/eneschopenka
[120] Daňový portál. [online]. Dostupné z: https://www.financnisprava.cz/cs/dane-elektronicky/danovy-portal
[121] Kolektiv autorů. Czech POINT: Historický vývoj a současná podoba. 1. vyd. Praha: Cevro Institut. 2015, ISBN 978-80-87125-30-4. s. 33

stránkách www.justice.cz představuje tzv. rozcestník českého soudnictví, z něhož lze postupovat na celou řadu dalších odkazů, přehledů, informačních zdrojů. Tento portál umožňuje jeho uživatelům vyhledávat ve veřejných rejstřících fyzických a právnických osob (např. v obchodním či insolvenčním rejstříku, spolkovém rejstříku, rejstříku společenství jednotek apod.), činit elektronická podání do veřejných rejstříků prostřednictvím tzv. ePodatelny, stahovat a vyplňovat formuláře pro insolvenční řízení (vč. přihlášení pohledávky), dává přehled o jednotlivých jednání a informace o stavu a průběhu řízení prostřednictvím institutu infoSoud a infoJednání, případně je zde možné podat návrh na vydání Elektronického platebního rozkazů a ověřit si je, a spoustu dalších možností. Jednou z přínosnou aplikací je rovněž aplikace zvaná infoData, což představuje „proklik“ na statistický portál, který umožňuje široké veřejnosti nahlédnout do statistických ročenek a výkazů soudů a státních zastupitelství, a dále do přehledných tabulek o vyřizování soudních agend, aj.[122] Jedním z velmi důležitých podportálů eJustice je infoDeska, neboť se jedná o elektronickou úřední desku resortu justice. Zde se vyobrazuje stejný obsah jako je na. listinné úřední desce, jenž je umístěna v. jednotlivých budovách justice. Tyto údaje mají však pouze informativní charakter.[123]

e) *COVID PORTÁL*. V současné době s probíhající pandemickou situací je nezbytné zmínit rovněž COVID PORTÁL dostupný na webové stránce www.covid.gov.cz, kde se občané mohou velmi lehce zorientovat v stávající situaci. Občané zde mohou nalézt jasně a srozumitelně vysvětlená opatření, jež platí na území České republiky, případně v jednotlivých regionech. Rovněž jsou zde odkazy na jednotlivé životní situace, ve který je možné se v rámci onemocnění COVID -19 ocitnout spolu s doporučením, jak se v takových situacích chovat. Občan si zde může ověřit jaké obchody a služby fungují a které jsou naopak zavřené, případně jaké aktivity jsou možné ve volném čase provozovat a jaké nikoli. Rovněž je možné přes tento portál využít možnosti registrace na očkování a zjistit si veškeré potřebné informace o vakcínách.

[122] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. ISBN 978-80-87576-36-6. s. 132

[123] infoDeska. Elektornická úřední deska resortu justice. [online]. Dostupné z: https://infodeska.justice.cz/

f) *Portál podnikatele (PP)*. Tento portál ještě není spuštěný, avšak je již v návrhu. Jednalo by se o portál, který by sloužil pouze podnikatelům, resp. pro usnadnění jejich komunikace se státem, a rovněž by poskytoval základní informace o právech a povinnostech podnikatelů. Kromě toho by dále PP umožňoval transakce i mezi samotnými podnikateli navzájem. I přesto že podnikatelé jsou běžnými občany a k tomu jim slouží Portál občana, jejich potřeby jsou specifické a od běžného nepodnikajícího občana odlišné. Proto by bylo vhodné zavést nový portál, který by se zaměřoval pouze na potřeby podnikatelů.[124]

[124] Egovernment: PORTÁL PODNIKATELE MŮŽE BÝT K DISPOZICI JEŠTĚ LETOS, POKUD TO PŮJDE DOBŘE. [online]. Dostupné z: https://www.egovernment.cz/inpage/portal-podnikatel/

4. Využívání eGovernmentu v praxi

Autorka je již druhým rokem zaměstnancem notáře na pozici notářského koncipienta.[125] Notář a jeho zaměstnanci mají přístup k většině služeb eGovernmentu. Proto se v této kapitole bude autorka snažit reflektovat své osobní zkušenosti s fungováním některých prvků eGovernemntu. Notář jako povolání, je povolání svobodné, avšak výkonem notářského úřadu[126] je pověřený státem. Náplní jeho práce je sepisování veřejných listin, správa majetku a další činnosti dle části první zákona č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů. Mimo to provádí notář pozůstalostní řízení v postavení tzv. soudního komisaře. Pozůstalostní řízení jsou notářům přidělována příslušným okresním soudem a tvoří podstatnou část jeho výkonu. Dále jsou notáři součástí projektu CzechPOINT a mohou tedy vydávat ověřené výstupy z Informačních systémů veřejné správy. To znamená, že občané mohou získat ověřené výpisy z rejstříku trestů, živnostenského rejstříku, obchodního rejstříku a z katastru nemovitostí i u jednotlivých notářů, nejen na kontaktních místech CzechPOINTu.

Notář ke své činnosti využívá velké množství služeb eGovernmentu a stejně tak na základě jeho pověření i jeho zaměstnanci. Jednou z nejvíce využívaných služeb je datová schránka, do které mají zřízený přístup všichni zaměstnanci notáře. Datová schránka představuje pro notáře a jeho zaměstnance hlavní komunikační kanál, neboť mají povinnost jejím prostřednictvím komunikovat s orgány veřejné správy a rovněž s ostatními fyzickými a právnickými osobami, které ji mají zřízenou. Datová schránka se využívá převážně v rámci činnosti soudního komisaře, neboť v rámci pozůstalostního řízení má notář za cíl zjistit zůstavitelů majetek, tzn. pro zjištění majetkových hodnot, pohledávek a dluhů komunikuje notář skrze datovou schránku nejen se soudy, exekutory a státními sociálními institucemi, ale rovněž s bankovními institucemi, orgány zájmové samosprávy, katastrálními pracovišti a jinými subjekty. Datovou schránku však využívá i v případě jeho ostatní činnosti, např. pro zasílání výpisů z obchodního rejstříku či pro podání návrhů na vklad do katastru nemovitostí, aj.

[125] Notářský koncipient se pod vedením a dohledem notáře připravuje na výkon funkce notáře a z pověření notáře vykonává přípravné a dílčí úkony notářské činnosti. Notářský koncipienti jsou zapsáni v seznamu notářských koncipientů vedeném příslušnou notářskou komorou.

[126] dle § 1 zákona č. 358/1992 Sb., o notářích a jejich činnosti se notářským úřadem rozumí soubor pravomocí k výkonu notářství a další činnosti stanovené zákonem (dále jen „činnost notáře“) trvale spojený s místem výkonu této činnosti.

Další z nejvíce využívaným institutem eGovenmentu notářem je CzechPOINT. K většině služeb CzechPOINTu mají pracovníci notáře přístup na základě elektronického certifikátu, který je umístěn na tzv. USB tokenu a každý z pracovníků má certifikát na své jméno. Tento certifikát může být veřejný nebo kvalifikovaný, podle toho, jaký úkon je jeho prostřednictvím potřeba vykonat. Vzhledem k tomu, že notáři jsou součástí projektu CzechPOINT, mají přístup do uživatelského rozhraní typu CzechPOINT@office, který je poskytován orgánům veřejné moci (vyobrazení uživatelského rozhraní CzechPOINT v příloze č. 1). Do tohoto rozhraní se přihlašují pomocí výše zmíněného certifikátu pro veřejné použití a současně svým přihlašovacím jménem a heslem. Poté je možné vyhotovit výstup z Informačního systému veřejné správy. Jedním z nich je výpis z rejstříku trestů jak fyzických, tak právnických osob. V případě, kdy je žadatel fyzickou osobou musí mít platný doklad totožnosti. Žadatelem může být jak občan České republiky, tak cizinci, kteří mají v České republice trvalý pobyt či povolení k pobytu. Po předložení průkazu totožnosti zadá zpracovatel rodné číslo žadatele a číslo průkazu totožnosti do internetového formuláře (vizualizace formuláře v Příloze č. 2), kde se následně vygeneruje žádost o vydání výpisu a žadatel ji podepíše. Tuto žádost pak musí pracovníci notáře archivovat v knize žádostí o výpis z rejstříku trestů a přidělí této žádosti značku ve tvaru T, řadové číslo a rok vyhotovení (např. T 1/2021). Na základě této žádosti pak zpracovatel odešle elektronickou žádost na Rejstřík trestů, který buď rovnou předá výpis, nebo pošle informaci o zařazení tzv. manuálního zpracování. Na základě podepsané písemné žádosti následně odešle pracovník Czech POINTu elektronickou žádost na Rejstřík trestů, který odpoví buď předáním výpisu, nebo informací o zařazení žádosti do tzv. manuálního zpracování. K vytištěnému výpisu z Rejstříku trestů doplní notář či pověřený pracovník ověřovací doložku. Dalším výstupem z rozhraní CzechPOINT@office je výpis z obchodního rejstříku. Ten se opět vyhotovuje zadáním identifikačního čísla společnosti do internetového formuláře, který je propojený s portálem Justice.cz. K výstupu se rovněž připojí ověřovací doložka. Výpis z obchodního rejstříku se však častěji vyhotovuje přímo z portálu Justice.cz, a k tomuto výstupu se pak připojuje opět ověřovací doložka. Stejným způsobem se tak vyhotovuje výpis z živnostenského rejstříku. Nejčastějším úkonem v rámci CzechPOINTu jsou kromě výpisů z rejstříku trestů bezesporu konverze dokumentů. V rámci CzechPOINT@office je možné provést konverzi z listinné podoby do podoby elektronické a naopak, případně lze konverzi

ověřit. V případě konverze z listinné podoby do elektronické podoby je nezbytné příslušný dokument naskenovat, nahrát do příslušného elektronického formuláře a systém k němu vygeneruje doložku, zaručující že dokument je originální a má stejnou váhu, jako v listinné formě, a vygeneruje výstup. V případě, že se jedná o úkony v rámci kanceláře, pak lze výstup uložit do složky v počítači. Pokud se jedná o konverzi na žádost žadatele, je výstup vydaný s identifikačním kódem, který je rovněž přístupovým do Úschovny CzechPOINTu, kde si může žadatel svůj dokument s doložkou vyzvednout. V opačném případě konverze je dokument opět zpřístupněn prostřednictvím Úschovny. Elektronický dokument se následně vytiskne a opět se připojí konvertující doložka prokazující jeho originalitu. Prostředí CzechPOINTu však notář a jeho pracovníci užívají i pro řízení o pozůstalosti, neboť mají přístup do evidence obyvatel. Díky zadání rodného čísla do internetového formuláře se notáři objeví referenční údaje o zůstaviteli. Dříve stačilo do formuláře zadat pouze spisová značka a rodné číslo, případně jméno, příjmení a datum narození. Od 1. 1. 2021 je zaktualizovaná verze a je zapotřebí zadat k rodnému číslo i jméno a příjmení (vizualizace formuláře v Příloze č. 3) Notáři jsou však přístupné pouze ty údaje, které jsou pro řízení nezbytné, tzn. žádné k žádným jiným údajům evidovaným v základních registrech přístup notář ani jeho zaměstnanci nemá.

Dále mají notáři a jeho zaměstnanci umožněn dálkový přístup do katastru nemovitostí. Díky tomuto přístupu může činit výpisy pro úřední potřebu, ale i pro žadatele z řad veřejnosti. K danému výstupu je pak na výběr, zda připojit opět ověřovací doložku či nikoliv.

Samozřejmě ve své činnosti každý den se v kanceláři užívají elektronické podpisy, a to opět prostřednictvím výše zmíněného certifikátu, kde si notář či jeho pracovník vybere tzv. kvalifikovaný certifikát, jehož prostřednictvím může vyhotovovat kvalifikovaný elektronický podpis.

Díky všem těmto přístupům ke službám eGovernmentu je práce v notářské kanceláři podstatně zjednodušená, a umožňuje klientům poskytovat kompletní služby. Např. při zakládání společnosti je nezbytné mít ověřené podpisy na čestných prohlášeních statutárních orgánů, výpisy z živnostenského rejstříku statutárních orgánů a výpis z katastru nemovitostí, a právě všechny tyto služby může notář klientovi poskytnout současně se založením společnosti a klient

tak nemusí chodit na jednotlivé úřady či na kontaktní místa CzechPOINTU a doručovat zpět dokumenty do kanceláře, čímž je mu rovněž ušetřen čas.

5. Klady a zápory eGovernmentu

Každý projekt má své klady a zápory a je důležité zhodnotit, jaké přínosy a jaká rizika s sebou přináší. Tak tomu je i v rámci elektronizace veřejné správy. Dle názoru autorky je eGovernment v současnosti velice významným pomocníkem veřejné správy. Usnadňuje život nejen občanům komunikujícím s veřejnou správou ale orgánům veřejné správy samotným. Výkon veřejné správy je díky elektronizaci efektivnější a rychlejší. Za více než pozitivní hodnotí autorka v souvislosti se službami eGovernmentu hlavně časové úspory jak dílčích orgánů veřejné moci, které pro svou činnost mají veškeré potřebné informace na jednom místě a jejich úkony jsou tedy méně časově náročné, tak občanů, kteří tomu tak mají stejně a již nemusejí navštěvovat více míst a úřadů pro získání jedné věci. Pozitivním pro autorku je také provázanost mezi jednotlivými informačními systémy, jež zajišťuje, že poskytované údaje jsou důvěryhodné a prověřené, díky čemuž je zjednodušena celá řada agend jednotlivých úřadů, např. notářských, jak již bylo uvedeno v předchozí kapitole. Autorka mezi klady řadí hlavně spuštění datových schránek a Portálu občana. Portál občana je autorkou považován za významný, neboť představuje lepší a snadnější dostupnost informací a dává občanům možnost podílet se na správě jejich údajů. To znamená, že mohou kontrolovat, zda údaje o nich evidované jsou správné, případně je mohou opravit či chybu nahlásit správci systému. Také se díky tomu mohou snadněji dostat k požadované služby a může je tak bezpečně využívat z domova. Kromě Portálu občana jsou pozitivně hodnocené i další portály, které přehledně popisují dané situace a intuitivně navedou občana k tomu, aby dosáhl svého požadavku. Za zdařilé považuje autorka i možnost přihlašovat se do jednotlivých portálů veřejné správy díky eObčance a dalším prostředkům elektronické identifikace. Převážně se jedná o nejnovější identifikační prostředek bankovní identita, díky níž lze bezpečně nejen využívat služeb jaké veřejná správa poskytuje, ale i např. skrze ni bezpečně nakupovat. Příznivě vidí autorka rovněž stále se novelizovanou legislativu ve spojitosti se stále se vyvíjející formou elektronizace.

Jak již bylo řečeno, žádný projekt se neobejde bez negativ a rizik, která s sebou přináší. Riziko, které tady bylo, je a bude spojené s eGovernmentem, bude vždy v oblasti kybernetiky. Vzhledem k tomu, že eGovernment je postaven na otevřenosti a transparentnosti veřejných služeb, tzn. zpřístupnění co nejvíce možnému počtu lidí, je zde vždy možná hrozba nějakého kybernetického útoku

na data, popř. únik dat, které všechny systémy společně uchovávají. I přes to, že je užívání systému a jeho bezpečnost legislativně upravena a rovněž zabezpečena různými informačními technologiemi, je vše založené stále jen na síti, tzn. že pokusy typu kybernetické kriminality budou hrozit vždy. Odstranění tohoto rizika je však prakticky nemožné. S tím jsou samozřejmě spojeny i vysoké náklady, a to nejen náklady na zabezpečení chodu eGovernmentu, ale i pořizovací náklady, náklady na školení zaměstnanců veřejné správy atp. Rovněž zde lze zařadit i náklady občanů, neboť pro některé prvky eGovernmentu je nezbytné mít nějaký speciální přístroj nebo doplněk (např. USB token, čtečku eObčanek, chytrý telefon aj).

Závěr

Česká republika započala svůj projekt elektronizace veřejné správy v reakci na zkušenosti ostatních států a rovněž díky přistoupení k Evropské unii, kdy se pomocí zavedení jednotlivých prvků snaží dosáhnout takové fungující veřejné správy, která bude představovat vyřízení věci bez zbytečných průtahů a bude vykazovat časové a finanční úspory jak pro občany, tak pro stát. Postupem času představuje strategické plány, reflektující modernizaci jednotlivých prvků elektronizace a rovněž pokrokovost v oblasti IT služeb. Elektronizace veřejné správy je širokým tématem, který je v dnešní době na denním pořádku každého státu Evropské unie. Jedná se o problematiku, jenž zasahuje do života každého z nás, jakožto uživatele služeb veřejné správy České republiky. O to víc, soustředíme-li se na stávající situaci na celém světě v důsledku pandemie způsobené onemocněním COVID - 19, kdy různá omezení kontaktu a vycházení a omezení úředních hodin způsobila využívání dálkových přístupů jednou tolik. Spousta z nás občanů zjistila a přijmula fakt, že postupný přesun z papírové formy do formy digitální je nevyhnutelný, a že dělat věci způsobem „na dálku“ může být opravdu pohodlnější, a hlavně efektivnější a rychlejší.

Cílem diplomové práce bylo seznámit čtenáře s pojmem eGovernment, jeho podstatou a jeho jednotlivými nástroji, a v závěru podat čtenáři určité zhodnocení vývoje elektronizace veřejné správy v České republice. Práce je hned z úvodu zaměřená na samostatný pojem eGovernment, resp. snaží se podat ucelené informace, co tento pojem vyjadřuje a čtenáři poskytuje stručný pohled na vývoj elektronizace veřejné správy v České republice. Kromě toho se snaží čtenáři přiblížit základní pojmy, jež s problematikou elektronizace úzce souvisí. Vzhledem k tomu, že proces digitalizace je úzce spojen s širokou škálou úkonů ve veřejné správě, poskytuje práce rovněž i základní přehled právních norem s ní související a zabývá se stručně i otázkou bezpečnosti a ochraně údajů. Druhá a třetí kapitola diplomové práce se zabývá symboly a jednotlivými prvky eGovernmentu. Vzhledem k vysokému počtu zavedených institutů práce poukazuje pouze na vybrané pilíře eGovernmentu. Především se jedná o takové, jež stály za vznikem celého procesu, jako je komunikační infrastruktura veřejné správy, datové schránky, CzechPOINT a základní registry, a dále ty, jež odpovídají moderní době a reflektují používaní chytrých telefonů a snadný a rychlý přístup do jednotlivých

aplikací veřejné správy, spolu s bezpečnou identifikací občana. Čtvrtá a pátá kapitola pak reflektovala osobní zkušenost autorky s využíváním eGovernmentu v praxi, a to z pozice „orgánu veřejné správy“, a zhodnocení kladů a záporů s odkazem na jednotlivá rizika, která digitalizace veřejné správy přináší.

Český eGovernment během posledních několika let udělal obrovský pokrok. Vybudoval již zmíněné základní pilíře elektronizace, tj. základní registry, Informační systém datových schránek a v neposlední řadě velmi úspěšnou síť kontaktních míst veřejné správy (Czech POINT). Rovněž nelze zapomenout na spoustu schválených a běžících projektů v samosprávách, kdy spoustu z nich podporuje digitalizaci běhu úřadu a zejména portálových nástrojů, díky nimž je možné se připojit do hlavního portálu digitalizace – Portálu veřejné správy. I přes to všechno, kdy se stát snaží nabídnout dálkový přístup tam, kde je to vůbec možné (prostřednictvím emailu, datových schránek či právě jednotlivých portálů individuálních oblastí veřejné správy), je pouze malá část populace, která by této možnosti využívala naplno. Stále je zde velká část populace, která možnost využívat tuto elektronickou komunikaci se státem nepřijímá. Dosud je tu papírová forma, která je v mnoha případech ještě pořád upřednostňovaná, a je nezbytné pamatovat i na papírové formuláře a žádosti.

Závěrem je nezbytné připomenout, že eGovernment se vyvíjí a jeho modernizace je nevyhnutelná, stejně tak, jako jeho užívání v praxi. Při jeho dalším vývoji do budoucna je však stále nutné brát zřetel hlavně na potřeby občanů a jejich možnosti elektronickou formu komunikace využívat, ať už z hlediska pořízení jednotlivých zařízení k tomu sloužících, tak z hlediska jejich IT gramotnosti a gramotnosti o fungování eGovernmentu jako takového. Tímto poukazuji hlavně na problém odborné literatury vztahující se k tomuto tématu, neboť vzhledem k neustále se vyvíjející digitalizaci a postupným novelám starších zákonů je často zastaralá a neúplná. Aktualizované verze a informace o jednotlivých prvcích eGovernmentu jsou samozřejmě dostupné na internetu a jednotlivých webových portálech veřejné správy, ale má opravdu každý občan možnost si tyto informace zjistit právě, opět, elektronickým způsobem?

Resume

The theme of this thesis is electronicisation of public administration, or eGovernment. Electronicisation of public administration is a broad theme that today is the daily order of every state of the European Union. This is an issue that affects everyone's lives as a user of public administration services of the Czech Republic. The aim of this thesis was to acquaint the reader with the concept of eGovernment, its essence and its individual tools, and at the end to give the reader a certain assessment of the development of electronicisation of public administration in the Czech Republic.

The thesis is divided into five chapters. Right from the beginning, it focuses on the independent term eGovernment, or tries to provide comprehensive information, what this term expresses and gives the reader a brief insight into the development of electronicisation of public administration in the Czech Republic. In addition, they try to bring the reader closer to basic concepts and legal norms, which are closely related to the issue of computerisation. It also deals with symbols and individual elements of the eGovernment, especially those that were behind the creation of the whole process, such as the communication infrastructure of public administration, data boxes, CzechPOINT and basic registers, as well as those that correspond to modern times and reflect the use of smartphones and easy and quick access to individual applications of public administration, together with safe identification of the citizen. In thesis, the author's personal experience with the use of eGovernment in practice and the assessment of pros and cons with reference to the individual risks posed by digitisation of public administration are reflected.

Seznam literatury

I. Prameny

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).

Zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky.

Zákon č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Zákon č. 110/2007 Sb., o některých opatřeních v soustavě ústředních orgánů státní správy, souvisejících se zrušením Ministerstva informatiky a o změně některých zákonů.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Zákon č. 111/2009 Sb., o základních registrech.

Zákon č. 250/2017 Sb., o elektronické identifikaci.

II. Literatura

BUDIŠ, P., HŘEBÍKOVÁ, I. Datové schránky. 1. vyd., Olomouc: Anag. 2010. ISBN 978-80-7263-617-4.

FELIX, Ondřej, Jiří KAUCKÝ, Jindřich KOLÁŘ, et al. Jak se (z)rodil eGON: reforma a elektronizace veřejné správy. Praha: CEVRO Institut, 2015, ISBN 978-80-87125-28-1.

Kolektiv autorů. Czech POINT: Historický vývoj a současná podoba. 1. vyd. Praha: Cevro Institut. 2015, ISBN 978-80-87125-30-4.

LECHNER, T., MATES, P. eGovernment v evropském prostředí. Správní právo. Praha: Ministerstvo vnitra ČR, 2012, roč. 45, č. 4, ISSN 0139-6005.

LIDINSKÝ, V. et al. eGovernment bezpečně. 1. vyd. Praha: Grada. 2008, ISBN 978-80-247-2462-1.

MATES, P., SMEJKAL, V. E-government v českém právu. Praha: Linde Praha, 2006, ISBN 80-7201-614-8.

MATES, P., SMEJKAL, V., E-government v České republice. Právní a technologické aspekty. Praha, Leges. 2012. ISBN 978-80-87576-36-6.

POMAHAČ, Richard a kol. Veřejná správa. 1. vydání. Praha: C. H. Beck, 2013. ISBN: 978-80-7400-447-6.

SMEJKAL, Vladimír a kol. Právo informačních a telekomunikačních systémů: právní a technologické aspekty. 2., aktualiz. a rozš. vyd. Praha: C.H. Beck, 2004. ISBN 80-7179-765-0.

ŠPAČEK, David. eGovernment: cíle, trendy a přístupy k jeho hodnocení. 1. vydání. Praha: C.H. Beck, 2012, ISBN 978-80-7400-261-8.

ŠPAČEK, David. Public management. V teorii a praxi. 1. vydání. Praha: C. H. Beck, 2016, ISBN: 978-80-7400-621-0.

ŠTĚDROŇ, B., Úvod do eGovernmentu v České republice: právní a technický průvodce. 1. vyd. Praha: Úřad vlády České republiky, 2007. ISBN 978-808-7041-253.

VAVROCHOVÁ, S., ČEJP, V., ŠTĚPÁNKOVÁ, M., SAMKOVÁ, B., PŘICHYSTAL, A. Vzdělávání v eGovernmentu. 1. vyd. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, a.s. 2014. ISBN 978-80-86847-74-0.

VODIČKA, M. 3D: Data, daně digitálně aneb ajťákem i proti své vůli. Praha: Wolters Kluwer, a.s., 2014, ISBN: 978-80-7478-671-6.

III. Internetové zdroje

a) *Časopisy*

eGovernment. Dostupné z: https://www.egovernment.cz/

Renkonstrukce státu. Dostupné z: https://www.rekonstrukcestatu.cz/

b) *Ostatní*

Bankovní identita. Dostupné z: https://bankovni-identita.cz/

Beck-online.cz.

COVID portál. Dostupné z: https://covid.gov.cz/

Culturenet. Dostupné z: https://www.culturenet.cz

CzechPOINT. Dostupné z: https://www.czechpoint.cz/

Daňový portál. Dostupné z: https://www.financnisprava.cz/

Digitální Česko. Dostupné z: https://www.digitalnicesko.cz/

Datové schránky. Dostupné z: https://www.datoveschranky.cz/

eIdentita. Dostupné z: https://info.eidentita.cz/

ePortál ČSSZ. Dostupné z https://www.cssz.cz/

E-pravo.cz. Dostupné z: https://www.epravo.cz/

Justice.cz. Dostupné z: https://www.justice.cz/

Ministerstvo vnitra České republiky. Dostupné z: https://www.mvcr.cz/

Národní úřad pro kybernetickou a informační bezpečnost. Dostupné z: https://www.govcert.cz/

Portál veřejné správy. Dostupné z: https://portal.gov.cz/

Portál zdravotních pojišťoven. Dostupné z: https://www.portalzp.cz/

Smart Administration. Dostupné z: http://www.smartadministration.cz/

Správa základních registrů. Dostupné z: https://www.szrcr.cz/

systém ASPI Wolters Kluwer.

Vláda České republiky. Dostupné z: https://www.vlada.cz/

Seznam obrázků

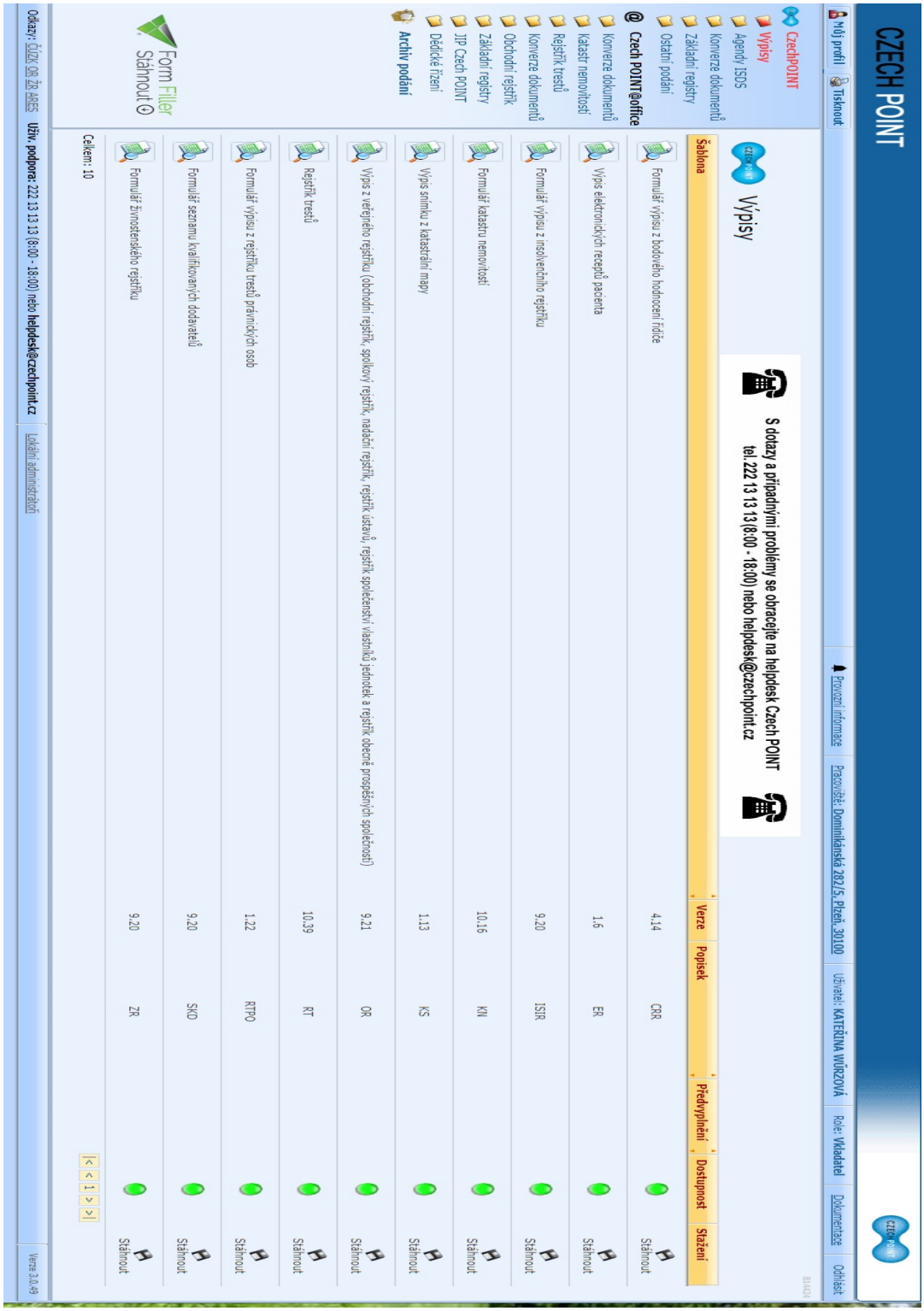
Přílohy

Příloha č. 1: Vzhled uživatelského rozhraní CzechPOINT.

Příloha č. 2: Vzhled formuláře pro výpis z Rejstříku trestů.

Příloha č. 3: Vzhled formuláře pro řízení o pozůstalosti.

Příloha č. 1: Vzhled uživatelského rozhraní CzechPOINT



Příloha č. 2: Vzhled formuláře pro výpis z Rejstříku trestů.

Ověřující:

Titul: Mgr. Příjmení: WŮRZOVÁ Jméno: KATEŘINA Titul:

ŽÁDOST O VÝPIS Z REJSTŘÍKU TRESTŮ

Žádost o výpis z Rejstříku trestů je podaná na základě žádosti o manuální zpracování? ANO ☐ NE ☒

Žádá o výpis z Rejstříku trestů zmocněnec/opatrovník? ANO ☐ NE ☒

Jednoznačné ztotožnění žadatele

Žadatel předloží doklad totožnosti a po ověření dokladu v registru obyvatel formulář zobrazí referenční údaje žadatele. Referenční údaje porovnejte s údaji v předloženém dokladu. V případě zjištění nesouladu vytiskněte odůvodnění zamítnutí podání žádosti.

Číslo dokladu Typ dokladu občanský průkaz občana ČR

Příloha č. 3: Vzhled formuláře pro řízení o pozůstalosti.

136954164

Ověřující:

Titul: Mgr. Příjmení: WŰRZOVÁ Jméno: KATEŘINA Titul:

Řízení o dědictví

Agenda: Soudní agenda a Justiční akademie

Činnostní role: Činnost soudního komisaře v řízení o pozůstalosti

Spisová značka:

Vyhledávání podle

☒ **Jména, příjmení a rodného čísla** ☐ **Jména, příjmení a data narození**

Jméno:

Příjmení:

Rodné číslo: