

Univerzita Karlova
Katedra pomocných věd historických
Obor veřejná správa a spisová služba



Bakalářská práce

Diana Gembická

Ukládání digitálních dokumentů
The storing of digital documents

Prohlašuji, že jsem diplomovou práci na téma „*Ukládání digitálních dokumentů*“ zpracovala samostatně. Veškeré použité prameny, byly citovány pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury.

Dne 26. 7. 2022

Poděkování

Na tomto místě bych ráda poděkovala PhDr. Daniele Brádlarové, Ph.D., za odborné vedení této práce a za cenné rady a připomínky, které pomohly k jejímu vypracování.

Abstrakt

Tato bakalářská práce má za cíl obeznámit čtenáře s procesem ukládání digitálních dokumentů v rámci výkonu spisové služby. V úvodu práce se budu zabývat základními pojmy ve spisové službě a životním cyklem digitálního dokumentu, kde přiblížím také legislativu, která tento proces upravuje. Dále představím elektronické systémy spisové správy pro vedení digitálních dokumentů. Také zde přiblížím i proces autorizované konverze a fungování datových schránek. Zde navážu i na to jak významnou roli mají digitální dokumenty a jejich ukládání ve fungování e-Governmentu. Na závěr budu zkoumat vedení spisové služby a ukládání digitálních dokumentů na obecním úřadu.

Hlavní metodou práce bude analýza.

Klíčová slova: spisová služba, dokument, datové formáty, datová schránka, spisový řád, autorizovaná konverze, e-Government, elektronické systémy spisové služby

Abstract

The aim of this bachelor's thesis is to acquaint the readers with the process of storing digital documents as part of the records management. In the beginning of the work, I will deal with the basic terms in the records management and the life cycle of a digital document, where I will also explain the legislation that regulates this proces. I will also present electronic records management systems for managing digital documents. I will also explain here the proces of authorized conversion and the functioning of data boxes. Here I will follow up on the important role of digital documents and their storage in the functioning of e-Goverment. In the end, I will examine the records management and the storage of digital documents at the municipal office.

The main method will be the analysis.

Key words: records management, document, data formats, data box, file plan, authorised conversion, e-Government, electronic records management systems

Obsah

Úvod	1
1. Základní pojmy a právní předpisy.....	2
1.2 Přehled právních předpisů	7
1.3.1 Právní předpisy vydané Českou republikou	7
1.3.2 Právní předpisy vydané Evropskou unií.....	9
2. Spisová služba.....	10
1.1.1 Vývoj spisové služby v historii	10
1.1.2 Vymezení spisové služby	10
2.1.3 Výkon spisové služby	11
1.1.3 Životní cyklus dokumentu	11
3. Důvěryhodnost digitálních dokumentů.....	15
3.1 Elektronický podpis	15
3.2 Elektronická pečeť.....	16
3.3 Časové razítko.....	18
3.4 Kvalifikovaný poskytovatel služeb vytvářejících důvěru	18
3.5. Ověřitelnost digitálních dokumentů.....	19
3.6. Datové schránky	20
3.6. Konverze dokumentů	23
4. Ukládání digitálních dokumentů	25
4.1 Ukládání dokumentů obecně	25
4.1.2 Ukládání analogových dokumentů.....	26
4.1.3 Ukládání digitálních dokumentů	26
4.1.4 Krátkodobé ukládání digitálních dokumentů	27
4.1.5 Střednědobé ukládání digitálních dokumentů	27
4.1.6 Dlouhodobé ukládání digitálních dokumentů	27
4.1.7 Datové formáty.....	27
4.2. Národní archiv	28
5. Ukládání digitálních dokumentů v Úřadu MČ Praha 15	31
Shrnutí	36
Závěr	37

Úvod

Vznik moderních technologií přinesl mnohé změny do každodenního běhu našich životů. Ať už jde o náš domov, práci nebo dokonce i prostředí škol, moderní technologie v současnosti můžeme najít všude. Tohoto vlivu neuniknula ani spisová služba a její zacházení s dokumenty.

Před vznikem informačních technologií a jejich rapidním rozvojem se práce s dokumenty výhradně zaměřovala na fyzické předměty, na kterých byly různými mechanickými nebo chemickými způsoby zachyceny informace. V minulosti šlo například o kamenné destičky, pergamen a pak samozřejmě i dnes využívaný papír.

Neustálý technologický rozvoj, se ale významně podílel na skutečnosti, že v dnešní době vznikají dokumenty především v digitální formě, a to v mnohém ovlivnilo i způsob výkonu spisové služby a ukládání tohoto typu dokumentu. Ukládání digitálních dokumentů má pro původce řadu praktických výhod. V první řadě se jedná o mnohem jednodušší a přehlednější způsob ukládání, který navíc šetří místo i čas zaměstnanců. Další výhodou je možnost neomezeného vytváření kopií takového dokumentu ve fyzické podobě (tzv. analogový dokument). Nicméně i digitální dokumenty mají své nevýhody, jako například možnost poškození dokumentu elektromagnetickým impulsem či může být zneužit neoprávněnou osobou (hacker).

Je zřejmé, že s nástupem tvorby tohoto typu dokumentu, jehož využití se neustále rozšiřuje a rozvíjí jak u samosprávných, tak i ve veřejnoprávních institucích, přišla na řadu i otázka jakým způsobem se tyto dokumenty budou ukládat a archivovat. Následně bylo potřeba vyřešit průkaznost jejich původu právní validity a neměnnosti v čase. Tyto věci jsou zcela nezbytné a to zejména z důvodu účelnosti dokumentu. Může se jednat například o digitální dokument, který prokazuje ukončení smluvního vztahu, existenci rozhodnutí veřejné moci. Také se může jednat o případ, kdy má tento dokument historickou hodnotu, a v rámci veřejného zájmu je důležité ho uchovat. Z toho důvodu je důležité se o digitální dokumenty a o způsob jejich ukládání starat se stejnou péčí jako je to u analogových dokumentů.

Tato práce se proto bude zabývat zejména rozbořem ukládání digitálních dokumentů, společně s přihlédnutím k jejich současné legislativní úpravě, v rámci České republiky i Evropské unie. Další důležitou částí je i rozbor souvisejících aspektů, mezi které patří spisová služba, podepisování a označování elektronických dokumentů, proces ukládání dokumentů ve veřejné správě, datové schránky a konverze dokumentů (autorizovaná i neautorizovaná).

Praktická část práce je věnována popisu ukládání digitálních dokumentů v městském úřadu městské části Prahy 15 dále jen ÚMČ Praha 15, s přihlédnutím k jejich příjmu a evidenci. Cílem práce je rozbor ukládání digitálních dokumentů, jejich znaků a identifikace možných zlepšení.

1. Základní pojmy a právní předpisy

V této části mé písemné práce chci přiblížit základní pojmy a právní předpisy, které budu při analýze ukládání digitálních dokumentů používat. U základních pojmů začnu rozborem dokumentu, jelikož bude v mé práci nejčastěji skloňován. Chci čitateli přiblížit co si má pod pojmem „dokument“ představit, jaké atributy by měl splňovat a na jaké typy ho můžeme rozlišovat. Dále se přesunu na další pojmy z oblasti spisové služby (př. Informace, písemnost) a k závěru kapitoly se zaměřím na právní předpisy, jež upravují výkon spisové služby v České republice a ty které vydala Evropská unie.

Dokument není ve spisové službě pouhým pojmem, ale i předmětem jejího zkoumání a jejího výkonu. Proto jsem se rozhodla začít právě ním. Co si ale můžeme představit pod pojmem dokument? Podle ustanovení paragrafu 2 pís. e) zákona č. 499/2004 Sb., *o archivnictví a spisové službě a o změně některých zákonů*, je dokumentem každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena.¹ **Původce** je každý subjekt, z jehož činnosti dokument vznikl. Patří sem i dokumenty, které byly původci doručeny nebo jinak předány.² Existují ale i další normy, na základě kterých bychom mohli dokument definovat. Například normou ISO 15489-1 je dokument definován jako informace vytvořené, získané a spravované organizacemi nebo osobami jako doklady a/nebo vzniklé při plnění jejich právních povinností nebo při jejich činnosti³. Nicméně předpokládám, že pro účely této bakalářské práce je zákonná definice plně dostačující.

Každý dokument se vyznačuje několika atributy:

- *„informační hodnota – dokument je nositelem informace, která má svou hodnotu.*
- *stálost – dokument je neměnný a stálý*
- *jazyk – dokument bývá vyjádřen v určitém jazyce; toto není nezbytný atribut a existují i dokumenty, které se vyjadřují v symbolice bez jazykové příslušnosti*
- *strukturovanost – dokument má vnitřní strukturu, která je závislá na jeho určení, povaze, okolnostech vzniku a dalších parametrech*
- *ucelenost – s dokumentem se nakládá jako s jednotkou, jako s celkem, který může být dělen pouze dočasně v rámci určitých procesů zpracování*
- *funkčních zabarvení – velmi významným atributem je také funkce dokumentů, která je určující pro mnoho specifických vlastností“⁴*

Dokument je dělen na dva typy - **analogový** a **digitální**. Analogový dokument existuje v listinné podobě, což znamená, že jsou na něm informace zachyceny písmem na materiálním podkladu. U digitálního nebo jinak řečeno elektronického dokumentu je jakýkoliv informace uchovávaná v elektronické podobě

Informace je základní jednotkou jakéhokoliv dokumentu. Stručně by se dala vymezit jako určité sdělení nehmotné povahy odrážející nějakou skutečnost (např. jev, děj chování...atd.). Může se jednat o informaci libovolné formy a typu (např. digitální, analogovou, multimediální...atd.). Sémiotika⁵ klade na informaci tři základní požadavky⁶:

¹ §2 pís. e) zákona č. 499/2004 Sb., *o archivnictví a spisové službě a o změně některých zákonů*

² §2 zákona č. 499/2004 Sb., *o archivnictví a spisové službě*

³ KUNT, M., LECHNER, T. *Spisová služba*. Praha: Leges, 2015, s. 74, 75

⁴ KUNT, M., LECHNER, T. *Spisová služba*. Praha: Leges, 2015, s. 76

⁵ Obecné označení vědních teorií, které se zabývají zkoumáním znaků a znakových soustav.

⁶ ŠLAPÁK, O. *Data, informace, znalosti*. E-LOGOS (Electronic journal for philosophy) 2003 [online] roč. 10, cit. 27.5.2022. Dostupné na: <https://e-logos.vse.cz/pdfs/elg/2003/01/11.pdf>

1. syntaktickou relevanci – subjekt, který informaci přijímá, musí být schopen informaci detekovat a rozumět jí
2. sémantickou relevanci – subjekt musí vědět, co informace znamená, tedy co vypovídá o něm a jeho okolí
3. pragmatickou relevanci – informace musí mít pro přijímací subjekt nějaký význam

Jelikož je tato práce z větší části zaměřená na digitální dokumenty, ještě se tomuto pojmu chci věnovat podrobněji. **Digitální dokument** nebo jiným názvem elektronický dokument se od analogového liší celou řadou specifických vlastností.

První rozdílem, který si dal označit za nejpodstatnější je postavení originálu dokumentu. Originál v analogové podobě je spojován s jedinečností dokumentu, která zajišťuje i jeho důvěryhodnost. Analogový dokument je vždy spojen s jeho nosičem (např. papír), a proto je obtížné vytvářet jeho věrné kopie. Digitální dokument není závislý na svém materiálním nosiči, a proto neexistuje jedinečný originál. To ale nevylučuje to, že i digitální dokumenty mohou být důvěryhodné.

Druhým rozdílem je odlišnost ve schopnosti smyslového vnímání mezi analogem a digitálem. Kupříkladu, informaci z listinné podoby dokumentu můžeme přečíst bez toho, abychom si nejdřív zajistili nějaké zprostředkované zařízení (např. počítač) jako v případě digitálního dokumentu.

Další odlišností je způsob vzniku digitálních dokumentů. K vytvoření digitálního dokumentu je potřeba stejně jako k jeho přečtení příslušné technické vybavení. Digitální dokument je možné vytvořit dvěma způsoby:

1. Vznik v elektronické podobě – dokument vzniká použitím textových či tabulkových editorů, nebo využitím jiných softwarových prostředků
2. Digitalizace - analogový dokument je převeden do digitální podoby

Způsob vzniku ovlivňuje i to jakou kvalitu může výsledný digitální dokument mít. Pokud dokument již vzniká jako digitální, je možné jeho kvalitu snadněji ovlivňovat, než u dokumentu, který vzniká digitalizací. Pokud je analogový dokument převeden na digitální pomocí **autorizované konverze** platí ustanovení v §22 zákona č. 300/2008 Sb., které zní: *„úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo v datovém souboru způsobem zajišťujícím shodu obsahu těchto dokumentů a připojení doložky o provedení konverze nebo úplné převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě způsobem zajišťujícím shodu obsahu těchto dokumentů a připojené doložky“*. Z toho vyplývá, že dokument, který vznikl provedením konverze má stejné právní účinky jako dokument, který do konverze vstupoval.⁷

Kvalitu digitálního dokumentu dále ovlivňuje i jeho datový formát. **Datové formáty** jsou důležitým aspektem každého digitálního dokumentu a ovlivňují jeho vytvoření, jeho použití a následné uložení. Jedná se o způsob kódování komponenty, který zajišťuje uložení dokumentu nebo jeho části (částí) pro účely zpracování výpočetní technikou a jeho znázornění. Datovým formátem jsou například formáty pdf, PDF/A, doc, docx, mp3, GIF...atd.⁸

Veškeré informace od vzniku digitálního dokumentu až po jeho vyřízení a uložení jsou obsaženy v tzv. **metadatech**. Popisují přímo souvislosti, obsah a strukturu dokumentu a také

⁷ §22 zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

⁸ §23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

jeho správu v průběhu času. Jedná se tedy například o informaci, kdo dokument vyřizoval nebo zde může být i zobrazen schvalovací proces.⁹

Pro zajištění právní validity digitálních dokumentů slouží nástroje vydávané **kvalifikovaným poskytovatelem služeb vytvářejících důvěru**. Ten poskytuje kvalifikovanou službu na základě písemné smlouvy.¹⁰ **Kvalifikovanou službou** se podle nařízení č. 910/2014 Sb. (dále jen eIDAS) rozumí služba, která poskytuje kvalifikovanou službu vytvářející důvěru, která splňuje požadavky v tomto nařízení. Mezi uvedené nástroje patří elektronický podpis, elektronická pečeť a elektronické časové razítko.

Elektronický podpis definuje článek č. 3 v odstavci 10 v Nařízení Evropského parlamentu a Rady Evropské unie č. 910/2014 „o elektronické identifikaci a službách vytvářející důvěru pro elektronické transakce“ jako data v elektronické podobě, která jsou připojena k datům jiným v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující se osoba používá k podepsání.

Rozlišujeme tři druhy elektronického podpisu:

1. Prostý

Jedná se o nejčastěji používanou formu elektronického podpisu. Není možné na jeho základě zaručit totožnost podepisující se osoby a nedodává právní validitu dokumentu.

2. Zaručený elektronický podpis

Musí splňovat následující požadavky, které stanovil článek č. 26 Nařízení č. 910/2014 (eIDAS):

- a) je jednoznačně spojen s podepisující se osobou
- b) umožňuje identifikaci podepisující se osoby
- c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou
- d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat

3. Kvalifikovaný elektronický podpis

Kvalifikovaný elektronický podpis je podle nařízení č. 910/2014 Sb. (eIDAS) zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

Dalším nástrojem pro zaručení právní validity digitálních dokumentů je **elektronická pečeť**, jež je tvořena daty v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ nebo integritu.¹¹ Zde vidíme, že pečeť se přímo váže k instituci, ve které byl dokument vytvořen, kdežto podpis se vztahuje přímo k podepisující se osobě.

Třetím nástrojem je **elektronické časové razítko**. Je také tvořeno daty v elektronické podobě, která spojují jiná data v elektronické podobě s určitým časovým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku.¹² Časové razítko se tedy vztahuje k okamžiku vzniku dokumentu.

⁹ Národní standard pro elektronické systémy spisové služby. In: Věstník MV ČR, částka 57/2017 (část II), s. 6

¹⁰ §2 zákona č. 297/2016 Sb., o službách vytvářejících důvěru

¹¹ Čl. 3 nařízení č. 910/2014 Sb. (eIDAS)

¹² Tamtéž.

Tyto nástroje jsou založeny na **kvalifikovaném certifikátu**, jež je v zákonu č. 297/2016 Sb. *o službách vytvářejících důvěru pro elektronické transakce* definován jako certifikát, který vydal kvalifikovaný poskytovatel služeb vytvářejících důvěru.¹³

Jednou možností validního doručení a odesílání digitálního dokumentu je **datová schránka**. Upravuje jí zákon č. 300/2008 Sb., *o elektronických úkonech a autorizované konverzi dokumentů*, který jí definuje jako elektronické uložení, které je určeno k doručování orgány veřejné moci, k provádění úkonů vůči orgánům veřejné moci a k dodávání dokumentů fyzických osob a právnických osob. Datové schránky zřizuje a spravuje Ministerstvo vnitra.

Doručenému nebo nově vzniklému digitálnímu dokumentu je původcem přidělen **jednoznačný identifikátor dokumentu (JID)**. JID je neoddělitelně spojený s dokumentem v systému eSSL. Obsahuje označení veřejnoprávního původce a alfanumerický kód.

K zajištění odborné správy digitálních dokumentů vzniklých z činnosti původce nebo jeho právních předchůdců slouží **spisová služba**. Tu tvoří soubor činností, mezi které patří příjem, evidence, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování dokumentů ve skartačním řízení¹⁴. Všichni veřejnoprávní původci musí vést spisovou službu v **elektronickém systému spisové služby (eSSL)**. Jedná se o informační systém pro správu dokumentů při výkonu elektronické spisové služby. Systém eSSL musí splňovat požadavky stanovené v národním standardu.¹⁵

Dokumenty jsou zařazeny do **spisu**. Ten by se dal nejstručněji popsat jako spojení dokumentů zabývající se stejnou věcí. Paragraf 17 správního řádu č. 500/2004 Sb. přímo stanovuje: „*v každé věci se zakládá spis. Každý spis musí být označen spisovou značkou. Spis tvoří zejména podání, protokoly, záznamy, písemná vyhotovení rozhodnutí a další písemnosti, které se vztahují k dané věci. Přílohou, která je součástí spisu, jsou zejména důkazní prostředky, obrazové a zvukové záznamy a záznamy na elektronických médiích. Spis musí obsahovat soupis všech svých součástí, včetně příloh, s určením data, kdy byly do vpsu vloženy*“¹⁶. Další definice je k nalezení v archivním zákoně č. 499/2004 Sb. v paragrafu 65: „*Při vyřizování dokumentů se všechny dokumenty týkající se téže věci spojí ve spis. Dokumenty v analogové podobě se vzájemně spojí fyzicky, dokumenty v digitální podobě se vzájemně spojí prostřednictvím metadat, vzájemné spojení dokumentu v analogové podobě a dokumentu v digitální podobě se činí pomocí odkazů*“¹⁷. Je tedy možné, aby spis měl materiální podobu (př. šanon, krabice) a i tak obsahoval dokumenty v digitální podobě nosiči. Vyřízením spisu s rozumí zpracování návrhu, jeho schválení, vyhotovení, podepsání a vypravení rozhodnutí nebo jiné formy vyřízení.¹⁸ Spisy jsou ukládány ve **spisovně**. Jedná se o místo pro uložení, vyhledávání a předkládání dokumentů pro potřebu původce a k provádění skartačního řízení. Spisovna vede evidenci o zapůjčování a nahlížení do dokumentů a spisů. V evidenci je spis veden pod **spisovou značkou**, což je evidenčním znak spisu. Podle vyhlášky č. 259/2012 Sb., *o výkonu spisové služby* může být spisovou značkou číslo jedací prvního (nebo institucí jiného určeného) dokumentu vloženého do spisu nebo sběrného archu.

Výkon spisové služby a skartačního řízení musí odpovídat vnitřním předpisům původce neboli **spisovému a skartačnímu řádu**. Upravují veškeré činnosti spisové služby u původce:

¹³ §15 zákona č. 297/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce*

¹⁴ §2 zákona č. 499/2004 Sb., *o archivnictví a spisové službě*

¹⁵ §63 zákona č. 499/2004 Sb., *o archivnictví a spisové službě*

¹⁶ §17 odst. 1 zákona č. 500/2004 Sb., správní řád

¹⁷ §65 odst. 1 zákona č. 499/2004 Sb., zákon o archivnictví a spisové službě

¹⁸ Tamtéž odst. 2

příjem, třídění, označování, evidence, rozdělování, vyřizování, oběh, vyhotovování, podepisování, odesílání, ukládání a vyřazování dokumentů v instituci.¹⁹

Spisový a skartační plán jsou součástí spisového řádu. Obsahují seznam typů dokumentů roztríděných do věcných skupin s vyznačenými spisovými znaky, skartačními znaky a skartačními lhůtami. Určení původci zasílají svůj spisový a skartační plán příslušnému správnímu archivu hned po jeho vydání nebo změně.

Skartační řízení je proces při, kterém se buď předají dokumenty archivu, pokud jím byly vybrány nebo budou řádným způsobem skartovány. Skartační řízení dokumentů se provádí až po uplynutí **skartační lhůty** dokumentů. Představuje určitou dobu, po kterou musí zůstat dokument uchován u původce. Začíná se počítat vždy od 1. ledna následujícího roku, kdy byl spis uzavřen nebo dokument vyřízen. Skartační řízení iniciuje původce podáním žádosti a **skartačního návrhu**, což je seznam dokumenty s uplynulou skartační lhůtou.

Po uplynutí skartační lhůty se dokument dostává do skartačního řízení. O tom jak s ním bude naloženo, rozhoduje jeho **skartační znak**. Skartační znak rozlišujeme na tři typy skartačního znaku:

- Skartační znak A (archiv) – po uplynutí skartační lhůty bude dokument přemístěn do příslušného správního archivu
- Skartační znak V (výběr) – o uplynutí skartační doby, bude dokument posuzován pracovníkem archivu, zda bude přemístěn do trvalé úschovy ve správním archivu nebo skartován
- Skartační znak S (skart) – po uplynutí skartační doby, bude dokument řádným způsobem skartován²⁰

¹⁹ §20 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

²⁰ Tamtéž §21

1.2 Přehled právních předpisů

Táto kapitola se bude zabývat přehledem a krátkým popisem platných právních předpisů, které upravují výkon spisové služby a ukládání digitálních dokumentů v České republice. Nejedná se pouze o právní předpisy vydané Českou republikou, ale i o právní předpisy vydané Evropskou unií.

1.3.1 Právní předpisy vydané Českou republikou

Začnu s právními předpisy, které se přímo týkají vzniku, doručování, evidence a následného ukládání ve veřejnoprávních původcích. Dále upravují i další činnosti v rámci spisové služby: autorizovanou konverzi, podepisování, pečetění a opatřováním časového razítka. Jedná se tedy o právní předpisy, které se zabývají technickou stránkou výkonu spisové služby a ukládáním digitálních dokumentů.

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů je nejspíš nejdůležitějším právním předpisem pro výkon spisové služby v České republice. Zabývá se ukládáním dokumentů jak v listinné, tak i v digitální podobě. Ukládáním digitálních dokumentů se přímo zabývá v §69a odst. 1 až 4 ve formě zvláštních ustanovení. Je zde popsán převod listinného dokumentu do digitální podoby a naopak a změna digitálního formátu dokumentu v digitální podobě. Dále se se tento paragraf zabývá ověřování původce před jeho převedením z digitální podoby a naopak, nebo také opatřením při vzniku dokumentu jeho převedením, kdy je původce povinen ho opatřit doložkou. Tento zákon také hodně ovlivňuje vytváření vnitřních směrnic veřejnoprávních původců, konkrétně spisového a skartačního řádu.

Zákon během své existence prošel četnými novelizacemi. Jeho sedmá novelizace patří mezi nejvýraznější. Zákonem č. 190/2009 Sb. se změnila jak definice některých pojmů včetně „dokumentu“ tak i „výkonu spisové služby“. Významně upravil seznam subjektů, jež mají povinnost vykonávat spisovou službu a také změnil výčet subjektů majících povinnost uchovávat dokumenty a umožnit výběr archiválií. Dále zavedl pojem „spisovna“.

Nicméně to proč se táto novelizace stala tak významnou je něco jiného. Tato novelizace zavedla v §63 ustanovení, ve kterém se stanovuje, že veřejnoprávní původci mají přednostně vykonávat elektronickou spisovou službu v elektronických systémech spisové služby. Dále v §64 nařídil veřejnoprávním původcům, kterým byla udělena povinnost vést spisovou službu elektronicky, aby zavedly evidenci dokumentů v elektronickém systému spisové služby.²¹

Národní standard pro elektronické systémy spisové služby vydalo Ministerstvo vnitra na základě §70 odst. 2 zákona č. 499/2009 Sb. První verze byla zveřejněna v roce 2009. Současná verze byla zveřejněna pod č. j. MV-33371-16/AS-2017. Její účinnost začal platit od 4. 7. 2017. Národní standard definuje pojmy vyskytující se ve spisové službě a její používané postupy při evidenci a ukládání digitálních dokumentů. Dříve zmíněný §70 zákona č. 499/2009 Sb. přímo stanovuje, co má Národní standard upravovat: „*Národní standard, který ministerstvo zveřejní ve Věstníku ministerstva a způsobem umožňující dálkový přístup, stanoví požadavky na elektronické systémy spisové služby, a to a) příjem dokumentů, b) označování a evidenci dokumentů, c) vyhledávání, odesílání a zobrazování dokumentů, d) ukládání dokumentů, e) vyřazování dokumentů a výběr archiválií, f) dokumentace životního cyklu elektronického*

²¹ Zákon č. 499/2004 Sb., o archivnictví a spisové službě

systému spisové služby, g) spisový a skartační plán, h) transakční protokol, i) správcovské funkce, j) metadata. “²²

Zavedení Národního standardu bylo pro správné fungování spisové služby ve veřejnoprávních původcích stěžejné, jelikož pomohla nastavit předobraz a pravidla, jak by tato služba měla být v elektronických systémech vykonávána.

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů upravuje a stanovuje podrobnosti výkonu spisové služby. Ukládání dokumentů upravuje §19, který stanovuje, že veřejnoprávní původci ukládají uzavřené spisy a vyřízené dokumenty podle věcných skupin a spisových znaků dle spisového řádu. Spisový řád dále stanoví postup původce při ukládání digitálních dokumentů.

Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů upravuje elektronické úkony orgánů veřejné moci nebo fyzických a právnických osob, jimž byla svěřena působnost ve veřejné správě. Dále upravuje systém datových schránek a autorizovanou konverzi.

Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů upravuje technické náležitosti provádění autorizované konverze dokumentů a technické náležitosti dokumentu, který vznikl autorizovanou konverzí nebo který bude konvertován.

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění pozdějších předpisů upravuje ukládání zpráv v datové schránce. Stanovuje, že doba uložení datové zprávy v datové schránce činí 90 dnů. Dále upravuje maximální velikost datové zprávy dodávané do datové schránky, přípustné formáty nebo technické a bezpečnostní zásady pro přístup do datové schránky. Pokud datová zpráva nesplňuje podmínky stanovené touto vyhláškou, má správce datové schránky pravomoc jí nepřijmout.

Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů obsahuje úpravu pro postupy poskytovatelů vytvářejících důvěru a stanovuje rozsah působnosti Ministerstva vnitra v oblasti služeb vytvářejících důvěru. Dále upravuje podmínky řádného podepisování, pečetění digitálního dokumentu a používání časového razítka.

Zavedením tohoto zákona bylo zrušena řada zákonů a vyhlášek. Patří sem zákon 227/2000 Sb., *o elektronickém podpisu a o změně některých dalších zákonů*, vyhláška č. 212/2012 Sb., *o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a o postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka* a Vyhlášku č. 378/2006 Sb., *o postupech kvalifikovaných poskytovatelů certifikačních služeb*.

Zákon č. 500/2004 Sb., správní řád, upravuje postupy orgánů moci výkonné. Tento zákon nespadá do technické části spisové služby, ale upravuje použití a vyřizování digitálního

²² §70 odst. 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě.

dokumentu v rámci výkonu orgánu moci výkonné. Také zde můžeme najít ustanovení pro podání dokumentů, tvorbu spisů a lhůty pro vyřízení.

1.3.2 Právní předpisy vydané Evropskou unií

Spisovou službu a správu a ukládání digitálních dokumentů upravují i právní předpisy vydaných Evropskou unií, které ovlivnili i tvorbu zákonů a vyhlášek vydaných v ČR.

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 zrušení směrnice 1999/93/ES dále známé pod zkratkou eIDAS. Cílem vydání tohoto nařízení bylo vytvoření soudržného rámce, který by v souvislosti se službami vytvářejících důvěru zabezpečil vysokou úroveň bezpečnosti a právní jistotu. Dále stanovuje požadavky pro poskytovatele služeb vytvářejících důvěru. Nařízení eIDAS dále definuje řadu pojmů, které byly již zmíněny v předchozí části: elektronický podpis, zaručený elektronický podpis, kvalifikovaný elektronický podpis, služby vytvářející důvěru či podepisující se osobu. Lze tedy říct, že eIDAS poskytuje jednotný právní základ pro digitální trh v Evropské unii.

Nařízení Evropského parlamentu a Rady (EU) 2016/79 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) nabylo účinnosti 1. 5. 2018. Zcela změnilo úroveň ochrany osobních údajů fyzických osob a jejich následné zpracování. Osobními údaji se v rámci GDPR rozumí „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen subjekt údajů)*“²³. Vliv nařízení GDPR na spisovou službu můžeme najít v čl. 4 odst. 2, který definuje pojem zpracování jako „*jakoukoliv operaci nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*“²⁴. V dalším článku 5 odst. 1 písm. b) je stanoveno že „*osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovány způsobem, který je s těmito účely neslučitelný, osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně za účelem archivace*“²⁵.

²³ Nařízení Evropského parlamentu a Rady (EU) 2016/679, čl. 4 odst. 1

²⁴ Tamtéž čl. 4 odst. 2

²⁵ Tamtéž čl. 5 odst. 1 písm. b)

2. Spisová služba

Spisová služba slouží k udržení pořádku ve správě dokumentů. V současné době, kdy každá instituce tvoří nespočetné množství jak analogových, tak i digitálních dokumentů, je stále víc znát důležitost správně vedené spisové služby. Pokud tato služba není vykonávána řádně, může to ovlivnit běh celé instituce. Může docházet k tzv. „papírování“ – začnou se tvořit zbytečné kopie, zavádí se dotazníky a formuláře k věci, která byla již několikrát zjišťována. To všechno způsobuje nedostatek relevantních informací, jejichž absence zpomaluje proces řízení a vydávání rozhodnutí. V opačném případě se samozřejmě tento proces pomocí efektivní spisové služby může ještě urychlit. Pro správně fungující spisovou službu je potřeba nejdřív splnit určité podmínky. Samozřejmě je potřeba splnit technickou stránku, ale také nastavit seznam pravidel, kterými se instituce bude řídit při užívání těchto dokumentů a jejich následném uložení, neboli je potřeba vytvořit efektivní Spisový řád, kterým se pracovníci instituce mohou řídit.

Uchování ve správě dokumentů určitý řád není pro lidstvo nic nového, neboť *lidská civilizace je založena na sdělování a zpracování informací, jejichž vyjádřením jsou dokumenty.*“ Již dříve zmíněné „papírování“ sužuje lidstvo přibližně od 16. století a dnes se rozšířilo i na dokumenty v digitální podobě. Spisová služba se tímto problémem zabývá a snaží se mu předejít. Lze jí považovat za základ informačního systému jakékoliv organizace. Norma ISO 15489-1:2016 ji definuje jako „*oblast managementu odpovědná za účinné a systematické řízení tvorby, přijímání, vedení, používání a vyřazování dokumentů, včetně procesů získávání a vedení důkazů o pracovních činnostech a transakcích ve formě dokumentů.*“²⁶ Ustanovení §2 písm. i) zákona č. 499/2004 Sb. spisovou službu definuje jako „*zajištění odborné správy dokumentů vzniklých z činnosti původce, popřípadě z činnosti jeho právních předchůdců, zahrnující jejich řádný příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, a to včetně kontroly těchto činností.*“²⁷

1.1.1 Vývoj spisové služby v historii

Počátky spisové služby na našem území můžeme sledovat již od počátku 16. století, v úzké souvislosti s existencí spisu (dále označovaném jako akta) a se vznikem prvních instrukcí pro úřadování. Nejstarší podoba těchto instrukcí jsou dochovány z prostředí dvorských úřadů. V 18. století došlo k rozsáhlému zavádění skutečné spisové služby do celého aparátu státu, církve a panství. To pomohlo formovat principy, které známe a aktivně používáme i dnes. Marie Terezie za své vlády vydala např. nařízení z 3. 12. 1746, které stanovilo povinnost vedení podacích protokolů pro doručené dokumenty. Její syn Josef II. vydal 22. prosince 1781 rozhodnutí, které zavedlo systém spisové evidence na základě čísla jednacím a podacím protokolu, který sloužil i ke kontrole vyřízení podání. Spisová služba se samozřejmě vyvíjela dál až do současného stavu. Nicméně dalo by se konstatovat, že některé prověřené postupy z 18. a 19. století jsou pořád aplikovatelné i v dnešní době. Principy při tvorbě spisových řádů z 50. let 20. století jsou využívány i dnes a inspirovali i úpravu platných právních předpisů²⁸.

1.1.2 Vymezení spisové služby

Zákon o archivnictví a spisové službě č. 499/2004 Sb., vymezuje spisovou službu v Hlavě III. V §63 odst. 1 stanovuje seznam původců, kteří mají povinnost vést spisovou službu:

²⁶ KUNT, M., LECHNER, T. *Spisová služba*. Praha: Leges, 2015, s. 15

²⁷ §2 písm. i) zákona č. 499/2004 Sb., *o archivnictví a spisové službě*

²⁸ KUNT, M., LECHNER, T. *Spisová služba*. Praha: Leges, 2015, s. 15-20

„spisovou službu vykonávají a) veřejnoprávní původci uvedení v §3 odst. 1 písm. a) až e) a k) až m), s výjimkou poskytovatelů zdravotních služeb, jde-li o vedení zdravotnické dokumentace, b) kraje, c) hlavní město Praha, d) obce s pověřeným obecním úřadem a obce se stavebním nebo matričním úřadem, e) městská část nebo městský obvod územně členěného statutárního města a městská část hlavního města Prahy, na něž byla statutem přenesena alespoň část působnosti obce s pověřeným obecním úřadem nebo působnosti obce se stavebním úřadem nebo matričním úřadem.“²⁹ Odst. 2 dále stanovuje, že veřejnoprávní původci vedou spisovou službu v elektronické podobě, pokud zvláštní okolnosti nevyžadují, aby spisová služba byla vedena v listinné podobě.

Dále je v §64 upraven příjem, označování, evidenci a rozdělování dokumentů. Vyřizování a podepisování v §65 a odesílání a ukládání dokumentů upravuje §67. Dále §66 obsahuje ustanovení o sestavování a přijímání spisového řádu a §69a upravuje digitální dokumenty.³⁰

Další důležité vymezení se nachází již v dříve zmíněném §70 odst. 2 o vydání Národního standardu, která podrobněji definuje technické požadavky pro elektronické systémy spisové služby.

Ke spisové službě se samozřejmě vážou i jiné právní předpisy např. zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi nebo vyhláška č. 259/2012, o podrobnostech výkonu spisové služby. Dle mého názoru je pro primární vymezení spisové služby zákon č. 499/2004 Sb., o archivnictví dostačující.

2.1.3 Výkon spisové služby

Výkon spisové služby můžeme rozdělit do jednotlivých fází: příjem dokumentů, evidence dokumentů, rozdělování dokumentů, oběh dokumentů, jejich následné vyřizování a tvorba spisů, vyhotovování dokumentů, podepisování a odesílání dokumentů. Závěrečnou fází tvoří ukládání dokumentů a spisů a výběr archiválií. Nedílnou součástí výkonu spisové služby je i jeho dohled a kontrola³¹.

Výkon spisové služby upravuje spisový řád. Jedná se o vnitřní předpis původce, kterým se musí řídit všichni zaměstnanci při vykonávání jejich pracovní činnosti. Musí se být vytvořen v souladu s právními předpisy a musí odpovídat skutečnému stavu původce. Jeho součástí musí být i spisový a skartační plán. Na základě spisového plánu seskupuje původce příbuzné dokumenty do skupiny a označuje je spisovým znakem. Pokud spisový plán obsahuje skartační režimy, jedná se o spisový a skartační plán.³²

1.1.3 Životní cyklus dokumentu

V této části bych chtěla přiblížit, jak spisová služba nakládá s dokumentem v praxi, neboli popsat životní cyklus dokumentu u původce.

Životní cyklus dokumentu začíná jeho **příjmem**. Ten se u veřejnoprávního původce většinou odehrává v podatelně. Nicméně veřejnoprávní původce nemůže odmítnout dokument, který byl doručen i mimo ji. Dokument může být doručen v analogové podobě (poštou, kurýrem, osobně) nebo v digitální podobě přes systém datových schránek, emailem nebo na přenosných nosičích dat. Původce zaeviduje datum doručení, jeho druh a přidělené číslo jednací. Dokument v analogové podobě musí být označen podacím razítkem (popřípadě je označena jeho obálka). V případě že se jedná o dokument v digitální formě, namísto podacího razítka bude pro označení použit jednoznačným identifikátor.

²⁹ §63 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě

³⁰ Tamtéž.

³¹ KUNT, M., LECHNER, T. *Spisová služba*. Praha: Leges, 2015, s. 89-236

³² Tamtéž s. 133-134.

Pokud byl digitální dokument podán přes systém datových schránek, má veřejnoprávní původce povinnost provést kontrolu zda je „*doručený dokument v digitální podobě včetně datové zprávy, v níž je obsažen, úplný, lze jej zobrazit uživatelsky vnímatelným způsobem, neobsahuje škodlivý kód, je v datovém formátu, ve kterém veřejnoprávní původci přijímají dokumenty v digitální podobě, a je uložen na přenosném technickém nosiči dat, na kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, je-li k doručení dokumentu užito přenosného technického nosiče dat.*“³³

Dále veřejnoprávní původce ověří „*platnost a) uznávaného elektronického podpisu a kvalifikovaného certifikátu pro elektronický podpis, na kterém je uznávaný elektronický podpis založen, b) uznávané elektronické pečeti a kvalifikovaného certifikátu, na kterém je uznávaná elektronická pečeť založena, c) uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, a d) kvalifikovaného časového razítka.*“³⁴ Pokud je veřejnoprávní původce schopen zjistit adresu elektronické pošty odesílatele, přes kterou byl digitální dokument doručen, odešle na tuto adresu potvrzení o doručení jeho zprávy³⁵.

Pokud je při ověřování doručeného analogového dokumentu zjištěno, že dokument nesplňuje podmínky stanovené veřejnoprávním původcem, pro jeho podání postupuje veřejnoprávní původce podle §4 odst. 2 vyhlášky 259/2012 Sb., který stanovuje že „*pokud veřejnoprávní původce zjistí, že doručení dokumentu v analogové podobě je neúplný nebo nečitelný, a je schopen určit odesílatele tohoto dokumentu a kontaktní údaje odesílatele, vyzoomí odesílatele o zjištěné vadě dokumentu a stanoví další postup pro její odstranění. Nepodaří-li se veřejnoprávnímu původci vadu doručeného dokumentu ve spolupráci s jeho odesílatelem odstranit, veřejnoprávní původce dokument dále nezpracovává. Není-li veřejnoprávní původce schopen určit odesílatele doručeného dokumentu, který je neúplný nebo nečitelný, a kontaktní údaje odesílatele, dokument dále nezpracovává.*“³⁶

Veřejnoprávní původce postupuje stejně i u nevyhovujícího došlého digitálního dokumentu „*pokud zjistí, že doručení dokumentu v digitální podobě včetně datové zprávy, v níž je obsažen, je neúplný, nelze jej zobrazit uživatelsky vnímatelným způsobem, obsahuje škodlivý kód, není v datovém formátu, ve kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, nebo není uložen na přenosném technickém nosiči dat, na kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, je-li k doručení dokumentu užito přenosného technického nosiče dat.*“³⁷ Pokud digitální dokument nesplňuje požadavky veřejnoprávního původce pro jeho podání a také se nepodaří ve spolupráci s jeho odesílatelem vadu odstranit, postupuje původce jako u analogového dokumentu a digitální dokument dále nezpracovává. Domnívám se že v případě kdy by ověření digitálního dokumentu nebylo vykonáno řádně a digitální dokument se dostal do oběhu instituce, vedlo by to nejen k problematickému vedení správního řízení, ale ovlivnilo by to i vydání rozhodnutí.

Dokument musí být zaevidován. Na základě §8 odst. 1 vyhlášky č. 259/2012 Sb. je ustanoveno že „*veřejnoprávní původce eviduje dokumenty v základní evidenční pomůcce. Základní evidenční pomůckou spisové služby vykonávané v elektronické podobě spisové službě je elektronický systém spisové služby. Základní evidenční pomůckou spisové služby vykonávané v listinné podobě je podací deník: podací deník je kniha vytvořená ze svázaných a očíslovaných*

³³ §2 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

³⁴ Tamtéž §4 odst. 1

³⁵ Tamtéž §4 odst. 2

³⁶ Tamtéž §4 odst. 2

³⁷ Tamtéž §4 odst. 3

listů tiskopisů, označená názvem veřejnoprávního původce, pro něhož je vedena, časovým obdobím v němž je užívána, a počtem všech listů.“³⁸

Neodkladně po evidenci dokumentu je ve fázi rozdělování přidělen osobě, jež bude mít na starosti jeho vyřízení. Kupříkladu se může jednat o pracovníka příslušného odboru městského úřadu, kterého se daná věc týká. Tato osoba následně daný dokument řádným způsobem vyřídí a to buď dokumentem, postoupením, vzetím na vědomí nebo jinými způsoby, které stanoví spisový řád daného původce.³⁹

Součástí činnosti veřejnoprávního původce i **vyhotovování dokumentů**. Mezi ně patří například různá sdělení, rozhodnutí, žádost nebo předvolání. I tyto dokumenty musí projít evidencí. Dále tyto dokumenty musí obsahovat název veřejnoprávního původce, číslo jednací či jméno, příjmení a funkci podepsané osoby. Životní cyklus těchto dokumentů nezačíná podáním ale vyhotovením záznamu, který bude následně povýšen na dokument. Tento proces souvisí s kontrolou v podobě schvalovacího procesu, podepisováním a následným zaevidováním dokumentu. Dokumenty vyhotovené veřejnoprávním původcem jsou buď následně odesílány dalším subjektům, kdy se jedná např. o předvolání, sdělení atd. Nebo v dalším případě zůstávají u původce (např. úřední záznamy, usnesení atd.). Odesílané dokumenty veřejnoprávního původce musí být opatřené razítkem, pečeti a podpisem.⁴⁰

Závěrečnou částí života dokumentu je jeho uložení, archivace nebo případná skartace. I táto část musí být zahrnuta a řádně upravena ve spisovém řádě původce. Původce by měl pracovat na úpravě s Národním standardem, zákonem č. 499/2004 Sb. a vyhláškou 259/2012 Sb.

Vyhláška č. 259/2012 Sb. se ukládáním dokumentů u původce přímo zabývá v §19 odst. 1 a 2. Podle odst. 1 „*Veřejnoprávní původce ukládá uzavřené spisy a vyřízené dokumenty podle věcných skupin a spisových znaků způsobem stanoveným ve spisovém a skartačním plánu ve spisovně. Veřejnoprávní původce stanoví ve spisovém řádu podrobnosti postupu ukládání dokumentů.*“⁴¹ Následně podle odst. 2 „*Veřejnoprávní původce před uložením kontroluje uzavřený spis a vyřízený dokument, jsou-li úplné, zda jsou v evidenční pomůcce správně zpracovány všechny povinné údaje a zda jsou dodrženy podmínky uzavření spisu.*“⁴² Předmětem této kontroly jsou následující položky:

1. Označení doručeného analogového dokumentu podacím razítkem a úplnost jeho vyplnění
2. Označení analogového dokumentu JID
3. Komplettnost spisu v analogové podobě
4. Počet listů analogového dokumentu, počet analogových příloh a počet listů těchto příloh
5. Celkový počet listů, popřípadě počet svazků
6. Převedení dokumentu v digitální podobě do výstupního datového formátu
7. Uvedení spisového znaku a skartačního režimu u všech dokumentů a spisů
8. Zápis v evidenční pomůcce a jeho úplnost, a to podle druhu evidence, ve které je dokument evidován
9. Uložení dokumentů a spisů v obalech, které zaručují jejich neporušitelnost a zachování jejich čitelnosti

³⁸ §8 odst. 1 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

³⁹ Tamtéž.

⁴⁰ Tamtéž §16.

⁴¹ §19 odst. 1 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

⁴² Tamtéž §19 odst. 2

10. Uložení dokumentů v digitální podobě zpracovaných před vyřízením na přenosných technických nosičích dat v elektronickém systému spisové služby nebo jejich převedení a opatření doložkou⁴³

Tyto podmínky by měly být uvedené v každém správně zpracovaném spisovém řádu. Spisový řád musí dále obsahovat i spisový a skartační plán původce. Při tvorbě skartačního řádu se musí původce řídit nejen právními normami zmíněnými výše, ale měl by brát ohled i na metodiky, které vydává Ministerstvo vnitra ČR nebo na pomocné informace, jež jsou uvedeny na stránkách Národních archivů.

⁴³ §19 odst. 2 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby

3. Důvěryhodnost digitálních dokumentů

3.1 Elektronický podpis

Elektronický podpis je důležitým institutem, který zabezpečuje právní validitu a autenticitu při používání digitálních dokumentů. Také je nástrojem pro bezpečnou elektronickou komunikaci. K jeho vytvoření jsou potřeba data pro vytvoření elektronického podpisu tzv. šifrovací klíč. K jeho ověření je nutný tzv. „certifikát“. Jedná se o dokument, který přímo souvisí s podepisující osobou, a na základě kterého tuto osobu můžeme identifikovat.

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 Sb. definuje elektronický podpis jako „*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.*“⁴⁴ Podepisující osobou se rozumí každá osoba, která vytváří elektronický podpis a tím se v elektronickém prostředí identifikuje.

U veřejnoprávních původců se dá narazit hlavně na 2 typy elektronického podpisu: **zaručený** a **kvalifikovaný**. Oba typy podpisů můžeme označit jako uznávané. Zaručený elektronický podpis je typ elektronického podpisu, který musí splňovat následující požadavky:

1. musí být spojen s podepisující osobou
2. umožňuje identifikaci podepisující se osoby,
3. je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou
4. je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Další úroveň je již dříve zmiňovaný kvalifikovaný podpis. V tomto případě se jedná vlastně o zaručený elektronický podpis, který je ale založený na kvalifikovaném certifikátu, vydaným akreditovaným poskytovatelem služeb vytvářejících důvěru. I tento podpis ale musí obsahovat údaje, na základě kterých je možné identifikovat podepisující osobu. Je rovnocenný vlastnoručnímu podpisu.⁴⁵

Podepisováním digitálních dokumentů se zabývá zákon č. 297/2016 Sb., *zákon o službách vytvářejících důvěru* který nahradil zákon č. 227/2000 Sb., *o elektronickém podpisu*. Ten ve svém §5 stanovuje, že pokud podepisováním digitálního dokumentu právně jedná stát, územní samosprávný celek, právnická osoba založená zákonem, nebo státem, či další z „*veřejnoprávních podepisujících*“ musí být použit výhradně kvalifikovaný elektronický podpis. V následujícím § 6 stanovuje, že pokud je digitální dokument podepsán v případě činění úkonu vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti, musí být výhradně použit pouze uznávaný elektronický podpis. Podle odst. 2 platí, že „*uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.*“⁴⁶

Certifikát pro elektronický podpis se dá definovat jako „*elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby.*“⁴⁷ Kvalifikovaný certifikát pro elektronický podpis musí být vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a musí splňovat několik dalších specifických požadavků, které jsou stanoveny v příloze 1 nařízení č. 910/2014 Sb: *a) označení alespoň ve formě vhodné pro automatické zpracování,*

⁴⁴ Čl. 3 odst. 10 nařízení č. 910/2014 Sb., eIDAS

⁴⁵ §5-§7 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

⁴⁶ Tamtéž.

⁴⁷ Čl. 3 odst. 14 nařízení č. 910/2014 Sb., eIDAS

že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis, b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž poskytovatel usazen, c) alespoň jméno podepisující osoby nebo pseudonym. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena, d) data pro ověřování platnosti elektronických podpisů, která odpovídají datům pro vytváření elektronických podpisů, e) označení začátku a konce doby platnosti certifikátu, f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru, g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává, h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g, i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu, j) pokud jsou data pro vytváření elektronických podpisů spojená s daty pro ověřování platnosti elektronických podpisů obsažena v kvalifikovaném prostředku pro vytváření elektronických podpisů, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.“⁴⁸

Zde je patrné, že hlavní rozdíl mezi těmito dvěma certifikáty, jsou informace, které musí obsahovat. U kvalifikovaného certifikátu není identifikovaná jen podepisující osoba, ale i kvalifikovaný poskytovatel služeb vytvářejících důvěru.

K ověření platnosti elektronického podpisu nám tedy slouží externí informace „konkrétně samotný certifikát, na kterém je zkoumaný podpis založen, dále všechny jeho nadřazené certifikáty (na příslušné certifikační cestě), a také informace musí být vztaženy k době, ke které platnost podpisu ověřujeme. Tedy k příslušnému posuzovanému časovému okamžiku. Samotné certifikáty (ať již jen „podpisový“ či jeho nadřazené certifikáty) mohou, ale také nemusí být vloženy přímo do podepsaného dokumentu (v případě interního podpisu), nebo začleněny do externího podpisu – tak aby byly k dispozici v okamžiku, kdy je podpis ověřován. Ale největší problém bývá s nezbytnými informacemi a stavu revokace všech těchto certifikátů (...). Připomeňme si, že v rámci ověřování musíme vždy zkontrolovat, zda nedošlo k revokaci (předčasněmu zneplatnění) některého z těchto certifikátů ještě v době jeho řádné platnosti. Pokud ale k ověření dochází po delší době od vzniku podpisu – a hlavně od skončení řádné platnosti samotných certifikátů – nemusí být takováto informace již dostupná. (...) Řešením může být to, že k podepsanému dokumentu (a jeho podpisu) se kromě samotného podpisu, časového razítka či razítek a všech relevantních certifikátů „přibalí“ také příslušná informace o stavu revokace certifikátů. Tak aby ten, kdo bude kdykoliv později ověřovat platnost podpisu, měl všechny potřebné údaje k dispozici.“⁴⁹

3.2 Elektronická pečeť

Elektronickou pečeť stejně jako elektronický podpis tvoří data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu. Elektronická pečeť teda vypovídá o tom, ve které instituci dokument vznikl na rozdíl od elektronického podpisu, který určuje osobu, která dokument vytvořila. Podobně jako u elektronického podpisu i u elektronické pečeti můžeme u veřejnoprávních původců na 2 typy elektronických pečeti: zaručenou a kvalifikovanou. Zaručená elektronická pečeť musí stejně jako zaručený elektronický podpis splňovat požadavky ustanovené v článku 36 v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 Sb. Tyto požadavky stanovují, že zaručená elektronická pečeť je:

1. jednoznačně spojena s pečeti osobou,

⁴⁸ Příloha 1 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 Sb.

⁴⁹ PETERKA, J. *Báječný svět elektronického podpisu*. Praha: 2011, s. 164

2. umožňuje identifikaci pečetící osoby
3. je vytvořena pomocí dat pro vytváření elektronických pečetí, která může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou
4. je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následující změnu dat.⁵⁰

Kvalifikovanou elektronickou pečeť tvoří zaručená elektronická pečeť, která je ale vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu⁵¹.

Certifikát pro elektronickou pečeť je tvořen „*elektronickým potvrzením, které spojuje data pro ověřování platnosti elektronických pečetí s určitou právníkou osobou a potvrzuje její název.*“⁵² Kvalifikovaný certifikát pro elektronickou pečeť musí být vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a obdobně jako u kvalifikovaného elektronického podpisu musí splňovat řadu požadavků, které stanovuje nařízení č. 910/2014 Sb.

Dá se říct že, požadavky jsou skoro totožné s požadavky pro kvalifikovaný certifikát pro elektronický podpis, nicméně pro lepší ujasnění co vlastně kvalifikovaný certifikát pro elektronickou pečeť musí obsahovat, jsem se rozhodla, že je tady beztak zmíním: „*a) označení alespoň ve formě vhodné pro automatické zpracování, že se certifikát vydává jako kvalifikovaný certifikát pro elektronickou pečeť, b) soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, c) alespoň jméno pečetící osoby a případně registrační číslo uvedené v úředních záznamech, d) data pro ověřování platnosti elektronických pečetí, která odpovídají datům pro vytváření elektronických pečetí, e) označení začátku a konce doby platnosti certifikátu, f) identifikační číslo certifikátu, které musí být jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru, g) zaručení elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele, který certifikát vydává, h) údaj o místě, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g);, i) údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu, j) pokud jsou data obsažena v kvalifikovaném prostředku pro vytváření elektronických pečetí, příslušnou poznámku, alespoň ve formě vhodné pro automatické zpracování.*“⁵³

Pečetění dokumentů opět upravuje zákon č. 227/2016 Sb., *o službách vytvářejících důvěru pro elektronické transakce*. To přímo popisuje § 8 výše zmíněného zákona, kde se stanovuje že „*nestanoví-li jiný právní předpis jako náležitost úkonu nebo právního jednání obsaženého v dokumentu podpis nebo tato záležitost nevyplývá z povahy úkonu nebo právního jednání, veřejnoprávní podepisující a jiná právníká osoba, činí-li úkon při výkonu své působnosti zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečeť.*“⁵⁴ Dle následujícího § 9 odst. 1 dále platí, že „*k pečetění elektronickou pečeť lze použít pouze uznávanou elektronickou pečeť, pečetí-li se elektronický dokument, kterým právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.*“⁵⁵ Uznávanou elektronickou pečeť se „*rozumí zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť.*“⁵⁶ K pečetění digitálních dokumentů lze použít i jiný typ pečeti, než uznávanou, ale jen v případě,

⁵⁰ Článek č. 36 tamtéž

⁵¹ Odst. 27 článků 3 tamtéž

⁵² Odst. 29 článku 3 tamtéž

⁵³ Příloha III Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 Sb., eIDAS

⁵⁴ §8 zákona č.227/2016 Sb., o službách vytvářejících důvěru

⁵⁵ §9 odst. 1 tamtéž

⁵⁶ §9 odst. 2 tamtéž

kdy se právně jedná jiným způsobem, než který je uveden ve výše zmíněném §8 zákona č. 227/2016 Sb.

3.3 Časové razítko

Časové razítko představuje důležitý prvek při ověřování právní validity digitálního dokumentu. Tvoří ho „*data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku*“. Podle tohoto ustanovení lze vidět, že hlavním smyslem časového razítka je doložení existence obsahu digitálního dokumentu ještě časovým okamžikem, který je stanovený v časovém razítku. Dále umožňuje následné ověření, zda nebylo s digitálním dokumentem nijak manipulováno od chvíle, kdy byl orazítkován. Manipulací se v této situaci myslí změna obsahu nebo formátu digitálního dokumentu.

Veřejnoprávní původce musí při vytvoření digitálního dokumentu používat kvalifikované časové razítko. Stejně jako u kvalifikovaného podpisu a kvalifikované pečeti musí splňovat podmínky stanovené v Nařízení eIDAS. Kvalifikované časové razítko „*a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat, b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem a c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.*“⁵⁷

Používání časového razítka rovněž upravuje zákon č. 227/2016 Sb., který v §11 stanovuje v odst. 1, že „*veřejnoprávní podepisující, který podepsal elektronický dokument, kterým činí úkon nebo právně jedná způsobem podle § 5, opatří podepsaný elektronický dokument kvalifikovaným časovým razítkem*“ a v odst. 2 že „*veřejnoprávní podepisující, který zapečetil elektronický dokument, kterým činí úkon nebo právně jedná, způsobem podle § 8, a osoba, která zapečetila elektronický dokument, kterým činí úkon při výkonu své působnosti, způsobem podle §8, opatří zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem.*“⁵⁸

3.4 Kvalifikovaný poskytovatel služeb vytvářejících důvěru

Kvalifikovaným poskytovatelem služeb vytvářejících důvěru se rozumí poskytovatel, který je nabízí jednu nebo více služeb vytvářejících důvěru a kterému dohlížející orgán udělil status kvalifikovaného poskytovatele. Mezi tyto služby patří i vydávání kvalifikovaných certifikátů pro elektronické podpisy a elektronické pečete, kdy kvalifikovaný poskytovatel služeb vystupuje jako „certifikační autorita“. Jak jsem již v předchozích částech zmiňovala, certifikát musí obsahovat data pro ověření elektronického podpisu, identifikační údaje osoby, která daný certifikát využívá a označení certifikační autority, jež daný certifikát vydala.

Kvalifikovaný poskytovatel poskytuje kvalifikovanou službu pouze na základě písemné smlouvy. Dále má povinnost uchovávat po dobu 10 let dokumenty související s vydáváním výše zmíněných certifikátů a kvalifikovaného elektronického razítka. Informace pro vydání kvalifikovaných certifikátů může čerpat v upraveném rozsahu z různých zdrojů, kam kupříkladu patří: základní registr obyvatel, základní registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci nebo informační systém evidence obyvatel.⁵⁹

⁵⁷ Článek 42 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 Sb., eIDAS

⁵⁸ §11 odst. 1 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

⁵⁹ Tamtéž. §2-§4a

3.5. Ověřitelnost digitálních dokumentů

Jak již víme, každý právně validní digitální dokument, by měl obsahovat kvalifikovaný elektronický podpis, kvalifikovanou elektronickou pečeť a kvalifikované časové razítko. Nicméně aby tyto doložky správně plnily svou funkci, je potřeba zajistit jejich dlouhodobou ověřitelnost a prokazatelnost. Je nutné zajistit všechna potřebná data (tzv. validační data), jež zajistí proces kontroly, která následně vyhodnotí jejich platnost, dlouhodobou ověřitelnost a průkaznost.

Ověřování je významnou částí i při uchovávání digitálních dokumentů. Požadavky, kterými by se tento proces měl řídit, upravuje zákon č. 499/2004 Sb. a to konkrétně v § 3 odst. 5:

- **Zajištění věrohodnosti původu digitálního dokumentu** souvisí s procesními postupy identifikace původu dokumentů (př. u doručeného dokumentu, je zjištěn odesílatel) a také s ověřováním elektronických zabezpečovacích prvků.
- **Zajištění neporušitelnosti obsahu digitálního dokumentu** zahrnuje jak procesní, tak technickou realizační rovinu. „*Procesní rovina souvisí s celkovou koncepcí úložiště, nastavením přístupových práv a povolených operací pro jednotlivé uživatele. Technická rovina zajišťuje neporušitelnost obsahu zejména prostředky elektronické značky (...) nebo obdobným technickým způsobem, např. ukládáním otisků*“⁶⁰ dokumentů.⁶¹
- **Zajištění čitelnosti digitálního dokumentu** souvisí s problematikou datových formátů a jejich zastaráváním. Jelikož jsou určení původci povinni zajistit příjem digitálních dokumentů alespoň v datových formátech stanovených jako výstupní datové formáty, nebo ve formátech, které jsou výstupem z autorizované konverze dokumentů. To znamená, že ERMS musí v rámci střednědobého uložení dokumentů minimálně tyto formáty ukládat a musí zajistit zachování jejich čitelnosti. Původce může využít dva způsoby, jak tento požadavek může splnit: 1) volbou volných datových formátů nebo za 2) migrací neboli změnou datového formátu na základě § 69 zákona č. 499/2004 Sb.
- **Přiměřená tvorba a správa k těmto dokumentům v souladu se zákonem č. 499/2004 Sb.** od zaevidování digitálního dokumentu v EMRS až po okamžik vyřízení vznikají metadata, u kterých je potřeba kontrolovat jejich správnost a úplnost.
- **Připojení údajů prokazujících existenci digitálního dokumentu v čase**⁶² je spíš čistě technická záležitost a lze pro to využít např. kvalifikované časové razítko.

Ověřování výše zmíněných elektronických prvků (elektronické pečete, elektronické podpisy, časové razítko) je komplikováno s omezující platností příslušných certifikátů, které se ukládají společně s dokumentem. Nicméně existují způsoby, jakým se tato situace dá vyřešit. Ve své knize citují Kunt a Lechner, citující Smejkal a Valáška, uvádějí „*pět obecných způsobů*

⁶⁰ „*Otisky dokumentů, tzv. HASH, jsou vytvářeny pomocí hashovací funkce, která libovolně velkému vstupu přikazuje krátký kód (otisk) o pevně definované délce a k tomu je jednosměrná a bezkolizní. Jednosměrnost znamená, že z otisku nelze zpětně jakýmkoliv způsobem spočítat původní obsah dokumentu. Proto se také někdy říká, že hashovací funkce nesmí být reverzní. Odolnosti proti kolizi, jako druhá ze jmenovaných vlastností, znamená, že musí být výpočetně nezvládnutelné nalezení libovolných dvou různých dokumentů se stejným otiskem. Detailně o hashovacích funkcích viz např. KLÍMA, V. Hašovací funkce, principy, příklady a kolize. Citace 12. 5.2014. Dostupné na: http://crypto-world.info/klima/2005/cryptofest_2005.htm#_Toc98987052 Tyto funkce jsou základem pro kontrolu integrity dat pomocí autentizačních prvků.*

In: KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 268

⁶¹ Tamtéž. 268

⁶² §3 odst. 5 zákona č. 499/2004 Sb., o archivnictví a spisové službě

vycházejících z aktuální právní úpravy v České republice, kterými lze nějakým způsobem překonat problém expirace kvalifikovaných certifikátů, a tedy zajistit dlouhodobou důvěryhodnost digitálních dokumentů. Konkrétně autoři citovaného příspěvku hovoří o vyžádání stejnopisu dokumentu, ověření zprávy v ISDS, institucionálně důvěryhodném repozitáři, provázaných otiscích (hash) a časových razítkách.⁶³ Dále pak autoři uvádějí, že v praxi se lze setkat s dvěma různými přístupy. První přístup je čistě technologického charakteru a je založen „na opakovaném přerazítkování digitálních dokumentů kvalifikovanými časovými razítky, a to vždy dříve, než skončí platnost certifikátu, na kterém je předchozí kvalifikované časové razítko založeno. Pokud je vždy přerazítkováním ověřeno předchozí časové razítko a informace o ověření je připojena k výsledku, který je přerazítkován, lze tímto řetězem razítek zajistit trvalou ověřitelnost aktuálního stavu dokumentu.“⁶⁴ Nicméně autoři dodávají, že tento přístup bude fungovat pouze za předpokladu, že „není předčasně zneplatněn certifikát autority, na kterém je stávající časové razítko založeno. Protože riziko revokace nelze nikdy vyloučit, nemůže uvedený postup přerazítkování dokumentů zajistit stoprocentní jistotu udržení trvalé ověřitelnosti celé posloupnosti připojovaných zabezpečovacích prvků, pouze ji významně zvyšuje.“⁶⁵

Druhý přístup, který Kunt a Lechner uvádí, je založen na procesním postupu vytváření transakčního protokolu. Který zaznamenává jakékoliv manipulace s dokumentem. Transakční protokol je v Národním standardu definován jako „důvěryhodný zápis informací o operacích provedených v eSSL, které ovlivnily nebo změnily entity nebo eSSL. Tyto informace umožňují dohledání, identifikaci, rekonstrukci a kontrolu těchto operací, stavu entit v minulosti a činnosti uživatelů.“⁶⁶ Dále podle bodu 5.3 rovněž Národního standardu platí, že „vzhledem k tomu, že eSSL musí být auditovatelným a důvěryhodným systémem, je stanovena povinnost exportu transakčního protokolu a jeho opatření autentizačními prvky (elektronický podpis nebo elektronická pečeť a elektronické časové razítko).“⁶⁷ Bod 5.3.3. dále ustanovuje, že „eSSL obsah transakčního protokolu za stanovený časový úsek, nejdéle však 1 den, automaticky na konci tohoto časového úseku uloží jako ztvárnění dokumentu v datovém formátu PDF/A nebo XMLD dle přílohy č. 6, který opatří elektronickým podpisem nebo elektronickou pečetí a elektronickým razítkem. Tento dokument eSSL zatřídí do příslušné věcné skupiny nebo do spisu“, toto slouží k prokázání všech operací, které byly s dokumentem vykonány.⁶⁸

3.6. Datové schránky

Pro důvěryhodného doručování a odesílání digitálních dokumentů byl vytvořen Informační systém datových schránek. Jedná se o uzavřený systém, jenž zajišťuje propojení mezi jednotlivými schránkami. Tento informační systém veřejné správy dále obsahuje informace o datových schránkách a jejich uživatelích. Jedná se například o jméno uživatele, identifikátor datové schránky, datum zřízení...atd. Jeho správcem je rovněž Ministerstvo vnitra a provozovatelem je Česká pošta, s. p. Na základě uzavřenosti systému ISDS nedochází k přenosu zpráv přes internet.⁶⁹

Datové schránky fungují v České republice již od roku 2009 a upravuje jich zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, jež je definuje jako „elektronické uložení, které je určeno k a) doručování orgány veřejné moci, b) provádění

⁶³ KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 277

⁶⁴ Tamtéž s. 277-278

⁶⁵ Tamtéž s. 278

⁶⁶ Národní standard pro elektronické systémy spisové služby. In: *Věstník MV ČR, částka 57/2017 (část II)*, bod 7.2. str. 51

⁶⁷ Tamtéž bod 5.3. str. 40

⁶⁸ Tamtéž bod 5.3.3. str. 41

⁶⁹ §14 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

*úkonů vůči orgánům veřejné moci, c) dodávání dokumentů fyzických osob, podnikajících osob a právnických osob.*⁷⁰

Jsou vydávány a spravovány Ministerstvem vnitra, ale provozovatelem systému ISDS je Česká pošta, s. p. Datové schránky jsou důležitou prvkem při komunikaci ve státní správě a jejich uživatelé se řídí „Provozním řádem informačního systému ISDS“, který vydává Ministerstvo vnitra ve spolupráci s Českou poštou, s.p. Datová schránka navíc nahrazuje jak elektronický tak i vlastnoruční podpis, jelikož jakýkoliv úkon učinění přes ní má stejné účinky jako úkon učiněný písemně a podepsaný.⁷¹

Datovou zprávu se rozumí data v elektronické podobě, zejména text, zvuk nebo audiovizuální nahrávka. Dokumenty, jež jsou datovou schránkou doručovány, mají formu datové zprávy.⁷² Od roku listopadu 2018 může být datová zpráva maximálně 50 MB veliká. V datové schránce je uložena po dobu 90 dní od přihlášení do datové schránky nebo po dobu 3 let, ode dne kdy byly datová zpráva doručena a nedošlo k přístupu do datové schránky.⁷³ Pro dlouhodobé uložení může uživatel využít službu České pošty tzv. datový trezor nebo si může datovou zprávu stáhnout do svého počítače. Datovým trezorem se rozumí elektronické úložiště, které bezpečně uchovává datové zprávy, které ale i nadále zůstávají pro uživatele viditelné v systému ISDS.⁷⁴

Jak již bylo výše zmíněno, datové schránky se můžou nechat zřídit fyzické, podnikající a právnické osoby a to bezplatně. Každá z těchto osob si může zažádat o zřízení jedné datové schránky.

Fyzická osoba musí být plně svéprávná a k získání datové schránky musí podat příslušnou žádost, která musí obsahovat náležitosti stanovené v §3 odst. 3 zákona č. 300/2008 Sb., čímž se rozumí její:

- a) jméno
- b) rodné příjmení
- c) den, měsíc a rok narození
- d) místo a okres narození; pokud se fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila
- e) státní občanství, není-li fyzická osoba státním občanem České republiky.⁷⁵

Dále žádost musí obsahovat i úředně ověřený podpis fyzické osoby v případě, že není žádost podávána na kontaktním místě veřejné správy. Pokud jsou splněny všechny podmínky, bude datová schránka zřízena do 3 dnů od podání žádosti.

Stejný postup se týká i podnikajících osob. Musí být podaná žádost a na jejím základě bude právnické osobě zřízená datová schránka. Skoro identické jsou i náležitosti, až na povinnost uvedení „identifikačního čísla podnikající osoby“ a „místa podnikání“.

Právnická osoba si rovněž můžou nechat zřídit datovou schránku, kterou bude užívat její oprávněný zástupce/i. Žádost právnické osoby musí obsahovat:

- a) název nebo obchodní firmu,
- b) identifikační číslo osoby, a nebylo-li přiděleno, registrační číslo, evidenční číslo nebo jiný obdobný údaj, byl-li přidělen

⁷⁰ §2 zákon č. 300/2008, o elektronických úkonech a autorizované konverzi

⁷¹ Tamtéž §18 odst. 2

⁷² Tamtéž § 19

⁷³ Vyhláška č. 194/2009 Sb., o stanovení podrobností

⁷⁴ Datový trezor In: <https://www.datoveschranky.info/aditivni-sluzby/datovy-trezor> [1. 8. 2022]

⁷⁵ § 3 odst. 3 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

- c) adresa sídla
- d) jméno, popřípadě jména, příjmení, datum narození a adresu pobytu osoby oprávněné jednat jménem právnické osoby
- e) stát registrace nebo evidence právnické osoby.⁷⁶

Dalším typem je datová schránka orgánu veřejné moci. Nejvíce se odlišuje od výše zmíněných tím, že mu Ministerstvo vnitra může zřídit více datových schránek. I tento orgán musí podat žádost, která musí obsahovat náležitosti stanovené rovněž zákonem č. 300/2008 Sb. Žádost musí obsahovat následovně:

- a) název orgánu veřejné moci a název vnitřní organizační jednotky orgánů veřejné moci, pro jejíž potřebu se datová schránka zřizuje nebo název agendy nebo činnosti orgánu veřejné moci, pro jejíž potřebu se datová schránka zřizuje
- b) identifikátor orgánů veřejné moci
- c) adresa sídla
- d) jméno, popřípadě jména, příjmení, datum narození a adresa pobytu osoby, již mají být zaslány přístupové údaje.⁷⁷

Žádost lze podat buď na kontaktním místě veřejné správy, dále může být zaslána na podatelnu Správce (Ministerstva vnitra) nebo může být podána online v prostředí klientského portálu ISDS po přihlášení Identity občana. Datová schránka je zpřístupněna po prvním přihlášení osoby, pro kterou byla schránka zřízena. K přihlášení osoba využije přístupové údaje, jež jí zaslalo Ministerstvo vnitra do vlastních rukou. Tyto údaje tvoří uživatelské jméno a heslo.⁷⁸

Každá datová schránka má svůj jedinečný identifikátor. Způsob jeho tvorby upravuje vyhláška č. 194/2009 Sb., ve které je ustanoveno, že „*správce informačního systému datových schránek vytváří identifikátor datové schránky automatizovaně s využitím algoritmů pro generování náhodných čísel.*“⁷⁹

Ministerstvo ruší datové schránky po uplynutí 3 let po zániku osoby nebo orgánu veřejné moci. Také ji může zrušit na žádost osoby, pro jejíž potřebu byla schránka zřízena nebo na žádost administrátora.

Do ISDS se fyzické a podnikající osoby mohou přihlásit různými způsoby. První možností je přihlášení pouze pomocí již výše zmíněného hesla a jména. Podle nařízení eIDAS se dá zařadit do nízké úrovně záruky systému elektronické identifikace. Sama musím s tímto tvrzením souhlasit. Jméno a heslo v dnešním světě, je velmi lehce zmanipulovatelné, a i proto se uživatelům doporučuje, aby využili jiné a bezpečnější způsoby z následujících možností. Do značné úrovně patří metoda využití autentizačního certifikátu, který vydal kvalifikovaný poskytovatel služeb vytvářejících důvěru. Nicméně nevýhodou pro uživatele, může být omezení využití datové schránky pouze na zařízení, kde je certifikát instalován.

Dále je tu možnost přihlašování pomocí SMS autentizace. Majitel datové schránky musí vždy zadat uživatelské jméno, heslo a nakonec jednorázový autentizační kód, který obdrží na svém mobilním zařízení. Poměrně novou možností je Mobilní klíč ISDS. Pomocí této aplikace nemusí uživatel zadávat jméno ani heslo. Na svém mobilním zařízení naskenuje pouze QR kód, který při přihlašování objeví, poté co uživatel zadá možnost přihlášení mobilním klíčem. Jako poslední a nejbezpečnější je přihlašování přes prostředek kvalifikovaného systému pro elektronickou identifikaci.⁸⁰

⁷⁶ § 5 odst. 4 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

⁷⁷ Tamtéž § 6

⁷⁸ Tamtéž § 10

⁷⁹ § 8 odst. 1 vyhlášky 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

⁸⁰ Tamtéž § 2

Kvalifikovaným systémem je podle §3 zákona č. 250/2017 Sb. „systém elektronické identifikace a) který spravuje kvalifikovaná správce systému elektronické identifikace, b) splňuje technické specifikace, normy a postupy alespoň pro jednu z úrovní záruky stanovených přímo použitelným předpisem Evropské unie upravujícím minimální technické specifikace, normy a postupy pro úroveň záruky prostředků pro elektronickou identifikaci, c) který umožňuje identifikační údaje jedinečně identifikují osobu v okamžiku vydání prostředku pro elektronickou identifikaci spojeny s danou osobou v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie a e) v jehož rámci je vydáván a používán pouze prostředek pro elektronickou identifikaci, který je spojen s osobou, kterou identifikuje, v souladu s technickými specifikacemi, normami a postupy pro příslušnou úroveň záruky stanovenými příslušným předpisem Evropské unie.“⁸¹ Do této kategorie patří informační systém veřejné správy tzv. Národní bod, jenž podporuje proces elektronické identifikace a autentizace pomocí kvalifikovaného systému.

Mezi jeho identifikační prostředky patří například eObčanka. Pro její využití musí mít uživatel aktivovaný elektronický čip na svém občanském průkazu a mít k dispozici čtečku pro tento čip. V dnešní době mají tuto čtečku některé notebooky nebo klávesnice přímo zabudované, ale lze jí zakoupit i samostatně. Dále musí mít uživatel nainstalovaný software eObčanky, skrz který bude identifikace probíhat. K identifikaci jsou využívána data z registru obyvatel.⁸²

Elektronická identifikace u právnických osob probíhá jinak. Jak je známo, za právnickou osobu, vždy jedná zástupce (fyzická osoba nebo osoby). Autorizaci této fyzické osoby posuzuje poskytovatel kvalifikované služby na základě. Za prvé musí dojít k identifikaci fyzické osoby. Po ztotožnění nabídne ISDS fyzické osobě seznam datových schránek, se kterými je oprávněna jednat. Autentizovaná osoba si tedy vybírá za koho a v jaké roli bude jednat. Informace o tomto oprávnění si obstarává ISDS z registru osob či z jiných zdrojů. Tyto informace může vést i na základě samotného sdělení majitele datové schránky. Nicméně je na samotném ISDS a kvalifikovaném poskytovateli online služeb, aby oprávnění k zastupování právnických osob ve svém prostředí řádně implementoval.⁸³

3.6. Konverze dokumentů

Konverzí dokumentů se rozumí úplné převedení dokumentu do digitální podoby nebo naopak. Existují dvě možnosti konverze a to buď převedení typu dokumentu podle § 69a zákona č. 499/2009 Sb. nebo autorizovaná konverze upravovaná zákonem č. 300/2008 Sb.

Konverzí podle § 69a se analogový dokument převede na digitální nebo naopak, ale nezaručuje rovnocenné právní účinky výstupního dokumentu se vstupním dokumentem. Většinou se používá při doručení analogového dokumentu, kdy ale musí být zaevidován do systému eSSL, pokud původce vede spisovou službu v elektronické podobě.⁸⁴

Autorizovanou konverzí se rozumí proces, kdy je dokument v analogové podobě převeden do podoby digitální nebo naopak, způsobem zajišťující shodu obsahu těchto dokumentů. K dokumentu musí být připojena doložka o provedení autorizované konverze. Za pomoci autorizované konverze má výstupní dokument stejné právní účinky, jako dokument, jenž do konverze vstupoval. Při užívání datových schránek je tato možnost velmi důležitá, jelikož dokumenty doručované přes ní jsou ve formě datové zprávy. Primární dokument nicméně může být analog a proto bylo nutné zavést způsob, jakým by ho bylo možné převést a přitom zachovat

⁸¹ §3 odst. 1 zákona č. 250/2017 Sb., o elektronické identifikaci

⁸² eObčanka In: <https://info.identitaobcana.cz/eop/> [1. 8. 2022]

⁸³ Elektronická identifikace právnických osob In: <https://www.mvcr.cz/clanek/elektronicka-identifikace-pravnickych-osob.aspx> [1. 8. 2022]

⁸⁴ § 69a zákona č. 499/2004 Sb., o archivnictví a spisové službě

jeho právní účinek. Podstatné tedy je, že dokument vzniklý autorizovanou konverzí má stejné právní účinky jako notářsky ověřená kopie.

Autorizovaná konverze se vždy provádí na žádost nebo z moci úřední. Na žádost je prováděná v kontaktních místech veřejné správy neboli Czech POINT a advokáti. Z moci úřední ji mohou provést pověřené orgány veřejné moci pro výkon své působnosti.⁸⁵

Postup autorizované konverze upravuje zákon č. 300/2008 Sb. a vyhláška č. 193/2009 Sb. Pokud se jedná o konvertování digitálního dokumentu, musí se provést kontrola platnosti elektronické podpisu, elektronické časového razítka, elektronické pečete a integrity pokud je zajištěná jiným způsobem. Po jejím provedení se k dokumentu připojí doložka, která se stává součástí výstupu. Obsah doložky se liší podle toho, zda byl dokument převeden z analogové podoby do digitální nebo z digitální do analogové.

Konverze nemůže být provedena u všech typů dokumentu. Dle odst. 4 § 24 zákona č. 300/2008 Sb., se konverze „neprovádí a) je-li dokument v jiné než v listinné podobě či v podobě datové zprávy, b) jde-li o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los sázenku, geometrický plán, rys nebo technickou kresbu, c) jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost, d) není-li z dokumentu v listinné podobě patrné, zda se jedná o 1. prvopis, 2. vidimovaný dokument, 3. opis nebo kopii pořízenou ze spisu, nebo 4. stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu, e) jde-li o dokument, který je výstupem, v jehož doložce je uveden údaj o tom, že vstup obsahuje viditelný prvek, který nelze plně přenést na výstup, f) jde-li o vidimovaný dokument, v jehož ověřovací položce je uveden údaj o tom, že dokument, ze kterého byl vidimovaný dokument pořízen, obsahoval viditelný zajišťovací prvek, g) v případě provedení konverze na žádost nebyl-li dokument obsažený v datové zprávě podepsán způsobem, se kterým jiný právní předpis spojuje právní jednání vůči státu v souvislosti s výkonem jeho působnosti účinky vlastnoručního podpisu, zapečetěn uznávanou elektronickou pečetí nebo označen elektronickou značkou toho, kdo dokument vydal nebo vytvořil; to neplatí, jde-li o legalizovaný dokument v elektronické podobě, h) v případě porušení integrity dokumentu obsaženého v datové zprávě, i) jde-li o dokument obsažený v datové zprávě, který nelze konvertovat do listinné podoby, například zvukový nebo audiovizuální záznam, j) pokud dokument nesplňuje technické náležitosti podle odstavce 3.“⁸⁶

Za konverzi by se dalo pokládat i běžné skenování analogového dokumentu nebo vtištění digitálního dokumentu. Nelze ale zaručit shodu vstupního a výstupního dokumentu. Tyto kopie následně slouží pouze jako pomůcka instituce a pozbývá právního účinku.

⁸⁵ § 22 a § 23 č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

⁸⁶ Tamtéž § 24 odst. 4

4. Ukládání digitálních dokumentů

4.1 Ukládání dokumentů obecně

Uložení dokumentů nebo jejich případná archivace představuje závěrečnou část aktivního životního cyklu každého dokumentu a to jak analogového tak i digitálního. Obecně dle § 68 odst. 1 zákona č. 499/2004 Sb., *o archivnictví a spisové službě* platí, že „*všechny vyřízené spisy a jiné dokumenty určeného původce jsou do doby trvání skartační lhůty uloženy ve spisovně. Dokumenty mohou být uloženy též ve správním archivu, pokud jej určený původce zřídil. Dokumenty se ukládají podle spisového řádu a skartačního plánu, a to zpravidla ihned po jejich vyřízení, pokud povaha věci nevyžaduje, aby zpracovatel měl vyřízený dokument déle; tato skutečnost se poznamenává v evidenční pomůcce podle § 64 odst. 3.*“⁸⁷ Skartační lhůtou se rozumí doba, během které musí být dokument uložen u původce.⁸⁸

Ne každý je povinen vést spisovou službu a uchovávat dokumenty. Původci, kteří mají tuto povinnost legislativně nařízenou, jsou vyjmenováni v § 3 odst. 1-4 zákona č. 499/2004 Sb. V první řadě se dle odst. 1 jedná o tzv. veřejnoprávní původce, mezi které řadíme: organizační složky státu; ozbrojené síly; bezpečnostní sbory; státní příspěvkové organizace; státní podniky; územní samosprávné celky; organizační složky územních samosprávních celků, vytvářejí-li dokumenty uvedené v přílohách č. 1 nebo č. 2 k tomuto zákonu; právnické osoby zřízené nebo založené územními samosprávnými celky, vytvářejí-li dokumenty uvedené v přílohách č. 1 nebo č. 2 k tomuto zákonu; vysoké školy; školy a školská zařízení s výjimkou mateřských škol, výchovných a ubytovacích zařízení a zařízení školního stravování (dále jen „školy“); zdravotní pojišťovny; veřejné výzkumné instituce; právnické osoby zřízené zákonem.

Veřejnoprávní původci při výkonu své činnosti, každý den přijímají nebo vytvářejí nespočetné množství dokumentů. V mnoha případech se může jednat o zásadně důležité dokumenty, které mají schopnost ovlivnit běh instituce nebo vývoj procesního řízení. Uchovávání těchto dokumentů je zásadní, a to nejen pro případné právní využití v budoucnosti, ale i pro jejich možnou významnou historickou hodnotu. Z tohoto důvodu je zřejmé, že jsou veřejnoprávní původci povinni umožnit výběr archiválií správním archivem.

Tato povinnost však není uvalena pouze na veřejnoprávní původce. Zákon o archivnictví a spisové službě v §3 odst. 2 stanovuje seznam tzv. soukromoprávních původců, kteří mají rovněž povinnost uchovávat dokumenty a umožnit výběr archiválií. Jedná se o: obchodní společnosti a družstva s výjimkou bytových družstev, pokud jde o dokumenty uvedené v příloze č. 1 k tomuto zákonu; politické strany, politická hnutí, spolky, odborové organizace, organizace zaměstnavatelů, církve a náboženské společnosti, profesní komory, nadace, nadační fondy a obecně prospěšné společnosti; notáři, pokud jde o dokumenty uvedené v příloze 1 k tomuto zákonu.⁸⁹

Dále v § 3 odst. 3 je ustanoveno, že i právní nástupci jak veřejnoprávních, tak i soukromoprávních původců převezmou výše uvedené povinnosti, jedná-li se o dokumenty, které podléhali této povinnosti již za činnosti předchozích původců.⁹⁰ Tyto povinnosti mají dle §3 odst. 4 zákona č. 499/2004 Sb., „*dále podnikatelé, kterým bylo uděleno státní povolení k provozování živnosti vedení spisovny.*“⁹¹

Samotným uložením dokumentů, ale jejich životní cyklus nekončí. Skutečný závěr představuje, až následným výběr archiválií z uložených dokumentů, kdy se oddělují dokumenty

⁸⁷ §68 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě

⁸⁸ Tamtéž § 2 pís. s)

⁸⁹ Tamtéž § 3 odst. 2

⁹⁰ Tamtéž § 3 odst. 3

⁹¹ Tamtéž § 3 odst. 4

bezpečné od dokumentů, které jsou vybrány k trvalému uložení v archivu. Archiválii definujeme jako „*takový dokument, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií.*“⁹² Dokumenty, které vybrány nebyly, budou vyřazeny a skartovány. Nicméně se nejedná, pouze o jednorázový akt. Skartační řízení se skládá se souhrnu různých úkonů, prováděných při plánovitém vyřazování dokumentů, kterým uplynula skartační lhůta a které jsou již pro potřeby původce zbytečné.

4.1.2 Ukládání analogových dokumentů

Při ukládání analogových dokumentů hraje velmi důležitou roli prostředí, kde budou dokumenty uchovávány. Nedostatečná bezpečnost, vlhkost, plíseň, prach nebo dokonce i sluneční světlo může dokument významně poškodit nebo dokonce i zničit. Původce z toho důvodu musí být při určení spisovny velmi obezřetný.

Požadavky na spisovnu, neboli místo kam jsou dokumenty po uzavření ukládány, a budovu ve které se nachází, jsou ustanoveny v odst. 4 písm. a) §68 v zákoně č. 499/2004 Sb., kde je uvedeno: „*Budova, v níž je umístěna spisovna nebo správní archiv, musí splňovat tyto podmínky:*

- a) *prostory pro ukládání dokumentů nesmí být ohroženy povodněmi,*
- b) *musí pro ni být zpracována požární dokumentace a musí být vybavena ručními hasicími přístroji; v prostorách pro ukládání dokumentů musí být umístěny pouze práškové hasicí přístroje,*
- c) *prostory pro ukládání dokumentů musí být zabezpečeny proti škodlivému působení přírodních vlivů a jevů vyvolaných činností člověka, a to zejména proti průniku vody, páry, dešťové a splaškové kanalizace, nebezpečných chemických a biologických látek nebo působením fyzikálních jevů a proti nadměrné prašnosti, které by mohly vést k poškození nebo zničení dokumentů*
- d) *prostory pro ukládání dokumentů musí být vybaveny regály pro ukládání dokumentů,*
- e) *prostory pro ukládání dokumentů musí být zajištěny proti vstupu nepovolané osoby.*“⁹³

V případě, že původce tyto požadavky nedodrží, dopustí se přestupku podle odst. 9 písm. c) § 74 zákona č. 499/2004 Sb., za což mu bude hrozit pokuta ve výši do 200 000 Kč.⁹⁴

Před tím než jsou analogové spisy předané do spisovny původce, musí být provedena kontrola pracovníkem příslušného odboru, který spis vyřizoval a uzavřel.

4.1.3 Ukládání digitálních dokumentů

Ukládáním digitálních dokumentů se rovněž rozumí „*zajištění věrohodnosti původu dokumentů, neporušitelnosti obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.*“⁹⁵ Na tomto ustanovení je vidět jak je právní validita digitálních dokumentů úzce propojena s jejich následným uložením. Oproti ukládání analogových dokumentů, má ukládání digitálních dokumentů určitá specifika. Hlavním rozdílem je skutečnost, že při chránění analogových dokumentů se chrání nosič, kdežto u digitálních dokumentů jsou chráněna data.

⁹² §2 písm. f) zákona č. 499/2004. Sb., o archivnictví a spisové službě

⁹³ Tamtéž § 68 odst. 4 písm. a)

⁹⁴ Tamtéž § 74 odst. 9 písm. c)

⁹⁵ Tamtéž. § 3 odst. 5

Před uložením digitálních dokumentů je potřeba udělat několik rozhodnutí o tom, jak toto uložení bude provedeno. Jak dlouho bude dokument uložen? Jak často se k nim bude přistupovat? Jaká je velikost a formát ukládaných dat? To jsou otázky, které ovlivňují tyto rozhodnutí.

4.1.4 Krátkodobé ukládání digitálních dokumentů

U krátkodobého ukládání platí, že „jeho doba je natolik krátká, že se není třeba významně zabývat otázkami trvanlivosti zvoleného úložiště (tj. tzv. degradací digitálních nosičů) a problematikou zastarávání datových formátů.“⁹⁶ Je to ovlivněno tím, že doba uložení je tak krátká, že se v mnoha případech se netýká spisové služby, ale jen např. doby doručení dokumentu.⁹⁷ Nicméně původce musí beztak dbát, aby byly zachovány požadavky na kvalitu digitálních dokumentů, mezi které se řadí důvěryhodnost, původnost, originalita a úplnost. Do krátkodobého ukládání můžeme řadit i samotnou tvorbu digitálních dokumentů.

4.1.5 Střednědobé ukládání digitálních dokumentů

V střednědobém typu ukládání digitálních dokumentů jsou dokumenty spravovány v elektronickém systému spisové služby s požadavkem vysoké dostupnosti, která je pro vyřizování dokumentů nezbytně nutná. Doba tohoto uložení není přesně stanovená. Může se jednat o dny, nebo dokonce roky. S ohledem na horní hranici této doby, je nutné se zabývat otázkami „vypršení platnosti kvalifikovaných certifikátů, zastaráváním datových formátů, degradací technických nosičů dat apod.“⁹⁸

4.1.6 Dlouhodobé ukládání digitálních dokumentů

Dlouhodobé ukládání digitálních dokumentů může nastat z různých osobních, bezpečnostních nebo legislativních okolností. Digitální dokumenty se ukládají v digitální spisovně v rámci elektronického systému spisové služby. Ani zde není přímo specifikována doba uložení. Skartační lhůta může být stanovena nejen na několik let, ale dokonce i na sto let (např. matriky, zdravotní dokumentace).

Nejdůležitější oblastí, na kterou by se mělo během dlouhodobého ukládání dbát, jsou formátová rizika. Má se na mysli přesněji zastarávání formátů, otevřenosti formátů, podpory formátů a jeho robustnosti⁹⁹. Tento typ ukládání musí splňovat již výše zmíněné požadavky stanovené zákonem č. 499/2004 Sb., v §3 odst. Dále musí splňovat požadavky ohledně výstupních formátů, kterými se budu zabývat detailněji níže.

4.1.7 Datové formáty

Pro ukládání digitálních dokumentů slouží omezená množina datových formátů, které jsou rozšířené, stabilní v čase, veřejně popsané a v případě budoucí potřeby je možné je jiným nástrojem převést do jiného datového formátu.

Elektronický systém spisové služby má být schopný pracovat s datovými formáty uvedených v §23 vyhlášky č. 259/2012 Sb. Mezi ně patří:

- Portable Document Format/Archive (PDF/A) a Portable Document Format (PDF)
- Portable Network Graphics (PNG)
- Graphics Interchange Format (GIF)

⁹⁶ KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 266

⁹⁷ Tamtéž s. 265

⁹⁸ Tamtéž s. 27

⁹⁹ KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 280

- Moving Picture Experts Group Phase 1,2,3 (MPEG-1, MPEG-2, MPEG-4)
- Audio Layer II a Audio Layer III
- Extensible Markup Language Document (XML)

Textový datový formát **Portable Document Format** neboli „**PDF**“ má výhodu v tom, že se dokument zobrazuje ve stejném rozvržení a formátování, v jakém byl původně vytvořen. Je nezávislý na softwaru, hardwaru i operačním systému, ve kterém byl původně vytvořen. To znamená, že se dokument zobrazuje na všech počítačích identicky. Nicméně nejde již do jeho obsahu zasahovat, což ovšem z hlediska ukládání dlouhodobého ukládání digitálních dokumentů lze považovat za výhodu. Přímo pro potřebu dlouhodobého ukládání byla vytvořena varianta **Portable Document Format/Archive** dále „**PDF/A**“. Byly z ní odstraněny určité vlastnosti původní verze „**PDF**“, které by mohly dlouhodobou archivaci zkomplikovat. Například audio a video prvky, javascripty a spustitelné soubory.¹⁰⁰

Datový formát **Portable Network Graphics** „**PNG**“ byl vytvořen pro k uchování rastrových obrazů. I přesto, že je primárně určen pro použití na internetu, potenciál jeho uplatnění je mnohem širší. Zejména jeho nezávislost na platformě s jeho dalšími znaky z něj dělají vhodný formát pro výměnu a dlouhodobou archivaci dat. Často je označován za nástupce „**GIFu**“ pro jeho lepší zobrazovací vlastnosti.¹⁰¹

Dalším datovým formátem pro zobrazování rastrové grafiky je **Graphics Interchange Format** „**GIF**“. Používá se hlavně pro zobrazování tzv. „webové grafiky“. Jedná se o jednoduchý formát, který může zobrazit jen nevelký počet barev a jednoduché čárové objekty.¹⁰²

Uchování audio-vizuálního záznamu bylo dlouhou dobu velmi obtížné, a to zejména u nedostatečné kvality technologie, která by uchování těchto záznamů dlouhodobě umožňovala. Bohužel to zapříčinilo i fakt, že mnoho starších záznamů po převodu do modernějšího typu formátů ztratilo data nebo se snížila jejich kvalita. V dnešní době je technologie natolik vyspělá, že po převedení zhoršení kvality dokumentu nehrozí. Mezi nejznámější využívané formáty patří **Moving Picture Experts Group** a to především „**MPEG-2**“.¹⁰³

4.2. Národní archiv

Národní archiv je definován jako správní úřad a ústřední archiv státu se sídlem v Praze. Je přímo řízen Ministerstvem vnitra. Patří mezi organizační složky státu a jeho rozpočet jeho součástí rozpočtové kapitoly ministerstva. Jeho hlavní náplní jeho vyhledávání a péče o archiválie.

Do jeho agendy patří i kontrola výkonu spisové služby a provádění výběru archiválií ve skartačním i mimoskartačním řízení. Národní archiv má významnou roli i v případě péče o archiválie v digitální podobě, přičemž dle §46 odst. 3 zákona č. 499/2004 Sb. to jsou: „*a) ukládá archiválie, v digitální podobě náležitých do jeho péče a archiválie v digitální podobě náležitých do péče Archivu bezpečnostních složek, státních oblastních archivů a archivů, které nejsou digitálními archivy a neukládají archiválie v digitální podobě na základě písemné dohody v jiném digitálním archivu; nejde-li o archiválie v digitální podobě náležející do jeho péče,*

¹⁰⁰ KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 273-275

¹⁰¹ *PNG-dokonalý formát pro přenos obrazových dat* In: <https://www.interval.cz/clanky/png-dokonalý-format-pro-prenos-obrazovych-dat/> [cit. 10.7.2022]

¹⁰² Soubory GIF In: <https://www.adobe.com/cz/creativecloud/file-types/image/raster/gif-file.html> [1. 8.2022]

¹⁰³ KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015 s. 271-272

*Národní archiv u uložených archiválií v digitální podobě pouze zajišťuje zachování neporušitelnosti jejich obsahu a čitelnosti, b) spravuje národní portál, c) plní archivy metodickou a poradenskou funkci v oblasti předarchivní péče o dokumenty v digitální podobě a v oblasti digitalizace archiválií v analogové podobě, d) provádí vědeckou a výzkumnou činnost na úseku životního cyklu dokumentů v digitální podobě, e) poskytuje archivům údaje potřebné pro evidenci archiválií v digitální podobě a služby pro shromažďování a zpřístupňování popisů archiválií v digitální podobě a replik archiválií v digitální podobě, f) vydává závazné stanovisko k žádosti o udělení oprávnění k ukládání archiválií v digitální podobě.*¹⁰⁴

Jak již bylo poznamenáno výše, národní archiv provádí výběr archiválií během skartačního řízení, které iniciuje původce, tím že podá žádost a vytvoří tzv. skartační návrh všech spisů a dokumentů, jimž uběhla skartační lhůta. Původce s příslušným archivem před zahájením řízení sjedná zástupce původce, kterému budou poskytnuty přístupové údaje pro realizaci skartačního řízení. Zástupce původce pak prostřednictvím portálu nahraje datové balíčky SIP vytvořené v eSSL. Po ukončení nahrávání zástupce stáhne poskytnutý seznam tvořící přílohu skartačního návrhu a ten zašle spolu s průvodním dopisem příslušnému archivu. Ten následně provede vyznačení výběru archiválií a pošle původci seznam dokumentů vybraných za archiválie a dokumentů určených ke skartaci. Původce následně tento seznam načte do svého systému eSSL. Po následném zpracování skartačního protokolu provede původce export datových balíčků SIP dokumentů, spisů a dílů typových spisů ze svého eSSL, které vždy obsahují datové soubory.

SIP balíčky dokumentů a spisů existujících pouze v analogové podobě obsahují pouze metadata, což je pouze obdoba skartačního návrhu. SIP balíčky jsou nahrány opět přes portál a provádí ho stejný zástupce původce, který měl na starosti skartační řízení. Současně jsou archivu předány analogové dokumenty a spisy, jež byly vybrány za archiválie.¹⁰⁵ SIP balíček musí obsahovat veškerá dostupná metadata, která k dokumentům nebo spisům patří a které původce vede v eSSL. Při vytváření SIP balíčku pro skartační řízení může původce využít validátor SIP, který kontroluje správnost formátů nahraných dokumentů. Tento validátor ovšem nepředstavuje žádnou formu certifikace, jedná se pouze o kontrolní pomůcku původce.¹⁰⁶ Pokud je SIP balíček označen za nevalidní, nebude ve skartačním řízení zpracován a původce ho bude muset vymazat a nahradit validním balíčkem.

Metadata obsažené v SIP balíčku popisují souvislosti, obsah a strukturu dokumentů a jejich správu v průběhu času. Můžeme rozdělit do tří hlavních skupin: popisná, konzervační a strukturální. Popisná metadata slouží převážně pro vyjádření obsahu dokumentu v rámci jeho životního cyklu (název původce, typ, kategorie atd.). Klíčová je pro tato metadata fáze příjmu, protože pokud nebudou některá z nich zachycena je skoro nemožné je později doplnit. Konverzační uchovává informace o formátu souboru, o případných změnách s digitálním obsahem, o migracích dokumentu...atd. Strukturální metadata slouží pro sdružení všech částí informačního balíčku do jednoho celku. Ukazují, jak spolu jednotlivé součásti dokumentu souvisí. Problém nastává při absenci metadat. Pokud jejich doplnění není možné, původce nemůže tyto dokumenty založit do SIP balíčku, a tudíž je nemůže zahrnout do skartačního řízení.¹⁰⁷

Vzhledem k tomu, že archivace digitálních dokumentů je oproti archivaci dokumentů analogových, pořád málo propracovaným tématem, zejména kvůli neustálým změnám

¹⁰⁴ § 46 odst. 3 zákona č. 499/2004 Sb., o archivnictví a spisové službě

¹⁰⁵ Informace pro veřejnoprávní původce In: <https://www.nacr.cz/wp-content/uploads/2019/01/vyber.pdf> [1. 8. 2022]

¹⁰⁶ Validátor SIP In: <https://validatorsip.nacr.cz> [1. 8. 2022]

¹⁰⁷ Národní digitální archiv: Technické řešení

In: <https://www.nacr.cz/vyzkum-publikace-akce/vyzkum/projekty/nda> [1. 8. 2022]

v technologii, byl vytvořen projekt Národního digitálního archivu (NDA). Jeho primárním účelem je oblast Digitalizace datových fondů a jejich archivace. Zavedení tohoto projektu přineslo řadu výhod pro původce, zejména možnost dlouhodobého uložení jejich digitálních archiválií bez toho aby byla ohrožena jejich důvěryhodnost. Dále to vylepšilo a zjednodušilo bádání i pro badatele, již preferují dálkový přístup, ať už ze zdravotních, dopravních nebo jiných důvodů. Pozitiva to přineslo i veřejným archivům, jako jsou například archivy vysokých škol.

Digitální archiv si můžou zřídit i jiné instituce a to zřizovatelé akreditovaných archivů podle §60a zákona č. 499/2004 Sb. Jako pomůcka pro postup a náležitosti k podání žádosti se používá Metodický návod č. 2/2018, *pro akreditaci digitálního archivu* vydaným Ministerstvem vnitra, který pracuje s ustanoveními v archivním zákoně. Žádost o digitální archiv musí kromě obecných náležitostí obsahovat:

- a) název a adresu sídla archivu a adresy míst staveb, ve kterých budou umístěna úložiště archiválií v digitální podobě
- b) podklady pro rozhodnutí, zda archiv splňuje podmínky stanovené v §61 odst. 2 a 4
- c) popis způsobu uložení archiválií v digitální podobě
- d) koncepci dlouhodobého uchovávání a ochrany dokumentů určených pro předávání do digitálního archivu,
- e) identifikaci ukládaných archiválií v digitální podobě
- f) seznam metadat týkajících se popisu archiválií v digitální podobě, popisu a evidence archivních souborů a popisu původců
- g) návrh provozního řádu digitálního archivu
- h) potvrzení Národního archivu o úspěšném provedení zkušebního přesunu archiválií v digitální podobě do Národního archivu.

Žádost následně posoudí Ministerstvo vnitra a Národní archiv, jež posuzuje hlavně technickou způsobilost zřizovatele pro ukládání digitálních dokumentů.¹⁰⁸

Dále se posuzuje i celkové fungování organizace, a jestli je vůbec schopná dlouhodobě plnit odpovědnost za dlouhodobé ukládání digitálních dokumentů. Vedení digitálního archivu může být finančně a technicky náročné, proto je dle mého názoru správné, že žádost posuzuje Národní archiv, který dokáže poznat, zda instituce splňuje všechny podmínky.

Ani v dnešní době nemá každá instituce technologické podmínky na dlouhodobé uchovávání svých digitálních dokumentů. S pomocí zákonem zřízeného Národního digitálního archivu se tento problém alespoň částečně dokázalo vyřešit. Ano pořád se vyskytují výhrady hlavně u zobrazování digitálních archiválií, na stránkách Národního archivního portálu. Nicméně pokud vezmeme v úvahu nápor digitalizace, který Národní archiv v posledních letech zažívá, pořád jde o dobře fungující projekt, jenž se do budoucna bude jistě technologicky a organizačně vyvíjet.

¹⁰⁸ § 60a zákona č. 499/2004 Sb., o archivnictví a spisové službě

5. Ukládání digitálních dokumentů v Úřadu MČ

Praha 15

Úřad městské části Praha 15, je jedním z veřejnoprávních původců uvedených v § 3 v zákoně č. 499/2004 Sb., *o archivnictví a spisové službě*. A jako takový musí splňovat legislativní požadavky pro ukládání dokumentů, ať už v jakékoliv formě. Tato část mé bakalářské práce se bude proto zabývat analýzou postupu Úřadu MČ Praha 15 při příjmu, evidenci a nakonec následného ukládání analogových a digitálních dokumentů v rámci jejich spisové služby. Zaměřím se i na analogové dokumenty hlavně z důvodu porovnání. Kromě analýzy se soustředím i na posouzení zda se jejich spisový řád dostatečně zabývá péčí o digitální dokumenty a zda vyhovuje současné legislativě.

Jak bylo již zmíněno Úřad městské části Prahy 15 je veřejnoprávním původcem, a z toho důvodu je povinen vést spisovou službu v elektronické podobě v elektronickém systému spisové služby. Za výkon spisové služby úřadu zodpovídá tajemník, nebo případně jeho stanovený zástupce.

Nakládání s dokumenty v Úřadu MČ Praha 15 je upraveno jeho organizační směrnicí č.j. ÚMČ P15 29985/2018, dále označovanou jako „*Spisový a skartační plán ÚMČ Praha 15*“. Při zpracování praktické části, bude pracovat nejen s ním, ale i se zkušenostmi, které jsem v průběhu své odborné stáže v ÚMČ Praha 15 získala.

Příjem dokumentů v Úřadě městské části Praha 15, podobně jako u jiných veřejnoprávních původců, začíná v centrální podatelně, která se nachází v přízemí úřadu. Zde jsou přijímány veškeré zásilky, které jsou úřadu adresovány.

Analogové dokumenty jsou ÚMČ Praha 15 doručovány pracovníkem České pošty s.p. v centrální podatelně. V případě, že jsou zásilky nevyplacené nebo poškozené, budou vyzvedávány individuálně pracovníkem centrální podatelny na pobočce České pošty s. p. Doporučené zásilky jsou předávány proti podpisu.

V případě, že je dokument doručen fyzickou osobou přijímá ho buď centrální podatelna původce, nebo zaměstnanec příslušného odboru. V obou případech může zažádat o potvrzení příjmu, kdy mu zaměstnanec kopii dokumentu označí otiskem podacího razítka původce s uvedením data převzetí dokumentu. Na vyžádání bude kopie opatřena i číslem jednacím, po kterým je dokument v eSSL evidován. Analogový dokument může být také přijatý, mimo budou zaměstnancem původce, který ho neprodleně musí předat do centrální podatelny k zaevidování. Pokud se jedná o ústné podání, věcně příslušný zaměstnanec o tom sepiše pořídí záznam a ten následně předá do centrální podatelny k zaevidování. I zde může doručující osoba požádat o potvrzení doručení dokumentu. V obou zmíněných případech podání mimo centrální podatelnu je čas doručení dokumentu, okamžik kdy je dokument předán do centrální podatelny a zaevidován do eSSL.

Jestli nastane případ, že je analogový dokument neúplný nebo poškozený, tak že jej nelze uživatelsky vnímatelným způsobem zobrazit a současně z něj určit kdo jej odeslal, centrální podatelna dokument nezpracovává.

Obchodní balík od Ministerstva vnitra ČR obsahující občanské průkazy, cestovní doklady a související dokumenty přebírá pověřený zaměstnanec OOSA (oddělení osobních dokladů a evidence obyvatel), který je po rozřídění zaeviduje do eSSL.

Následně jsou všechny analogové dokumenty označeny štítkem s čárovým kódem vygenerovaným z e-spisu nebo otiskem podacího razítka, jež obsahují: název původce, datum

doručení dokumentu, číslo jednací nebo evidenční číslo ze samostatné evidence, počet listů dokumentu, počet listinných příloh a počet listů příloh, počet a druh dokumentů v nelistinné podobě.

Pokud bude analogový dokument konvertován, připojí se k jeho digitálnímu výstupu doložka automaticky. Tato konverze se provádí kontaktním místě veřejné správy Czech POINT.

Dle mého názoru jde o kvalitně zpracovanou část spisového řádu o příjmu analogových dokumentů. Původce zde pracuje s platnou legislativou a postupy jsou zde dostatečně popsány. Pokud bych jí měla porovnat s následujícím přijímáním digitálních dokumentů, přijde mi lépe zpracovaná a více rozsáhlá.

Příjem **digitálních dokumentů** se uskutečňuje buď přes datové schránky, nebo na přenosném nosiči. Příjem pomocí systému datových schránek provádí centrální podatelna, která se řídí provozním řádem informačního systému datových schránek, který vydává MV ČR. Digitální dokumenty dále mohou být doručeny i na zveřejněných adresách elektronické podatelny ÚMČ Praha 15: podatelna@praha15.cz nebo podatelna@p15.mepnet.cz.

V následní části se již spisový řád příjmem dokumentů skrz datové schránky nezabývá. Zákon č. 300/2008 Sb. přitom uvádí, že „dokument, který byl dodán do datové schránky, je doručen okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k dodanému dokumentu.“¹⁰⁹ Což je pro příjem digitálních dokumentů z právního hlediska dost podstatná informace. Také zde není uvedeno, jak s těmito zprávami nakládá zaměstnanec centrální podatelny a jestli má vůbec nějaké pravomoce. Dle mého názoru je v tomto ohledu spisový řád zbytečně stručný, a do budoucna by se měla jeho pozornost na toto téma zaměřit.

Dále podle spisového řádu centrální podatelna u datové zprávy (e-mailů) zjišťuje, zda datová zpráva a dokument odpovídají požadavkům ÚMČ Praha 15. Tyto požadavky nejsou přímo ustanoveny ve spisovém řádu, pouze se odkazuje na webové stránky úřadu www.praha15.cz. Zde jsou uvedeny typy datových formátů pro digitální dokumenty nebo přehled datových nosičů, které jsou centrální podatelnou akceptovány. Tento postup je v souladu s § 2 píš. f) odst. 3 vyhlášky 259/2012 Sb., kde je stanoveno: „veřejnoprávní původce s výjimkou veřejnoprávního původce, u něhož to neumožňuje zvláštní povaha jeho působnosti, zveřejní na své úřední desce, a nezřizuje-li ji, na svých internetových stránkách, informace o provozu podatelny a o podmínkách přijímání dokumentů s tím, že alespoň uvede f) přehled dalších datových formátů dokumentů obsažených v datové zprávě, ve kterých veřejnoprávní původce přijímá dokumenty v digitální podobě, včetně jejich technických, popřípadě jiných parametrů“.¹¹⁰

Následně se v podatelně provádí kontrola, zda je datová zpráva a dokument v ní v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru a elektronických transakcích. Což znamená ověření platnosti uznávaného nebo kvalifikovaného elektronického podpisu, uznávané nebo kvalifikované elektronické pečeti nebo kvalifikovaného časového razítka.

V případě že byl, při kontrole centrální podatelnou zjištěn škodlivý kód, musí být odesílatel informován a vyzván, aby vadu odstranil. Podatelna vede evidenci všech odmítnutých dokumentů v e-spisu pod kolonkou „počet vyřazených podání“. Samozřejmě i zde se původce řídí pravidlem, že pokud se škodlivý kód nepodaří ve spolupráci s odesílatelem odstranit, centrální podatelna digitální dokument nezpracovává. V případě že neobsahuje žádný škodlivý

¹⁰⁹ § 17 odst. 3 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi

¹¹⁰ § 2 píš. f) odst. 3 vyhlášky 259/2012 Sb., o podrobnostech výkonu spisové služby

kód, bude digitální dokument v nezměněné podobě uložen v úložišti doručených datových zpráv.

Pokud je ÚMČ Praha 15 doručen digitální dokument fyzickou osobou na přenosném nosiči (CD, USB...atd.), zaměstnanec podatelny převeden dokument z přenosného nosiče na elektronickou podatelnu a přenosný nosič buď vrátí fyzické osobě, nebo se stane součástí spisu jako příloha. Fyzické osobě bude následně vystaveno potvrzení o doručení dokumentu. Digitální dokumenty na přenosných nosičích přijímají i zaměstnanci na pracovištích Czech POINT při konverzi dokumentů na žádost. Pokud by byl digitální dokument na přenosném nosiči doručen jinému zaměstnanci, musí být i tak přijat přes centrální podatelnu.

Po přijetí digitálního dokumentu musí obsluha podatelny zajistit, aby byl dokument zaevidován do elektronického systému spisové služby (e-spisu) a předán příslušnému zaměstnanci nebo ho rovnou předá příslušnému zaměstnanci k zaevidování do evidence dokumentů. Všechny doručené dokumenty v digitální podobě, které byly ÚMČ Praha 15 doručeny nebo vznikly v rámci výkonu jeho činnosti se prostřednictvím eSSL označí a spojí s jednoznačným identifikátorem.

Pokud nastane situace, kde doručený digitální dokument není ve výstupním datovém formátu, bude po označení do něj převeden. Autorizovaná konverze je prováděna dle zákona č. 300/2008 Sb. Je prováděna na žádost fyzických nebo právnických osob na kontaktních místech veřejné správy (Czech POINT), nebo pro potřebu veřejnoprávního původce prostřednictvím CzechPOINT@office. Po převedení je k dokumentu rovněž připojena doložka.

Spisový řád ÚMČ Praha 15 dle mého názoru splňuje všechny legislativní požadavky pro příjem digitálních dokumentů ustanovené jak ve vyhlášce 259/2012 Sb. tak v zákoně č. 499/2004 Sb., *o archivnictví a spisové službě*. Má jediná výhrada se týká datových schránek. I přesto, že se přímo odkazuje na provozní řád datových schránek vydávaným Ministerstvem vnitra ČR, jsou datové schránky velmi důležitou součástí životního cyklu digitálních dokumentů, a proto by měly být zpracovány ve spisovém řádu obsáhleji. Zejména, když vezmeme v úvahu, že od roku 2023 budou datové schránky, pro některé občany povinné (př. podnikatelé).

Evidence dokumentů ÚMČ Praha 15 se provádí v základní evidenční pomůcce spisové služby ÚMČ Praha 15. Tím je jeho systém eSSL neboli e-spis. Jak již bylo výše uvedeno po doručení, je dokument zaevidován do e-spisu a spojen s jednoznačným identifikátorem. Poté je dokument označen číslem jednacím, které obsahuje vždy zkratku označení původce, pořadové číslo zápisu dokumentu, lomeno čtyřčíslicím kalendářního roku.

E-spis vede o každém dokumentu ÚMČ Praha 15 následující údaje:

„a) pořadové číslo dokumentu, pod nímž je evidován v evidenci dokumentu (dále jen pořadové číslo), b) datum doručení dokumentu nebo datum vytvoření dokumentu veřejnoprávním původcem c) údaje o odesílateli v rozsahu údajů stanoveném pro vedení údajů o odesílateli dokumentu ve jmenném rejstříku; jde-li o dokument vytvořený veřejnoprávním původcem, uvede se slovo „Vlastní“, d) identifikace dokumentu z evidence dokumentů odesílatele, je-li jí dokument označen, e) ...u dokumentů v digitální podobě počet příloh, f) stručný obsah dokumentu (předmět, věc), g) označení odboru původce, kterému byl dokument přidělen k vyřízení; pokud je určena k vyřízení dokumentu fyzická osoba, uvede současně její jméno, popřípadě jména, a příjmení h) způsob vyřízení, údaje o adresátovi v rozsahu údajů stanoveném pro vedení údajů o adresátovi dokumentu v jmenném rejstříku, datum odeslání, ...u dokumentů v digitální podobě počet příloh, ch) spisový znak a skartační režim...,i) jednoznačný identifikátor dokumentu, j) informace o tom zda je dokument v digitální nebo v analogové podobě, k) záznam o provedení výběru archiválií, l) identifikátor o dokumentu uloženého

v *digitálním archivu*.¹¹¹ Toto ustanovení je v přímé souvislosti s § 10 vyhlášky č. 259/2012 Sb.

Evidenci také nepodléhají analogové a digitální dokumenty, které nemají úřední charakter.

Část evidence dokumentu rovněž hodnotím kladně. Dle mého je zde uvedeno vše potřebné a nic bych neměnila.

K **vyhotovování dokumentů** používají zaměstnanci úřadu jednotný hlavičkový papír s předtištěnými údaji. V záhlaví je vždy uvedeno číslo jednacích odesílatele, vlastní číslo jednacích, spisová značka, telefon, fax, jméno a příjmení vyřizujícího, email datum vyhotovení, přesná a úplná adresa adresáta. Dále se uvádí i počet příloh a počet listů příloh u analogového dokumentu. V případě, že se vyhotovený dokument bude doručovat v digitální podobě, vyhotoví pověřená úřední osoba, odpovědná za analogové vyhotovení rozhodnutí jeho elektronickou verzi s tím, že na místě otisku úředního razítka vyjádří tuto skutečnost slovy „otisk úředního razítka“. Oprávněná osoba následně připojí k dokumentu kvalifikovaný elektronický podpis a kvalifikované časové razítko a převede ho do výstupního datového formátu. Zaměstnanec, jemuž byl dokument přidělen k vyřízení, rozhodne o jeho finální podobě.

Oprávnění k **podepisování dokumentů** upravuje podpisový řád ÚMČ Praha 15. Případně může být zaměstnanci přiděleno jednotlivé zmocnění k podepisování dokumentů. Jak již bylo zmíněno, dokument v digitální podobě podepisuje oprávněný zaměstnanec, jenž k němu připojí kvalifikovaný elektronický podpis a kvalifikované časové razítko. Pokud nastane případ, že je dokument podepsán dvěma podpisy, bude podpis osoby s vyšší funkcí umístěn vpravo.

Po vyřízení a uzavření jsou **analogové spisy a dokumenty** přemístěny do centrální spisovny, která je umístěna v přízemí budovy ÚMČ Praha 15. Zde budou uloženy až do vypršení jejich skartačních lhůt a zařazení do skartačního řízení. Před předáním do spisovny musí být spisy a dokumenty zkontrolovány, který je vyřizoval a uzavřel. Kontrola se zaměřuje na úplnost spisů a dokumentů, které by správně měli obsahovat tyto atributy: 1. označení podacím razítkem a plnost jeho vyplnění, 2. označení JID, 3. kompletnost spisu, 4. počet listů dokumentu, počet příloh a počet listů příloh, 5. celkový počet listů spisu (případně počet svazků), 6. převedení dokumentu v digitální podobě do výstupního datového formátu, 7. uvedení spisového skartačního znaku a skartačního režimu, 8. zápis v evidenci dokumentů a jeho úplnost (podle evidence), 9. uložení dokumentů a spisů v obalech. V případě smíšených spisů je analogová část uložena v centrální spisovně a digitální část v digitální spisovně.

Pokud zaměstnanec spisovny, při kontrole najde ve spisech ztráty nebo nesrovnalosti, požádá pověřeného zaměstnance daného oddělení, aby dodal protokoly o ztrátách, nebo nesrovnalosti opravil.

Průběhu skartačního řízení jsou analogové spisy a dokumenty posuzovány na základě jejich spisového znaku. Všechny spisy a dokumenty pověřený zaměstnanec uspořádá do skartačního návrhu, který předloží správnímu archivu. Spisy a dokumenty, které byly ve skartačním řízení vybrány za archiválie, budou předány správnímu archivu k uložení. O tomto procesu se budu věnovat i u digitálních dokumentů.

Ukládání analogových dokumentů v ÚMČ Praha 15 je ve spisovém řádě zpracováno kvalitně a legislativně správně. Je tu dostatečně upravená kontrola i proces skartačního řízení. Pokud bych tuto část měla porovnat s digitální, je rozhodně i více obsáhlá.

¹¹¹ Spisový řád ÚMČ Praha 15, VII. Evidence dokumentů str. 13

Ukládání digitálních dokumentů ÚMČ Praha 15 je ve spisovém řádě rovněž velmi stručně zpracované téma. Jak již bylo výše zmíněno, digitální dokumenty se ukládají v digitální spisovně (e-spis) a dále se tam předávají k uložení. Před vyřízením digitálního dokumentu a uzavřením spisu se provede kontrola jeho digitální podoby. Jedná se o kontrolu datových formátů na základě § 23 vyhlášky č. 259/2012 Sb. Dále se provádí kontrola úplnosti, kterou má na starosti zaměstnanec, jež dokument nebo spis vyřizoval a uzavřel.

Zaměstnanec spisovny, který při kontrole najde ve spisech ztráty nebo nesrovnalosti, požádá pověřeného zaměstnance daného oddělení, aby dodal protokoly o ztrátách, nebo nesrovnalosti opravil. Až poté jsou spisy uloženy do centrální spisovny.

Část skartačního řízení je také málo obsáhlá, hlavně pro oblast digitálních dokumentů. Základní požadavky ale splněny jsou. Přípravu skartačního řízení má na starost, vždy příslušný zaměstnanec centrální spisovny. Ten uspořádá dokumenty s uplynulými skartačními lhůtami navrženým navrženými do skartačního řízení do přehledných jednotek.

Vůbec se zde nepracuje s požadavky Národního standardu. Zejména s požadavkem 3.1.34., který upravuje sjednocení skartačních znaků dokumentů ve spise a to nejpozději k datu uzavření tohoto spisu. Není zde upraven výběr digitálních archiválií a povinnost původce předání jejich replik a metadat příslušnému správnému archivu. Dále se spisový řád vůbec nezmiňuje o SIP balíčcích a jejich náležitostech, ve kterých tyto repliky a metadata mají být shromážděny. Přitom je tento postup uvedený ve vyhlášce 259/2012 Sb. a také i v požadavcích Národním standardu. Dle mého názoru je to zásadní informace, která by měla být ve spisovém řádu uvedena.

Po předchozí analýze je možné tvrdit, že spisový řád ÚMČ Praha 15 není v rámci tématu digitálních dokumentů a jejich ukládání obsáhlý. I přesto myslím, že základní legislativní požadavky splnění jsou. Z mého pohledu je kvalitně zpracován jak příjem, tak i evidence dokumentů. Otázkou ale zůstává, jestli tato podoba bude dostačující i za pár let. Velmi mě překvapilo nedostatečné zaměření na datové schránky, zejména když počet jejich uživatelů dále narůstá. Přitom někteří veřejnoprávní původci jím ve svém spisovém řádě poskytují větší prostor, jako například spisový řád Ministerstva spravedlnosti ČR. V jeho znění je přímo upraveno přijímání dokumentů přes datovou schránku i její používání. Myslím, že vzhledem k předpokládanému rozšíření datových schránek v roce 2023 u podnikajících osob, je jejich propracovanější úprava potřebná.

Část ukládání digitálních dokumentů nebo jejich skartační řízení shledávám až přehnaně stručné a nedostačující. Požadavky zde skoro nejsou uvedené, až na zmínku o kontrole před předáním do centrální spisovny. Také bych čekala využití Národního standardu a ustanovení o SIP balíčcích a o předávání digitálních archiválií.

Zastávám stanovisko, že by se ÚMČ Praha 15 měl ve svém spisovém řádu tématu digitálních dokumentů více zabývat a lépe zpracovat jejich úpravu. I přesto, že nevíme, jak budoucnost bude za pár let vypadat, rozhodně můžeme říct, že technologický pokrok bude pokračovat dál, a rozhodně bude vyžadovat i více propracovanou úpravu vnitřních norem původce.

Shrnutí

I přesto, že téma ukládání digitálních dokumentů a jejich následná archivace v České republice, je poměrně stále nové a neustále se tato oblast rozšiřuje, lze konstatovat, že legislativní stránka v tomto ohledu je dostačující. Úprava zákona č. 499/2004 Sb., o archivnictví a spisové službě a vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, se dá určitě hodnotit kladně. Jsou přehledné a v mnohém usnadnily a sjednotily tvorbu spisových řádů, u veřejnoprávních původců. Pozitivní vliv na organizaci spisové služby přinesl i Národní standard pro eSSL, který v mnohém pomohl urychlit a zjednodušit zavedení elektronické spisové služby u původců.

Jediný problém vidí v roztržitosti této legislativy. Spisovou službu a digitální dokumenty obecně upravuje mnoho právních norem různé právní síly. Při psaní této bakalářské práce mi to přišlo chvílemi matoucí a myslím, že pro výkon spisové služby u původců by to mohlo způsobit problémy při vytváření spisového řádu.

Dále myslím, že někteří původci, nepřistupují k digitálním dokumentům a k otázce jejich ukládání se stejnou vážností, jakou přikládají analogovým dokumentům. Například jak tomu bylo u spisového řádu ÚMČ Praha 15, kde bylo téma digitálních dokumentů jen velmi málo zpracované. Samozřejmě to může být i způsobené tím, že elektronická spisová služba a digitální dokumenty jsou po původce pořád poměrně nová záležitost, zejména když vezmeme v úvahu, že výkon spisové služby byl po staletí zaměřený pouze na fyzické dokumenty. Jistý vliv na tuto problematiku má i technická oblast, která samozřejmě s digitálními dokumenty úzce souvisí, a ve které se i v současnosti opravdu vyzná jen malá skupina lidí.

Nicméně zastávám stanovisko, že i přes výskyt jistých nedostatků si spisová služba v ukládání digitálních dokumentů v České republice vede dobře a i systém kontroly je dostačující. Také se myslím, že se původci rychle adaptovali na výkon spisové služby v elektronické podobě.

Ať jsou názory na toto téma jakékoliv, využívání digitálních dokumentů bude jistě jen narůstat. Z toho důvodu by jim původci měli věnovat více pozornosti.

Závěr

Uchovávání dokumentů pro jejich pozdější využití je od nepaměti znakem lidské civilizace. Vhodný a bezpečný způsob ukládání těchto dokumentů je klíčový pro zamezení ztráty nebo poškození informací z těchto dokumentů. V současnosti se situace ohledně správy a ukládání dokumentů radikálně liší, a to zejména kvůli pokroku v odvětví informačních technologií a jejich neustále rostoucího vlivu. Nyní je lidstvo schopno vytvářet, uchovávat a zpřístupňovat nesčetné množství dokumentů a informací. Nicméně i tyto dokumenty je potřeba uchovávat se stejnou pečlivostí a z toho důvodu je důležité nacházet efektivní a bezpečné způsoby jejich ukládání.

Při psaní této práce jsem došla k závěru, že téma ukládání digitálních dokumentů je velmi složité a rozsáhlé téma, které se jistě do budoucna bude dále vyvíjet. Prolínají se zde otázky jak technické, tak i právní. Zejména technický aspekt má velký vliv na tvorbu legislativy. Nemyslím jen nedostatečné znalosti pracovníků nebo nedostatek IT pracovníků v pracovní sféře, ale i každodenní využívání technologií v běžném životě, které zvyšuje možné riziko neoprávněného zásahu nebo ztrátu dat.

Samozřejmě je ale zřejmé, že jsou si tvůrci legislativy v ČR a i na úrovni EU, těchto problémů vědomi a snaží jím předcházet. Na území ČR je dle mého názoru legislativní úprava ukládání digitálních dokumentů a zabezpečení jejich právní validity, zpracována velmi kvalitně a dostatečně. Rozhodně za klíčové pro úpravu považuji zákon 499/2004 Sb. a vyhlášku 259/2012 Sb. Dále velmi užitečným pokládám Národní standard vydaný Ministerstvem vnitra, který rozhodně usnadnil a urychlil zavedení systémů elektronické spisové služby v ČR. Pokud bych ale měla právní úpravě něco vytknout, byla by to roztržitost této úpravy do více právních předpisů s různou právní silou. Myslím, že je to pro výkon spisové služby matoucí, především když vezmeme v úvahu, že technologický pokrok vyžaduje i nové aktualizace a vydání nových právních předpisů.

Potřeba řádného způsobu ukládání digitálních dokumentů, bude do budoucna však pořád aktuálnější, zejména z důvodu neustále stoupajícímu počtu vytváření tohoto typu dokumentu, jak veřejnoprávními původci, tak i soukromoprávními. Do budoucna se také dá předpokládat mnohem širší využití datových schránek, což znamená další nejen další nárůst tohoto počtu, ale i potřebu zachování právní validity těchto dokumentů.

Důležité je i řádný výběr digitálních archiválií a jejich uložení a přístup k nim. Období pandemie nám ukázalo, jak důležitý může být dálkový přístup k informacím. Dle mého názoru, v tomto ohledu postupuje Národní archiv správným směrem, i přesto že lze ještě mnohé zlepšit. Nicméně chápu, že proces digitalizace nebo i neustálá snaha držet krok s technologickým pokrokem je v této oblasti velmi náročná.

Ohledně mé praktické části této práce musím konstatovat, že spisový řád ÚMČ Praha 15 neupravuje digitální dokumenty a jejich ukládání s dostatečnou vážností, s jakou se zaměřuje na dokumenty analogové. Na druhou stranu byl zpracován v roce 2018, což znamená, že pracuje s aktuální legislativou nebo na ni ve svém obsahu odkazuje.

Dále je zde velmi dobře zpracované téma právní validity digitálních dokumentů, což je dle mého názoru pro výkon ÚMČ Praha 15 jako veřejnoprávního původce zásadní. A však když vezmeme v úvahu, že ÚMČ Praha 15 je veřejnoprávního původce, měl by jako takový brát svou úlohu ve výkonu spisové služby a ukládání dokumentů s větší pečlivostí.

Jsem si ale vědoma, že to není pouze problém ÚMČ Praha 15, a jistě se najdou i jiné instituce, jak veřejnoprávní tak soukromoprávní, které se nacházejí v podobné nebo i v žalostnější situaci.

Do budoucna ale rozhodně můžeme počítat s pořád víc narůstajícím vlivem technologií a to jak v každodenním životě, tak i ve státní správě a samosprávě. Svět digitálních dokumentů se proto nikdy nepřestane proměňovat a společně s nimi i náš přístup k nim.

Zdroje

Monografie

- 1) KUNT, M. – LECHNER, T. *Spisová služba*. Praha: Leges, 2015. ISBN 978-80-7502-083-3
- 2) LECHNER, T. *Elektronické dokumenty v právní praxi*. Praha: Leges, 2015. ISBN 978-80-87576-41-0
- 3) PETERKA, J. *Báječný svět elektronického podpisu*. Praha: CZNIC, 2011. CZNIC. ISBN 978-80-904248-3-8.

Internetové zdroje

- 1) ŠLAPÁK, O. *Data, informace, znalosti*. E-LOGOS (Electronic journal for philosophy) 2003 [online] roč. 10, [cit. 27. 5. 2022]
Dostupné z : <https://e-logos.vse.cz/pdfs/elg/2003/01/11.pdf>
- 2) Datový trezor [cit. 1. 8. 2022]
Dostupné z : <https://www.datoveschranky.info/aditivni-sluzby/datovy-trezor>
- 3) *PNG-dokonalý formát na pro přenos obrazových dat* [cit. 10. 7. 2022]
Dostupné z : <https://www.interval.cz/clanky/png-dokonalý-format-pro-prenos-obrazovych-dat/>
- 4) Soubory GIF [cit. 1. 8. 2022]
Dostupné z : <https://www.adobe.com/cz/creativecloud/file-types/image/raster/gif-file.html>
- 5) Informace pro veřejnoprávní původce [cit. 1. 8. 2022]
Dostupné z : <https://www.nacr.cz/wp-content/uploads/2019/01/vyber.pdf>
- 6) Validátor SIP [cit. 1. 8. 2022]
Dostupné z : <https://validatorsip.nacr.cz>
- 7) Národní digitální archiv: Technické řešení [cit. 1. 8. 2022]
Dostupné z : <https://www.nacr.cz/vyzkum-publikace-akce/vyzkum/projekty/nda>

Právní předpisy

- 1) Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
- 2) Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi
- 3) Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

- 4) Zákon č. 250/2017 Sb., o elektronické identifikaci
- 5) Zákon č. 500/2004 Sb., správní řád
- 6) Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
- 7) Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů
- 8) Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek
- 9) Národní standard pro elektronické systémy spisové služby, zveřejněný Oznámením Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby ze dne 4. 7. 2017, č. j. MV-33371- 16/AS-2017
- 10) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- 11) Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů