

Univerzita Karlova

Filozofická fakulta

Katedra pomocných věd historických a archivního studia



Bakalářská práce

Datové schránky

Data Boxes

Pavla Gajárková

Poděkování

Chtěla bych poděkovat za spolupráci obzvláště své vedoucí práce PhDr. Daniele Brádlkové, Ph.D., za její vstřícný přístup, odborné rady, silnou podporu a trpělivost. Dále bych chtěla poděkovat všem kolegům z Národního filmového archivu za jejich podporu a chtěla bych především poděkovat rodině, přátelům a příteli za trpělivost a podporu.

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 20. července 2019

.....
Jméno a příjmení

Abstrakt

Tato bakalářská práce se zabývá problematikou datových schránek. Zaměřuje se na historický vývoj datových schránek, jejich význam a právní vymezení. Zabývá se jejím dopadem na legislativní rámec ČR. Další část práce tvoří analýza vývoje eGovernmentu v České republice, kde systém datových schránek patří ke specifiku a prioritám českého eGovernmentu.

Praktickou částí je dotazníkový výzkum, zaměřený na dlouhodobé ukládání a užívání datových schránek veřejnými archivy.

Výzkum sleduje reálné, praktické používání datových schránek. K vypracování této práce bude použita aktuální, odborná literatura a související právní normy.

Klíčová slova: datová zpráva, datová schránka, eGovernment, Czechpoint, elektronický dokument, elektronický podpis, elektronická pečeť, časové razítko

Abstract

This bachelor thesis is dedicated to data data boxes, their development throughout the time, their significance and legal definition. The theoretical part of my thesis is focused on the impact of data data boxes on the legislative framework in the Czech Republic, and it covers the development of eGovernment in the Czech Republic where data data boxes are considered as one of the eGovernment priorities.

In my research I am using questionnaire methodology in which I have focused on the longterm stowage and usage of data boxes by public archives.

This part of my study is dedicated to the objective and practical use of data boxes in the system.

The thesis is based on current and relevant scientific sources, titles and legal policies.

Key words: *data message, data box, eGovernment, Czechpoint, electronic document, digital signature, trusted timestamping, electronic seal*

Obsah

Úvod.....	1
Pojmy	3
1. eGovernment.....	7
1.1 Souhrnný vývoj eGovernmentu v České republice.....	7
1.2. Státní informační politika – cesta k informační společnosti (SIP).....	8
1.3. Portál veřejné správy	11
1.4. Ministerstvo informatiky České republiky.....	11
1.5. Současný eGovernmentu v České republice	12
1.5.1. Organizační struktura	12
1.6. Symboly eGovernmentu.....	12
2.Czech POINT.....	13
2.1 CzechPOINT@office	15
2.2.CzechPOINT@home	15
2.3.E-identita	16
2.4. Výsledky statistického průzkumu ohledně využívání služeb Czech POINTu.....	16
2.5. Autorizovaná konverze	17
3.Datové schránky	19
3.1. Zavedení datových schránek v Českém právním řádu.....	21
3.2. Technická příprava a implementace datových schránek.....	25
3.3. Současný stav datových schránek v právním řádu.....	26
3.4. Zřízení datové schránky různými druhy subjektů	26
3.5. Přístup do datové schránky a oprávnění k přístupu	28
3.6. Přístupové údaje k datové schránce	28
3.7. Elektronické přihlašování.....	29
3.8. Identifikátor datových schránek	29
3.9. Znepřístupnění datové schránky	29
3.10. Zneplatnění přístupových údajů k datové schránce	30
3.11. Zrušení datové schránky	30
3.12. Doručování dokumentů orgánů veřejné správy (OMV)	31
3.13.Fikce doručení	32
5. Datová zpráva	33
5.1. Praktické odesílání datových zpráv.....	35
5.2. Ukládání datových zpráv.....	35
5.3. Pozitiva datových schránek.....	35
5.4. Statistické údaje	36

6.Ověřovací prostředky elektronického dokumentu	37
6.1.Elektronický podpis	37
6.2. Uznávaný elektronický podpis	38
6.3.Elektronická značka	38
6.4.Kvalifikované časové razítko	39
6.5.Kvalifikovaná elektronická pečeť	39
6.6.Kvalifikované certifikáty	40
6.7.Certifikační autorita	40
8.Závěr	59
9.Seznam zdrojů.....	61

Úvod

Cílem mé bakalářské práce je přiblížit datové schránky jak po teoretické, tak praktické stránce. Datové schránky jsou i po více než deseti letech provozu velmi diskutované a aktuální téma, které má své odpůrce i zastánce

Vývoj, který předcházel zavedení datových schránek v České republice byl komplikovanější, a vedla k nim delší cesta, než se původně očekávalo. Elektronizace veřejné správy a úřadování jako takového, začala v 90. let 20. století, ale vyznačovala se značnou mírou chaotičnosti a právní neukotveností. Proto bylo nutné tuto oblast právně zastřešit a zaměřit se na bezpečnou a právně garantovanou elektronickou komunikaci mezi státem a dalšími subjekty, a to zejména: fyzickou osobou, právnickou osobou či fyzickou podnikající osobou. Tento způsob komunikace musel být autentizován, aby nedošlo k jejímu padělání a možnému zneužití. Původně byla datová schránka určena především pro orgány veřejné moci, ale v této době je využívána jako komunikační prostředek i pro další subjekty.

Téma datových schránek jsem si vybrala kvůli tomu, že jsou velmi důležitou a specifickou součástí elektronizace veřejné správy. Díky svému působení ve státní správě, konkrétně v Národním filmovém archivu, pracuji s datovou schránkou každý den.

Informace obsažené v mé práci jsem čerpala z internetových stránek České pošty, která je poskytovatelem datových schránek a na svých internetových stránkách uveřejňuje nejaktuálnější informace z této oblasti. Neopominutelným dalším zdrojem byly internetové stránky Českého statistického úřadu, který na svém webu poskytuje veřejnosti výsledky ze svých statistických výzkumů. Dalším důležitým informačním zdrojem byly internetové stránky Ministerstva vnitra České republiky. Kromě důvěryhodných internetových stránek jsem čerpala i z aktuálních právních norem, viz dále.

Největší množství informací jsem čerpala z následujících právních norem. Datová schránka jako elektronický komunikační prostředek, je především vymezen v *zákoně č. 300/2008 sb., o elektronických úkonech a autorizované konverzi dokumentů*, a poté ve *Vyhláše č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek*. Dále se datové schránky objevují ve *vyhláše č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů*; v *zákoně č. 365/2000 Sb., o informačních systémech veřejné správy*; v *zákoně č. 99/1993 Sb., občanský soudní řád*; v *zákoně č. 280/2009 Sb., daňový řád* a v *nařízení*.

Zdroje, ze kterých jsem čerpala, tvoří také z části literatura, která se zaměřuje na problematiku eGovernmentu a datových schránek.

Teoretická část bakalářská práce je rozdělena do 6 samostatných kapitol. V první kapitole se zabývám eGovernmentem a jeho souhrnným vývojem a současným stavem v České republice. Vysvětluji zde základní pilíře eGovernmentu a jejich využití, dále pak který orgán veřejné moc řídí eGovernment, jaké jsou jeho symboly a co konkrétně znamenají.

Ve druhé kapitole popisují projekt Czech POINT a jeho vývoj v ČR. Dále se zajímám o kontaktní místa Czech POINT, kde se nacházejí a co poskytují aktuálně za služby. Popisují zde také dvě další rozhraní Czech POINTu, a to CzechPOINT@office a CzechPOINT@home. Poté analyzuji výsledky průzkumu Českého statistického úřadu o využívání služeb Czech POINTu.

Ve třetí velké kapitole se zaměřuji na datové schránky. Vysvětluji zde, co datové schránky jsou, k čemu slouží a jejich členění. Rozebírám možnosti dalšího využití služeb informačního systému datových schránek. Zajímám se zde o způsob vytvoření datové schránky. Objasňuji zde, který subjekt má povinnost si zřídit datovou schránkou ze zákona, a kdo si zřizuje datovou schránku na vlastní žádost. V této kapitole popisují také historický vývoj datových schránek u nás. A věnuji se celkovému ukotvení datových schránek v právním řádu.

Ve čtvrté kapitole se primárně zajímám o datovou zprávu. Konkrétně o ukládání datových zpráv, formát datové zprávy, odesílání datových zpráv a formáty přílohy datových zpráv a vysvětluji pojem *fikce doručení*. Analyzuji statistické údaje o datových zprávách a datových schránkách.

Pátá kapitola práce pojednává o ověřovacích prvcích elektronických dokumentů. V jednotlivých podkapitolách se zabývám elektronickým podpisem, kvalifikovaným časovým razítkem, kvalifikovanou pečetí a jejich náležitostmi. Pojednávám zde také o tom, co jsou kvalifikované certifikáty a certifikační autority.

Poslední kapitolou této práce je analýza výstupů z vyplněných výzkumných dotazníků. Účelem dotazníku bylo zjištění praktického využití datových schránek veřejnými archivy ve veřejné správě. A dalším předmětem zkoumání bylo zjistit, jak se datové schránky začlenily do každodenní agendy veřejných archivů, neboť od zavedení informačního systému datových schránek uběhlo deset let. Také mě zajímala frekvence používání datových schránek, a zda jsou veřejné archivy spokojeny, či nespokojeny s formou datových schránek. Absence zpracování praktického využití datových schránek veřejnými archivy, mě přiměla k tomu zaměřit se právě na toto téma.

Pojmy ¹

Analogový dokument je dokument v listinné podobě, obrazové podobě a zvukové nosiče mimo disket, DVD, CD, přenosných nosičů dat.

Archiv je instituce, jejímž úkolem je všestranná péče o archiválie.

Časové razítko kvalifikované elektronické je dle zákona 227/2000 Sb., § 2 datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Číslo jednací slouží k identifikaci dokumentů. Obsahuje vždy označení nebo zkratku označení původce, pořadové číslo zápisu dokumentu v podacím deníku nebo systému elektronické spisové služby a označení určeného časového období, kterým je zpravidla kalendářní rok, v němž je dokument evidován; popřípadě označení nebo zkratku označení organizační jednotky původce nebo jiné znaky, charakterizující skutečnosti související s dokumentem

Dokument je v širším slova smyslu každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či elektronické, který je spojen s činností původce (byl jím vytvořen nebo mu byl doručen), včetně evidenčních pomůcek jakéhokoli druhu a formy.² Norma ISO15489 vymezuje dokument jako, informaci vytvořenou, získanou a spravovanou organizacemi nebo osobami jako doklady anebo vzniklé při plnění jejich právních povinností nebo při jejich činnosti.

Datový formát je způsob kódování komponenty, který zajišťuje uložení dokumentu nebo jeho části (částí) pro účely zpracování výpočetní technikou a jeho znázornění. Datovými formáty jsou například: pdf, PDF/A, xml, html/htm, odt, ods, odp, txt, rtf, doc, xls, ppt, jpg/jpeg, png, tiff, gif, mpeg1/mpeg2, wav, mp3.

¹ Pojmy jsou použity a zkopírovány ze spisového a skartačního řádu a plánu Masarykova ústavu a Archivu Akademie věd. *Masarykův ústav a Archiv Akademie věd České republiky [online]. Copyright © [citace 31.07.2018].*

Dostupné z: https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2017/11/13/09-55-12/vzorovy-spisovy-rad_12_2017.pdf

² KUNT, Miroslav a Tomáš LECHNER. *Spisová služba*. Praha: Leges, 2015, ISBN 978-80-7502-233-2, s. 74

Elektronická podatelna je zařízení elektronického systému spisové služby umožňující příjem, vyhledávání, předávání a odesílání elektronických dokumentů. Slouží k provádění úkonů prostřednictvím datové schránky a veřejné sítě internet (e-mailu), tj. k příjmu, vyhledávání, předávání a odesílání elektronických dokumentů, které byly prostřednictvím datové schránky nebo internetem doručeny nebo budou jejich prostřednictvím odeslány.

Elektronická spisovna je funkční složka elektronického systému spisové služby určená k uložení, vyhledávání a předkládání dokumentů pro potřebu organizace (původce) a k provádění skartačního řízení v rámci informačních činností zajišťovaných tímto systémem.

Elektronický dokument dle článku 35, odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 je: *„jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.“*³

Elektronická pečeť kvalifikovaná je dle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, odst.27: *„je zaručená elektronická pečeť která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečeti a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť“*⁴

Elektronický podpis zaručený musí být jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby, je vytvořen pomocí dat pro vytváření e-podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou a je ke zprávě, která je tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Elektronický systém spisové služby je informační systém určený ke správě dokumentů ve smyslu ustanovení § 2 písm. 1) a § 63 odst. 3 a 4 zákona č. 499/2004 Sb., ESSL je základní evidenční pomůcka spisové služby vykonávané v elektronické podobě. ESSL je vždy nadřazen všem samostatným evidencím používaným na jednotlivém pracovišti. Dokumenty evidované v samostatných evidencích nejsou zpravidla evidovány v ESSL. V ESSL lze spravovat elektronické dokumenty a metadata analogových dokumentů.

³ Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, 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. 35 odst. 3

⁴ Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, 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 odst. 27

Informační systém veřejné správy dle zákona č. 365/2000 Sb., §2, písm. b, je ISVS „*informačním systémem veřejné správy funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. 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*“⁵

Jednoznačný identifikátor dokumentu (JID) je znak neoddělitelně spojený s dokumentem zajišťující jeho nezaměnitelnost a jedinečnost. Každý záznam v elektronickém systému spisové služby je automaticky označen jednoznačným identifikátorem, kterým je údaj v metadatech. JID obsahuje označení nebo zkratku instituce a alfanumerický kód. Je-li pro JID užit otisk podacího razítka, popř. jiný technologický prostředek podobného určení, nemusí obsahovat alfanumerický kód.

Metadata obsahují data popisující souvislosti, obsah a strukturu dokumentu a jeho správu v průběhu času.

Spisovna a je místo centralizovaného uložení vyřízených dokumentů původce do doby uplynutí skartačních lhůt. Při umístění spisovny je nutné splnit požadavky stanovené § 68 odst. 4 zákona č. 499/2004 Sb.

Původce je každý subjekt, z jehož činnosti dokument vznikl; a za dokument vzniklý z činnosti původce se považuje rovněž dokument, který mu byl doručen nebo jinak předán.

Skartační lhůta je doba, během níž musí být dokument uložen u původce. Skartační lhůta dokumentu se počítá vždy od počátku roku následujícího po vzniku dokumentu.

Skartační řízení je postup, při kterém se vyřazují dokumenty, jimž uplynuly skartační lhůty a jež jsou nadále nepotřebné pro činnost původce. Za řádné provedení skartačního řízení odpovídá původce a jeho právní nástupce, kteří jsou povinni umožnit příslušnému archivu odborný dohled na provádění skartačního řízení a výběr archiválií ve skartačním řízení. Konkrétní provedení skartačního řízení upravují § 7–10 a § 13–15 zákona č. 499/2004 Sb.

Skartační znak vyjadřuje hodnotu dokumentu podle jeho obsahu a označuje způsob, jakým bude posuzován ve skartačním řízení nebo mimo skartační řízení. Skartační znak „A“ (archiv) označuje dokumenty, které musí být zachovány. Skartační znak „V“ (výběr) označuje dokumenty, u nichž nelze předem jednoznačně stanovit, zda půjde o bezvýznamné

⁵ Zákona č. 365/2000 Sb., §2, písm. b

dokumenty či o dokumenty archivní povahy. Z těchto dokumentů se vyberou ve skartačním řízení závažné dokumenty, které jsou přiřazeny ke skupině „A“, zbývající dokumenty zařadí do skupiny „S“. Skartační znak „S“ (skart) označuje dokumenty krátkodobého významu, bez historické hodnoty, které se mohou po uplynutí skartačních lhůt a po provedení skartačního řízení vyřadit a zničit.

Spisová značka je evidenční znak spisu. Spisovou značkou může být číslo jednacích iniciálních (prvního) nebo jiného pracoviště určeného dokumentu vloženého do spisu nebo sběrného archu; popř. název nebo jiné označení, které pracoviště pro své účely obvykle užívá či je z jiných důvodů považuje za účelné.

Spisová služba a je soubor činností, které se týkají zajištění odborné správy dokumentů vzniklých z činnosti původce, popř. z činnosti jeho právních předchůdců. Odborná správa dokumentů zahrnuje jejich řádný příjem, označování, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, opatřování razítkem nebo technologickým prostředkem obdobného určení, odesílání, ukládání, zapůjčování a vyřazování ve skartačním řízení, včetně kontroly těchto činností.

Spisovna je místo centralizovaného uložení vyřízených dokumentů původce do doby uplynutí skartačních lhůt.

Spisový a skartační plán je schéma (ukládací klíč) pro rozdělení dokumentů do pevně stanovených skupin podle zásad desetinného třídění doplněné o skartační znaky a skartační lhůty.

Spisový a skartační řád je vnitřní předpis instituce upravující veškeré úkony spojené s příjmem, tříděním, označováním, evidencí, rozdělováním, vyřizováním, oběhem, vyhotovováním, podepisováním, odesíláním, ukládáním a vyřazováním dokumentů (skartační řízení).

Škodlivý kód je chybný datový formát nebo počítačový program způsobilý přivodit škodu na informačním systému, programovém vybavení nebo informacích úřadu, popřípadě způsobilý poškodit úřad zneužitím informací. Projevem tzv. škodlivého kódu je rovněž stav, kdy dokument není uživatelsky vnímatelný – čitelný.

Transakční protokol je soubor informací o operacích provedených v elektronickém systému spisové služby, které ovlivnily nebo změnily entity. Tyto informace umožňují rekonstrukci historie těchto operací. Transakční protokol umožňuje kontrolu provedených operací

1. eGovernment

Definice

eGovernment se snaží za pomoci moderních elektronických nástrojů zefektivnit, zpřístupnit a zrychlit úkony ve veřejné správě. Zároveň se snaží zajistit dostupnější, efektivnější a levnější služby pro občany.⁶ eGovernment lze doslovně překládat jako elektronické vládnutí (electronic – government). eGovernment můžeme definovat také obecně, jako elektronizaci veřejné správy. Zásadou modernizace veřejné správy je, že mají být v oběhu data, avšak ne občan.

Základními pilíři eGovernmentu v České republice jsou:

- a) informační systém datových schránek
- b) základní registry
- c) Czech POINT⁷

K výše uvedeným pilířům se budu věnovat podrobně v dalších kapitolách.

1.1 Souhrnný vývoj eGovernmentu v České republice

V této části kapitoly bude uveden vývoj eGovernmentu v ČR od 90. let až po současnost. Již v roce 1991 vznikla zvláštní komise k zajištění odstranění nejednotnosti informačních systémů - *Komise vlády ČR pro SIS* (státní informační systém). Tato Komise měla řídit vývoj jednotného státního informačního systému. V roce 1991 bylo přijato usnesení č. 208/1991 Sb., o řešení SIS, které směřovalo k otevřeným informačním systémům.⁸ Týkalo se zejména; *registru občanů, hospodářských subjektů, nemovitostí, územně identifikačního registru* a zahrnovalo i jednotný informační systém veřejné správy. Zpráva o výsledcích práce komise nebyla zveřejněna. Usnesení vlády ČR ze 4. února 1992 pouze zmiňuje cíle následujících koncepčních dokumentů. Pravomoci komise byly přeneseny nakonec na Ministerstvo pro hospodářskou politiku. Podle vládního usnesení se předsedou komise stal ministr pro hospodářskou politiku a rozvoj, který měl za úkol vypracovat kvalitní pracovní zázemí komise. Výše uvedené ministerstvo mělo za úkol předložit vládě koncept

⁶eGovernment - Ministerstvo vnitra České republiky. eGovernment České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit.13.4.2019]

Dostupné z: <https://www.mvcr.cz/clanek/co-je-egovernment.aspx>

⁷VAVROCHOVÁ Simona, ČEJP Vlastimil, ŠTĚPÁNKOVÁ Monika, SAMKOVÁ Bohuslava, PŘICHYSTAL Aleš, *Vzdělávání v eGovernmentu*, Vysoká škola manažerské informatiky, 2014, ISBN 978-80-86847-74-0, s. 4

⁸ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s. 54

informačního systému, který zahrnuje návrh resortních informačních systémů a státní informační soustavy, včetně návrhu na systém základních registrů.

V roce 1995 vláda odsouhlasila návrh na výstavbu státního informačního systému České republiky. Součástí tohoto systému měl být: *registr nemovitostí a obyvatel, registr sociálních dávek, zdravotní pojištění a registr ekonomických subjektů*. Po zrušení Ministerstva hospodářství převzal tyto pravomoci Úřad vlády ČR, Oddělení pro řízení Státního informačního systému.

V roce 1996 vznikl nový Úřad pro informační systém (ÚSIS), který převzal pravomoci Ministerstva hospodářství a Úřadu vlády v této oblasti. Úřad vlády bohužel svůj úkol propojit informační systémy veřejné správy nenaplnil.⁹

Jednotlivé rezorty postupovaly podle svého přesvědčení a nakupovaly ICT zařízení podle vlastních potřeb bez centrálního řízení. Koordinaci nad informační politikou převzala následně v roce 1998 Rada vlády pro informační politiku. Předseda tohoto orgánu zastával též funkci místopředsedy vlády pro hospodářskou politiku. Rada měla za úkol kontrolovat a řídit práci při realizaci státní informační politiky, dále pak měla hodnotit opodstatněnost výše finančních prostředků, vynakládaných na informační systémy. Členy Rady tvořilo kromě předsedy dalších 18 zástupců ústředních úřadů.¹⁰

1.2. Státní informační politika – cesta k informační společnosti (SIP)

V tomto dokumentu se objevují úvahy, jako např.: *„Cesta k informační společnosti je podporována současnou technologickou revolucí, která je založena na vzájemném propojení informačních, komunikačních a masově-mediálních technologií. Jejím výsledkem je dramatické snížení prostorového a časového omezení a zvýšení přístupu k množství veřejných informací. Oproti předchozím technologickým vlnám je vliv propojených informačních, komunikačních a mediálních technologií charakterizován širokou plošností a vysokou rychlostí pronikání do všech oblastí společnosti. Změny se ve velmi krátké době dotknou prakticky veškerého průmyslu i služeb, veřejného i soukromého sektoru, celé společnosti v práci i mimo ni, vzdělávání i zábavy v každodenním životě. Informační společnost tak zásadně změní podnikání, veřejnou administrativu i život každého občana.“*¹¹

⁹ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, ISBN 978-80-7400-261-8, 2012, s. 54

¹⁰ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s. 55-56

¹¹ Vláda České republiky. Vláda ČR (c) 2009-2019 [online], všechna práva vyhrazena [cit. 16.6.2019]

Dostupné z: <https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089>

Hlavními prioritami bylo zjednodušení a zefektivnění veřejné správy, kdy byly zpracovány nejdůležitější okruhy:

- Informační gramotnost veřejnosti a zaměstnanců institucí státní správy.
- Informatizovaná demokracie – měl být zajištěn přístup k informacím, prostřednictvím portálu veřejné správy.
- Rozvoj informační správy veřejných systémů.
- Komunikační struktura – vytvoření komunikačního prostředí veřejné správy informačního systému veřejné správy veřejné správy.
- Důvěryhodnost informačních systémů.
- Bezpečnost ochrana osobních údajů informačních systému.
- Elektronický obchod.
- Transparentní ekonomické prostředí – v soukromé i veřejné sféře.
- Informační společnost – vytvoření bezpečného krizového managementu a ochrana životního prostředí. Tento bod nebyl nijak specifikován a SIP s touto oblastí nepočítal.

Zlomovým obdobím eGovernmentu v České republice je období vymezené lety 1998-2000.¹² V roce 1998 se začala vláda zabývat strukturou eGovernmentu v České republice a zásadním výsledkem tohoto procesu, bylo v roce 2000 přijetí stěžejního zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS). Význam zákona spočíval především v tom, že nahrazoval množství do té doby v České republice speciálních právních norem. Zákon se současně stal nástrojem pro další období transformace právních norem, aby byly přizpůsobeny k připravovaným programům eGovernmentu.

Další etapou vývoje eGovernmentu bylo vytvoření *základních registrů: registr ekonomický subjektů, registr územní identifikace, registr nemovitostí a registr obyvatel*. Každý z těchto registrů měl mít svůj vlastní orgán, který měl být jeho správcem. Zásadním úkolem této etapy bylo zajistit propojenost mezi jednotlivými registry.

Dále měla vzniknout kontaktní místa veřejné správy, která měla být součástí celouzemní sítě. Informace měly být shromážděny centrálně, pouze na jednom určeném místě. Kontaktní místa, kromě funkce sbírání informací, měla také fungovat jako informační

¹²ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.56

centrum pro občany a měla poskytovat i aktuální formuláře. Postupem času měla tato místa fungovat, jako sjednocený úřad, který přijímá žádosti.¹³

V dalších letech bylo důležité propojit základní registry a realizovat bezpečnou výměnu informací mezi jednotlivými registry. Zásadní prioritou bylo zřízení jednotného portálu. Slabinou akčního plánu bylo, že nedefinoval ve všech projektech odpovědnou instituci a nedefinoval také, jak projekty manažersky realizovat.¹⁴

K reálnému ukotvení základních registrů byl přijat již výše uvedený zákon č. 365/2000 Sb., o ISVS. Byl to zásadní cíl celého vývoje elektronických systémů v České republice. Tento zákon měl zajistit bezpečnost a efektivnost komunikace mezi samostatnými informačními systémy státní správy. Jednou ze základních povinností, kterou tento zákon stanovil, bylo zveřejňovat informace o vedených informačních systémech.¹⁵

Informační systémy veřejné správy se musely také přizpůsobit dříve odsouhlasenému zákonu č. 106/1999 Sb., o svobodném přístupu k informacím a zákonu č. 101/2000 Sb., o ochraně osobních údajů. Díky zákonu o informačních systémech veřejné správy vznikl *Úřad pro veřejné informační systémy*, který byl ústředním správním úřadem pro rozvoj a vytváření informačních systémů veřejné správy. Tento úřad nahradil dřívější Úřad pro informační systém. Mezi zásadní úkoly nově vytvořeného ústředního úřadu patřilo analyzovat a vyhodnocovat další potřeby a aktuální stav informačních systémů veřejné správy. Dalším úkolem byla kontrola a spolupráce při vytváření a správě Portálu veřejné správy, s Radou vlády České republiky. Úřad vydával také pověření k vykonání atestací fyzickým a právnickým osobám. Při porušení povinností orgánu veřejné moci či provozovatele informačního systému mohl uložit pokutu až do výše 1 milionu Kč.¹⁶

Významnou právní normou, která byla odsouhlasena byl zákon o elektronickém podpisu č. 227/2000 Sb., který definoval, za jakých podmínek je umožněno poskytovat certifikáty a rozlišil elektronický podpis a zaručený elektronický podpis. Elektronickým podpisem byla identifikovaná osoba jednoznačně spojená s datovou zprávou a tato osoba měla certifikát používat a spravovat pod vlastní dohledem. Tento zákon ovlivnil znění další

¹³ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.58

¹⁴ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.59

¹⁵ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.61-62

¹⁶ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.63

zákonů, jako je zákon č. 150/2002 Sb., správní řád a zákon č. 99/1963 Sb., občanský soudní řád.¹⁷

1.3. Portál veřejné správy

Tento portál byl zřízen v roce 2003 na internetovém portálu *www.portal.gov.cz*, prozatím jako zkušební. Ostrý provoz portálu veřejné správy byl spuštěn v roce 2004. Smlouva o poskytování služeb byla uzavřena s vybraným dodavatelem, tehdejšími Českým Telecomem. Na počátku používání obsahoval portál informace o řešení zásadních životních událostí či informace o platných zákonech a aktuální adresáty veřejné správy. Postupně byl portál modifikován a přibývaly zde další možnosti, usnadňující výkon veřejné správy. Jako zavedení všech nových elektronických služeb, tak i portál potřeboval čas na to, aby se vyvíjel a byl dostatečně schopný propojit základní registry a byl uživatelsky bezpečný.¹⁸

Portál veřejné správy byl také vytvořen s cílem usnadnit občanům komunikaci s úřady. Měl zajistit přístup k informacím veřejných orgánů. Vznikl na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Portál slouží široké veřejnosti, ale také pro veřejnou správu, samosprávu, cizince, živnostníky a další soukromé organizace.

Oblasti, u kterých portál zajišťuje přístup informací se přímo věnuje § 6 písm. f zákona č. 365/2000 Sb., o základních informačních systémech veřejné správy následovně: *„Portál veřejné správy zajišťuje přístup k informacím získaným na základě informační činnosti [§ 2 písm. a)] veřejných orgánů zejména v oblasti sociálního zabezpečení, zdravotnického zabezpečení, správy veřejných financí, dotací, veřejných zakázek, státní statistické služby, evidence a identifikace osob, jejich součástí a práv a povinností těchto osob či jejich součástí a tvorby a publikace právních předpisů.“*¹⁹

1.4. Ministerstvo informatiky České republiky

Ministerstvo bylo zřízeno v roce 2013 jako ústřední orgán pro informační politiku. Na tento orgán veřejné moci byla přenesena působnost Úřadu pro informační systémy, ale také úsek spojů Ministerstva dopravy a pravomoci v oblasti elektronického podpisu z Úřadu pro ochranu osobních údajů. Ministerstvo informatiky pracovalo na nové Státní a informační

¹⁷ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.63

¹⁸ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.71

¹⁹ Zákon č. 365/2000 Sb., o základních informačních systémech veřejné správy, § 6, písm. f

a komunikační politice e-Česko. Cílem bylo následovat předchozí koncepty a následovat akční plán pro evropskou politiku eEuropa 2005.²⁰

Jeho úkolem fakticky bylo zavést eGovernment v České republice. Do činnosti rezortu patřily regulační (vyhlášky a návrhy novel v oblasti eGovernmentu); koordinační a metodické (vytváření různých metodik); rozvoj elektronických služeb a informačního systému veřejné správy, osvětová (účast na konferencích, školení pro zaměstnance); udělování sankcí a využití portálu veřejné správy. Na Ministerstvo informatiky byla přenesena působnost Úřadu pro informační systémy, ale také úsek spojů Ministerstva dopravy a pravomoci v oblasti elektronického podpisu z Úřadu pro ochranu osobních údajů. Ministerstvo informatiky mělo poměrně krátkou existenci, kdy byla v roce 2007 jeho činnost zastavena a část jeho agendy byla převedena na Ministerstvo vnitra ČR.²¹

1.5. Současný eGovernmentu v České republice

1.5.1. Organizační struktura

V současné době je ústředním orgánem pro celý projekt eGovernmentu Ministerstvo vnitra, konkrétně Útvar Hlavního architekta eGovernmentu. Primárními činnostmi útvaru jsou: digitální expertízy a vývoj rozvíjení nových myšlenek; podpora zvyšování digitálních dovedností; určení standardů pro digitalizaci veřejné správy; schvalování a posuzování důležitých ICT programů veřejné správy a oprava nedostatků těchto programů před řádným vypsáním veřejné zakázky. Tento útvar také připomínkuje nové právní normy v souladu s požadavky moderní veřejné správy v oblasti elektronizace.

1.6. Symboly eGovernmentu

Vizuálním symbolem projektu eGovernment je postava eGona, která přirovnává projekt k lidskému organizmu. Jednotlivé části těla mají své funkce a jsou navzájem provázané. Celkově má postava eGona symbolizovat především moderně fungující úřad, zároveň také prvotní projekty eGovernmentu v ČR.²²

²⁰ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.69

²¹ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s.72,73

²² Ministerstvo vnitra České republiky. eGovernment – Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit.16.6.2019]
Dostupné z: <https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu.aspx>

Egona tvoří:

Mozek představující základní registry, které jsou zásadním prvkem při elektronizaci veřejné správy. Základní registry se řídí zákonem č. 111/2009 Sb. o základních registrech. V České republice existují v současné době čtyři základní registry a to: *registr obyvatel, registr práv a povinností, registr osob a registr územní identifikace*.

Srdce symbolizuje tzv. eGovernment act – Zákon č. 300/2008 Sb., elektronických úkonech a autorizované konverzi dokumentů, který je stěžejní pro eGovernment.

Oběhová soustava – KIVS – Tato zkratka vychází z názvu Komunikační infrastruktura veřejné správy.

Prsty znázorňují kontaktní pracoviště Czechpoint.²³

Dalším symbolem eGovernmentu kromě eGona je **Klaudie**. Ta má představovat moderní partnerku, která znázorňuje cloud computing. Klaudie má za cíl zaručit levnější a efektivnější ICT projekty.²⁴

2.Czech POINT

Zkratka Czech POINT vychází z názvu *Podací Ověřovací Informační Národní Terminál*. Czech POINT je ukotven především v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy. Je to projekt, který má za cíl zpřístupnit informace občanům, a zároveň jim poskytnout kvalitní služby. Síť kontaktních pracovišť Czech POINT je primárním prostředníkem při komunikaci občana se státem a poskytuje vybrané služby občanům (které představím v této části práce). Díky rozsáhlé síti, zahrnující celou Českou republiku může občan využívat potřebné služby z jednoho místa, aniž by musel navštívit několik úřadů. Data, která je možné získat či si je ověřit přes Czech POINT jsou získávána z neveřejných nebo veřejných informačních rejstříků.

Czech POINT funguje v České republice od roku 2008. Patří mezi priority „českého“ eGovernmentu, o jehož reálné zavedení se pokoušelo několik vlád. Realizace Czech POINTu se podařila až druhé vládě Ing. Mirka Topolánka. Nejdříve bylo vytvořeno

²³ eGovernment - Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 16.6.2019]

Dostupné z: <https://www.mvcr.cz/clanek/co-je-egovernment.aspx>

²⁴ Klaudie – Informační servis - Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 16.6.2019]

Dostupné z: <https://www.mvcr.cz/clanek/ministerstvo-vnitra-predstavilo-klaudii-novy-symbol-egovernmentu>

testovací prostředí Czech POINT a poté se rozběhl Czech POINT naplno. Od vzniku Czech POINTu se zvětšil počet kontaktních míst po celé České republice a služby, které nabízí, se stále rozrůstají.²⁵

Kontaktní pracoviště se nacházejí především na pobočkách České pošty. Dalšími kontaktními místy, jsou: obecní úřady, úřady městských částí nebo městských obvodů, zastupitelské úřady, notáři a matriční úřady. Ministerstvo vnitra udělilo autorizace i dalším právním subjektům, jako jsou Hospodářská komora a banky.

Kromě České republiky se nacházejí pro občany ČR také kontaktní místa v zahraničí, která jsou umístěna na velvyslanectvích ČR. Nyní se v zahraničí nachází celkem 57 poboček Czech POINT. Občan České republiky si tak může z ciziny řešit například, žádost o volební průkaz, zřízení datové schránky nebo zapomenuté přístupové údaje do datové schránky.²⁶

Rozlišujeme tyto základní kategorie poskytování služeb Czech POINTu:

- *„výpisy z informačních systémů veřejné správy*
- *podání vůči státní správě*
- *datové schránky*
- *výpisy ze základních registrů*
- *konverze na žádost a další související služby*
- *zprostředkovaná identifikace osoby*²⁷

Aktuálně poskytované služby prostřednictvím kontaktních míst Czech POINT:

- *„Autorizovaná konverze dokumentů*
- *Centrální úložiště ověřovacích doložek*
- *Datové schránky*
- *Podání do registru účastníků provozu modulu autovraků ISOH*
- *Přijetí podání podle živnostenského zákona*
- *Úschovna systému Czech POINT*
- *Vydání ověřeného výstupu ze Seznamu kvalifikovaných dodavatelů*
- *Výpis z bodového hodnocení řidiče*
- *Výpis z insolvenčního rejstříku*

²⁵ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011 s. 45

²⁶ eGovernment - Ministerstvo vnitra České republiky. eGovernment Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 25.4.2019] Dostupné z: <https://www.czechpoint.cz/public/novinky/>,

²⁷ Czech POINT reg.č. CZ.1.06/1.1.00/03.05921, © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 18.6.2019]

Dostupné z: <https://www.czechpoint.cz/public/verejnost/sluzby/>

- Výpis z Katastru nemovitostí
- Výpis z Obchodního rejstříku
- Výpis z Rejstříku trestů
- Výpis z Rejstříku trestů právnické osoby
- Výpis z Živnostenského rejstříku
- Základní registry²⁸

Dalšími doplňkovými službami, které Czech POINT nabízí:

- „Dočasná úschovna dokumentů v PDF či ZFO formátu
- Uložiště ověřovacích doložek, které slouží k ověření autenticity dokumentu“²⁹

2.1 CzechPOINT@office

Czech POINT má další rozhraní a to CzechPOINT@office, které je přímo určeno pro orgány veřejné moci a úřady, není tedy dostupný pro veřejnost³⁰. CzechPOINT@office nabízí formuláře, které jsou nápomocné úředníkům při výkonu své funkce. Orgány veřejné moci a úřady mohou díky tomuto „internímu Czech POINTu“ vystavovat různé výpisy a opisy.

Úředník má možnost vyhledávat v těchto agendách:

- výpis a opis z Rejstříku trestů
- výpisy ze základních registrů
- autorizovaná konverze z moci úřední
- agendy matrik
- agendy ohlašoven
- agendy soudů

2.2.CzechPOINT@home

CzechPOINT@home je internetové rozhraní, které je určeno zejména pro vlastníky datových schránek, kteří jejím prostřednictvím mohou vyplnit elektronické formuláře a získat dálkově výpisy z určitých rejstříků do své datové schránky. Nemusí tedy navštívit ani

²⁸ Czech POINT reg.č. CZ.1.06/1.1.00/03.05921, © 2019 Ministerstvo vnitra České republiky [online], všechna práva vyhrazena [cit. 18.6.2019]Dostupné z: <http://www.czechpoint.cz/public/statistiky-a-informace/aktualni-dostupnost-sluzeb>

²⁹ Czech POINT reg.č. CZ.1.06/1.1.00/03.05921, © 2019 Ministerstvo vnitra České republiky [online], všechna práva vyhrazena [cit. 18.6.2019]

Dostupné z:<https://http://www.czechpoint.cz/public/statistiky-a-informace/aktualni-dostupnost-sluzeb>

³⁰ Czech POINT reg.č. CZ.1.06/1.1.00/03.05921, © 2019 Ministerstvo vnitra České republiky [online], všechna práva vyhrazena [cit.19.6.2019]

Dostupné z: <http://www.czechpoint.cz/public/urednik/sluzby-pro-uredniky/>

kontaktní pracoviště Czech POINT.³¹ Český statistický úřad zjistil o CzechPOINT@home, následující údaje za rok 2017: „Nejčastěji šlo o výpisy z Bodového hodnocení řidičů (5,4 tis. výpisů) a z Rejstříku trestů (4,6 tis.).“³²

2.3.E-identita

Další alternativou, jak se občan může dostat k informacím, týkajících se např. jeho osoby, majetku či správního řízení je webová stránka <https://www.eidentita.cz> a zde se má možnost občan přihlásit číslem občanského průkazu a zadáním hesla. Je nutné disponovat elektronickým občanským průkazem, tzv. „eObčanka“, která je vydávána od 1. 7. 2018.³³

2.4. Výsledky statistického průzkumu ohledně využívání služeb Czech POINTu

Z výsledků průzkumu Českého statistického úřadu za rok 2017 vyšlo najevo, že celkový počet kontaktních míst Czech POINT k 31. 12. 2017 byl 7 536. Z toho bylo 5 937 kontaktních míst na obecních úřadech (79%) a 984 kontaktních míst na poště (13%).

V roce 2017 bylo na kontaktních místech Czech POINT poskytnuto více než 2 000 000 výstupů. Toto množství zůstává konstantní od roku 2012, kdy se pohybuje okolo 2 100 000 milionu ročně. V roce 2017 bylo také nejpoužívanější službou získání různých výpisů z veřejných rejstříků. Jejich počet se pohyboval okolo 1 522 000 výpisů z celkového počtu žádostí, což tvořilo přibližně tři čtvrtiny. Mezi nejčastějšími žádostmi o výpisy z rejstříků patřily: výpisy z rejstříku trestů (902 000), výpisy z katastru nemovitostí (282 000), výpisy z obchodního rejstříku (180 000). Počet výpisů z obchodního a katastru nemovitostí mají tendenci se v posledních letech se snižovat.

Další často využívanou službou v témže roce byla autorizovaná konverze dokumentů, a to primárně z elektronické do listinné podoby. Počet vykonaných konverzí tvoří přibližně

³¹ Czech POINT reg.č. CZ.1.06/1.1.00/03.05921, © 2019 Ministerstvo vnitra České republiky [online], všechna práva vyhrazena [cit.3.6.2019]

Dostupné z: <https://www.czechpoint.cz/public/czechpoint-office>

³² Český statistický úřad, Kód: 062026-18, [online] Rozvoj informační společnosti v České republice a zemích EU, [cit. 10.4.2019]

Dostupné z: https://www.czso.cz/documents/10180/94876554/06202618.pdf/b7166a40-93fa-41a4-bb4c-ee06722d51e8?redirect=https%3A%2F%2Fwww.czso.cz%2Fcsu%2Fczso%2Fvolna-mista%3Fp_p_id%3D3%26p_p_lifecycle%3D0%26p_p_state%3Dmaximized%26p_p_mode%3Dview%26_3_groupId%3D0%26_3_keywords%3D062026-18%26_3_struts_action%3D%252Fsearch%252Fsearch%26_3_redirect%3D%252Fweb%252Fczso%252Fkatalog-produktu-vydavame

³³ eIdentita [online], © 2019 SPRÁVA ZÁKLADNÍCH REGISTRŮ, [citace 10.4.2019]

Dostupné z: <https://www.eidentita.cz/Home>

necelou čtvrtinu a jejich počet se pohybuje okolo 473 000 výstupů. Český statistický úřad sleduje nárůst například u autorizovaných konverzí z listinné do elektronické podoby. Pro porovnání, v roce 2012 bylo vydáno přibližně 50 000 konverzí a v roce 2017 to již bylo bezmála 200 000 konverzí.

Datovou schránku si v roce 2012 zřídilo na vlastní žádost 14 000 subjektů a ze zákona celkem bylo zřízeno 32 000 datových schránek. V roce 2017 zažádalo o zřízení vlastní datové schránky 44 000 subjektů a ze zákona v témže roce bylo zřízeno 35 000 datových schránek.³⁴

V roce 2009 byl zaveden CzechPOINT@office pro úředníky, kteří si mohou ověřovat údaje či podávat žádosti. V roce 2017 bylo zaznamenáno 6 300 000 výstupů. Tyto výstupy byly například výpisy ze základních registrů, autorizovaná konverze dokumentů či zápisy do matriky. Ve většině případů, je CzechPOINT@office využíván k převodu listinného dokumentu do elektronické podoby a obráceně. Tímto způsobem bylo v roce 2017 převedeno 5 000 000 dokumentů.³⁵

2.5. Autorizovaná konverze

Jednou ze služeb poskytující Czech POINT je autorizovaná konverze. Jedná se o proces, kdy se převede elektronický dokument do listinné podoby, nebo listinný dokument do elektronické podoby. Při autorizované konverzi rozlišujeme dva typy dokumentů. Výstup a vstup. Výstup je konvertovaný dokument, který vznikl konverzí. Vstup je elektronický nebo dokument v listinné podobě, který je konvertován. U dokumentu musí být ověřena shoda obsahu a k takto vytvořenému dokumentu je přiložena ověřovací doložka, která dle zákona č. 365/2000 § 9a, odst. 1, obsahuje:

„ a) údaj o ověření toho, že ověřený výstup odpovídá výstupu z informačního systému veřejné správy,

b) údaj o tom, z kolika listů se skládá ověřený výstup,

³⁴ Český statistický úřad, [cit. 10.4.2019], [online], Kód: 062026-18, Rozvoj informační společnosti v České republice a zemích EU

Dostupné z: <https://www.czso.cz/csu/czso/rozvoj-informacni-spolecnosti-v-ceske-republice-a-zemich-eu>

³⁵ Český statistický úřad, [cit. 25.4.2019], Rozvoj informační společnosti v České republice a zemích EU, Kód: 062026-18

Dostupné z: <https://www.czso.cz/csu/czso/rozvoj-informacni-spolecnosti-v-ceske-republice-a-zemich-eu>

c) údaj o tom, že ověřený výstup obsahuje částečný výpis z informačního systému veřejné správy, pokud neobsahuje výstup úplný,

d) místo a datum vyhotovení doložky o ověření,

e) pořadové číslo, pod kterým je ověření vedeno v evidenci ověření výstupu z informačního systému veřejné správy,

f) otisk úředního razítka a podpis ověřujícího. ‘‘

Konvertovaný dokument je pevně spojen s touto doložkou a je považován za jednu listinu. Vytvořený dokument pomocí autorizované konverze má stejné právní účinky, jako ověřená kopie dokumentu.³⁶

Ověřování verifikačních prvků při autorizované konverzi

Osoba provádějící autorizovanou konverzi nejdříve ověří platnost verifikačních prvků, pokud je dokument obsahuje. Mezi verifikační prvky patří; kvalifikovaný elektronický podpis, kvalifikovaná e-pečeť, kvalifikované časové razítko.³⁷

Evidence vzniklých konverzí

Každá autorizovaná konverze dokumentu se eviduje. Eviduje ji subjekt, který autorizovanou konverzi provedl, tento záznam se uchovává po dobu 10 let od provedené konverze. Záznam obsahuje údaje dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 26:

a) pořadové číslo, pod kterým je konverze vedena v evidenci provedených konverzí

b) datum provedení konverze

c) konkrétní označení vstupu a datum jeho sepsání, je-li datum ve vstupu obsaženo,

d) údaj o uhrazení správního poplatku nebo odměny notáře (uvedení čísla dokladu, kterým byl uhrazen) nebo údaj o osvobození od správního poplatku s odkazem na právní předpis ‘‘³⁸

³⁶ Zákona č.365/2019 Sb., o informačních systémech veřejné správy, §9a, ods. 2

³⁷ Zákon č. 300/2008 Sb., Zákon o elektronických úkonech a autorizované konverzi dokumentů, §24

³⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 26

3. Datové schránky

Informační systém datových schránek je právně ukotven zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Systém byl spuštěn do plného provozu 1. července 2009. Zřizovatelem informačního systému datových schránek je Ministerstvo vnitra České republiky. Provozovatelem tohoto informačního systému je Česká pošta, s. p.

Datové schránky jsou vnímány jako další historický článek ve vývoji poštovní komunikace, který přirozeně navazuje na vývoj doručovací sítě. Vývoj doručovací sítě má pozitivní vliv na přirozené začlenění fyzické a datové komunikace na základě hybridních služeb. Další státy, kde se setkáme s tím, že je hlavním provozovatelem tohoto typu komunikace Národní poštovní operátor je např. Portugalsko, Francie či Estonsko. Jednou ze strategií, jak zavést datové schránky je určit povinnost vést datovou schránku podle zákona či vyhlášky. Tímto určením povinností je dosaženo podstatné začlenění používání služby datových schránek³⁹. Od spuštění informačního systému datových schránek, byla několikrát aktualizována legislativa, která s tímto informačním systémem souvisí. Byly rozšířeny účely, pro které je datová schránka funkční a zlepšovala se uživatelská platforma datových schránek⁴⁰. Na začátku fungování datových schránek si odesílaly zprávy pouze mezi sebou orgány veřejné moci.⁴¹

Datovou schránku definuje zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů v §2 následovně:

„Datová schránka je elektronické úložiště, které je určeno k

- a) doručování orgány veřejné moci,*
- b) provádění úkonů vůči orgánům veřejné moci,*
- c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.“⁴²*

³⁹ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, 1. vydání, ISBN 9788087125298, 2014, s.25

⁴⁰ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, 1. vydání, ISBN 9788087125298, 2014, s.33

⁴¹ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, 1. vydání, ISBN 9788087125298, 2014, s.23

⁴²Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 2

Datové schránky jsou rozlišovány následovně:

- datová schránka orgánu veřejné moci
- datová schránka právnické osoby
- datová schránka podnikající osoby
- datová schránka fyzické osoby

Datová schránka může být zřízena ze zákona či na vlastní žádost. Ze zákona je povinnost zřídit datovou schránku orgánům veřejné moci, advokátům, insolvenčním správcům, daňovým poradcům, organizačním složkám podniků zahraničních právních osob zapsaných v obchodním rejstříku, právníkům osobám zřízeným zákonem a právníkům osobám zapsaných v obchodním rejstříku.⁴³

V informačním systému datových schránek (ISDS) se nacházejí základní informace o jednotlivých datových schránkách. Na prvním místě je to identifikátor datové schránky. Dále pak datum a čas vytvoření datové schránky (s uvedením hodiny, minuty a sekundy). Důležitou informací je přesný čas přihlášení příslušné osoby do datové schránky, a zároveň s údaji identifikující osobu.⁴⁴ Další úkony, které jsou systému ISDS vedeny, jsou datum odeslání a doručení dokumentu.⁴⁵

V tomto informačním systému se též uvádějí neveřejné údaje, které slouží pouze pro potřeby ministerstva vnitra (provozovatele ISDS): název a sídlo orgánu veřejné moci, organizační sloučení podniku zahraniční právnické osoby, která je zapsaná v obchodním rejstříku. Používá je jenom ministerstvo a není přípustné je poskytnout jiné osobě.⁴⁶

Ministerstvo vnitra ČR také vede veřejný seznam fyzických osob, právníků osob a orgánů veřejné moci, které mají vytvořenou a zpřístupněnou datovou schránku.⁴⁷ Na základě žádosti fyzické osoby, která má vytvořenou a zpřístupněnou datovou schránku se informace o této osobě zničí.⁴⁸

⁴³ KRŮŽ, Josef, *Řízení administrativních a správních procesů*, 1. vyd.2014, Česká zemědělská univerzita v Praze, ISBN 978-80-213-2315-5, s.124

⁴⁴ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 14, odst. 3 a-c

⁴⁵ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 14, odst. 3, písm. D

⁴⁶ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 14, odst. 4

⁴⁷ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 14, odst. 1

⁴⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 14, odst. 4

Informační systém datových zpráv poskytuje další související služby, mezi které patří:

- datový trezor
- poštovní datová zpráva
- notifikace o doručení datové zprávy
- zvýšení zabezpečení přístupu k datové schránce
- zajištění dlouhodobé platnosti datové zprávy
- přístup prostřednictvím mobilní aplikace
- přístup v elektronickém bankovníctví (od roku 2013 ČSOB)⁴⁹

3.1. Zavedení datových schránek v Českém právním řádu

Základní myšlenka o zrealizování datových schránek u nás probíhala v rámci iniciativy eStát mezi lety 2005-2006. V té době to byla v České republice velmi převratná představa. V roce 2006 byly datové schránky vytyčeny, jako jedna z hlavních priorit českého eGovernmentu. Již v roce 2006 byl vytvořen a zveřejněn návrh zákona o elektronizaci některých procesních úkonů v oblasti orgánů veřejné moci. Tento návrh se snažil uspořádat několik podstatných záležitostí, jako: jednoznačné určení fyzické osoby u elektronické komunikace, autorizovanou konverzi, tzv. legalizaci elektronického podpisu. Návrh zákona též zaváděl institut elektronické prepážky a samozřejmě institut datových schránek. Návrh chtěl docílit toho, aby datová schránka byla nástrojem ke vzájemné komunikaci mezi orgány veřejné moci, fyzickými osobami a právníckými osobami.

V následujících letech probíhaly jak politické, tak odborné diskuze, jak realizovat způsob komunikace pomocí datových schránek. Důležitou otázkou bylo přijetí optimální legislativní úpravy, a to zejména v kontextu dalších projektů, jakým byl např. Czech POINT.⁵⁰

Zásadním rokem byl rok 2008, kdy byl poslaneckou sněmovnou a senátem odsouhlasen návrh zákona, který vešel v platnost 1. 7. 2009. *Zákon č. 300/2008 sb., o elektronických úkonech a autorizované konverzi dokumentů* (tzv. zákon o datových schránkách), který je stále, i po několika novelizacích, základním pilířem informačního systému datových schránek. Tento zákon vymezil, jakým způsobem budou datové schránky využívány v elektronické komunikaci. Jak již bylo řečeno výše, upravoval komunikaci prostřednictvím datových schránek mezi orgány veřejné moci fyzickými, právníckými osobami a mezi orgány veřejné moci navzájem. Vytvoření tohoto zákona mělo vliv i na další

⁴⁹ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, ISBN 9788087125298, Praha, 1.vydání, 2014, s. 29

⁵⁰ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, ISBN 9788087125298, Praha, 1.vydání, 2014, s. 31

právní normy, do kterých se některé ustanovení přenesly. „Zákon o datových schránkách“ pozměnil zákon č. 297/2016 Sb., o elektronickém podpisu; zákon č. 499/2004 Sb., o archivnictví a vyhlášku č. 259/2012 Sb., o spisové službě; zákon č. 150/2002 Sb., správní řád; zákon č. 99/1963 Sb., občanský soudní řád. Norma definovala, jak elementární principy a procesy datových schránek, tak vymezovala práva a povinnosti uživatelů. Paradoxní bylo, že byl zákon ještě před nabytím své účinnosti novelizován. Novelizace se týkala metody úhrady nákladů na provozování datových schránek. Náklady jsou hrazeny z prostředků státního rozpočtu, a to konkrétně z kapitoly všeobecná pokladní správa. Navíc přibýlo nařízení, že právnické osoby mají svou vzájemnou komunikaci zpoplatněnou. Zároveň bylo rozhodnuto o přechodné době, pro následnou aktivaci datových schránek tzv. povinných subjektů.

S přijetím výše uvedené novely byla zároveň schválena novela zákona č. 499/2004 Sb., o archivnictví a spisové službě, jenž logicky navazoval na koncept datových schránek. Novelizovaný archivní zákon upravil především celou problematiku výkonu spisové služby v elektronické podobě.

Prováděcí vyhláška č. 194/2009 Sb., o stanovení podrobností a užívání informačního systému datových schránek, ze dne 23. června 2009. ustanovila procesní a technické podrobnosti pro používání datových schránek. Tato právní norma také vymezila přípustné formáty datové zprávy, bezpečnostní podmínky odesílání datových zpráv, náležitosti přístupových údajů, a přihlašování do datové schránky.

Ustanovení v zákoně č. 300/2008 Sb., dodaly stávajícímu systému možnosti doručování dokumentů v elektronické podobě. Po spuštění datových schránek se očekávalo, že datové schránky zcela nahradí současný způsob komunikace s orgány veřejné moci. Předpokládalo se, že datové schránky budou schopny provádět i další úkony vzhledem k orgánům veřejné moci.

Postupně mělo Ministerstvo vnitra zveřejnit seznam datových schránek fyzických, právnických osob a orgánů veřejné moci a zprostředkovat dálkový přístup k tomuto seznamu. Bezplatně a na vlastní žádost bylo také možné zřídit datovou schránku pro právnické osoby, fyzické osoby a fyzické podnikající osoby. Výjimku tvořili pouze exekutoři, notáři, insolvenční správci, daňoví poradci a advokáti na které se vztahovalo přechodné období. Po uplynutí přechodného období jim byla datová schránka zřízena automaticky.⁵¹

Zákonem stanovená povinnost, kterou zákon o datových schránkách stanovil, měla být elektronická komunikace mezi orgány veřejné moci. Ovšem zákon také uvádí, a to pouze v

⁵¹ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s. 83

případě že to umožňuje povaha dokumentu. Orgán veřejné moci usuzuje sám, zda to povaha dokumentu umožňuje. Výjimkou je doručování přímo na místě. Stanovuje také povinnost doručovat elektronický dokument pomocí datové schránky osobám, které mají zřízenou datovou schránku. Při schválení první verze zákona o datových schránkách, tak byla určena maximální velikost datové zprávy na 10 MB.

Definovala tyto oblasti:

- Velikost datové zprávy
- Přípustné formáty souborů přenášených datovou zprávou
- Bezpečnostní podmínky přihlašování k datovým schránkám
- Dobu uložení datové zprávy v datové schránce

V září roku 2009 po schválení účinnosti zákona o datových schránkách bylo zjištěno, že si schránku vytvořilo necelých 270 000 uživatelů. Očekávalo se však, že počet bude kolem 600 000 vytvořených datových schránek. Největší počet subjektů, které si schránku zaktivovaly, byly fyzické osoby. Bylo jich více než 29%. Pouhé 3% tvořily orgány veřejné moci. Dostupné informace k datu 31. prosinci 2009 ukázaly, že bylo vytvořeno 369 381 datových schránek a posláno bylo přes 5 milionů datových zpráv.

Provozovatelem byla Česká pošta a správcem informačního systému byla Telefónica 02, a. s. Na konci června 2011 se zvýšil počet vytvořených datových schránek na více než 422 000. Tento počet zahrnuje fyzické osoby, fyzické podnikající osoby, právnické osoby a orgány veřejné moci. Ke stejnému datu bylo odesláno již 50 milionů datových zpráv. U právnických osob, které vlastní datovou schránku, zřízenou ze zákona, byla v některých případech datová schránka používána jen pasivně. To znamená, že byly pouze přijímány datové zprávy. Aby bylo podpořeno aktivní používání datových schránek i u těchto případů, bylo ze zákona nařízeno posílat přes datovou schránku vybrané typy dokumentů, např. daňové přiznání.⁵²

Zákonem byla definována též tzv. *fikce doručení*, kdy je dokument poslaný do datové schránky považovaný za automaticky doručení, 10. dnem od jeho doručení. Elektronický dokument zaslaný datovou schránkou nemusel být podle zákona elektronicky podepsán, protože dokument poslaný prostřednictvím datové schránky je chápán jako dokument s elektronickým podpisem. Respektive, datová schránka validuje elektronický dokument.

⁵² ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s. 84

Jenom v případě, že to vyžadovala jiná právní či interní norma bylo vyžadováno připojení ověřeného elektronického podpisu.

Ministerstvo vnitra České republiky kladlo důraz na to, že datová schránka není e-mailová schránka a pokud dotyčný posílá zprávu pomocí datové schránky, tak komunikuje s úřadem nikoliv s individuálním úředníkem. Rozdíl mezi e-mailovou a datovou schránkou byl podle Ministerstva vnitra takový, že datová schránka zajišťovala bezpečnou komunikaci, která byla ošetřena autentizačními prvky.

Mezi pozitivní věci, které přinesly datové schránky je, že byly odhaleny díky nim již neaktivní soukromé společnosti a byl od nich vyčištěn obchodní rejstřík. Datové schránky napomohly také k opravě neplatných záznamů a zvýšila se úspěšnost doručování a vymahatelnost práva.

Datové schránky měly být zapojeny do protikorupčních opatření, kdy měly být zveřejněny informace o veřejných zadávacích řízeních. Tento návrh projednávala Národní ekonomická rada a efektem tohoto kroku mělo být propojení informačního systému datových schránek s informačním systémem veřejných zakázek a Czech POINTu.

Datové schránky se potýkaly od začátku s problémy, jako příklad lze uvést nedostačující informovanost ze strany veřejnosti. Podnikatelé neměli dostatek informací o tom, že si datovou schránku mohou zdarma vytvořit a posílat jejím prostřednictvím daňové přiznání. Na druhou stranu také samotné orgány veřejné moci neupřednostňovaly posílání elektronických dokumentů subjektům skrze datovou schránku. Nadále přežívala obvyklá praxe, vyžádat si podepsaný analogový dokument a poslat jej klasicky poštou, než ho poslat datovou schránkou bez elektronického podpisu.

Dalším problémem lze uvést nespolehlivé údaje v adresáři, týkající se adres např. úřadů či právnických osob.

Lidé byli zvyklí při e-mailové komunikaci na to, že e-maily byly dlouhodobě ukládány v elektronické poště, ale u datových schránek tomu tak není. Proto bylo nutné opakovat, že je datová schránka krátkodobým uložištěm a že je nutné datovou zprávu z datové schránky „stáhnout“, nejlépe do elektronického systému spisové služby. Po 90 dnech je datová zpráva z datové schránky automaticky smazána. Další problém byl v chybovosti seznamu adresátů datových schránek, proto se stávalo, že byla datová zpráva odeslána nesprávnému subjektu. Údaje nebyly aktuální a často nepřesné. K používání datových schránek skrze internetové rozhraní bylo nutné instalovat software 602xml filler, což ale fakticky znamenalo

znevýhodňování některých uživatelů. Na některých operačních systémech totiž tento druh softwaru nefungoval.⁵³

Jak již bylo řečeno, zavedení datových schránek ovlivnilo Zákon č. 499/2004 Sb., o archivnictví a spisové službě, na jehož základě byl poté schválen *Národní standard pro elektronické systémy spisové služby*, který byl vydán v roce 2009. Národní standard obsahuje seznam povinných funkcionalit pro výrobce jak elektronických systémů spisové služby, tak informačních systémů spravujících dokumenty. Pomáhá vytvářet sjednocující prostředí pro elektronickou komunikaci a elektronizaci veřejné správy. Novelizace zákona určovala také období pro výše uvedenou úpravu výkonu spisové služby, které mělo trvat až do roku 2012. Zákon č. 190/2009 Sb., kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, pole využitelnost datových schránek se rozšířil.⁵⁴

3.2. Technická příprava a implementace datových schránek

V České republice byl vybrán model veřejného informačního systému na základě poskytování zpoplatněných služeb. Státu se díky tomu zmenšila počáteční investice do zavedení systému. Za hlavního provozovatele systému datových schránek, byla na základě výběrového řízení vybrána Česká pošta a Ministerstvo vnitra ČR s ní následně uzavřelo příslušnou smlouvu, na jejímž základě má Česká pošta statut provozovatele a systémového integrátora.

Ministerstvo vnitra vedle výše uvedené smlouvy podepsalo, 19. 12. 2008, dohodu o spolupráci se zástupci sedmi dodavatelů elektronických systémů spisových služeb. Dohoda se vztahovala na vytvoření jednotné technické specifikace pro komunikaci ESSL a datových schránek. Dalších 50 dodavatelů ESSL se k dohodě připojilo nejpozději do července 2010. Následná implementace systému datových schránek probíhala nejdříve spuštěním pilotního ověřovacího provozu na určených úřadech a organizacích, poté spuštěním otevřeného rozhraní. Účel otevřeného rozhraní bylo veřejné testování systému. Systém datových schránek byl spuštěn do plného provozu 1. 7. 2009.⁵⁵

⁵³ ŠPAČEK David, *eGovernment cíle, trendy a přístupy k jeho hodnocení*, C. H. Beck, 2012, ISBN 978-80-7400-261-8, s. 87

⁵⁴ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, ISBN 9788087125298, 1. vydání, 2014, s. 24

⁵⁵ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, 1. vydání, 2014, s. 32-33

3.3. Současný stav datových schránek v právním řádu

3.4. Zřízení datové schránky různými druhy subjektů

Fyzické osoby

Fyzická osoba má možnost si zřídit datovou schránku na základě žádosti, kterou lze podat na kontaktním místě Českého podacího ověřovacího informačního národního terminálu, známého pod názvem Czech POINT.⁵⁶ Fyzická osoba si datovou schránkou zřídí bezplatně na základě vyplněné žádosti a datová schránka je poté vytvořena do 3 dnů od podání žádosti.⁵⁷ Fyzická osoba má ze zákona právo na to si zřídit pouze jednu datovou schránku. Žádost má své náležitosti, jako jsou: jméno, popřípadě jména, příjmení, rodné příjmení, den, měsíc a rok narození, místo a okres narození; pokud se fyzická osoba narodila v cizině, místo narození a stát, na jehož území, státní občanství, není-li fyzická osoba státním občanem České republiky.⁵⁸ Žádost také musí obsahovat úředně ověřený podpis fyzické osoby. Pokud žádost splňuje požadavky z § 4-5 zákona č. 300/2008 Sb. je datová schránka Ministerstvem vnitra České republiky žadateli zřízena. V případě jakýchkoli formálních nebo faktických nedostatků žádosti, je žadatel vyzván k nápravě, a pokud je žadatel (fyzická osoba) neodstraní, ministerstvo vnitra této osobě datovou schránku nezřídí.

Fyzická podnikající osoba

Ministerstvo vnitra zřizuje fyzické podnikající osobě datovou schránku bezplatně do 3 pracovních dnů od podání žádosti. Fyzická podnikající osoba má právo si zřídit pouze jednu datovou schránku. Po zapsání v zákonem stanovených evidencích je vytvořena ministerstvem datová schránka: advokátům, statutárnímu auditorovi, daňovému poradci a insolvenčnímu správci. Informace potřebné k vytvoření datové schránky jsou: jméno, popřípadě jména, a příjmení, popřípadě obchodní firma, rodné příjmení, den, měsíc a rok narození, místo a okres narození; pokud se podnikající fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila, státní občanství, není-li podnikající fyzická osoba státním občanem České republiky, identifikační číslo osoby, bylo-li přiděleno, místo podnikání, popřípadě sídlo.

⁵⁶ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 4

⁵⁷ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 4 odst. 1

⁵⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 4 odst. 4

Žádost, která je podána fyzickou podnikající osobou musí být opatřena úředně ověřeným podpisem podnikající fyzické osoby.⁵⁹

Právnícká osoba

Datovou schránku si právnícká osoba vytvoří na základě žádosti Ministerstvo vnitra ČR do 3 pracovních dnů od podání žádosti. Opět se jedná o bezplatnou službu. Právnícká osoba musí být řádně zapsána v obchodním rejstříku. Právnícká osoba má ze zákona nárok na zřízení jedné datové schránky. Žádost musí obsahovat následující náležitosti: název nebo obchodní firma; identifikační číslo osoby; a nebylo-li přiděleno, registrační číslo; evidenční číslo nebo jiný obdobný údaj, byl-li přidělen; adresa sídla; jméno, popřípadě jména; příjmení; datum narození a adresa pobytu osoby oprávněné jednat jménem právnícké osoby; stát registrace nebo evidence právnícké osoby. Ze zákona je stanovena povinnost, že žádost musí obsahovat úředně ověřený podpis osoby oprávněné jednat jménem právnícké osoby.⁶⁰

Orgán veřejné moci

Ministerstvo vnitra bezplatně zřídí datovou schránkou orgánu veřejné moci. Zřízena je co nejdříve po vzniku orgánu veřejné moci a kdy je zapsán do evidence dle jiného právní normy, neprodleně po zapsání do rejstříku orgánů veřejné moci a soukromoprávních uživatelů.

Orgán veřejné moci může mít více datových schránek. Datová schránka je pak zřízena do 3 dnů od podání žádosti. Tato datová schránka je vytvořena především pro potřebu vnitřní organizační jednotky nebo k provádění vybrané agendy nebo určeného působení orgánu veřejné moci.

Náležitosti, které jsou obsaženy v žádosti o datovou schránkou jsou: název orgánu veřejné moci a název vnitřní organizační jednotky OVM, pro jejíž potřebu se datová schránka zřizuje nebo název agendy nebo činnosti OMV, pro jejíž potřebu se datová schránka zřizuje; identifikátor OVM; adresa sídla; jméno, popřípadě jména; příjmení; datum narození a adresa pobytu osoby, jíž mají být zaslány přístupové údaje. Pokud orgán veřejné moci splňuje veškeré povinnosti dané zákonem, je mu zřízena další datová schránka.⁶¹

⁵⁹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 4, odst. 6

⁶⁰ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 5, odst. 1

⁶¹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 6, odst. 2

Orgány územních samosprávných celků

Orgány územních samosprávných celků mají možnost si na základě vlastní žádosti zřídit jednu datovou schránku. Nicméně pokud orgán územních samosprávných celků zažádá o zřízení další datové schránky, je možné vytvořit i další datovou schránku⁶².

3.5. Přístup do datové schránky a oprávnění k přístupu

U fyzických osob má přístup do datové schránky osoba, která si datovou schránku zřídila a je oprávněna do ní vstupovat a byla pro ni zřízena⁶³. Do datové schránky podnikající fyzické osoby má přístup pouze ta podnikající fyzická osoba, pro kterou byla datová schránka zřízena⁶⁴.

V případě právnických osob, má přístup do datové schránky osoba, která je k tomu oprávněna; statutární orgán právnické osoby, nebo člen statutárního orgánu právnické osoby či vedoucí organizační složky. Přístup do datové schránky orgánů veřejné moci mají vedoucí orgánů veřejné moci, pro které byla datová schránka vytvořena.⁶⁵ Dále jsou to osoby, které jsou administrátory či další konkrétně určené osoby podniku či orgán veřejné moci.⁶⁶

Přístup do datové schránky mají orgány veřejné moci a právnické subjekty ze zákona propojeny s ESSL nebo jiným informačním systémem. Česká republika zvolila cestu otevřeného integračního rozhraní, kterým může propojit datovou schránku jakýkoliv dodavatel informačního systému.⁶⁷

3.6. Přístupové údaje k datové schránce

Osoba oprávněná k přístupu se přihlašuje prostřednictvím přístupových údajů do datové schránky.⁶⁸ Přístupové údaje získá od Czech POINTu na základě žádosti. Údaje dojdou doporučeně do vlastních rukou písemnou formou dopisem od provozovatele datové schránky nebo si je lze vyzvednout osobně⁶⁹. Datová schránka je aktivována prvním přihlášením osoby, osoba se musí ale přihlásit nejpozději do 15 dnů od doručení údajů.⁷⁰

Každý uživatel datových schránek má své jedinečné uživatelské jméno a heslo.⁷¹ Uživatelské jméno je náhodně generované, skládá se z 6 až 12 znaků.⁷² Heslo se skládá z 8 až

⁶² Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů § 7, odst. 7

⁶³ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8 odst. 1

⁶⁴ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8 odst. 3

⁶⁵ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8 odst. 4

⁶⁶ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 8 odst. 6, písm. a

⁶⁷ CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, ISBN 9788087125298, Praha, 1. vydání, 2014, s. 29

⁶⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 9, odst. 1

⁶⁹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 10, odst. 1

⁷⁰ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 10, odst. 2

⁷¹ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 1, odst. 1

32 generovaných znaků. Kombinace je složena z písmen (různých velikostí), číslic a speciálních znaků.⁷³ Heslo k přihlášení do datové schránky nesmí být stejné jako uživatelské jméno.⁷⁴

3.7. Elektronické přihlašování do datové schránky

Pro elektronické přihlášení je používán webový portál *www.mojedatovaschranka.cz*. Přihlášení se provádí pomocí přihlašovacích údajů, které poskytne správce datových schránek.⁷⁵

Jestliže se uživatel se 5x za sebou, chybně přihlásí do datové schránky, tak správce informačního systému datových schránek doručí uživateli do 1 hodiny od posledního přihlášení do zadané e-mailové adresy zprávu, že se někdo neoprávněně chtěl dostat do datové schránky. Uživatele, který je přihlášen v informačním systému datových schránek a po dobu 30 minut je v nečinnosti, správce automaticky odhlásí. V případě, že je uživatel přihlášen prostřednictvím elektronické spisové služby, tak je přihlášen stále a automaticky se neodhlašuje.⁷⁶

Oprávnění uživatelé datových schránek mají možnost si kdykoliv změnit své přihlašovací heslo v systému datových schránek.

3.8. Identifikátor datových schránek

Identifikátor datové schránky konkrétně je vymezen v § 8 vyhlášky č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek:

„Správce informačního systému datových schránek vytváří identifikátor datové schránky automatizovaně s využitím algoritmů pro generování náhodných čísel. Identifikátor datové schránky je pro každou datovou schránku jedinečný“⁷⁷

3.9. Znepřístupnění datové schránky

Ministerstvo vnitra má pravomoc znepřístupnit datovou schránku v případě úmrtí osoby, pro kterou byla schránka zřízena, nebo na základě nabytí právní rozhodnutí o zbavení

⁷² Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 1, odst.2

⁷³ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 1, odst.4

⁷⁴ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 1, odst. 6

⁷⁵ Zákon č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 2

⁷⁶ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek § 3 odst. 2

⁷⁷ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 8

či omezení způsobilosti osoby k právním úkonům.⁷⁸ Dalšími důvody mohou být, že je osoba omezena na osobní svobodě z důvodu vzetí do vazby, ve výkonu zabezpečovací detence, ochranného léčení nebo ochrany zdraví lidu a ve výkonu trestu odnětí svobody.⁷⁹

3.10. Zneplatnění přístupových údajů k datové schránce

Při ztrátě přihlašovacích údajů do datové schránky Ministerstvo vnitra České republiky zneplatní přístupové údaje osoby oprávněné k přístupu, v co nejkratší dobu po jejím oznámením. Současně osobě zašle do vlastních rukou nově vytvořené přístupové údaje.⁸⁰

3.11. Zrušení datové schránky

Orgánem veřejné moci, který má právo zrušit datovou schránku je ministerstvo vnitra. Prvním důvodem pro zrušení datové schránky je úmrtí uživatele. Zrušení datové schránky se děje po uplynutí 3 let od smrti fyzické osoby, eventuálně v den, který je určen rozhodnutím soudu, jako den úmrtí⁸¹.

Druhým důvodem je zaniknutí živnosti, zánik právnické osoby nebo orgánu veřejné moci. Ve všech uvedených případech musí uběhnout 3letá zákonná lhůta, než je datová schránka definitivně zrušena.⁸²

Při používání datových schránek zákon pamatuje i na přestupky, kdy každý konkrétní případ posuzuje MV ČR. Přestupky jsou uvedeny v § 26 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu a jedná se o následující přestupky:

„Fyzická osoba se dopustí přestupku tím, že užije datovou schránku k šíření

a) nevyžádaných obchodních či jiných obtěžujících sdělení,

b) počítačového programu, který může poškodit informační systém datových schránek, údaj v něm obsažený nebo výpočetní techniku držitele datové schránky.

(2) Za přestupek lze uložit pokutu do

a) 10000 Kč, jde-li o přestupek podle odstavce 1 písm. a),

b) 20000 Kč, jde-li o přestupek podle odstavce 1 písm. b).“

V zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu § 26b je následující u podnikajících fyzických osob:

⁷⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 11, odst. 1, písm. c

⁷⁹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 11, odst. 1, písm. d

⁸⁰ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 12, odst. 1

⁸¹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 13, písm. a

⁸² Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 13, písm. b, c, d.

„Podnikající fyzická osoba nebo právnická osoba se dopustí přestupku tím, že užije datovou schránku k šíření

a) nevyžádaných obchodních či jiných obtěžujících sdělení,

b) počítačového programu, který může poškodit informační systém datových schránek, údaj v něm obsažený nebo výpočetní techniku držitele datové schránky.

(2) Za přestupek lze uložit pokutu do

a) 10000000 Kč, jde-li o přestupek podle odstavce 1 písm. a),

b) 20000000 Kč, jde-li o přestupek podle odstavce 1 písm. b)“⁸³

3.12. Doručování dokumentů orgánů veřejné správy (OMV)

Umožňuje-li to povaha dokumentu, orgán veřejné moci upřednostňuje komunikaci se subjektem prostřednictvím datové schránky. Dovoluje-li to charakter dokument a zpřístupnění datové schránky, posílá OMV datové zprávy také fyzickým, právnickým a podnikajícím osobám prostřednictvím datové schránky.⁸⁴ Elektronický dokument, který byl doručen prostřednictvím datové schránky, je okamžikem přihlášení uživatele či určené osoby brán jako doručení⁸⁵. Dokument je považován jako doručení, i když oprávněná osoba se nepřihlásila po doručení elektronického dokumentu po dobu 10 dnů.⁸⁶ Doručení elektronického dokumentu prostřednictvím datové schránky, má stejné právní účinky jako doručení do vlastních rukou.⁸⁷ Pokud není z bezpečnostních důvodů použita forma posílání přes datovou schránku, je možné upřednostnit jinou alternativní elektronickou možnost komunikace⁸⁸. Úkon, který je vykonán fyzickou či právnickou osobou nebo pověřenou osobou, prostřednictvím datové schránky je považován na stejné právní úrovni, jako když je úkon proveden písemnou formou a je podepsaný.⁸⁹

Čas a fikce doručení datové zprávy

V případě, že se jedná o připomínkové jednání či o správní řízení, jsou údaje jako přesný čas a datum doručení datové zprávy, velmi důležité. V případě doručení datové zprávy, např v pátek v 17:00, kdy pracovník úřadu otevřel datovou zprávu až pondělí, bere se

⁸³ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentu, § 26

⁸⁴ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, odst. 1

⁸⁵ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, odst. 3

⁸⁶ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, odst. 4

⁸⁷ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, odst. 6

⁸⁸ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 17, odst. 7

⁸⁹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 18, odst. 2

jako reálný část doručení 17:00 v pátek. Na vyřizující lhůty nemá vliv, kdy se zaměstnanec přihlásí do datové schránky, resp. ji otevře.⁹⁰

Působnost ministerstva v oblasti datových schránek

Ministerstvo připojuje k datové zprávě data, která prokazují jedinečnost každé datové schránky. Dodá datovou zprávu odesílateli a zajišťuje také informaci o doručení datové zprávy do datové schránky.⁹¹

3.13. Fikce doručení

Fikce doručení je termín, kterým lze označit lhůtu 10 dnů, po které je datová zpráva považována automaticky za doručenu.

Orgán veřejné moci odesílá datovou zprávu prostřednictvím datové schránky podnikatelskému subjektu či fyzické osobě, tak je zákonně daná fikce doručení lhůta 10 dnů, po které je následovně zpráva brána jako za zprávu přečtenou.

Pro průběh řízení, je důležitá fikce doručení, neboť podporuje právní jistotu a pokračování ve správním či jiném řízení.

V opačném případě, kdy fyzický či podnikatelský subjekt posílá datovou zprávu prostřednictvím datové schránky, je důležitý čas doručení datové zprávy do datové schránky.

Při komunikaci mezi soukromými subjekty, je pokládán za moment doručení přihlášení některé ze soukromých subjektů do datové schránky.⁹²

⁹⁰ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011 s.

⁹¹ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, § 20, odst. a

⁹² CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, ISBN 9788087125298, Praha, 1. vydání, 2014, s. 24

5. Datová zpráva

Datová zpráva jsou elektronická data, která jsou přenášena prostředky pro elektronickou komunikaci a lze je uchovávat na záznamových médiích, které jsou používány při vyřizování. Datová zpráva se skládá z obálky datové schránky a obsahu datové schránky, což jsou přiložené přílohy ke zprávě. A dále z doručky, kterou je možné si stáhnout. Doručka se vytvoří automaticky při doručení datové zprávy do datové schránky.⁹³

Zákon vymezuje datovou zprávu jako dokument, který prostřednictvím datové schránky doručen fyzické osobě, právnické osobě orgánem veřejné moci. Pokud je datová zpráva určena přímo do vlastních rukou, odesílatel označí v datové zprávě tento údaj.⁹⁴

Přílohy, které jsou připojeny k datové zprávě, musí být v jasně definovaných formátech, dle přílohy č. 3, vyhlášky 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

„a) *pdf (Portable Document Format)*

b) *PDF/A (Portable Document Format for the Long-term Archiving)*

c) *xml (Extensible Markup Language Document)*

d) *fo/zfo (602XML Filler dokument)*

e) *html/htm (Hypertext Markup Language Document)*

f) *odt (Open Document Text)*

g) *ods (Open Document Spreadsheet)*

h) *odp (Open Document Presentation)*

i) *txt/csv (prostý text)*

j) *rtf (Rich Text Format)*

k) *doc/docx (MS Word Document)*

l) *xls/xlsx (MS Excel Spreadsheet)*

m) *ppt/pptx (MS PowerPoint Presentation)*

n) *jpg/jpeg/jfif (Joint Photographic Experts Group File Interchange Format)*

⁹³ MATES, Pavel, SMEJKAL Vladimír, *Egovernment v České republice, právní a technologické aspekty*, Leges, 2012, Praha, 978-80-87576-36-6, s. 29

⁹⁴ Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, §19, odst.1

- o) png (Portable Network Graphics)*
- p) tif/tiff (Tagged Image File Format)*
- q) gif (Graphics Interchange Format)*
- r) mpeg1/mpeg2 (Moving Picture Experts Group Phase 1/Phase 2)*
- s) wav (Waveform Audio Format)*
- t) mp2/mp3 (MPEG-1 Audio Layer 2/Layer 3)*
- u) isdoc/isdocx (Information System Document) verze 5.2 a vyšší*
- v) edi (mezinárodní standard EDIFACT, standardy ODETTE a EANCOM pro elektronickou výměnu obchodních dokumentů - EDI)*
- w) dwg (AutoCAD DraWinG File Format) verze 2007 a vyšší*
- x) shp/dbf/shx/prj/qix/sbn/sbx (ESRI Shapefile)*
- y) dgn (Bentley MicroStation Format) verze V7 a V8*
- z) gml/gfs/xsd (Geography Markup Language Document)’,⁹⁵*

Z praktického hlediska je pro používání datových schránek nejobvyklejší formát přílohy datové zprávy: pdf, pdf/A, doc, docx, xml, xls, xlsx, nebo jpg. Celou datovou zprávu včetně jejich příloh, obálky a dodejky lze uložit ve formátu ZFO. Program k otevření a uložení takového formátu je volně ke stažení, pod názvem Software 602, Form Filler.

Velikost datové zprávy, která je odesílána uživatelem do jiné datové schránky je maximálně 20 MB.⁹⁶ Pokud zpráva přesahuje datových objem více než 20 MB, není možné datovou zprávu odeslat.⁹⁷ Datová zpráva, která nemá správný datový formát se neodešle.⁹⁸ Další příčinou neodeslání datové zprávy je možný výskyt škodlivého kódu, který může poškodit informační systém datových schránek.⁹⁹ V malé podkapitole se věnuji přímo praktickému odesílání datových zpráv.

⁹⁵Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, příloha č. 3

⁹⁶ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 5

⁹⁷ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 7, písm. a

⁹⁸ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, § 7, písm. b

⁹⁹ Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, §7, písm. c

5.1. Praktické odesílání datových zpráv

V téhle malé podkapitole se věnuji faktickému popisu odesílání datových zpráv. Po přihlášení do informačního systému datových schránek zvolíme možnost Napsat zprávu. Pomocí aktuálního adresáře je možné nalézt potřebný subjekt, kterému odesíláme datovou zprávu. Po vybrání subjektu vyplníme údaje jako je věc (název dokumentu, jako je např. daňový domicil), pomocné údaje jako jsou možnosti, že bude zpráva doručena přímo do rukou určité osoby, nebo uvedeme konkrétní jméno a příjmení odesílatele datové zprávy. V dalším řádku lze uvést zmocnění, a to přímo s číslem příslušného paragrafu, včetně odstavce a písmena zákona. Podstatnými údaji jsou číslo jednacích (odesílatele i subjektu, kterému je určena datová zpráva) a spisová značka. V posledním kroku vložíme vybraný elektronický dokument ve správném formátu a odešleme.

Pokud osoba posílá podání prostřednictvím datové schránky, tak nemusí být podepsán elektronickým podpisem, jelikož přihlášením do datové schránky se osoba identifikuje.¹⁰⁰

Doručenka

Datová zpráva obsahuje kromě přiložené přílohy také doručenkou. V doručence nalezneme informace o konkrétním čase doručení zprávy. Další údaj vedený v doručence je, že se oprávněná osoba už přihlásila do datové schránky a čas přihlášení. Datovou zprávu lze stáhnout z datové schránky i s doručenkou, která tvoří digitální obálku. V této obálce je uvedeno, komu byla datová zpráva odeslána včetně spisové značky, čísla jednacích, ID datové schránky, od jakého subjektu je odeslána, datum doručení, datum odeslání a čas odeslání.

5.2. Ukládání datových zpráv

Datové zprávy jsou v datové schránce uloženy po celkovou dobu 90 dnů, poté jsou nenávratně vymazány. Proto je důležité uchovávat datové zprávy i jiným způsobem, například v elektronickém systému spisové služby či je uložit v bezpečném interním uložišti, nebo do placeného datového trezoru, který poskytuje Česká pošta.

5.3. Pozitiva datových schránek

Jako hlavní pozitivum datových schránek lze jmenovat, že vlastník datové schránky se může do datové schránky přihlásit a využívat přístup do dalších informačních systémů, jako je informační systém sociální správy a finanční správy. Každý rok uživatel datové schránky obdrží zprávu o využití, jeho údajů orgány veřejné moci a kdo sleduje tyto údaje v registru

¹⁰⁰ DRÁBKOVÁ, Tereza, *Doručování ve správním řízení se zaměřením na elektronické formy komunikace*, Wolters Kluwer ČR, Praha, ISBN 978-80-7552-723-3 2017, s. 55

obyvatel. Uživatel může využít vyšší formu autentizačního přihlášení a novou příchozí datovou zprávou upozorní pomocí SMS zprávy či notifikací do e-mailové schránky.

5.4. Statistické údaje

Český statistický úřad v roce 2018 vydal tiskovou zprávu s informací, že stále více datových schránek si zařizují i osoby, které nejsou podnikajícími subjekty. Datové schránky si oblíbilo mnoho občanů a jsou často zřizovány na vlastní žádost. Zpráva poskytuje informaci také o tom, že bylo v roce 2017 posláno 102,8 milionu datových zpráv. Počet transakcí, které byly uskutečněny prostřednictvím datových schránek se rok od roku zvyšují. Mezi lety 2012-2017 narostl jejich počet dvojnásobně. V roce 2012 bylo posláno 45, 4 milionů datových zpráv a v roce 2017 bylo posláno už 102,8 milionu. Subjekt s nejvyšším počtem poslaných zpráv jsou orgány veřejné moci tedy 70 % všech transakcí, které byly provedeny skrze datové schránky.

Další zajímavou skutečností, kterou zjistil Český statistický úřad je, že objem zpráv poslaných občany se mezi rok 2013 až 2017 zvýšil 5x. To znamená, že v roce 2013 bylo odesláno necelých 100 tisíc transakcí a v roce 2017 už těchto transakcí přes datové schránky bylo už 5x vyšší.

Kromě poslaných datových zpráv občané také využívali aplikaci Czechpoint@home, kde mezi nejvíce používané služby patřily žádosti o výpisy z veřejných a neveřejných rejstříků. Konkrétně byl nejvíce žádaný výpis z Bodového hodnocení řidičů, kde bylo uskutečněno 5400 transakcí a žádost o výpis z trestního rejstříku. Těchto žádostí bylo 4 600. Czechpoint@home lze využívat z počítačového zařízení či mobilního telefonu z domova.

Ze zprávy vyplývá také to, že i občané, kteří nevlastí datovou schránku využívají elektronických formulářů, které poskytují konkrétní úřady a ty mohou odeslat online formou. V roce 2017 tak využilo elektronickou komunikaci s úřadem v České republice 14 % osob.

Za rok 2017 přibylo 80 tisíc nových datových schránek. Z větší části byly datové schránky vytvořeny na základě žádosti (56%) a druhou možností bylo, že byly datové schránky vytvořeny ze zákona (44%). Vlastníci nově vytvořených datových schránek byly především právnické osob či fyzické podnikající osoby. Fyzickým nepodnikajícím osobám bylo v roce 2017 na základě jejich žádosti vytvořeno skoro 23 tisíc nových datových schránek.

Transakce, které jsou prováděny přes datové schránky se rok od roku zvyšují. V porovnání s rokem 2012 kdy bylo posláno 45, 4 milionů datových zpráv, tak v roce 2017 bylo posláno až dvojnásobně více zpráv a to 102,8 milionů.¹⁰¹

6.Ověřovací prostředky elektronického dokumentu

6.1.Elektronický podpis

Elektronický podpis je autentizačním prvkem elektronického dokumentu a zajišťuje jeho právní validitu a integritu. Elektronický podpis je založen na základě kvalifikovaného certifikátu, který vydává akreditovaný poskytovatel certifikačních služeb, nebo jiný elektronický prostředek fungující na podobných technologických principech.¹⁰²

Elektronický podpis je ve své podstatě číslo. Jako s číslem s ním pracují pouze programy, které ověřují jeho platnost, naproti tomu člověk, uživatel s ním tímto způsobem nepracuje.¹⁰³ Elektronický podpis zajišťuje integritu konkrétního dokumentu. Potvrzuje tedy to, že je dokument celistvý a neměnný. V praxi se setkáváme také s variací pojmu elektronický podpis, a to s pojmem digitální podpis. Elektronický podpis je logicky spojen s dokumentem a je součástí datové zprávy.¹⁰⁴

Primární právní normou, ve které je zakotven elektronický podpis je 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, ze které vycházejí další normy. Nařízení definuje elektronický podpis článkem 3, odstavec 10:

„data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání“¹⁰⁵

V České republice je legislativně vymezeno používání elektronického podpisu v zákoně č. 297/2016 Sb., o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce. Zákon stanovil tzv. přechodné období, kdy byly vydávány

¹⁰¹ Český statistický úřad [online], Katalog produktů-Datové schránky si zřizují i nepodnikající osoby, [cit. 17.4.2019]

Dostupné z: <https://www.czso.cz/csu/czso/-datove-schranky-si-zrizuji-i-nepodnikajici-osoby>

¹⁰² KUNT, Miroslav a Tomáš LECHNER. *Spisová služba*. Praha: Leges, 2015, s. 58, ISBN: 978-80-7502-233-2

¹⁰³ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s.29

¹⁰⁴ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 30

¹⁰⁵ Nařízení evropského parlamentu a rady (EU) č. 910/2014, čl. 3, odst. 10

elektronické podpisy na základě původního zákona o elektronickém podpisu a současně na základě výše uvedeného nového zákona. Toto období skončilo 19. září 2018, kdy bylo možné používat pouze kvalifikovaný elektronický podpis.¹⁰⁶

6.2. Uznávaný elektronický podpis

Dle zákona č. 297/2016 Sb., o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce se definuje uznávaný elektronický podpis § 6, odst. 2:

„Uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.“

Uznávaným elektronickým podpisem lze ověřit, že datovou zprávu podepsala osoba, která je uvedena na kvalifikovaném certifikátu. Další možnost, kterou umožňuje je ověření, že elektronický dokument nebyl nějak pozměněn a dále je možné oprávněně předpokládat, že se osoba s obsahem elektronického dokumentu seznámila a s ním souhlasí.

Orgán veřejné moci, je povinen každý elektronický dokument podepsat uznávaným elektronickým podpisem. Elektronický podpis lze být využíván na smlouvách v elektronické podobě či na elektronických podáních

Ověřuje, že datovou zprávu označila osoba uvedena na kvalifikovaném certifikátu. Umožňuje ověření, že zpráva nebyla po okamžiku podepsání nějak pozměněna. Předpokládá se, že bez přímého ověřování došlo k označení, které bylo automatizované.

6.3. Elektronická značka

Elektronická značka je obdobná elektronickému podpisu. Elektronickou značku uplatňovaly právnické osoba a používala se též na fakturách. Elektronická značka se užívala pouze do roku 2018, kdy ji podle zákona č. 297/2016 Sb., o elektronickém podpisu nahradila kvalifikovaná elektronická pečeť.¹⁰⁷

Elektronická značka se může používat jako označení datové zprávy jako vydané a také jako výstup informačního systému veřejné správy. Dokáže označit transakční protokol vytvořeného elektronickým systémem spisové služby.¹⁰⁸

Rozdíl mezi elektronickým podpisem a elektronickou značkou

Rozdíl mezi elektronickým podpisem a elektronickou značkou je, že elektronický podpis vytváří sama fyzická osoba. Kdežto elektronickou značku může vytvářet počítačový

¹⁰⁶ eGovernment-Služby vytvářející důvěru, Ministerstvo vnitra České republiky. eGovernment Ministerstvo vnitra České republiky [online]. Copyright © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena [citace 27.4.2019]

Dostupné z: <https://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx>

¹⁰⁷ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, ISBN 978-80-904248-3-8, 2011, s. 34

¹⁰⁸ KUNT, Miroslav a LECHNER Tomáš, *Spisová služba*, Leges, ISBN 978-80-7502-233-2, 2015, s. 65

program, nebo elektronický systém To znamená, že to nemusí procházet vůbec přes fyzické osoby, ale je tím označován výstup z informačních systémů.¹⁰⁹

6.4.Kvalifikované časové razítko

Časové razítko je poskytováno certifikační autoritou. Prokazuje dobu, kdy vznikl digitální dokument, a proto se často používá u účetních dokladů, jako jsou faktury. Všeobecně je užíváno tam, kde je potřeba vědět, jak dokument vypadal v době, kdy byl označen časovým razítkem. U časových razítek na rozdíl od elektronického podpisu subjekt platí každé použité časové razítko. U elektronického podpisu je placený obvykle certifikát na 1 rok, bez omezení počtu použití.¹¹⁰

Nařízení eIDAS a právní účinky časového razítka, oddíl 6, čl.41, odst. 1:

„Elektronickému časovému razítku nesmí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko“¹¹¹

6.5.Kvalifikovaná elektronická pečeť

Elektronická pečeť slouží k zachování integrity, autenticity a jistotu původu elektronického dokumentu. Podepisující právnická osoba pečetí potvrzuje, že se s dokumentem seznámila. Elektronická pečeť stejně jako elektronický podpis musí fungovat s platným certifikátem od kvalifikovaného poskytovatele služeb vytvářejících důvěru. Tak jak je tomu i elektronického podpisu, musí elektronická pečeť splňovat určité podmínky, které stanovuje nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce. Elektronickou pečetí se stvrzuje, že podepsaný dokument existoval v momentu pečetění. Elektronickou pečetí se zaručuje, že digitální dokument má stejnou právní hodnotu jako vtištěný podepsaný dokument. V případě elektronického dokumentu, který je opatřen elektronickou pečetí, je zapotřebí ještě časové razítko. Elektronická pečeť nahrazuje elektronickou značku.

Požadavky podle nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce vymezuje článek 36:

„a) je jednoznačně spojena s pečetící osobou

b) umožňuje identifikaci pečetící osoby

¹⁰⁹ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 34

¹¹⁰ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 35

¹¹¹ Nařízení eIDAS, odd. 6, čl. 41, odst. 1

c) je vytvořena pomocí dat pro vytváření elektronických pečeti, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou

d) je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.¹¹²

6.6. Kvalifikované certifikáty

Kvalifikovaný certifikát je druh potvrzení.¹¹³ Potvrzení, jehož pomocí můžeme ověřit platnost elektronického podpisu. Vydáním certifikátu kvalifikovanou certifikační autoritou je potvrzeno, že poskytovaný klíč patří určité osobě.¹¹⁴

Vytvořený certifikát obsahuje:

- Veřejný klíč
- Jméno a další údaje
- Datum počátku platnosti
- Datum ukončení platnosti
- Jméno certifikační autority
- Sériové číslo¹¹⁵

6.7. Certifikační autorita

V České republice máme tři certifikační autority, které poskytují kvalifikované certifikáty. Máme celkem tři certifikační autority v ČR:

- První certifikační autorita, a.s.
- eIdentity, a.s.
- Česká pošta, s.p.¹¹⁶

Pro certifikační autoritu se používá zkratka CA. V zákonech a vyhláškách je používán termín poskytovatel certifikačních služeb.¹¹⁷ Lze jí označit také jako třetí nezávislý subjekt, který je důvěryhodný.¹¹⁸

¹¹² Nařízení eIDAS, čl. 36

¹¹³ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 37

¹¹⁴ KRÍŽ, Josef, *Řízení administrativních a správních procesů*, 1. vyd.2014, Česká zemědělská univerzita v Praze, ISBN 978-80-213-2315-5, s. 127

¹¹⁵ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0,2011, s. 60

¹¹⁶ Úvodní strana-eGovernment-Služby vytvářející důvěru a elektronická identifikace, © 2019 Ministerstvo vnitra České republiky, všechna práva vyhrazena, [cit. 16.7.2019]

Dostupné z: <https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>

Certifikační autorita zaručuje jedinečnost subjektů dle použité identifikace subjektů. Provedení těchto úkonů potvrdí certifikační autorita podpisem svým soukromým klíčem, a poté vydá tento certifikát.¹¹⁹ Díky vydání certifikátu si nemusejí subjekty navzájem vyměňovat klíče a certifikační autorita tím zajistí správnost a bezpečné uchování privátního klíče¹²⁰.

Pokud kvalifikovaný poskytovatel certifikačních služeb splňuje všechny specifické požadavky k poskytování certifikátu dostane akreditaci od státu.¹²¹

Například, platnost elektronického podpisu, jak již bylo uvedeno je na dobu určitou. Neznamená to však, že je to doba platnosti dokumentu. Po uplynutí doby platnosti certifikátu není zcela jisté, že informace v dokumentu jsou potvrzené certifikátem.¹²²

¹¹⁷ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011, s. 60

¹¹⁸ PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 42

¹¹⁹ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011, s. 60

¹²⁰ MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŮŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011, s. 61

¹²¹ Peterka Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8, s. 42

¹²² Peterka Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8 s. 75

7. Praktická část

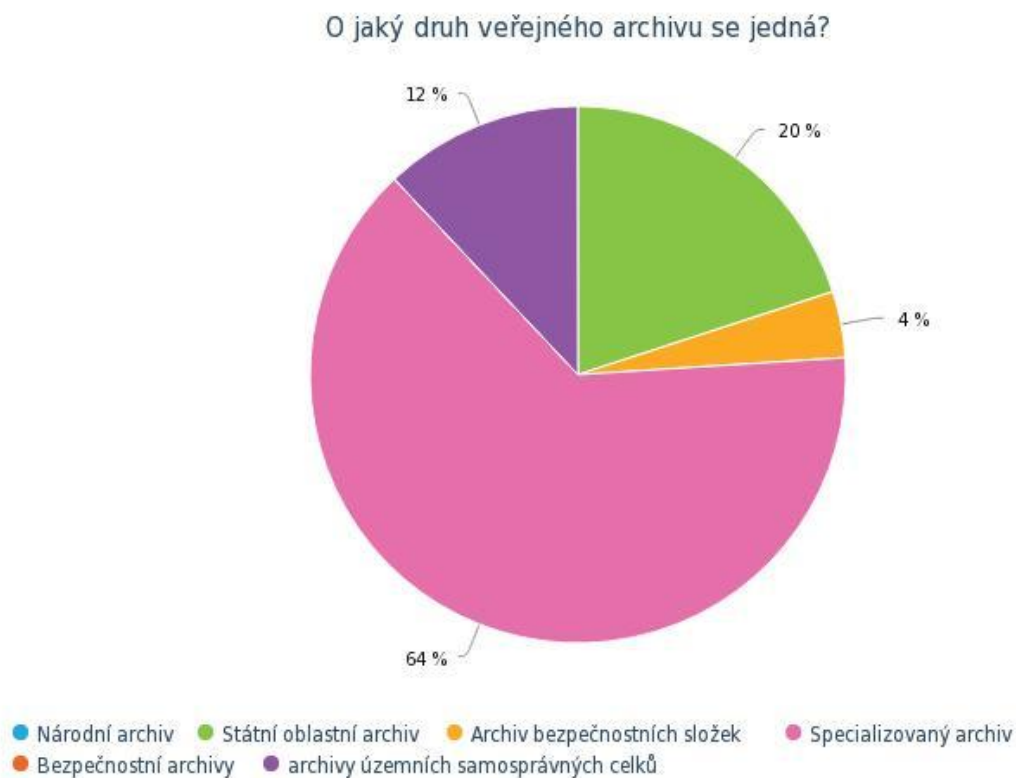
V praktické části práce byla zvolena forma výzkumu pomocí dotazníku. Dotazník byl vytvořen na internetové stránce *www.surveymonkey.com*, poté pomocí přiloženého hypertextového odkazu byl zaslán všem veřejným archivům v České republice prostřednictvím e-mailu.

Dotazník je určen všem veřejným archivům v České republice. Podle soustavy archivů do veřejných archivů patří: *Národní archiv, specializované archivy, státní oblastní archivy, archivy územních samosprávných celků, archivy bezpečnostních složek.*

Ze 45 oslovených veřejných archivů vyplnilo dotazník 25. V následujících grafech budou představeny výsledky dotazníku. Dotazník se skládá ze 16 otázek.

Datové schránky jsou v provozu již 10 let a je to využívaný prostředek k elektronické komunikaci, z tohoto důvodu mě zajímalo, jak ve veřejných archivech pracují s datovou schránkou. Cílem dotazníku je dozvědět se, jak často s datovými schránkami pracují, a jak jsou celkově spokojeni či nespokojeni s datovou schránkou.

1. Otázka, o jaký druh veřejného archivu se jedná?



Prvotní otázka je velmi obecná ale přesto podstatná, tedy o jaký druh veřejného archivu se jedná. Z odpovědí můžeme analyzovat, že nejčastěji vyplnily dotazník specializované archivy, a to celkem 64% z dotázaných. 20% tvořily odpovědi od Státních oblastních archivů. Třetí nejpočetnější skupinou, která vyplnila dotazník, byly archivy územně samosprávných celků (12%). Tuto skutečnost si vysvětlují tak, že je nejvíce zastoupeno těchto archivů v archivní síti v České republice. Nejmenší procento tvoří Archiv bezpečnostních složek (4%), který je jenom jeden.

2. Používáte datovou schránku?



Druhá otázka je zaměřena na používání datové schránky. Nejvyšší procento má v tomto grafu odpověď ano (80%). Odpověď ne je tvoří 20% všech odpovědí

3. Kdo využívá nejčastěji datovou schránku ve Vaší instituci?



U této otázky, která se zaměřuje na využívání datových schránek se u se ukázalo, že nejčastějším spravujícím datovou schránku je pracovník podatelny (56%). Druhá nejčastější odpověď byla, že pracuje s datovou schránkou jiný pracovník (16%). Třetí nejčastější odpovědí bylo, že datovou schránku spravuje sekretářka (12%). Ředitel/ředitelka veřejného archivu spravuje ve veřejném archivu podle výsledků v nejméně případech (8%).

4. Jak často během týdne používáte datovou schránku

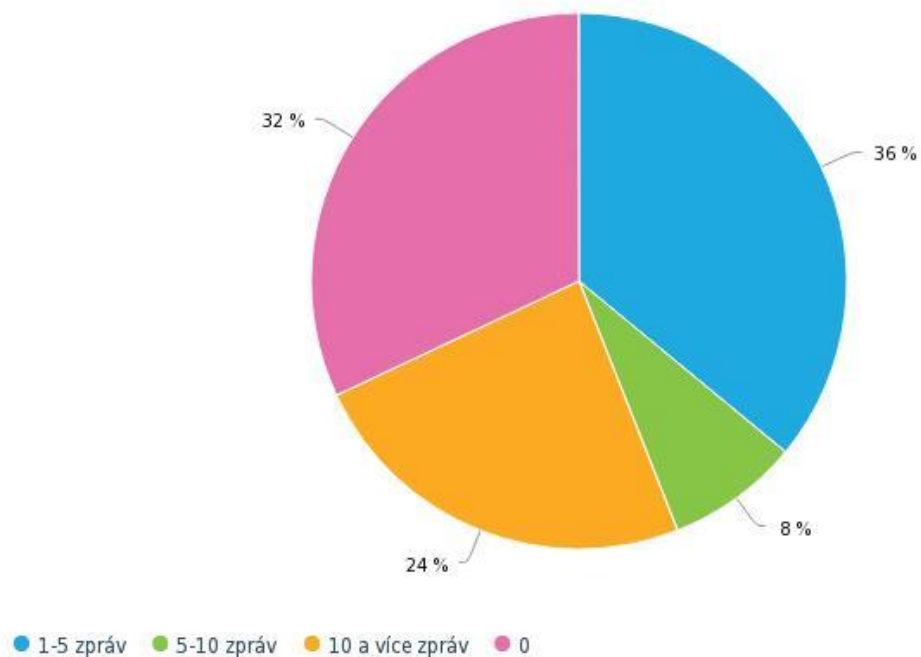
Jak často během týdne používáte datovou schránku?



Čtvrtá otázka měla za cíl zjistit, jak často během týdne používají veřejné archivy datovou schránku. Výsledky ukázaly, že nejčastěji je datová schránka používána veřejnými archivy 3x a více týdně (32%). Druhou nejčastější odpovědí bylo 1-2x týdně (28%). Veřejné archivy používají datovou schránku 2-3x týdně (12%).

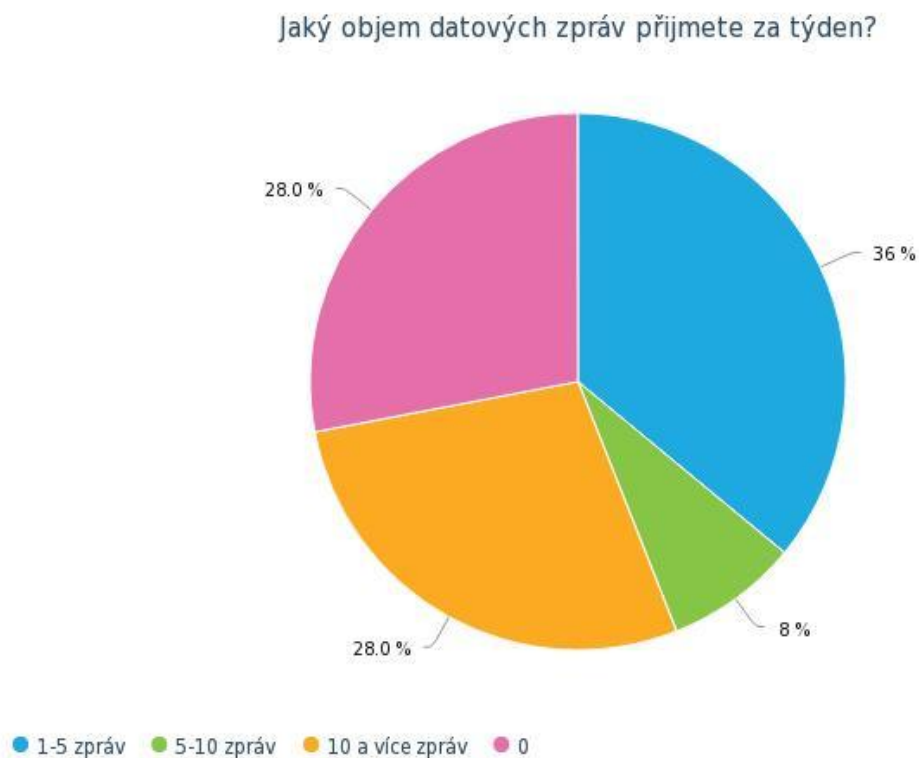
5. Jaký objem datových zpráv posíláte za týden

Jaký objem datových zpráv posíláte za týden?



Nejčastější odpovědí při této otázce bylo 1-5 zpráv za týden (36%). Druhou nejčastější odpovědí bylo 0 (32%). Třetí nejčastější odpovědí bylo, že veřejné archivy posílají 10 a více datových zpráv týdně (24%). 5-10 datových zpráv týdně posílá 8% z dotázaných veřejných archivů.

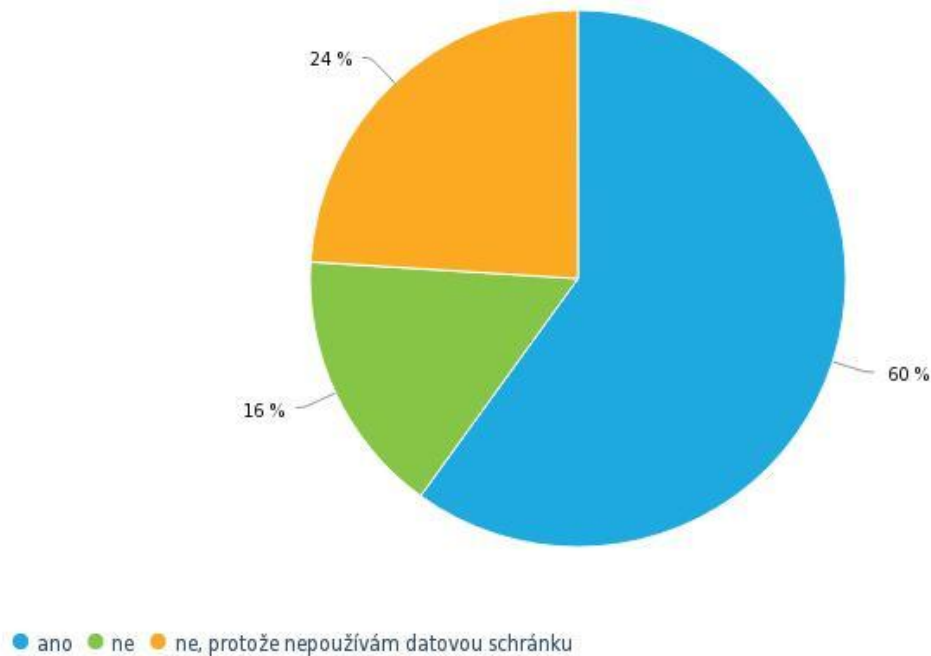
6. Jaký objem datových zpráv přijmete za týden?



V této odpovědi lze analyzovat, že nejvíce zvolily archivy odpověď 1-5 zpráv týdně (36%). Odpovědi 0 a 10 a více zvolilo stejně 28% z dotázaných. Nejmenší procento z dotázaných zvolilo odpověď, že přijme za týden 5-10 zpráv (8%).

7. Jsou zprávy z datové schránky (odeslané i přijaté) podepisovány e-podpisem a potvrzeny e-razítkem?

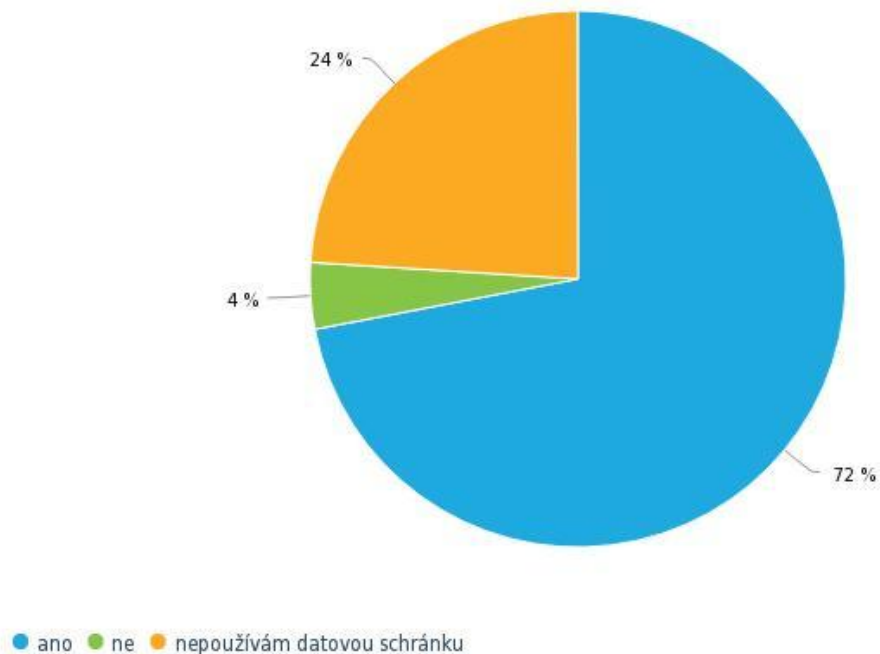
Jsou zprávy z datové schránky (odeslané i přijaté) podepisovány e-podpisem a potvrzeny e-razítkem?



Tato otázka se zabývala tím, zda jsou zprávy z datové schránky podepsány e-podpisem a potvrzeny e-razítkem (myšleno časové razítko). V 60% procentech je to splněno. Menší procento 16% tedy nejsou podepsány. Můžeme usoudit, že se veřejné archivy berou e-podpis, jako už běžnou věc.

8. Je pro Vás jednoduché používat datovou schránku?

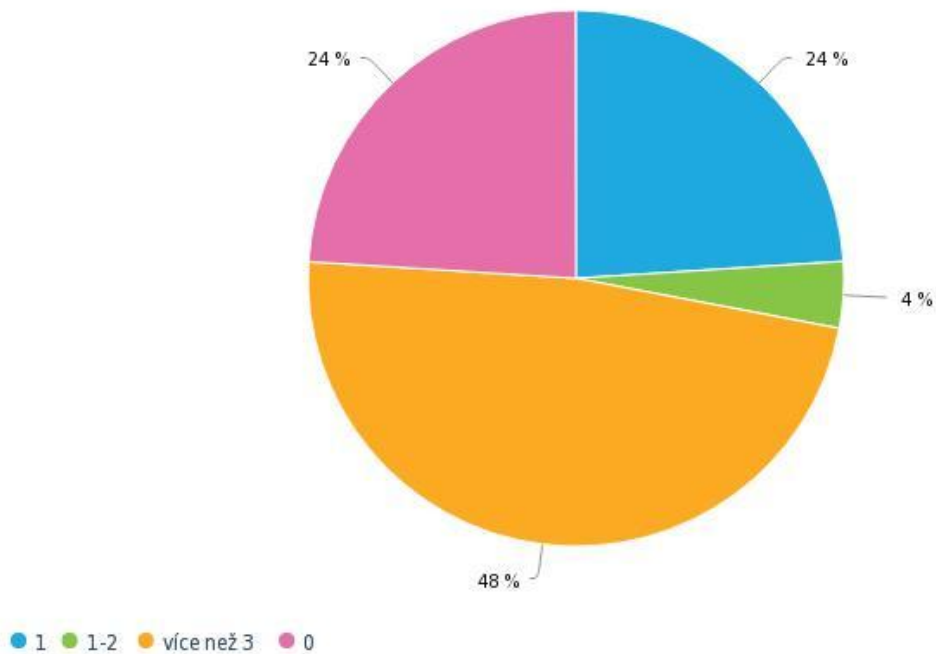
Je pro Vás jednoduché používat datovou schránku?



V následujícím grafu je možné analyzovat celkem jednoznačnou odpověď, a to že jsou datové schránky pro vysoké procento pracovníků veřejných archivů přijatelné (72%). S tímto tvrzením nesouhlasí 4% z dotázaných.

9. Kolik pracovníků archivu využívá datovou schránku ve Vaší instituci?

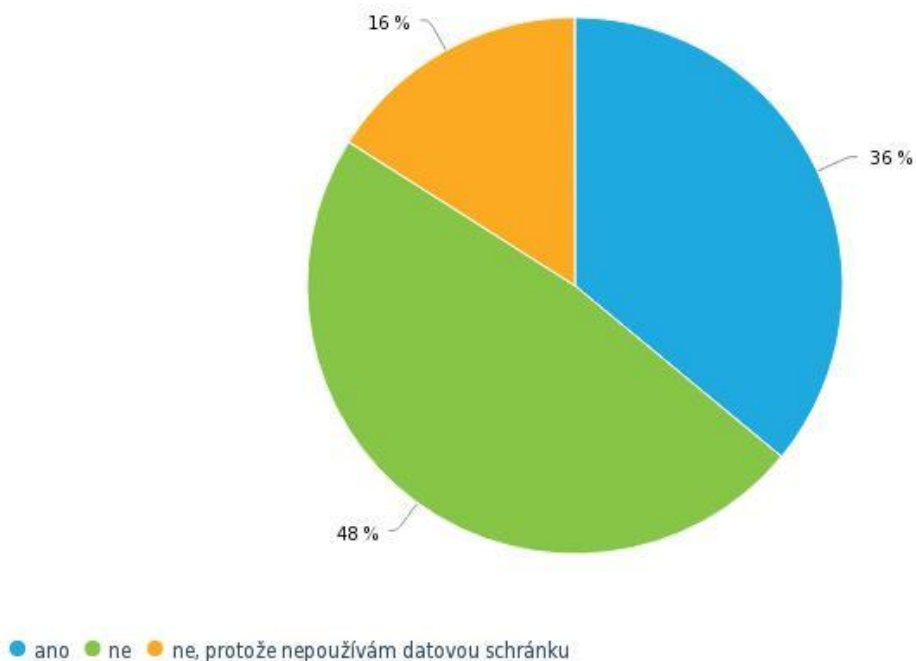
Kolik pracovníků archivu využívá datovou schránku ve Vaší instituci?



Počet zaměstnanců, kteří používají datovou schránku v instituci je více jak 3 osoby (48%). Druhé nejvyšší procento odpovědí bylo, že 0 (24%). Třetí odpovědí bylo, že jeden pracovník (24%). Poslední odpovědí bylo 1-2 pracovníků (4%)

10. Využívají také fyzické osoby možnost zasílat např. Žádosti či jiné dokumenty prostřednictvím datové schránky do Vaší instituce?

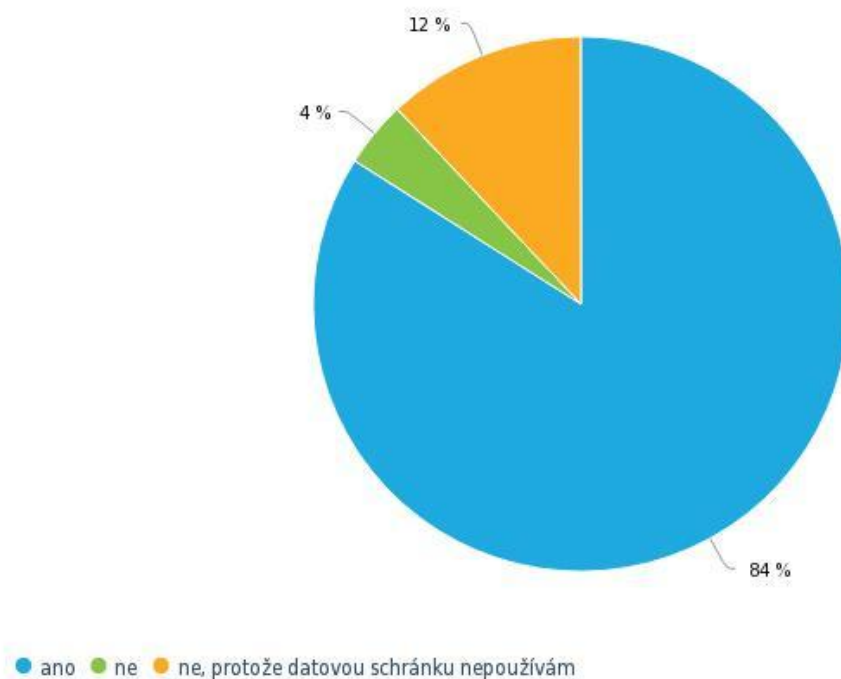
Využívají také fyzické osoby možnost zasílat např. žádosti či jiné dokumenty prostřednictvím datové schránky do Vaší instituce?



Z grafu lze analyzovat, že nejvyšší procento odpovědí tvoří, že fyzické osoby nevyužívají možnost zasílat datové zprávy do veřejného archivu (48%). Avšak nemalé procento odpovědělo, že využívají (36%). Zbylé procenta tvoří ty, kteří nepoužívají datovou schránku (16%).

11. Využívají také právnické osoby možnosti prostřednictvím datové schránky zasílat např. Žádosti či jiné dokumenty do Vaší instituce.

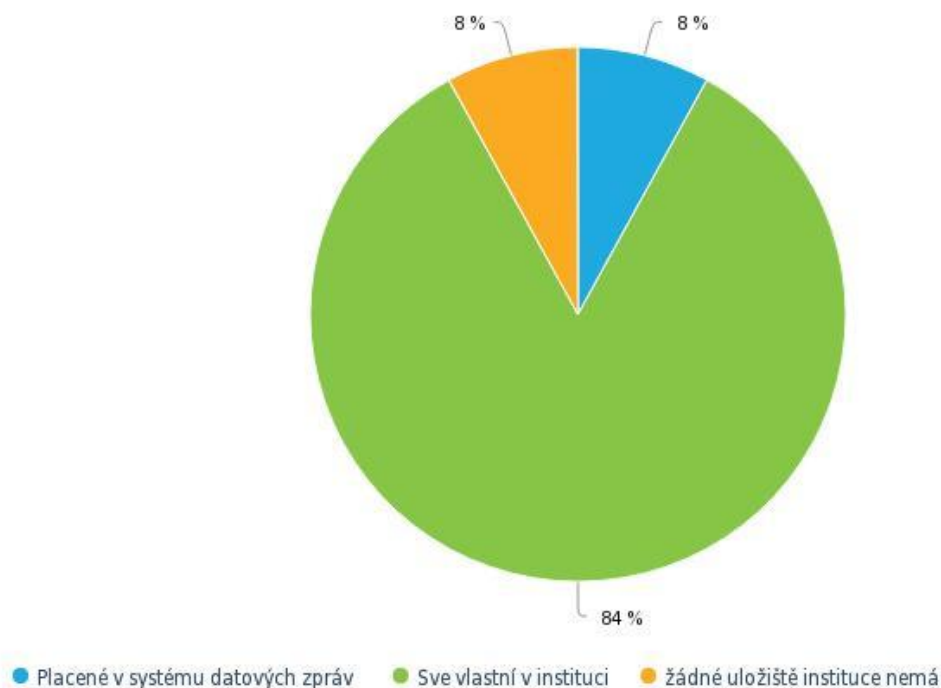
Využívají také právnické osoby možnosti prostřednictvím datové schránky zasílat např. žádosti či jiné dokumenty do Vaší instituce?



Při této otázce 84% z oslovených veřejných archivů, které vyplnily dotazník odpovědělo, že právnické osoby používají datovou schránku ke komunikaci s veřejným archivem. 4% uvedlo, že ne. Zbývající 12% zvolilo odpověď ne, protože datovou schránku nepoužívají.

12. Jako uložení datových zpráv využíváte možnosti placeného uložení systému datových schránek nebo máte vlastní uložení v instituci

Jako uložení datových zpráv využíváte možnosti placeného uložení systému datových schránek nebo máte vlastní uložení v instituci?

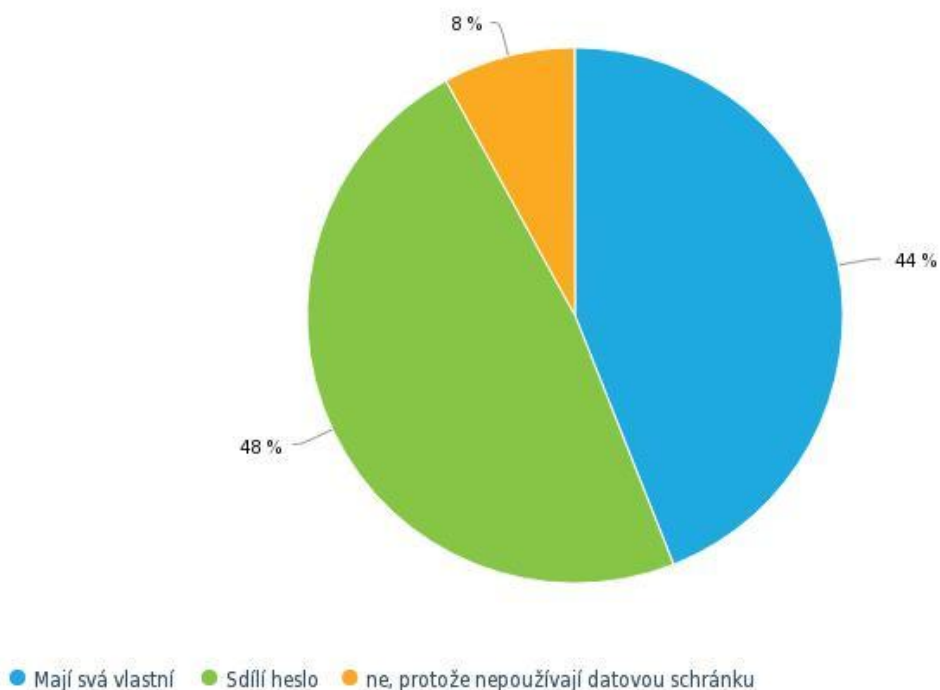


Datové zprávy v datové schránce se ukládají po maximálně 90 dnů po uběhnutí této lhůty, jsou datové zprávy smazány. Instituce a jakýkoliv jiný uživatel datové schránky proto musí vytvořit systém, jak datové zprávy uchovávat efektivně a dlouhodobě. Možností je mnoho a z grafu lze usoudit, že veřejné archivy si vytvořily svou vlastní alternativu ukládání datových zpráv (84%).

Další možností pro ukládání datových zpráv je placené uložení v informačním systému datových zpráv. Tuto možnost využívá 8% veřejných archivů. Odpověď žádné uložení instituce nemá je brána, jako vůbec datovou schránku nevyužívají (8%).

13. Sdílí pracovníci heslo do datové schránky či mají svá vlastní

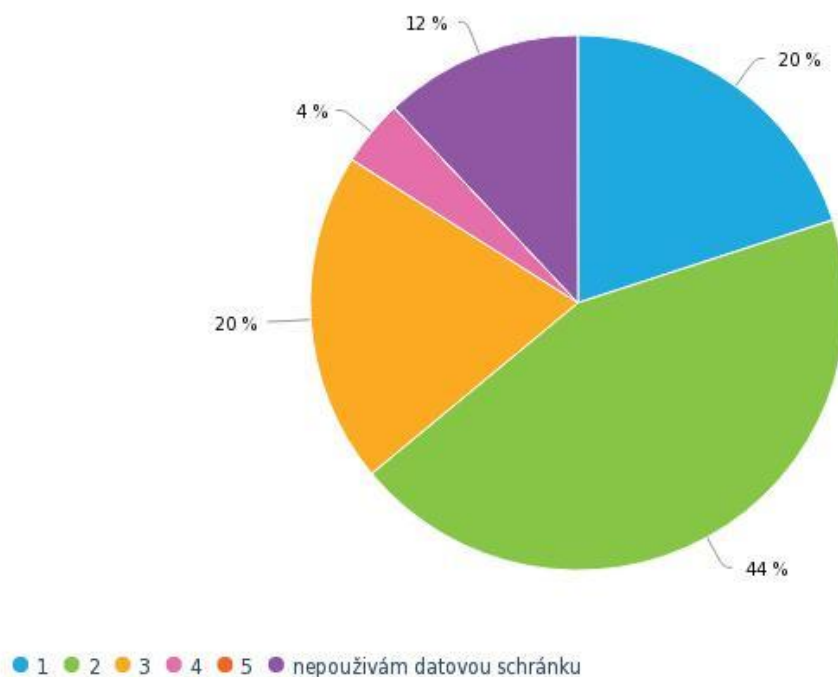
Sdílí pracovníci heslo do datové schránky, či mají svá vlastní?



Tato otázka se zaměřila na sdílení hesla k datové schránce. V případě, že více zaměstnanců využívá datovou schránku, je jednodušší sdílet pouze jedno heslo. Z bezpečnostního hlediska je vhodné, aby každý uživatel měl své heslo. Výsledky ukazují, že 48% sdílí jedno heslo. V 44% mají zaměstnanci veřejných archivů své vlastní heslo k datové schránce.

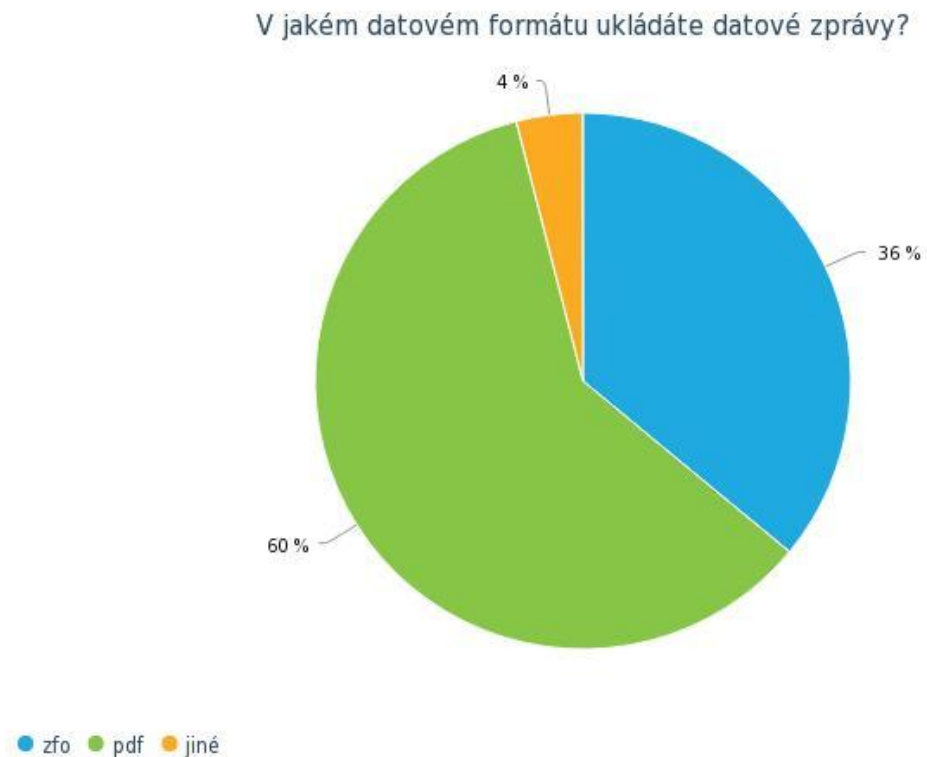
14. Jak byste hodnotila/a celkový systém datových schránek? Zvolte prosím číslo na škále od 1-5, jako ve škole

Jak byste hodnotil/a celkový systém datových schránek? Zvolte prosím číslo na škále od 1-5, jako ve škole.



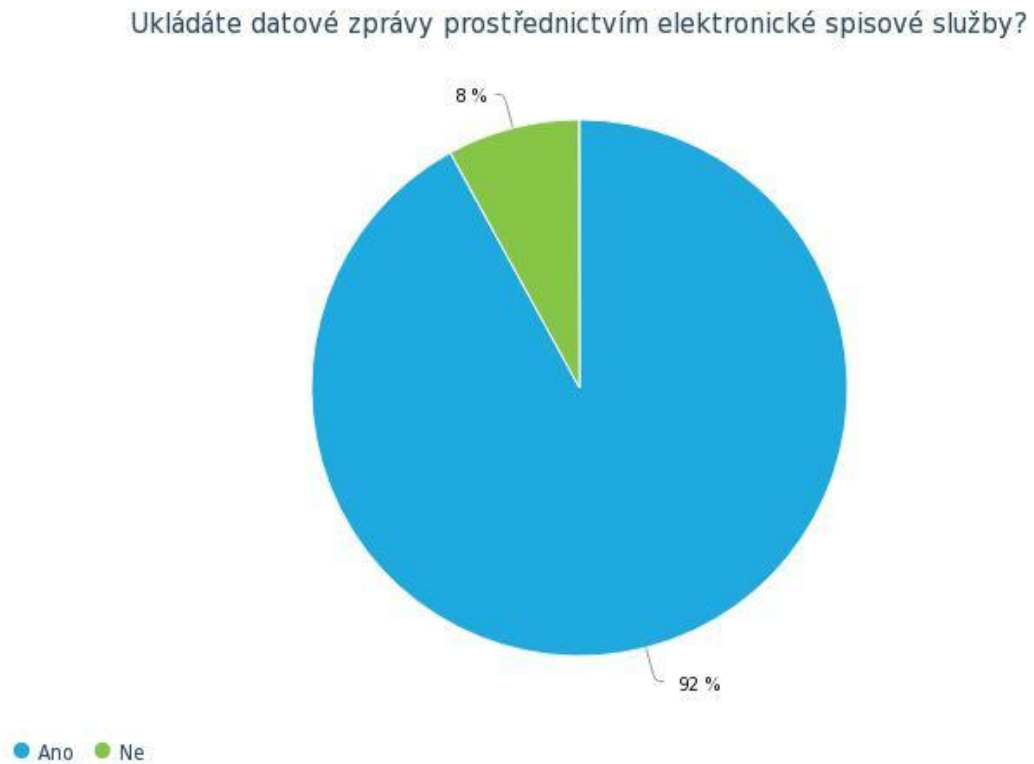
Celkové hodnocení lze sledovat v následujícím grafu. V této škále bylo zvoleno triviální hodnocení datových schránek. Nejvíce byly datové schránky hodnoceny známkou 2 (44%), dále pak procentuálně stejně známkou 1 a 3 (20%). Známkou 4 hodnotily 4% z dotázaných. A zbylých 12% nepoužívá datovou schránku.

15. V jakém datovém formátu ukládáte datové zprávy?



Předposlední otázka se zabývala tím, v jakém datovém formátu jsou ukládány v instituci datové zprávy. Nejčastější odpovědí bylo, že ve formátu pdf (59.1%), dále zfo (36.4%) a poslední možností bylo jiné (4.5%).

16. Ukládáte datové zprávy prostřednictvím elektronické spisové služby?



Poslední otázka tohoto dotazníku se zabývala ukládáním datových zpráv prostřednictvím elektronické spisové služby. Z odpovědí lze analyzovat, že 95,5% veřejných archivů ukládá datové zprávy pomocí elektronické spisové služby. Veřejné archivy, které tuto formu ukládání nezvolily je menší počet (4,5%).

8. Závěr

Cílem mé bakalářské práce bylo přiblížit datové schránky po teoretické a praktické stránce. V mém bádání jsem se zaměřila, jak na historický vývoj datových schránek v České republice, také jsem měla za cíl zjistit aktuální informace týkající se datových schránek. Dalším cílem bylo přiblížit ukotvení datových schránek v českém právním systému.

Z předchozích kapitol je zřejmé, že informační systém datových schránek je stále více využívaným komunikačním prostředkem, a že se nejen plně osvědčil v rámci elektronizace veřejné správy, ale stal se jedním ze základních pilířů českého eGovernmentu. V současnosti je datová schránka využívána nejen orgány veřejné moci, právníckými osobami, podnikatelskými subjekty, ale stále hojněji též fyzickými osobami.

V teoretické části se zabývám vývojem a aktuálním stavem českého eGovernmentu, který úzce souvisí s datovou schránkou. Dále se zajímám o projekt Czech POINT a jeho vývoj včetně deskripce aktuálních služeb. Výsledky z výzkumu Českého statistického úřadu ukázaly, že celkově jsou kontaktní místa Czech POINT umístěna nejčastěji na obecních úřadech a na poště. Nejžádanějším druhem výpisu byl v roce 2017 výpis z rejstříků trestů, naopak klesá počet žádostí o výpisy z obchodního rejstříku. U údajů o autorizované konverzi dokumentů je zřejmé, že narůstá počet konverzí, a to z listinné do elektronické podoby.

Následně se věnuji celkově datovým schránkám, jak praktické, tak teoretické stránce. V následujících kapitolách se věnuji datové zprávě a ověřovacím prostředkům, jako jsou kvalifikované časové razítko, kvalifikovaná pečeť, certifikáty a kvalifikovaný podpis. Datové schránky se osvědčily za jejich dobu existence, jako spolehlivý komunikační prostředek, který disponuje aktuálním adresářem a doplňkovými službami, jako je například posílání notifikací do e-mailové schránky, využití datových trezorů či možná instalace aplikace přímo do mobilního telefonu.

Budoucnost datových schránek odhaduji jako přirozeně rozrůstající se informační systém, který se bude stále vyvíjet. Bude také přibývat konstantně více datových schránek rozdílných subjektů, a díky tomu se bude zvyšovat počet poslaných datových zpráv. Díky datovým schránkám a Czech POINTu mohou občané vyřizovat své věci z domova či na kontaktním místě. Z tohoto důvodu není nutné v mnoha případech fyzicky řešit potřebné záležitosti přímo na úřadě. Co však považuji za nutné je a je také argumentem odpůrců datových schránek je, aby byla se navýšena velikost přílohy datové zprávy. Dalším bodem, který stojí za zmínku je dbát více na informovanost občanů ohledně datových schránek.

Úřady a jiné další instituce jsou zvyklé zasílat dokumenty listinnou formou, tudíž nevyužívají možnost odesílat dokumenty do datové schránky subjektů, které si ji zřídily.

Praktická je část tvořena grafy z vyplněných dotazníků na téma datové schránky, který byl zaměřen konkrétně na veřejné archivy. Dotazník byl mnou vytvořen a rozeslán pomocí e-mailové komunikace všem veřejným archivům. Co musím však zmínit je, že tyto oslovené archivy byly velmi vstřícné k vyplňování dotazníku. Z výsledků dotazníků byly zjištěny informace o tom, jak často jsou používány datové schránky, kým v instituci jsou používány, jak jsou spokojeni či nespokojeni s datovou schránkou. V jakém formátu jsou ukládány datové zprávy, a jakým způsobem jsou tyto zprávy ukládány. Z výsledků vyplynulo mnoho informací, které mohou doplnit chybějící znalosti v oblasti používání datových schránek veřejnými archivy.

Mezi zajímavé informace, které byly vyhodnoceny z dotazníků jsou, že vysoké procento veřejných archivů ukládá datové zprávy pomocí elektronického systému spisové služby. Další informací je, že nejčastěji jsou datové zprávy ukládány ve formátu pdf, veřejné archivy mají své vlastní uložení a méně jich využívá možnost placeného uložení. Většina veřejných archivů je podle výsledků mého výzkumu s datovými schránkami celkově spokojena. V oblasti odesílání datových zpráv jsou často využívány právníckými osobami, a také větší část archivů uvedla, že fyzické osoby odesílají též do archivů datové zprávy. Z výsledků bylo také zjištěno, že v instituci ve většině případů používá datovou schránku 3 a více zaměstnanců a sdílí jedno heslo. Dokumenty jsou z velké části případů podepsány elektronickým podpisem a jsou opatřeny elektronickým razítkem. Objem přijatých zpráv se pohybuje okolo 1-5 zpráv týdně. Je patrné, že jsou týdně datové schránky zaměstnanci používány často. A nejčastěji s datovou schránkou v instituci pracuje pracovník podatelny.

9. Seznam zdrojů

Literatura

KUNT, Miroslav a Tomáš LECHNER, *Spisová služba*, Praha: Leges, 2015, ISBN 978-80-7502-083-3

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

CEVRO Institut, *Datové schránky, historický vývoj a současná podoba*, Praha, 1.vydání, ISBN 9788087125298

KŘÍŽ, Josef, *Řízení administrativních a správních procesů*, 1. vyd., 2014, Česká zemědělská univerzita v Praze, ISBN 978-80-213-2315-5

DRÁBKOVÁ, Tereza, *Doručování ve správním řízení se zaměřením na elektronické formy komunikace*, Praha, Wolters Kluwer ČR, 2017, ISBN 978-80-7552-723-3

MARCHAL Stanislav A., PROKEŠ Josef, ŠTĚDRŇ Bohumír, VANÍČEK Zdeněk, *Právní aspekty eGovernmentu v České republice*, Linde Praha, ISBN: 978-80-7201-855-0, 2011

PETERKA Jiří, *Báječný svět elektronického podpisu*, CZ.NIC, 2011, ISBN 978-80-904248-3-8

VAVROCHOVÁ Simona, ČEJP Vlastimil, ŠTĚPÁNKOVÁ Monika, SAMKOVÁ Bohuslava, PŘICHYSTAL Aleš, *Vzdělávání v eGovernmentu*, Vysoká škola manažerské informatiky, 2014, ISBN 978-80-86847-74-0

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

Internetové zdroje

<https://www.mua.cas.cz/sites/default/publicFiles/SOUBORY/2017/11/13/09-55-12/vzorovy-spisovy-rad>

<https://www.mvcr.cz/clanek/co-je-egovernment.aspx>

<https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089>

<https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu.aspx>

<https://www.mvcr.cz/clanek/co-je-egovernment.aspx>

<https://www.mvcr.cz/clanek/ministerstvo-vnitra-predstavilo-klaudii-novy-symbol-egovernmentu.aspx>

<https://www.czechpoint.cz/public/novinky/>

<http://www.czechpoint.cz/public/urednik/sluzby-pro-uredniky/>

<https://www.czechpoint.cz/public/czechpoint-office>

<https://www.czechpoint.cz/public/verejnost/sluzby>

<https://www.czechpoint.cz/public/statistiky-a-informace/aktualni-dostupnost-sluzeb/>

<https://www.czso.cz/csu/czso/rozvoj-informacni-spolecnosti-v-ceske-republice-a-zemich-eu>

https://www.czso.cz/documents/10180/94876554/06202618.pdf/b7166a40-93fa-41a4-bb4c-ee06722d51e8?redirect=https%3A%2F%2Fwww.czso.cz%2Fcsu%2Fczso%2Fvolnamista%3Fp_p_id%3D3%26p_p_lifecycle%3D0%26p_p_state%3Dmaximized%26p_p_mode%3Dview%26_3_groupId%3D0%26_3_keywords%3D062026-18%26_3_struts_action%3D%252Fsearch%252Fsearch%26_3_redirect%3D%252Fweb%252Fczso%252Fkatalog-produktu-vydavame

<https://www.czso.cz/csu/czso/-datove-schranky-si-zrizuji-i-nepodnikajici-osoby>

<https://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx>

<https://www.eidentita.cz/Home>

<https://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx>

Právní předpisy

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

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

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

Zákon č.365/2019 Sb., o informačních systémech veřejné správy

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

Interní předpisy

Vzorový spisový a skartační řád pracovišť AV ČR