SBORNÍK KONFERENCE

2019

isSS

1.–2. dubna 2019 Hradec Králové
22. ročník konference
Doprovodná mezinárodní konference V4DIS

isSS
LOCAL AND REGIONAL INFORMATION SOCIETY
V4DIS

S podporou města Hradec Králové

CALENDARIUM REGINA

generální partner

hlavní partneři

Vydáno u příležitosti 22. ročníku konference ISSS

ZÁŠTITU KONFERENCÍM POSKYTLI

Andrej Babiš, předseda vlády České republiky
Jan Hamáček, 1. místopředseda vlády a ministr vnitra
Klára Dostálová, ministryně pro místní rozvoj
Vladimír Dzurilla, vládní zmocněnec pro IT a digitalizaci
Asociace krajů České republiky
Jiří Běhounek, hejtman Kraje Vysočina, předseda IT komise AKČR

OBSAH

NAŘÍZENÍ EIDAS ANEB VELKÉ ZMĚNY V OBLASTI ELEKTRONICKÉ KOMUNIKACE

Mgr. Adéla Bušová, vedoucí právního týmu a trvale spolupracující advokátka v CÍSAŘ, ČEŠKA, SMUTNÝ s.r.o., advokátní kancelář

Uplynuly již více než dva roky od nabytí účinnosti nařízení Evropského parlamentu a Rady (EU) 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, zkráceně nazývaného nařízení eIDAS (dále jen „**Nařízení**“).

Cílem Nařízení je především vytvoření nového fungujícího systému pro bezpečnou elektronickou komunikaci mezi podniky, občany a orgány veřejné moci v Evropské unii, odstranění stávajících překážek přeshraničního využívání prostředků pro elektronickou identifikaci, prohloubení důvěry v elektronické transakce v celé Evropské unii a zvýšení efektivnosti veřejných a soukromých on-line služeb a elektronického obchodu. Toho chce Nařízení docílit pomocí stanovení podmínek uznávání prostředků elektronické identifikace, pravidel pro služby vytvářející důvěru a právního rámce pro elektronické podpisy, pečetě, časová razítka apod.

V době vstupu Nařízení v platnost již v České republice existovala samostatná vnitrostátní úprava, která danou problematiku upravovala odlišně. Jednalo se zejména o zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (dále jen „**Zákon o elektronickém podpisu**“), který tak musel být z důvodu přijetí Nařízení zrušen. Za účelem řádné implementace Nařízení do vnitrostátních právních předpisů, pak byla odložena účinnost některých ustanovení Nařízení. V této přechodné době zákonodárce přijal komplexní legislativní balíček, kterým se upravují jednotlivé povinnosti vyplývající z Nařízení.

Jedná se zejména o tzv. adaptační zákon, neboli zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (dále jen „**Zákon o službách vytvářejících důvěru**“), který upravuje obecná pravidla používání elektronických podpisů, elektronických pečetí a elektronických časových razítek v České republice a právě jímž byl zrušen Zákon o elektronickém podpisu. Přijat byl rovněž zákon č. 250/2017 Sb., o elektronické identifikaci (dále jen „**Zákon o elektronické identifikaci**“), jenž upravuje elektronickou identifikaci a používání občanských průkazů pro účely přístupu k on-line službám kvalifikovaných poskytovatelů. Třetím přijatým zákonem[1] došlo k novelizaci dalších více než 60 právních předpisů, jichž se Nařízení dotýká, jedná se např. zákon o občanských průkazech, zákon o archivnictví a spisové službě, a další. Shora uvedený výčet právních předpisů, kterých se Nařízení dotklo, však rozhodně není možné považovat za konečný.[2]

Předmět úpravy, hlavní změny a nové povinnosti

Centrálním pojmem pro jednotlivé elektronické služby upravované Nařízením jsou tzv. „služby vytvářející důvěru“. Těmi se dle Nařízení rozumí takové elektronické služby, které jsou poskytovány zpravidla za úplatu a které spočívají zejména ve vytváření, uchovávání a ověřování shody a platnosti elektronických podpisů, pečetí, časových razítek aj. Jakýmsi vyšším stupněm služeb vytvářejících důvěru jsou pak tzv. „kvalifikované služby vytvářející důvěru“, jejichž poskytovatelé (kvalifikovaní poskytovatelé

1 Zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

2 Nařízení ve svém textu např. výslovně předpokládá, že se při jeho výkladu a aplikaci bude postupovat mj. v souladu s nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

služeb vytvářejících důvěru), se dobrovolně rozhodli absolvovat certifikační proces a získat tak tento status, se kterým se pojí jisté výhody (jako je např. možnost používání tzv. značky důvěry), na druhé straně však také rozsáhlejší povinnosti.

Účinnost Nařízení je pak spojena s velkým množstvím legislativních změn, které s sebou přináší také celou řadu nových povinností, jež budou mít významné dopady nejen na orgány veřejné moci, ale i na soukromé osoby. Je však třeba v této souvislosti poznamenat, že Nařízení nedopadá na všechny poskytovatele služeb vytvářejících důvěru, neboť se nevztahuje např. na poskytování služeb, které jsou využívány výhradně v rámci uzavřených systémů, mezi určeným okruhem účastníků a bez žádného vlivu na třetí osoby.

Značnou změnu můžeme pozorovat v oblasti elektronických podpisů. Za nejvyšší formu elektronického podpisu považuje Nařízení tzv. **kvalifikovaný elektronický podpis, který má rovnocenný právní účinek jako podpis vlastnoruční**. Vytvoření kvalifikovaného elektronického podpisu vyžaduje použití kvalifikovaného prostředku pro vytváření elektronických podpisů. Požadavky na kvalifikované prostředky pro vytváření elektronických podpisů stanovuje Nařízení v příloze II, přičemž takovým kvalifikovaným prostředkem může být např. čipová karta.

Ode dne 19. 9. 2018 v této souvislosti došlo ke změně stávající praxe elektronického podepisování u všech správních úřadů. Zákon o službách vytvářejících důvěru totiž stanovuje **tzv. veřejnoprávním podepisujícím**[3] **povinnost používat k podpisu kvalifikovaný elektronický podpis**. Díky existenci zaručeného elektronického podpisu u nás před nabytím účinnosti příslušných ustanovení Nařízení existovala dočasná výjimka[4] umožňující nadále namísto kvalifikovaného elektronického podpisu používat zaručený elektronický podpis, který ovšem musel být opatřený certifikátem vydaným kvalifikovaným poskytovatelem služeb vytvářejících důvěru. **Platnost výjimky však skončila k 18. 9. 2018 a od 19. 9. 2018 tedy nastává plná účinnost rozhodných ustanovení Nařízení.** Co se týče právního jednání soukromé osoby vůči veřejnoprávnímu podepisujícímu, lze k podepisování elektronickým podpisem použít pouze uznávaný elektronický podpis, tzn. zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. K jednání mezi osobami soukromého práva plně postačí podpis „prostým" (dle Zákona o službách vytvářejících důvěru tzv. „jiným") elektronickým podpisem. Elektronickému podpisu pak nesmějí být upírány právní účinky pouze z důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy, jak vyplývá z článku 25 Nařízení.

Elektronická pečeť poskytuje důkaz o původu a integritě daného dokumentu. Dle definice Nařízení se jedná o „*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*". Pokud není právním předpisem stanoveno, a ani z povahy právního jednání nevyplývá, že náležitostí právního jednání obsaženého v dokumentu je podpis, má veřejnoprávní podepisující, příp. jiná právnická osoba jednající při výkonu své působnosti, povinnost dokument v elektronické podobě opatřit **kvalifikovanou elektronickou pečetí**. Veřejnoprávním podepisujícím tak lze rozhodně doporučit vyhotovení metodiky či úpravu interních předpisů, které stanoví jasná pravidla pro používání elektronického podpisu a elektronické pečetě.

Časové razítko spojuje datum a čas s daty takovým způsobem, aby bylo přiměřeně zamezeno možnosti nezjistitelně změnit určitá data. Veřejnoprávní podepisující má povinnost opatřovat podepsané či zapečetěné elektronické dokumenty **kvalifikovaným elektronickým časovým razítkem**. Jednou ze změn v této oblasti je pak potřeba se o **elektronické dokumenty aktivně starat. Už tedy nebude postačovat jednou označit dokument časovým razítkem, které bude platné navždy**, ale je třeba **platnost časových razítek kontrolovat a případně dokument tzv. přerazítkovat**, tedy označit novým časovým razítkem.

Na subjekty veřejného sektoru dále dopadá povinnost akceptovat elektronicky podepsané dokumenty. Musí být také schopny **ověřit platnost elektronických podpisů, pečetí a časových razítek** na příchozích dokumentech, ať už byly tyto vydány v České republice nebo v zahraničí.

3 Dle ust. § 5 písm. a) se jedná o stát, územní samosprávný celek, právnickou osobu zřízenou zákonem nebo právnickou osobou zřízenou nebo založenou státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem. Nařízení tyto subjekty označuje jako subjekt veřejného sektoru.

4 Viz. § 19 odst. 1 zákona o službách vytvářejících důvěru.

Nařízení upravuje také oblast **elektronického doporučeného doručování**. U dat odeslaných a přijatých prostřednictvím kvalifikované služby doporučeného doručování platí domněnka integrity dat, jejich odeslání identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnosti data a času odeslání a přijetí.

S Nařízením se také pojí požadavek interoperability. S účinností od **29. 9. 2018** Nařízení zavádí **povinnost subjektů veřejného sektoru členských států rozpoznávat a uznávat elektronické identifikace** (eID) **občanů z jiných členských států Evropské unie**. Od tohoto data tedy musí všechny veřejné služby, které umožňují vzdálenou elektronickou identifikaci, být schopny pracovat s prostředky z oznámených evropských systémů.

Rizika spojená s nesplněním povinností vyplývajících z Nařízení

Je třeba, aby byly Subjekty veřejného sektoru na všechny tyto nové významné změny připraveny, což v praxi představuje především zajištění potřebných technických nástrojů, úpravu informačního systému takovým způsobem, aby byl připraven na příjem elektronických dokumentů a jeho portálové služby byly schopné bezpečně identifikovat a autentizovat uživatele. Nedostatečná příprava na nové povinnosti vyplývající z Nařízení a souvisejících právních předpisů, může značně zkomplikovat činnost subjektů veřejného sektoru.

Za nutnost lze považovat také řádnou právní a organizační přípravu. Hlavním rizikem, které v souvislosti s novými povinnostmi vyvstává, je totiž právě neinformovanost a nepřipravenost zaměstnanců. Subjekt veřejné správy by tak měl zejména dbát na včasnou úpravu vnitřních předpisů a metodických pokynů, řádné informování a zaškolení svých zaměstnanců stran nových povinností a postupů tak, aby byli zaměstnanci připraveni na jejich plnění.

Není-li veřejný subjekt schopen dostát nově účinným povinnostem, vystavuje se riziku, že jím vydávané či podepisované dokumenty budou **neplatné pro nedostatek formy**. Nebude-li subjekt veřejného práva schopen akceptovat elektronické či elektronicky podepsané dokumenty, provést elektronickou identifikaci, či způsobí-li nedodržením svých povinností neplatnost vydávaných či podepisovaných dokumentů, vystavuje se také riziku **soudních sporů**. Kromě zvýšené administrativy a nákladů spojených s opravou a opětovným zasláním neplatných dokumentů hrozí subjektům veřejného práva zejména povinnost **nahradit škodu**, která jinému subjektu vznikla v důsledku porušení jeho povinností, nesprávného úředního postupu či chybně vydaného či podepsaného dokumentu.

Ze všech výše uvedených skutečností jednoznačně vyplývá, že (nejen) veřejná správa čelí celé řadě nových povinností, jejichž plnění by neměla brát na lehkou váhu. V případě, že se subjekt veřejného práva nestihl dosud na účinnost Nařízení a z něj plynoucí povinnosti připravit, měl by tak učinit co nejdříve, aby tak maximálně eliminoval případné negativní následky, v nejzazším případě až způsobení škody dotčeným osobám, plynoucí z nedodržení jeho zákonných povinností.

PROJEKT ELEKTRONICKÝCH VÝZEV K PLATBÁM MÍSTNÍCH POPLATKŮ

Mgr. Milan Čigáš, MěÚ Litoměřice
Mgr. Jan Brychta, Mgr. Tomáš Lechner, Ph.D., TRIADA, spol. s r. o.

Motivace

Oblast výběru místních poplatků je pro každou obec velmi významnou záležitostí, neboť se jedná o nezanedbatelnou část rozpočtových příjmů. A to těch příjmů, které lze navíc, na rozdíl například od daňových příjmů, dopředu poměrně dobře predikovat a hlavně lokálně ovlivňovat vydáváním příslušných místních vyhlášek. Mantinely jsou stanoveny zákonem č. 565/1990 Sb., o místních poplatcích, který výčtem určuje konkrétní možné poplatky, jež obec může vybírat. Kvalita výběru stanovených poplatků závisí na mnoha okolnostech, přičemž mezi časté úvahy zastupitelstev a odpovědných vedoucích pracovníků patří problematika snížení procenta neplatičů. Následné vymáhání nedoplatků, které s ohledem na rovnost přístupů musí obec realizovat, má většinou poměrně nízkou celkovou efektivitu, protože náklady řízení bývají často srovnatelné s vymáhanými částkami, ne-li dokonce vyšší. Proto je dobré hledat cesty, které předcházejí vzniku neplatičů, přičemž jednou z nich je efektivní a cílené rozesílání informací o povinnostech poplatníků.

S rozvojem informační společnosti je jistě vhodné i místní samosprávou využívat co nejvíce informační kanály, na které jsou občané zvyklí ze soukromého sektoru. Dodavatele energií, mobilní operátoři, pojišťovny a další subjekty soukromého sektoru se snaží snižovat náklady a zvyšovat efektivitu komunikace jejím přesunem do elektronické podoby. Veřejná správa má v tomto ohledu složitější situaci, neboť musí mnohem pečlivěji ověřovat adresáty informací a zajišťovat s vyšší mírou jistoty, že se informace dostaly do rukou příslušným osobám. Pravidla ochrany osobních údajů daná GDPR samozřejmě platí pro všechny správce, bez rozdílu, zda se jedná o veřejnou či soukromou instituci, avšak veřejná správa musí k tomu dodržovat další postupy specifikované procesními právními předpisy. V případě obcí jde zejména o správní řád a v případě poplatků zejména o daňový řád.

Z hlediska přesné identifikace konkrétní fyzické osoby v elektronickém světě je bezpochyby nejdůvěryhodnější elektronická identita založená na pravidlech daných nařízením eIDAS a zákonem č. 250/2017 Sb., o elektronické identifikaci, která je v současné podobě (s podmínkou vysoké míry důvěry) implementována v čipu nově vydávaných občasných průkazů. Pokud bychom však spoléhali pouze na tuto cestu identifikace, nabízeli bychom službu v současné době jen pro velmi omezený okruh občanů, což je v rozporu s motivací projektu řešení zvýšení efektivity informovanosti občanů o jejich konkrétní poplatkové povinnosti.

Proto jsme přistoupili k celkové formulaci projektu elektronických výzev k platbám místních poplatků s maximálním využitím stávajících jednoduchých komunikačních kanálů a zároveň s využitím moderních a pro občany jednoduše zpracovávaných informací jako jsou QR kódy. Pokud tímto způsobem lze vhodně nastavit adekvátní vnitřní procesy a otevřít tím též cestu pro využití rozvíjejících se portálových řešení založených na elektronické identifikaci a platebních bran, které mohou postupně sloužit jako další prvky zvyšující efektivitu celkového řešení.

V rámci projektu jsme identifikovali čtyři stěžejní oblasti, které je třeba řešit. Jedná se o:

- nastavení pravidel pro zpracování osobních údajů pro novou službu,
- metodiku sběru kontaktních údajů,
- technické aspekty cíleného rozesílání informací
- a problematiku slučování plateb.

Zpracování osobních údajů

Osobní údaje, které jsou shromažďovány pro stanovení výše poplatkové povinnosti, vycházejí jednak z citovaného zákona o místních poplatcích, a jednak z pravidel stanovených místními vyhláškami. Zřejmě právě proto existuje nejednotnost názorů, zda důvodem pro toto zpracování osobních údajů je splnění právní povinnosti podle čl. 6 odst. 1 písm. c) GDPR, nebo jde o zpracování prováděné při výkonu veřejné moci podle čl. 6 odst. 1 písm. e) GDPR. V každém případě na základě principu „minimalizace údajů" lze pro účely místních poplatků zpracovávat pouze údaje vycházející buď z procesních předpisů vztahujících se k poplatkům (zejména daňový řád), nebo dále specifikovaných vyhláškou, např. informace o zdravotním postižení, které může znamenat snížení sazby daného poplatku. Nelze libovolně přidávat další údaje, aniž by tyto byly podloženy konkrétním důvodem a patřičným opodstatněním.

Pro účely cíleného rozesílání elektronických informací je třeba zpracovávat specifické kontaktní údaje jako e-mailová adresa a popř. též telefonní číslo, které jsou jednoznačně osobními údaji a které nejsou podloženy přímo ani jedním z výše uvedených předpisů. Jsou tedy dvě možnosti, jaký pro jejich zpracování zvolit zákonný důvod:

a) veřejný zájem podle čl. 6 odst. 1 písm. e) GDPR,

b) souhlas se zpracováním osobních údajů podle čl. 6 odst. 1 písm. a) GDPR.

Zvýšení efektivity výběru místních poplatků a snížení nákladů na činnost veřejné správy nahrazením papírové komunikace (např. klasického rozesílání složenek) elektronickými komunikačními kanály, to jsou jistě důvody, které jsou veřejným zájmem, a proto by bylo možné uvedený zákonný důvod zpracování dle bodu a) využít. Avšak je zde jeden problém, a tím je názor, že rozesílání informací e-mailem (byť cíleným konkrétnímu adresátovi) je zveřejněním osobních údajů (pokud jsou v e-mailu uvedeny, nebo k ně mu přiloženy v příloze). A v takovém případě musí správce zajistit přiměřenou míru ochrany, aby nemohlo dojít k neoprávněném přístupu k těmto údajům. V praxi se často využívá různých šifrovacích metod a sdělení hesla adresátovi jiným nezávislým komunikačním kanálem. Tyto metody ale snižují komfort pro cílové osoby a mohly by působit proti cílené efektivitě a poskytnutí užitečné elektronické služby občanům.

Proto se kloníme k názoru, že bude vhodnější využít jako zákonný důvod souhlas se zpracováním osobních údajů, který by byl rozšířen (samozřejmě se zachováním všech principů GDPR) na nešifrované zasílání platebních pokynů a informací o poplatkové povinnosti. Mimochodem, tento postup je používán například i službou eRecept. Aby byla splněna povinnost, že se jedná o souhlas informovaný, musí být jasně uveden především správce osobních údajů, účel zpracování, dále doba, na kterou je souhlas poskytován, způsob odvolání souhlasu a odkaz na webové stránky s kompletními informacemi o zpracování osobních údajů. Je třeba také vyřešit, jakým způsobem bude občan ohlašovat změnu těchto kontaktních údajů.

V každém případě platí, že by toto nové zpracování osobních údajů mělo být před zahájením zpracování posouzeno pověřencem pro ochranu osobních údajů.

Metodika sběru kontaktních údajů

Ideálně ke každému poplatníkovi by bylo třeba přiřadit příslušné kontaktní údaje v podobě e-mailové adresy, resp. telefonního čísla. V případě ohlášení vzniku poplatkové povinnosti mohou být tyto údaje součástí vyplňovaného formuláře, avšak s ohledem na výše identifikovaný důvod zpracování osobních údajů musí být dostatečně odděleny a podloženy samostatným souhlasem, jehož udělení či neudělení nesmí mít žádný vliv na výši poplatkové povinnosti. S ohledem na pravidla ochrany osobních údajů tedy nelze poplatníky, kteří sdělí příslušné údaje, jakkoliv zvýhodňovat vůči těm, kteří souhlas se zpracováním svých osobních údajů neudělí.

Pro uvedení těchto kontaktních údajů z hlediska jejich přiřazení k dané osobě (důvěryhodnosti vazby) platí stejná pravidla, jako pro sdělení doručovací adresy nebo dalších údajů potřebných pro stanovení výše poplatkové povinnosti, jako je třeba prokázání zdravotního postižení. Měly by být tedy nastaveny obdobné komunikační kanály typu podepsaný listinný dokument zaslaný poštou, elektronický dokument podepsaný uznávaným elektronickým podpisem podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, nebo webový portál s využitím ověření identity podle zákona č. 250/2017 Sb., o elektronické identifikaci, s podmínkou vysoké míry důvěry dané identity.

Je třeba zdůraznit, že poskytnutí kontaktních údajů poplatníkem pro účely elektronického zasílání výzev k platbám místních poplatků je zcela odlišná situace od poskytnutí těchto údajů pro účely zasílání všeobecných informací ze strany úřadu anebo v rámci krizového řízení, kdy postačuje prosté zadání e-mailové adresy anebo telefonního čísla do webového formuláře, neboť následné rozesílané informace jsou vždy zcela obecného charakteru a neobsahují osobní údaje, což v případě zasílání výzev k platbám místních poplatků neplatí.

Pro ohlášení změny kontaktních údajů lze patrně akceptovat navíc i elektronickou zprávu zaslanou z jednoho z evidovaných kontaktů, aniž by zde musel být přítomen uznávaný elektronický podpis. Co se týká případného odvolání souhlasu, pak lze uvedený postup aplikovat jistě s ohledem na podmínku snadného odvolání souhlasu danou GDPR.

Z pohledu občana se v každém případě bude jednat o komplikace, neboť z komerční sféry je zvyklý na plnou elektronickou komunikaci bez ověřování. Navíc většina občanů patrně nevnímá rozdíl mezi nákupem v e-shopu a platbou místního poplatku. Je však nutné si uvědomit (a tuto informaci i dále šířit), že agenda místních poplatků je regulována zákony a dodržení všech postupů je klíčové například pro případné vymáhání nedoplatků. V tomto se veřejná správa od komerčního sektoru zásadně odlišuje.

Technické aspekty

Základní formou by měl být jednoduchý e-mail „Výzva k zaplacení místního poplatku“ s PDF přílohou. Obsahem PDF přílohy bude podrobný rozpis platby, instrukce pro zaplacení a QR kód pro platbu mobilem. Dále je možné přiložit i „fakturu“ ve formátu ISDOC. To dává poplatníkovi minimálně následující možnosti zaplacení:

- zobrazit PDF přílohu na počítači, otevřít bankovnictví v mobilu, načíst QR kód,
- zadat (zkopírovat) platební údaje přímo do elektronického bankovnictví, nebo
- načíst přílohu ve formátu ISDOC do elektronického bankovnictví, které tento formát podporuje.

V budoucnu by bylo možné posílat i odkaz na tzv. push platbu – předpřipravenou platbu pomocí platební karty (či jiným způsobem). Podmínkou je však uzavření smlouvy o využití platební brány úřadem.

Z hlediska technických aspektů plánované služby je třeba věnovat pozornost i samotnému odeslání většího množství e-mailů najednou. Je vhodné, aby měl každý e-mail všechny náležitosti, které pomohou snížit riziko, že bude vyhodnocen jako nevyžádaná pošta (tzn. nastavení SPF, DKIM).

Zároveň je třeba řešit, jak efektivně naložit s výzvami pro poplatníky, kteří neposkytli kontaktní údaje.

Problematika slučování plateb

Rozšířenou praxí při hrazení místních poplatků je slučování více platebních povinností do jedné platby. Tento postup je samozřejmě poplatníky preferován, ať již při hotovostní úhradě, tak při úhradě bankovním převodem zejména z důvodu snížení transakčních nákladů. Při úhradě převodem a také jakýmkoliv jiným bezhotovostním způsobem je pak problém párování takové sloučené platby vůči pohledávkám, pokud toto sloučení není dopředu vhodně nastaveno a identifikováno v systému.

V praxi se lze setkat s několika různými požadavky na slučování z pohledu poplatníků:

- sloučení více poplatků jednoho poplatníka – např. poplatek za komunální odpad a poplatek za psa,
- sloučení poplatků za rodinu/domácnost – tento požadavek je typický pro poplatek za komunální odpad,
- sloučení účelově rozdělených poplatků – např. poplatek za prvního psa na jednu osobu, poplatek za druhého psa účelově evidovaného na jinou osobu, aby se poplatník vyhnul zvýšené sazbě poplatků za druhého vlastního psa.

V případě realizovaného projektu, který samozřejmě cílí na provádění bezhotovostních úhrad, je největším rizikem sloučení platby poplatníkem z vlastní vůle, neboť výsledkem je pak elektronicky nespárovatelná platba. Aby bylo toto riziko sníženo, bylo by třeba přistoupit k možnosti vytváření sloučených plateb dopředu, tedy již před rozesláním vlastní výzvy, nebo v rámci por-

tálového řešení sice po rozeslání primárních výzev, ale před zaplacením poplatku poplatníkem, kdy by tento musel o sloužení platby „požádat“, čímž by se mu vygenerovaly nové platební dispozice.

Je potřeba posoudit, jaké jsou přínosy a náklady jednotlivých variant.

Zcela bez nákladů na vstupu je úplné „zakázání“ slučování, tedy situace, kdy každá platba má vlastní variabilní symbol a pro každou poplatník obdrží samostatné platební instrukce, které samozřejmě mohou být sloučeny do jednoho e-mailu, ale obsaženy v různých přílohách. Nicméně v případě více plateb se objevují dvě rizika. První, jež bylo zmíněno, je sloučení platby poplatníkem zcela libovolně, jehož výsledkem je nespárovatelná platba. Druhé je ignorování více příloh, kdy poplatník reaguje jen na první platební instrukce a mylně se domnívá, že tím má poplatkovou povinnost splněnou.

Výhodnější je tedy zřejmě cesta automatickém spojování plateb jednoho poplatníka, které má pouze limity v přesné identifikaci stejné osoby, aby nedošlo k mylnému automatickému spojení různých osob (dopady též na neoprávněné zpřístupnění osobních údajů), nebo naopak nedůslednému spojení jedné osoby. Základem jsou tedy kvalitní vstupní data v podobě čistě vedeného rejstříku poplatníků s využitím ověřování údajů ze základních registrů.

Asi nejsložitější je situace u požadavku sloučení více poplatků za rodinu/domácnost. Uvedené vazby nejsou primárně k dispozici a musely by být řešeny stejným způsobem jako u sdělení kontaktních údajů, tedy prohlášením poplatníka v rámci ohlášení poplatku. Tento postup bývá často aplikován u místního poplatku za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů vybíraného podle citovaného zákona č. 565/1990 Sb., však s ohledem na složitost následných procesů u vymáhání případných nedoplatků se od možnosti aplikování prohlášení společného plátce ustupuje. Otázkou je však, jak se k této možnosti postavit ve světle realizovaného projektu elektronických výzev k platbám místních poplatků, kdy by bylo možné toto sloučení vytvořit automatizovaně na základě spojení „jednoho poplatníka“, pokud bychom jako znak shodnosti použili sdělené kontaktní údaje. Domníváme se, že tento postup by bylo však třeba dopředu avizovat v informovaném souhlasu se zpracováním osobních údajů včetně umožnění varianty s tímto postupem nesouhlasit. Tedy např. jako druhý oddělený souhlas.

Sloučení účelově rozdělených poplatků patrně není nutné vůbec řešit, neboť je poplatníky zpravidla prováděno z důvodu finanční úspory, a v takovém případě samozřejmě nemusí úřad vycházet vstříc.

Na závěr této části rozboru je jistě vhodné ještě upozornit, že při slučování více plateb do jedné mohou nastat problémy v situaci, kde je uhrazena částka v jiné výši, než bylo předepsáno. V takovém případě informační systém nemůže automaticky provést plné párování platby a rozhodnout jaký význam má rozdíl v částkách (přeplatek/nedoplatek) a je nutný zásah úředníka. Nicméně pokud budou sloučené platby generovány navrhovaným automatizovaným způsobem v nějaké z uvedených variant, lze očekávat i automatizované zpracování na straně poplatníka (QR kód, ISDOC), které riziko chyby v částce či dalších údajích potřebných pro spárování platby významně snižuje.

Shrnutí

Zasílání elektronických výzev k úhradě poplatků bude mít určitě vliv na zlepšení platební morálky a oproti jiným srovnatelně adresným listinným způsobům (zejména složenkám) bude levnější. Určitým problémem může být očekávání vyššího komfortu služby ze strany občanů, kteří si běžně neuvědomují specifika a pravidla fungování veřejné správy a budou tuto službu porovnávat se zkušenostmi z komerční sféry (např. s nakupováním v e-shopech nebo placením mobilním operátorům apod.). Jde zejména o poměrně složité předání kontaktních údajů (nutno zajistit soulad s ochranou osobních údajů a s procesem případného vymáhání nedoplatků) a o obtížně zajistitelné automatické slučování plateb za různé poplatky nebo poplatníky v rodině. V každém případě je nutné porovnat toto řešení se stávajícím stavem a zajistit, aby elektronické výzvy k platbám přinesly oběma zúčastněným stranám výhody, které povedou ke snížení počtu neplatičů a k pozitivnímu vnímání nové elektronické služby poskytované úřadem.

PŘÍPRAVA DOKUMENTŮ PRO ULOŽENÍ A REALIZACI ELEKTRONICKÉHO SKARTAČNÍHO ŘÍZENÍ

Ing. Stanislav Fiala, lektor spisové služby

Úvod

Zásadní změna při správě dokumentů byla uskutečněna zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, a novelizací zákona č. 499/2004 Sb., o archivnictví a spisové službě. Na konci roku 2009 většina původců řešila problematiku příjmu a odesílání dokumentů v digitální podobě. V průběhu dalších let pak byla řešena zejména problematika oběhu a vyřizování dokumentů v digitální podobě. Středem pozornosti posledních let byla ochrana osobních údajů, užití elektronických podpisů, pečetí a časových razítek. Základní úkony správy dokumentů v digitální podobě většina původců v posledních deseti letech tedy má lépe či hůře řešeny. Kam je nutné upřít pozornost a úsilí při správě dokumentů do budoucna? Jednoznačně je to problematika přípravy dokumentů pro uložení a realizace elektronického skartačního řízení. Na první pohled jednoduchý text zákona se stává složitější, pokud si původce uvědomí, že povinnost je obecná a vztahuje se na všechny dokumenty, tedy i na ty vedené v samostatných evidencích.

Je možné konstatovat, že správa dokumentů v digitální podobě, jejich příprava pro uložení a následnou realizaci elektronického skartačního řízení je v porovnání s dokumenty v analogové podobě řádově náročnější. U dokumentů v digitální podobě je nutné kromě základních evidenčních údajů (metadat) pečovat o samostatný digitální dokument. Je nutné řešit správu metadat vztahující se k digitálnímu dokumentu, jeho komponentám, autentizačním znakům a v neposlední řadě řešit i proces změny datového formátu (dle § 69 zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů). Zásadními okamžiky životního cyklu dokumentu v digitální podobě jsou uzavření spisu, předání spisu do spisovny a přípravě skartačního návrhu. Dalším důležitým okamžikem je vytvoření skartačního návrhu (ve formě SIP), zpracování XML pro zasílání údajů o rozhodnutí ve skartačním řízení, předání dokumentů vybraných za archiválii do péče příslušnému archivu ve formě SIP a zpracování XML pro zasílání údajů o potvrzení přejímky s identifikátorem Národního digitálního archivu. Elektronické skartační řízení lze v elektronickém systému spisové služby uskutečnit pouze tehdy, je-li tento elektronický systém spisové služby **v souladu s požadavky Národního standardu pro elektronické systémy spisové služby** ve Věstníku Ministerstva vnitra.

Požadavky zákona č. 499/2004 Sb., o archivnictví a spisové službě

Citovaný zákon č. 499/2004 Sb. dává pro oblast přípravy dokumentů a spisů pro uložení ve spisovně následující pokyny:

- § 3 odstavec 5 – V případě dokumentů v digitální podobě se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a **čitelnosti, tvorba a správa metadat** náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase. Uvedené vlastnosti musí být zachovány **do doby provedení výběru archiválií**.
- § 65 odstavec 5 – Po vyřízení věci se spis uzavře. **Uzavřením spisu** se rozumí kompletace všech dokumentů patřících do spisu, kontrola a doplnění údajů podle § 66 odst. 3 před uložením do spisovny a **převedení dokumentů** v digitální podobě **do výstupního datového formátu** a jejich **opatření metadaty** podle národního standardu.

Ukládání a následné vyřazování dokumentů ve skartačním řízení nelze uskutečnit bez předchozích přípravných úkonů. Jejich realizace znamená pro zaměstnance původce mnoho dalších povinností, z nichž některé je sice možno realizovat automatizo-

vaně v elektronickém systému spisové služby ovšem některé musí realizovat lidským zásahem oprávněný uživatel. Pro zajištění přípravy dokumentů pro uložení v digitální podobě a následnou realizaci skartačního řízení je nezbytné zajistit:

- kompletaci spisů,
- uzavírání spisů,
- kontrolu metadat dokumentů a spisů,
- změnu datového formátu dokumentu v digitální podobě do výstupního datového formátu,
- soulad elektronického systému spisové služby s národním standardem.

Zákonem stanovené požadavky jsou obecné a platí pro všechny dokumenty evidované v základní evidenční pomůcce, ale i pro dokumenty evidované v samostatných evidenčních pomůckách původce. Důležité je uvědomit si, že povinnost zajistit „převedení dokumentů v digitální podobě do výstupního datového formátu a jejich opatření metadaty podle národního standardu“ znamená lidskou práci a finanční prostředky nutné k zajištění zákonných povinností. Zákonodárce klade na bedra původců tyto povinnosti bez ohledu na označení dokumentu skartačním znakem A, V nebo S.

Možnost změn

Po desetileté praktické zkušenosti s péčí o dokumenty v digitální podobě je nutné hodnotit principy elektronicky vedené spisové služby a efektivitu nákladů vynaložených pro zajištění řádného výkonu spisové služby. Pro zjednodušení péče o dokumenty veřejnoprávních původců je vhodné **sjednotit přístup archivů k žádostem** původců o udělení **trvalého skartačního souhlasu**. Pro snížení nákladů, zmenšení zátěže a povinností veřejnoprávních původců je účelné změnit ustanovení zákona. Zákon by měl stanovit povinnost **převést dokument v digitální podobě** do výstupního datového formátu a **opatření metadaty** při uzavření spisů s uvedeným skartačním znakem A nebo skartačním znakem V se skartační lhůtou delší 10 let. U dokumentů s uvedeným skartačním znakem **S nebo V s lhůtou kratší deseti let** by byla tato povinnost uplatněna až v okamžiku, kdy byl dokument vybrán za archiválii.

PORTÁL OBČANA POHLEDEM UŽIVATELŮ

Ing. Jan Jarolímek, Ph.D., Ing. Miloš Ulman, Ph.D., Ing. Martin Lukáš, Ph.D.
Katedra informačních technologií PEF, Česká zemědělská univerzita v Praze

Abstrakt

V příspěvku jsou shrnuty zkušenosti 546 vysokoškolských studentů s Portálem občana. Všichni se na portál osobně registrovali a následně hodnotili informovanost, způsob registrace, připravenost úředníků, poskytované služby a přínosy pro občany.

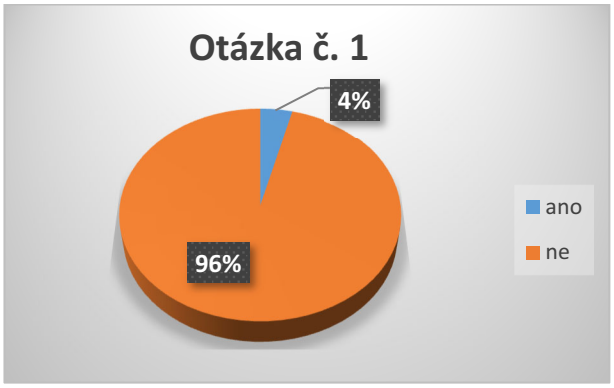
Úvod

V červenci 2018 byl spuštěn Portál občana (https://obcan.portal.gov.cz), určitý podportál Portálu veřejné správy, který má vytvořit pro občany rozhraní pro jednotnou elektronickou komunikaci s veřejnou správou. V době spuštění bylo deklarováno 37 dostupných služeb, v únoru 2019 je to pak již přes 60. Způsob přihlášení je možný třemi způsoby: pomocí datové schránky, nové eOP a identifikačního prostředku „Jméno, heslo, SMS“. Tato známá fakta jsou východiskem pro hodnocení Portálu občana pohledem uživatelů.

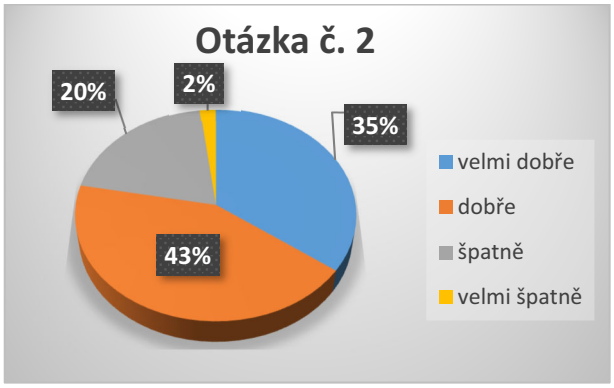
Hodnocení Portálu občana

Hodnocení Portálu bylo zpracováno studenty v rámci absolvování předmětu Informační systémy ve státní správě a samosprávě na oboru Veřejná správa a regionální rozvoj České zemědělské univerzity v Praze. Probíhalo v období prosinec 2018, až únor 2019. Jednalo se o studenty denního studia (109) a kombinovaného (dálkového) studia (337) magisterského stupně, celkem tedy bylo zpracováno 546 hodnocení z území 9 krajů. Každý student se musel do Portálu občana přihlásit (zvolený způsob přihlášení: 5,1 % datovou schránkou, 94.9 % „Jméno, heslo, SMS“), zpracovat popis a SWOT analýzu funkčnosti a přínosů. Tato práce byla následně prezentována a kontrolována v rámci výuky. Na základě těchto zkušeností studenti odpovídali na následující otázky.

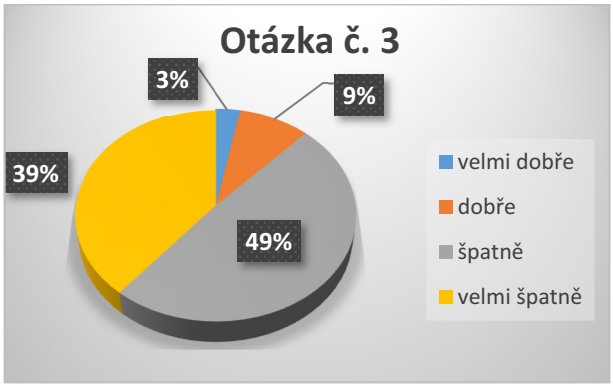
1. Věděli jste o existenci Portálu občana před informací v tomto kurzu?



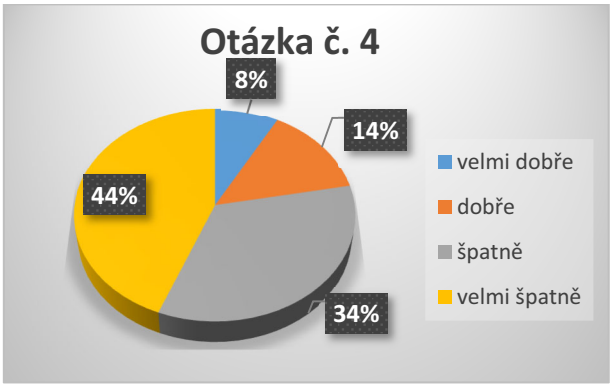
2. Jak hodnotíte záměr vytvoření Portálu občana?



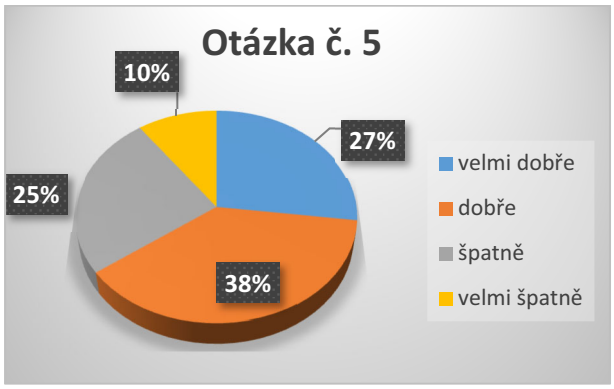
3. Jak hodnotíte dostupnost a kvalitu informací o Portálu občana?



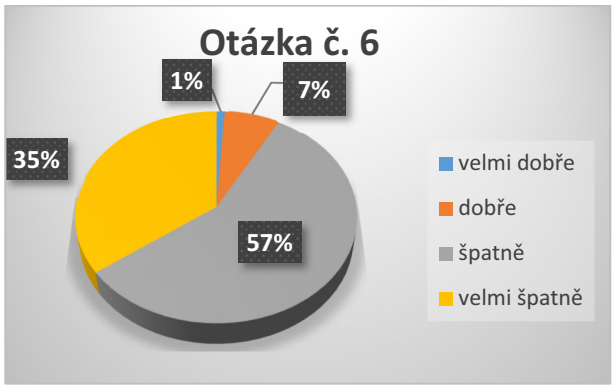
4. Jak hodnotíte připravenost úředníků pro vyřízení podkladů pro přihlášení na Portál občana?



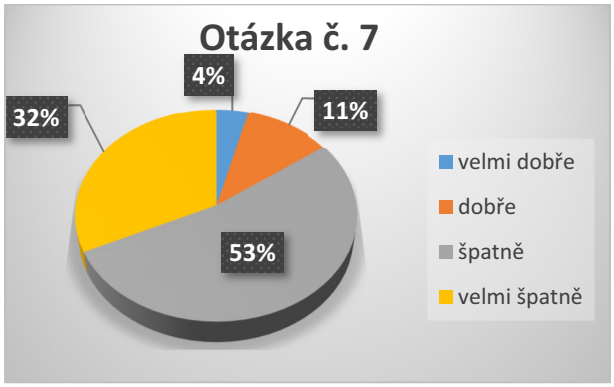
5. Jak hodnotíte jednotné přihlašování k poskytovaným službám?



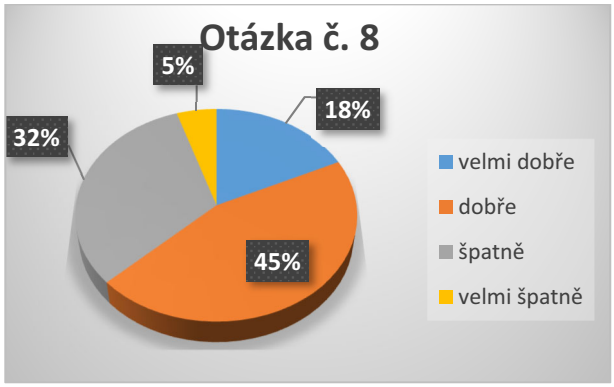
6. Jak hodnotíte rozdílné prostředí poskytovaných služeb?



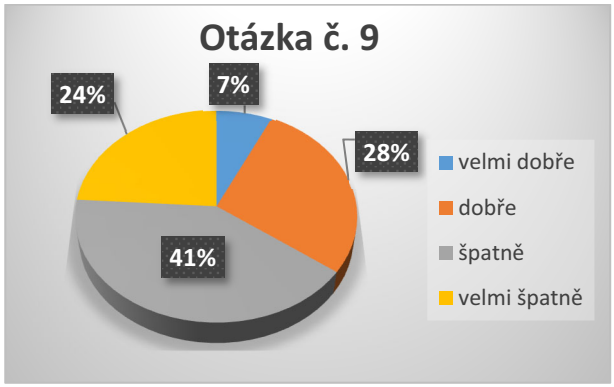
7. Jsou pro Vás akceptovatelné požadavky na plnohodnotné využití Portálu občana? (eOP + datová schránka)



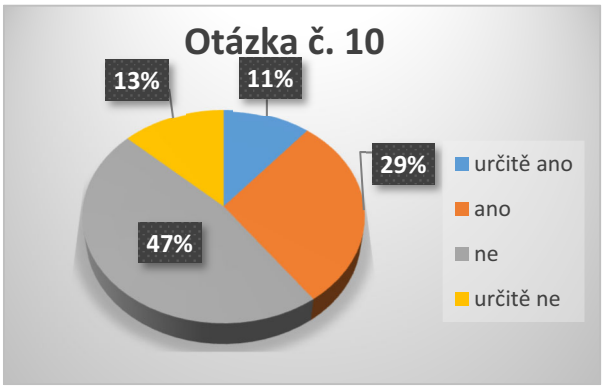
8. Jak hodnotíte vzhled a uživatelské rozhraní Portálu občana?



9. Jak vnímáte zabezpečení Vašich osobních dat na Portálu občana?



10. Budete za stávajících podmínek i nadále využívat služeb Portálu občana?



Co z těchto odpovědí vyplývá a jaké vyvodit ponaučení?

- Je zjevné, že záměr vytvoření Portálu občana jako sjednocujícího nástroje pro elektronickou komunikaci s veřejnou správou je vnímán pozitivně (78 %). Tento princip je také již dlouhodobě osvědčen v zahraničí a je nutné si přiznat, že Česká republika dohání to, co v minulých letech zameškala.
- Zjevné je také, že při přípravě a spuštění Portálu občana byla naprosto opomenuta informovanost cílové skupiny, pro kterou je určen, tedy občanů. Značně problematická je také připravenost úřadů na podporu zapojení občanů, zde je však znatelný posun v čase, kdy zainteresovaní úředníci jsou schopni poměrně rychle akceptovat novou technologii.
- Většina respondentů (63 %) hodnotí pozitivně vzhled a uživatelské rozhraní Portálu občana.
- Problematická je však dostupnost deklarovaných služeb. Zásadním způsobem je ovlivněna způsobem přihlášení, bez datové schránky toho uživatel příliš nezíská. Zde pak narážíme na nedůvěru k využití datových schránek fyzickými osobami v souvislosti s následnou povinností jejich využívání a souvisejícími sankcemi. Využití eOP dle evropského standardu také nepřináší, vzhledem k nemožnosti doručování zpráv, mnoho užitku.
- Další problematickou oblastí, zásadním způsobem opomíjenou, je naprostá rozdílnost ve způsobu poskytovaných služeb od jednotlivých úřadů. Portál občana řeší jednotné přihlašování, což je jistě přínosem, pozitivně hodnotí 65 % respondentů, ale dále existuje mnoho technologicky i funkčně rozdílných platforem, které jako celek nejsou pro uživatele příliš přívětivé. Příklady ze zahraničí ukazují, že i zde je možná standardizace.
- Poměrně špatně je uživateli vnímáno zabezpečení osobních dat, nicméně v kontextu realizovaného průzkumu je to více emociální hodnocení způsobené množstvím shromážděných a zobrazených osobních dat, než hodnocení technického provedení. Je ale třeba brát v úvahu tento stav, který může mít vliv na další zapojování nových uživatelů.
- Zjištění, že po registraci a podrobném prostudování funkcionalit Portálu občana většina respondentů (60 %) nemá zájem jej za stávajících podmínek dále využívat, může být pro tvůrce Portálu občana určitým varováním.

Závěr

Uváděné hodnocení je první studií, která spíše než konečné výsledky poskytuje podklady pro formulování dalších průzkumů. V rámci výzkumné činnosti na Katedře informačních technologií ČZU v Praze je připravováno strukturované šetření, které dokáže postihnout vývoj Portálu občana a především rozvoj elektronické komunikace s veřejnou správou ve větším detailu a také v čase. Pro testování uživatelského rozhraní (použitelnost a UX) je využívaná Laboratoř pro studium lidského chování (HUBRU).

Informační zdroje

Kalina Jan: Portál veřejné správy 2.0 – Portál občana [online] eGovernment. Dostupné na: https://www.egovernment.cz/inpage/portal-verejne-spravy-2-0-portal-obcana/ [Citace 06.03.2019]

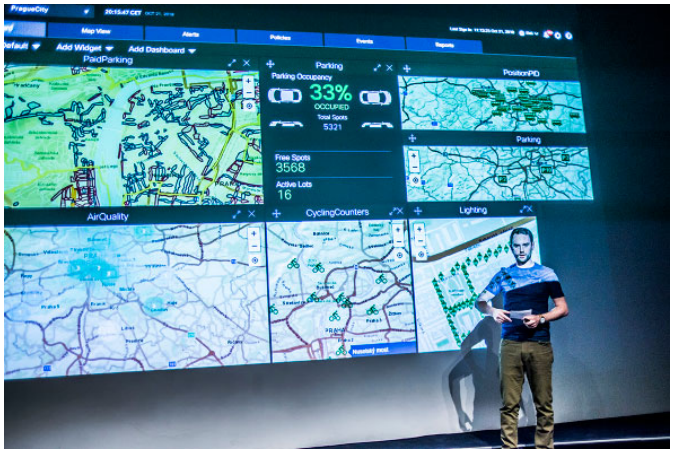
Peterka Jiří: Jak funguje a co nabízí Portál občana? [online]. Lupa.cz. Dostupné na: https://www.lupa.cz/clanky/jak-funguje-a-co-nabizi-portal-obcana/ [Citace 06.03.2019]

Kontaktní adresa

Ing. Jan Jarolímek, Ph.D., Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, Katedra informačních technologií, Kamýcká 129, 165 00 Praha Suchdol, e-mail: jarolimek@pef.czu.cz

SMART PRAGUE: OD KONCEPTU K REALIZACI

Kolektiv autorů Operátor ICT, a.s.



Prezentace dashboardu datové platformy

Před českou metropolí stojí nové výzvy. Jak se postavit k rozvoji veřejného prostoru udržitelným způsobem, který přinese obyvatelům větší komfort a nové služby? Jak reagovat na rostoucí počet obyvatel naší metropole, a tedy větší nároky na infrastrukturu města? Zodpovědět tyto otázky pomáhá Praze městská společnost **Operátor ICT**, jejímž úkolem je testování a zavádění inovací do života města. Řada technologických novinek je zaváděna do městského prostoru v režimu pilotního provozu, který zaručí otestování technologie, a teprve po vyhodnocení jejích přínosů se rozhoduje o jejím případném plošném rozšíření. Snižujeme tak riziko zbytečných investic do nových technologií, jejichž reálný užitek by byl minimální.

Vznikla proto **koncepce Smart Prague 2030**, která je postavena na využívání nejmodernějších technologií k proměně metropole v příjemnější místo pro život. Koncepce Smart Prague vychází z celosvětově známého konceptu Smart Cities. Vznikla v roce 2017 na základě dlouhodobých priorit města stanovených zejména jeho strategickým plánem a sledováním světových trendů v technologickém vývoji. Bylo definováno šest klíčových oblastí, kde má zavádění moderních technologií nejvýznamnější pozitivní dopady: **Mobilita budoucnosti, Chytré budovy a energie, Bezodpadové město, Atraktivní turistika, Lidé a městské prostředí** a **Datová oblast**.

Klíčem k úspěchu je spolupráce, otevřenost a sdílení

Klíčové pro úspěch Smart Prague 2030 je zapojení městských společností a městských částí stejně jako spolupráce s akademickým sektorem. Operátor ICT plní v celém procesu roli manažera při koordinaci naplňování koncepce. O realizaci jednotlivých projektů rozhodují orgány města, které využívají především doporučení Komise Rady hl. m. Prahy pro rozvoj konceptu Smart Cities v hl. m. Praze složené ze zastupitelů města napříč politickou reprezentací a vybraných expertů a expertek.

Energetický ekosystém: zavádění úsporných řešení v městských budovách

Operátor ICT nyní pracuje na komplexním řešení a nabídce služeb v oblasti energetického managementu. Na základě zkušeností z pilotních projektů nastavuje své produkty pro další partnery z oblasti veřejné správy či pro městské části. Pomocí vlastní metodiky a na ni vázaného softwaru může nabídnout kompletní přípravu a řízení energeticky úsporných projektů v budovách jak památkově chráněných, kde má zkušenosti s použitím metody EPC či energetickým managementem, tak i v budovách mimo

památkovou péči, kde je možnost výměny oken, zateplení obálky budovy a také úpravy a řízení technologií, kde je opět možnost využití EPC a energetického managementu.

Minimální úspory, kterých je možné dosáhnout energetickým managementem, se pohybují přes 10 % ročně, což činí necelých 5 mil. korun za rok, a životnímu prostředí odlehčíme ročně o více než 2 tuny CO_2. Metodou EPC jsme schopni MHMP ušetřit minimálně 11 % ročně, což činí 7,2 mil. korun za rok, a životnímu prostředí odlehčíme ročně o více než 3 tuny CO_2.

Mezi hlavní přínosy patří úspory za energie, snížení provozních nákladů, zvýšení komfortu uživatelů a návštěvníků budov, zajištění snadno dostupného komplexního přehledu o hospodaření a stavu budov jako nástroje pro správu i rozhodování vlastníka či správce a sběr dat pro další použití a optimalizaci veřejných budov.

Datová platforma Golemio jako srdce konceptu Smart Prague

Golemio, datová platforma hlavního města Prahy, má klíčový strategický význam, protože propojuje všechny oblasti, a je tak srdcem všech dalších inovačních projektů v našem hlavním městě. Rozhodování na základě datové analýzy je dnes pro město životně důležité. A právě celoměstská datová platforma umožňuje poprvé v historii města vyhodnocovat a interpretovat městská data jako celek. V rámci společnosti Operátor ICT proto dali dohromady kvalitní tým lidí, který se městskými daty zabývá a má k tomu potřebné nástroje.

Datová platforma Golemio integruje městská data, vytváří analýzy dat včetně vizualizací a předkládá návrhy na využití dat v praxi. Jedinečnost projektu Golemio spočívá v komplexní práci s daty. Celý proces začíná sběrem dat a jejich integrací, následuje analýza a vizualizace dat, závěrečná zpráva a poté publikace datové sady na webu golemio.cz. Veřejný datový portál Golemio, spuštěný v červnu 2018, funguje jako prezentační vrstva pro veřejnost, kde jsou data dávána do kontextu a oblastí a vizualizována. Součástí webu je také veřejně dostupná metodika práce s daty, sdílení „know-how“ datové platformy s veřejností.

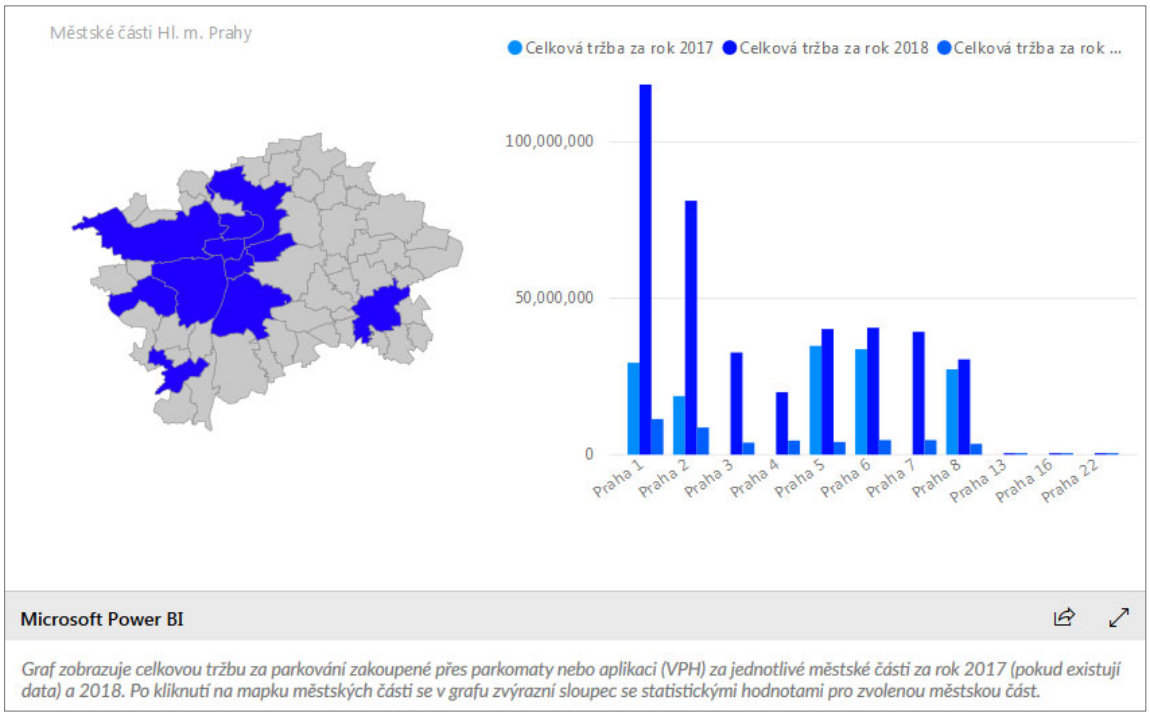
Městské prostředí skýtá obrovské množství dat týkajících se různých oblastí, jako je kvalita ovzduší, hluk, pohyby lidí, aut, dostupnost služeb, meteodata, monitoring zeleně či odpadové hospodářství. Jak tedy přistupovat k takovému závalu dat? Nejde nám jen o kvantitu, ale také – a to především – o kvalitu. Cílem datové platformy totiž není být skladištěm všech dat po celé Praze. Začínáme proto u dat, která mají největší potenciál zlepšit život v Praze, a samozřejmě především tam, kde už data můžeme získat. Zároveň ale usilujeme o získání a zpřístupnění dat z prozatím uzavřených zdrojů, o nichž ale víme, že budou ku prospěchu. Naším záměrem je skrze data propojovat veřejný sektor, akademickou sféru, soukromý sektor a občany, motivovat třetí strany, aby nad kvalitními daty vytvářely kvalitní aplikace.

Srovnání podlažnosti budov VS měřené koncentrace NO_2 na lampách v Karlíně

Hlavním cílem datové platformy je poskytnout městu, veřejným organizacím a městským společnostem službu sdílení a zpracování dat a veřejnosti a soukromým firmám poskytnout data v otevřeném formátu. V průběhu roku 2019 proto plánujeme nasadit vlastní software datové platformy, otevřený a šitý na míru našim potřebám a zkušenostem.

Vlastní nástroje a nabídka služeb

Datová platforma začíná v letošním roce nabízet své služby pro městské části, realizuje projekty ve spolupráci s městskými společnostmi, ale také spolupracuje s malými i velkými podniky, které jsou ochotny spolupracovat při poskytování a analýze dat v rámci města. Mezi současné nabízené služby patří odborné konzultace při zavádění datové platformy, tvorba pravidel a detekce nastavení, vizualizace a reportingy, veškerá práce s open daty v rámci veřejné správy a další služby. Operátor ICT disponuje vlastním týmem datových specialistů, kteří jsou schopni reálně posoudit příležitosti datových sad a jejich efektivní využití.



Tržby za parkování podle městských částí

Multikanálový odbavovací systém – komplexní řešení veřejné dopravy

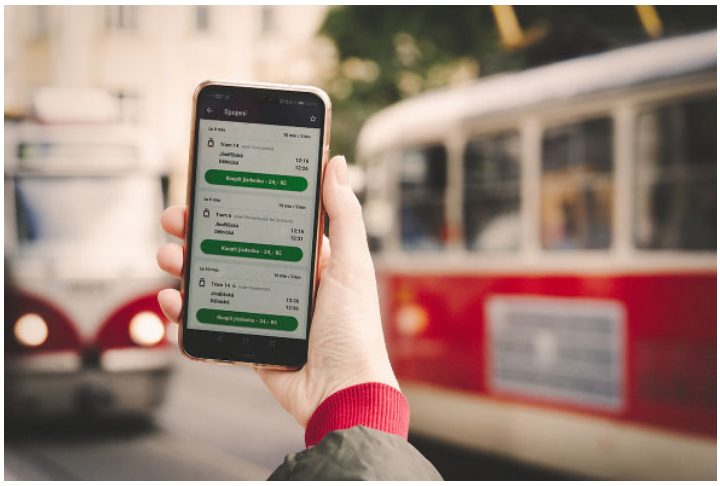
Jedním z hlavních projektů společnosti Operátor ICT je tzv. Multikanálový odbavovací systém, který v průběhu roku 2018 kompletně modernizuje, sjednocuje a liberalizuje systém odbavování v Praze a Středočeském kraji. Operátor ICT je hlavním tvůrcem a manažerem projektu ve spolupráci s Dopravním podnikem hl. m. Prahy, Ropidem, Českými drahami, Středočeským krajem a dalšími partnery.

Digitalizace nosičů, přímý online prodej a moderní technologie

Projekt zahrnuje několik realizačních částí – kompletní management dopravní a městské karty, odbavovací systém včetně všech zařízení, zprovoznění online prostředí pro nákup dopravních kupónů nebo mobilní aplikaci pro pohodlný nákup krátkodobých jízdenek v rámci veřejné dopravy. Po zprovoznění všech částí systému se Operátor ICT zabývá dalším rozvojem, pracuje na zlepšení pro uživatele a v rámci e-shopu a mobilní aplikace připravuje nové služby, např. možnost nakupovat dlouhodobé kupóny přes mobilní aplikaci, využívat aplikaci jako nosič nebo integrovat do aplikace Google Pay a Apple Pay.

Mobilní aplikace jako nosič dopravních kupónů

Aplikace vyhledá dopravní spojení podle vaší polohy a doporučí nejlevnější jízdenku s platností 30 minut až 3 dny pro cestu veřejnou dopravou v rámci Pražské integrované dopravy (PID). Výhodou aplikace je schopnost pracovat s aktuálními informacemi o dopravě v rámci Pražské integrované dopravy, a to včetně výluk a mimořádností. Máte jistotu, že aplikace vyhledala nejrychlejší možnou cestu. Zaplacení jízdenky probíhá pomocí uložené platební karty, pomocí aplikace Masterpass nebo v blízké budoucnosti i s využitím Apple Pay/Google Pay. Jízdenka zakoupená přes mobilní aplikaci je platná ve všech pásmech PID, tedy i v integrovaných částech Středočeského kraje, včetně vlaků ČD.



Snadné vyhledávání spojení a rychlý nákup jízdenky s platností 30 minut až 3 dny přímo v aplikaci

Aplikace dále zobrazuje přehled parkovišť P+R a jejich aktuální obsazenost, takže mají řidiči přehled, kde mohou odstavit svůj automobil a pokračovat pohodlně veřejnou dopravou. Další šikovnou funkcí je nákup až deseti jízdenek najednou, které si cestující aktivuje podle potřeby. Zakoupenou jízdenku můžete navíc předat dalšímu uživateli. Aplikace je vhodná pro všechny české i zahraniční návštěvníky Prahy, kteří chtějí bezstarostně cestovat po Praze. Aplikace je ke stažení zdarma v App Store a Google Play. Více na **app.pidlitacka.cz**

Nabídka integrace systému a vývojových služeb

Rozvoji projektu se nově věnuje tým strategického rozvoje a obchodu. Operátor ICT zároveň plánuje své zkušenosti, infrastrukturu, vývojové kapacity či řízení projektu nabídnout do dalších regionů. Cílem Operátora ICT je oslovit další kraje a nabídnout realizaci dopravně-odbavovacího systému včetně inovací dopravní karty např. formou pre-paid ve vazbě na mobilní aplikace města, přehlednou a rychlou správu městských poplatků, služeb v návaznosti na rozvoj a strategii v oblasti e-governmentu.

Záměrem technologické společnosti Operátor ICT je nově stanovený standard dopravního odbavování nabídnout co nejširší veřejnosti v rámci celé České republiky. Projektový tým Operátora ICT je připraven tento revoluční odbavovací systém modifikovat pro potřeby dalších krajů. Zároveň nabízí spolupráci v rámci zavádění inovací, poskytnutí vývojových kapacit například pro zavedení mobilních aplikací, které souvisejí s dopravou nebo správou města.

HYBRIDNÍ SPIS JE REALITA

Mgr. Tomáš Lechner, Ph.D.,
Vysoká škola ekonomická v Praze, Národohospodářská fakulta, Katedra práva

Úvod

Elektronizace veřejné správy má své limity, mezi které patří například legislativní rámec, rozpočtové zdroje apod. [1] Míra elektronizace nikdy nemůže překročit míru rozvoje informační společnosti z důvodu problematiky digitálního vyloučení [3]. Avšak to v žádném případě neznamená, že by se neměla elektronizace veřejné správy rozvíjet vůbec, neboť má poměrně velký (a též ekonomický) potenciál, který je vhodné využít [4]. Jedním z významných aspektů procesu elektronizace veřejné správy je obecná otázka důvěryhodnosti elektronických nástrojů a služeb [1]. Jako důkaz lze ocitovat ustanovení čl. 25 odst. 1 nařízení eIDAS: „Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy."

Položme si otázku, proč je takové ustanovení vůbec třeba. Všichni běžně pracujeme s výpočetní technikou, a přesto potřebujeme pro elektronickou podobu dokumentů a podpisů stále zajišťovat podporu v jejich rovnoprávnosti s podobou listinnou i takovým ustanovení. Dokladem, že samotné možnosti elektronické komunikace a elektronizace procesů nestačí a je třeba je vynucovat a deklaratorně „zrovnoprávňovat", je například i nově vznikající návrh zákona o právu na digitální služby [5]. Ale třeba jednou přijde doba, kdy se i v právním předpisu dočteme větu jako „listinnému dokumentu nesmí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má listinnou podobu".

Ve světle postupné digitalizace veřejné správy a procesu, který probíhá již mnoho let (viz např. [1], [2] a [6]), je zřejmé, že nelze očekávat okamžité „přepnutí" z listinné do digitální podoby a okamžitou úplnou digitalizaci všech procesů veřejné správy, byť tyto cíle jsou vytčeny v mnoha strategických dokumentech [9]. Proto se musíme vypořádat s postupným přechodem od analogového úřadování k digitálnímu, k čemuž jednoznačně patří hybridní spis. Tento termín není definován v žádném právní předpise, takže si řekněme, že pod ním budeme rozumět spis, který obsahuje listinné a digitální dokumenty dohromady.

Základní statistické výzkumy dat poskytovaných elektronickými systémy spisových služeb ukazují, že poměrné zastoupení hybridních spisů v čase narůstá a původci se musí tedy ve stále větší míře vypořádat s otázkami typu, jak tyto spisy spravovat, jak je ukládat a jak je vyřazovat ve skartačním řízení nebo mimo něj. V tomto příspěvku budeme na tyto položené otázky hledat základní odpovědi.

Formy vedení spisové služby

Zákon č. 499/2004 Sb., o archivnictví a spisové službě, v aktuálním znění, připouští dvě možnosti vedení spisové služby, a sice listinnou a elektronickou (blíže viz též [2]). V některých případech se zaměňuje forma vedení spisové služby s formou spravovaných dokumentů, což je ale špatně. Neznamená to, že tyto dvě formy spolu vůbec nesouvisí, ale z jedné automaticky neplyne druhá. Jinými slovy:

- Listinná forma vedení spisové služby neznamená, že se původce nemusí starat o vhodné, byť časově omezené, uložení přijatých digitálních dokumentů. Ale znamená, že všechny přijaté elektronické dokumenty původce převádí do listinné podoby a všechny vlastní dokumenty primárně vytváří v listinné podobě, tedy přinejmenším si ukládá listinné stejnopisy dokumentů vzniklých z vlastní činnosti původce.
- Elektronická forma vedení spisové služby znamená, že elektronický systém spisové služby se stává primární evidenční pomůckou a že plně spravuje evidované elektronické dokumenty a dále metadata o všech evidovaných listinných dokumentech. Co se týká dokumentů a spisů, tak tedy musí jít o úplnou elektronickou evidenci všech dokumentů bez rozdílu

formy. Přijaté listinné dokumenty mají být zpravidla konverzovány do elektronické podoby, nicméně nikde není upřesněno, jak se k formulaci „zpravidla“ postavit. Asi nejlepší přístup je vždy, když to povaha přijatého dokumentu umožňuje. Ale konkrétní stanovení podmínek je v kompetenci původce a musí být uvedeny v jeho spisovém řádu. Vlastní dokumenty by opět měly být tvořeny v souhlasné, tedy v tomto případě elektronické formě, ale už se trochu rozcházejí přístupy k tomu, jaký stejnopis vlastního dokumentu má být ukládán. Zda vždy elektronický, pokud to povaha dokumentu umožňuje, nebo ve formě souhlasné s formou, jakou je případně odesílán adresátovi. Z pohledu procesu elektronizace je jednoznačně správnější ten první jmenovaný přístup.

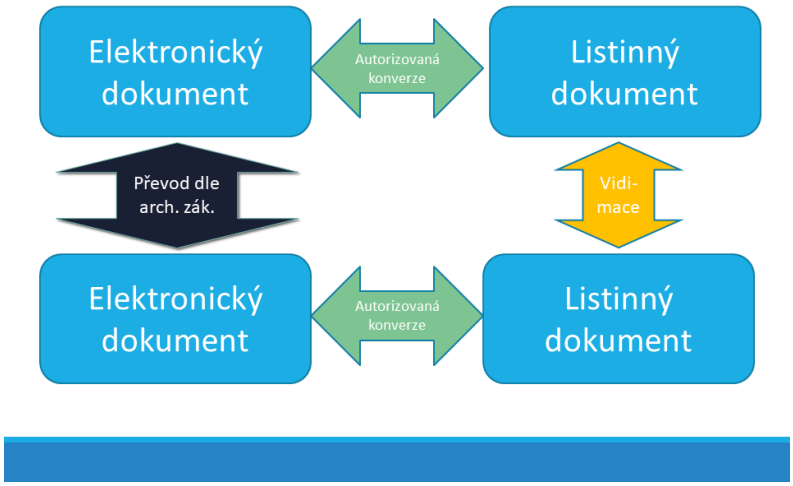
Z formy vedení spisové služby plynou další návazné povinnosti. Např. pokud původce vykonává spisovou službu v elektronické podobě je povinen následně také skartační řízení vést v elektronické podobě (ke skartačnímu řízení v elektronické podobě viz [2] kap. 3.10). A právě tyto návaznosti někdy vedou k tomu, že si původci vybírají z každého typu vedení spisové služby něco a nevedou ani jednu formu řádně (Srovnej např. [7]), čímž se samozřejmě dopouštějí přestupku podle zákonu č. 499/2004 Sb.

Konverze dokumentů

Elektronizace veřejné správy je postupný proces, v rámci něhož dochází k postupné elektronizaci procesů a entit, které do procesů vstupují. V případě spisové služby jde o elektronizaci dokumentů, přičemž jsou praktické důvody, proč určitý dokument je třeba v listinné podobě (např. adresátem je fyzická osoba, která nemá zřízenou datovou schránku) a proč určitý dokument je třeba v elektronické podobě (např. adresátem je právnická osoba nebo jiný orgán veřejné moci, které mají datovou schránku zřízenu obligatorně [8]). V případě, kdy jde o dokument, jehož tvůrcem je původce, lze vždy vytvořit potřebný stejnopis či druhopis příslušného dokumentu (v řeči Národního standardu pro elektronické systémy spisové služby jde o různá ztvárnění téhož dokumentu). Ale v případě, kdy jde o dokument doručený, je při potřebě jiné formy třeba udělat příslušnou konverzi.

Právní rámec je dán buď zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který zavádí tzv. autorizovanou konverzí, jejímž výstupem je dokument se stejnou právní váhou jako dokument, který do procesu konverze vstupuje, anebo zákonem č. 499/2004 Sb., který také zavádí pravidla pro důvěryhodnou konverzi dokumentů. Výsledkem této konverze je dokument se stejnou právní vahou jako vidimovaná (ověřená) kopie dokumentu. Možnosti vzájemných konverzí forem dokumentů a ověřených kopií a změn datového formátu digitálních dokumentů jsou sumarizovány ve schématu na Obr. 1.

Ve všech případech je důvěryhodnost podložena zejména připojením ověřovací doložky a podpisem ověřující osoby, který je v případě listinného výsledku vlastnoruční a v případě elektronického výsledku kvalifikovaný elektronický podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, a podle nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.



Obr. 1: Schéma možností důvěryhodných převodů a konverzí dokumentu.

Hybridní spisy

Zákon č. 499/2004 Sb. o archivnictví a spisové službě, v aktuálním znění, stanoví v § 65 odst. 1 následující:

„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."

Tedy tento předpis jednoznačně předjímá existenci hybridních spisů obsahujících jak elektronické, tak listinné dokumenty. Pro spojení dokumentů různých forem je v ustanovení zaveden tzv. odkaz, jehož formální ani faktická definice není dále upřesněna. Je tedy otázkou praxe, jak tento odkaz realizovat. Odpověď budeme hledat ve třech rovinách, které odpovídají oblastem specifikovaným v úvodu:

- oblast tvorby spisu v době, kdy je spis otevřen a jsou do něj postupně vkládány dokumenty,
- oblast uložení spisu ve spisovně,
- oblast zařazení spisu do skartačního návrhu a následné předání archivu k trvalému uložení.

Ve všech diskusích se zaměříme na elektronickou formu vedení spisové služby, protože v listinné podobě by vlastně hybridní spisy neměly vznikat, jak bylo diskutováno výše.

Hybridní spis ve spisové službě

V době, kdy je spis otevřen a dochází k přikládání dokumentu do spisu, jsou všechna metadata o spisu včetně metadat o vložených dokumentech a o jejich vložení vedena v elektronickém systému spisové služby. Protože spisová služba je pro elektronický způsob vedení také primární evidenční pomůckou, měl by být vždy fyzický obsah spisu porovnáván právě s touto evidencí. A tedy:

- Pokud úředník pracuje přímo v systému spisové služby, má v něm celkový přehled o obsahu spisu včetně informací o tom, který dokument je analogový, a tedy existuje zároveň ve fyzické podobě, a který je elektronický, a tedy jeho dostupnost je přímo zprostředkována elektronickým systémem spisové služby.
- Pokud úředník pracuje s fyzickou částí spisu, měla by v něm existovat informace o vložených elektronických dokumentech. Avšak díky rychlosti dostupnosti těchto dokumentů z elektronického systému spisové služby jako primární evidenční pomůcky, by tato informace měla být co nejstručnější. Např. jeden vložený list papíru, na který se operativně poznamenává informace o elektronických dokumentech způsobem, podle kterého je lze co nejrychleji vyhledat v evidenční pomůcce, tedy například pomocí čísla jednacího anebo jednoznačného identifikátoru. Je naprosto nevhodné, aby tento odkaz byl řešen celkovým prostým výtiskem elektronického dokumentu, neboť tento způsob degraduje výhody elektronického vedení spisové služby, je neekonomický (náklady na tisk), nešetrný k životnímu prostředí (zbytečná spotřeba papíru) a z pohledu procesu elektronizace je též „nevýchovný", tedy nepodporuje změnu způsobu úřadování směrem k cílové celkové elektronizaci.

Trochu složitější je problematika nahlížení do spisu, která s ohledem na ochranu osobních údajů a další pravidla má v elektronické podobě komplikovanější řešení. Proto bývá často zjednodušena tím, že se spis udržuje celkově souběžně v listinné podobě, přičemž elektronické dokumenty jsou ve fyzické podobě vloženy pouze jako prostý výtisk, tedy bez jakéhokoliv dokladu ověření. Právě tento postup je ale učebnicovým příkladem nevhodného řešení, kdy se nehledají nové cesty, ale překážky se řeší návratem k původním procesům. Samozřejmě, že je vždy třeba situaci posuzovat dle konkrétního kontextu. Ale argument, že se musí všechno vytisknout jen proto, že by náhodnou někdo mohl přijít do spisu nahlížet, je jednoznačně plošně nesprávný.

Hybridní spis ve spisovně

Po uzavření spisu je spis uložen po dobu plynutí skartační lhůty ve spisovně (blíže k procesu uzavření spisu viz [2] kap. 3.5.3). V případě elektronického vedení spisové služby se evidence dokumentů a spisů uložených ve spisovně stává přímočarým pokračování předchozí evidence. Tedy není zde již oddělená archivní kniha, ale sám elektronický systém spisové služby by

měl (dle zákona musí) poskytovat informace o všech entitách uložených ve spisovně, které před tím prošly evidencí ve spisové službě.

Součástí uzavření spisu je výtisk soupisu dokumentů ve spisu (anebo sběrného archu, pokud je spis veden tímto, podle názoru autora v době elektronických systém sice nevhodným, avšak legislativou povoleným, způsobem). A právě tento soupis musí u každého dokumentu obsahovat informaci, zda jde o dokument analogový nebo digitální. Pro analogové dokumenty musí navíc zahrnovat přesnou informaci o uloženém množství, počtu listů a příloh. Uvedený soupis obsahu spisu tedy jednoznačně obsahuje zákonem požadované odkazy, které již nemusí být řešeny žádným jiným způsobem.

Hybridní spis ve skartačním řízení a v archivu

Elektronické vedení spisové služby znamená též elektronickou formu skartačního řízení. Skartační návrh vychází opět z primární evidence vedené v elektronickém systému spisové služby a jeho stěžejním obsahem jsou jednotlivé SIP balíčky obsahující metadata o všech zařazených dokumentech a spisech. Pro formální stránku tohoto návrhu je tedy nepodstatná forma vložených entit, samozřejmě ve smyslu návrhu jako takového, nikoliv obecné informace o entitě, protože údaj o formě dokumentu či spisu je jedním ze stěžejních metadat, které SIP balíček obsahuje.

Stěžejní součástí skartačního řízení je samozřejmě práce archiváře, který provádí výběr dokumentů a spisů, jenž mají trvalou hodnotu a stanou se tak archiváliemi. V případě posouzení spisů může archivář vycházet z metadat, nebo si vyžádat spis k předložení. Pro spisy, které jsou celé v elektronické podobě, stačí předat SIP balíčky včetně digitálních komponent, pro spisy v analogové podobě je třeba fyzické prohlédnutí. U hybridních spisů se musí spojit obě akce, nicméně jejich spojení rozhodně není důvodem pro tištění digitálních dokumentů. Spíš by se dalo hovořit o snaze digitalizace analogové části spisu, která ale může narazit na technické překážky, a proto i zde je třeba naučit se zvládat proces spojující práci s digitálními a analogovými dokumenty dohromady.

Následné uložení archiválií v archivu v případě hybridních spisů bývá často archiváři označováno jako „noční můra“, protože část entity je ve fyzické podobě v archivu a část je dostupná v rozhraní národního digitálního archivu spravovaného Národním archivem. Ona „noční můra“ v podobě určité vnímané nejistoty, kde se tedy spis nachází a jak jej lze dohledat, je ale dle názoru autora obdobnou situací jako u nahlížení do spisu v první diskutované oblasti. Působí tedy v této problematice více síla zvyku než nějaké faktické překážky, které by bránily nový stav věci akceptovat a naučit se se s ním vhodně vypořádat.

Shrnutí

Hybridní spisy jsou neoddiskutovatelně realitou stávajícího úřadování orgány veřejné moci všech úrovní. Je třeba před tímto faktem nezavírat oči, ale naopak se snažit vypořádat se s ním tak, abychom otevírali cestu stále větší míře elektronizace a nebrzdili její rozvoj zbytečným převodem dokumentů do listinné podoby v případech, kdy se ve spisu jiné listinné dokumenty vyskytují a nejsou prostředky (ve zcela obecném smyslu, tedy zejména technické, ekonomické a organizační) na převod všech dokumentů do elektronické podoby.

Literatura

[1] WEST, D. M. *Digital government*. New Jersey: Princeton University Press, 2005. 234 s. ISBN 978-0-691-13407-9

[2] KUNT, M., LECHNER, T. *Spisová služba*. 2. aktual. vyd. Praha: Leges, 2017. 384 s. Praktik. ISBN 978-80-7502-233-2.

[3] NORRIS, P. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide.* Cambridge: Cambridge University Press, 2001.

[4] UBALDI, B. CH. The impact of the Economic and Financial crisis on e-Government in OECD Member Countries. *European Journal of ePractice*, roč. 5, č. 11, s. 5-18. ISSN 1988-625X.

[5] LECHNER, T. Nová práva na digitální služby. *OBEC&finance*. 2018, roč. XXIII, č. 4, s. 55. ISSN 1212-1363. Veřejná správa online, příloha časopisu Obec & finance.

[6] ŠPAČEK, D. *eGovernment – cíle, trendy a přístupy k jeho hodnocení.* Praha: C. H. Beck, 2012, 258 s. ISBN 978-80-7400-261-8.

[7] STODŮLKA, Z. *Elektronizace spisové služby jako nástroj transparentního výkonu veřejné moci.* In Konference ISSS 2018, Hradec Králové. Dostupné na <http://www.isss.cz/archiv/2018/download/prezentace/na_stodulka.pdf>.

[8] POLČÁK, R., a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, 656 s. ISBN 978-80-7598-045-8.

[9] Vládní program digitalizace České republiky 2018+: Informační koncepce České republiky. Dostupné na <https://www.mvcr.cz/soubor/vladni-program-digitalizace-ceske-republiky-2018-digitalni-cesko-informacni-koncepce-cr.aspx>.

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/43/2018 „Analýza ekonomických, právních a dalších dopadů obecného nařízení o ochraně osobních údajů (GDPR)“.

ÚNIKY DAT
JAK SI NEJLÉPE CHRÁNIT SVOU VNITROFIREMNÍ SÍŤ

Jan Linhart, H-Square ICT Solutions
Tibor Tvardzik, Palo Alto Networks

Dávno pryč jsou časy, kdy bylo možné považovat interní zdroje a uživatele za důvěryhodné. Velká většina úniků dat má totiž jednoho společného jmenovatele – tím je uživatel, který byl označen za důvěryhodného, a z tohoto důvodu mu byla přidělena větší oprávnění, než reálně k výkonu svého povolání potřeboval.

Zřejmě nejznámějším příkladem takového úniku je Edward Snowden, který získal a zveřejnil ohromné množství vysoce citlivých dat, ke kterým by v případě správně nastavených oprávnění nemohl mít přístup. Na základě podobných událostí pomalu dochází k přehodnocení toho, jak obecně přistupovat k zabezpečení firemního IT.

Nejčastěji používaným bezpečnostním modelem je ve většině organizací takový, jenž je založen na ochraně venkovního perimetru společnosti. Podnět pro jeho vznik lze hledat desítky let zpátky, v době, kdy společnosti a organizace přestaly z důvodu rychlého úbytku používat v interních sítích k adresaci veřejné IP adresy.

Nástupem privátních IP adres ale došlo k rozdělení světa uvnitř a vně organizace a logicky se přešlo k ochraně tradičním postupem, tedy ke stavbě zdi mezi vnitřní částí, kterou je nutné chránit, a venkovním nebezpečným prostředím.

Typický průběh útoku

Pokud se však podíváme na průběh většiny současných útoků, tento způsob ochrany se ukazuje jako naprosto nevyhovující. Jestliže si útočník vybere vaši organizaci za cíl, zpravidla podnikne následující kroky.

Prvním z nich je fáze získání informací. Tu lze rozdělit na pasivní část, kdy se shromažďují volně dostupné údaje, zejména ze sociálních sítí, a na část aktivní, kdy dochází ke skenování portů, hledání zranitelností v používaném softwaru, a zejména k sociálnímu inženýrství.

Po získání informací útočník vytvoří či zakoupí nástroj, který se použije pro průnik do interní sítě. Tento nástroj se následně doručí do jednoho z interních počítačů, které jsou umístěné již za perimetrovou ochranou.

Způsobem takového doručení může být například e-mail, velmi osvědčenou metodou ale je i jednoduché pohození Flash disku nebo paměťové karty před vchodem do dané společnosti (tzv. baiting).

S pravděpodobností, která se blíží jistotě, se najde jedinec, který prozkoumá, co se na daném disku nebo v emailu nachází. Jakmile se škodlivý kód spustí, je z interní sítě navázán zabezpečený kanál do řídicího centra a dochází k ovládnutí počítače.

Útok pokračuje pokusem o získání kontroly nad dalšími počítači v interní síti. Vzhledem k tomu, že již má přístup k jednomu počítači, může velice snadno zjistit verze nainstalovaných programů a jejich známé zranitelnosti.

S vysokou pravděpodobností budou i ostatní stanice v síti obsahovat stejné verze programů se shodnými zranitelnostmi, které je pak velmi jednoduché využít k ovládnutí zbylých prvků v síti.

V tuto chvíli je útočník už za perimetrem – v důvěryhodné síti, na důvěryhodném počítači. Znamená to snad, že se překonáním perimetru stal důvěryhodným? Necháme ho se v rámci této důvěryhodné sítě pohybovat bez kontroly a nutnosti autorizace?

Pravděpodobně to není úplně nejlepší nápad. Částečně tomuto problému zabrání interní perimetry, ale i jejich překonání je v podstatě pouze otázkou času.

Obecně lze konstatovat, že perimetr tvořený firewallem je stále velmi silným nástrojem, ale nesmí to být jediný nástroj pro zabezpečení organizace. V průběhu času se organizace nespoléhaly pouze na firewall a doplňovaly bezpečnostní systémy dalšími prvky, jakými jsou IPS, antivirus, webová proxy, SIEM apod.

Typicky však výběr neprobíhal jako doplnění celku, ale snahou bylo koupit co nejlepší dostupný produkt. Výsledkem byla velice heterogenní bezpečnostní infrastruktura. Bohužel s každým ze systémů zároveň nepřibyla pracovní místa bezpečnostních analytiků.

Stejný počet lidí tak musel následně řešit řádově vyšší počty bezpečnostních událostí, kterých přibývalo s každým dalším prvkem zapojeným do bezpečnostního systému organizace. A se zvyšujícím se počtem i sofistikovaností útoků se stal tento přístup ke správě bezpečnosti neúnosným.

Moderní přístup

Základní požadavky na moderní komplexní bezpečnostní řešení je proto nutné předefinovat:

- Musí se zajistit schopnost zaznamenat každý z výše popsaných kroků útoku a v reálném čase jej zablokovat. Vzhledem k tomu, že ne všechny kroky lze detekovat prostřednictvím jednoho bezpečnostního prvku, je potřeba vytvořit komplexní systém zabezpečení skládající se z více komponent.
- Komponenty systému musejí být vzájemně provázané, tak aby detekce události jedním prvkem spustila řetěz protiopatření na dalších prvcích do systému zařazených.
- Systém musí být připraven pro automatizaci. Čas bezpečnostních analytiků a správců je příliš drahocenný, a proto je nutné co nejvíce rutinních operací dělat bez jejich zásahu.
- Systém musí být připraven pro jednoduché doplnění nového detekčního mechanismu. Ve chvíli, kdy výběr a nasazení detekčního systému založeného na nových poznatcích a trendech trvá rok nebo i více, je organizace po nepřiměřeně dlouhou dobu nechráněná před typy útoků, které by bylo možné v případě rychlého nasazení inovovaného řešení účinně eliminovat.

Komplexní systém zabezpečení musí být schopen poskytnout minimálně následující funkce:

- Ochranu a řízení síťového provozu nejen v rámci tradičních sítí, ale také v rámci veřejného cloudu. Zástupcem prvků této kategorie jsou firewally nové generace, které poskytují možnost řídit provoz na úrovni aplikací, činit dekrypci šifrovaného provozu, detekci a zastavení známých i neznámých hrozeb nalezených v síťovém provozu, kontrolu URL apod.

  Palo Alto Networks toto řeší použitím Next-Generation firewallu, který rozděluje tyto dva světy, chrání vnitřní část sítě prováděním detailní inspekce provozu a aplikováním bezpečnostních profilů. Tento přístup k bezpečnosti oceňuje i Gartner, který řadí Palo Alto Networks mezi top výrobce v magic kvadrantu pro Next-Gen firewally již od roku 2012.

- Ochranu koncových stanic. Pokročilým systémem pro ochranu koncových stanic je produkt Traps od Palo Alto Networks, který je schopný bez použití definic založených na signaturách chránit jak před malwarem, tak před exploity – známými i tzv. zero-day útoky. To všechno s minimálním dopadem na hardwarové prostředky operačního systému.
- Kontrolu dat aplikací SaaS (Software-as-a-Service) použitím Aperture. Při používání aplikací SaaS jako například MS Office365, Dropbox apod. může dojít ke snadnému sdílení dokumentů, které obsahují citlivá a osobní data. Nejen z důvodu vysokých sankcí daných nařízeními GDPR je nutné mít tato data pod plnou kontrolou. Aperture obsahuje zabudované kontroly pro dodržování GDPR a také umožňuje jeho vynucování nebo generování reportů v uživatelsky přívětivé formě.
- Detekce a zamezení šíření nákazy v síti použitím unikátního systému pro detekci a odezvu Cortex XDR. Systémy pro detekci anomálií v síťovém provozu mohou zjišťovat a následně pomocí dalších prvků bezpečnostního systému zablokovat anomální chování. V souvislosti s detekcí anomálie je potřeba získat co největší množství informací ze sítě, koncového

bodu a z cloudu. Nestačí znát, jaká IP adresa danou akci vykonala, ale i kdo byl na stanici přihlášený, jaký proces inicioval spojení, jestli byl daný proces zhodnocen jako škodlivý apod., a také tyto informace korelovat pro odhalení anomálií a škodlivého chování v síti.

Další opatření

Kromě nasazení provázaných bezpečnostních nástrojů je nutné přejít i ke změně koncepce a vyvarovat se zažitých mechanismů spojených s důvěrou – tzv. trustem. Jedním ze základních předpokladů je chovat se k interním zdrojům stejně, jako by byly zdroji externími.

Následným krokem je vykonávání autentizace a autorizace, kdykoliv je to možné. Pokud se pro přístup do síťové infrastruktury požaduje pouze autentizace stanice a ta má následně povolený přístup kamkoliv do sítě, je potřeba se na tento nedostatek zaměřit.

Nelze od sebe oddělovat stanici a uživatele, který ji používá. Tyto dvě entity je nutné ve tvorbě pravidel brát jako jeden celek. Zároveň s tím musí dojít k zavedení principu nejnižších možných oprávnění, kdy se nikomu nepřidělí práva nad rámec nezbytně potřebných pro plnění jeho pracovních povinností.

Pro přístup k aplikacím obsahujícím jakákoliv citlivá data je nutné použít multifaktorovou autentizaci. Pro aplikace, které tento typ autentizace nepodporují nativně, je třeba tento způsob zajistit na úrovni síťových zařízení.

Naprosto nezbytnou součástí bezpečnosti je i patch management. Velké množství útoků přichází ze zneužití známých zranitelností, na které jsou už k dispozici opravy. Pokud budou systémy aktuální, riziko úspěšného útoku se výrazně snižuje.

Doporučuje se též zamezit horizontálnímu šíření provozu mezi koncovými body umístěnými v jedné VLAN. I tento provoz by měl být vždy autorizovaný. Toho lze docílit šifrováním dat, ať již za pomoci technologií pracujících na druhé vrstvě modelu ISO/OSI, nebo vynucením always-on VPN, nezávisle na tom, jestli se daná stanice nachází v internetu nebo v interní síti.

V Palo Alto Networks věříme, že pro efektivní zastavení sofistikovaných kybernetických útoků je nutné sjednotit data ze sítě, koncových stanic i z cloudu. Aplikováním behaviorální analýzy a strojového učení můžeme odhalit hrozby z jakéhokoli zdroje, poskytnout kompletní obraz o každé hrozbě a automaticky zjistit zdroj problému.

ELEKTRONICKÉ SKARTAČNÍ ŘÍZENÍ V PRAKTICKÉ PODOBĚ

Ing. Zdeňka Marková, Renata Dymešová, MěÚ Chvaletice
Mgr. Tomáš Lechner, Ph.D., Triada, spol. s r. o.

Úvod

Skartační řízení je proces, při kterém dochází k výběru dokumentů a spisů uložených ve spisovně úřadu, přičemž výsledkem tohoto procesu jsou buď archiválie, které jsou dále ukládány v příslušných archivech, nebo souhlas s nevratným zničením nepotřebných dokumentů a spisů. Povinnost provádět pravidelně skartační řízení plyne pro všechny veřejnoprávní původce jednak ze zákona č. 499/2004 Sb., o archivnictví a spisové službě, a jednak z nařízení Evropského parlamentu a Rady (EU) č. 679/2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které zakazuje zpracovávat osobní údaje po dobu delší, než je nezbytně nutné k naplnění příslušného účelu zpracování. Konkrétní postup skartačního řízení musí každý původce upřesnit ve svém spisovém řádu, neboť příslušné předpisy dávají určitou volnost ve stanovení některých místních specifik. Blíže k procesu skartačního řízení viz publikaci [1].

Od roku 2012 preferované vedení spisové služby v elektronické podobě znamená také elektronizaci procesu skartačního řízení. Na konferenci CNZ konané v říjnu loňského roku bylo prezentováno, že v roce 2017 proběhlo 63 těchto skartační řízení v elektronické podobě, z čehož bylo 32 dotaženo do podoby přejímky analogových a digitálních archiválií, a v roce 2018 (tedy do října uvedeného roku) bylo těchto řízení realizováno 100 a jen 18 z nich bylo dotaženo do fáze přejímky archiválií [2]. Podle výroční zprávy Moravského zemského archivu bylo jen v tomto archivu za rok 2017 provedeno přes 1800 skartačních řízení [3], což znamená, že na celou Českou republiku lze odhadnout počet těchto řízení až k 10 tisícům za rok, a tedy procento elektronických skartačních řízení je stále velmi malé.

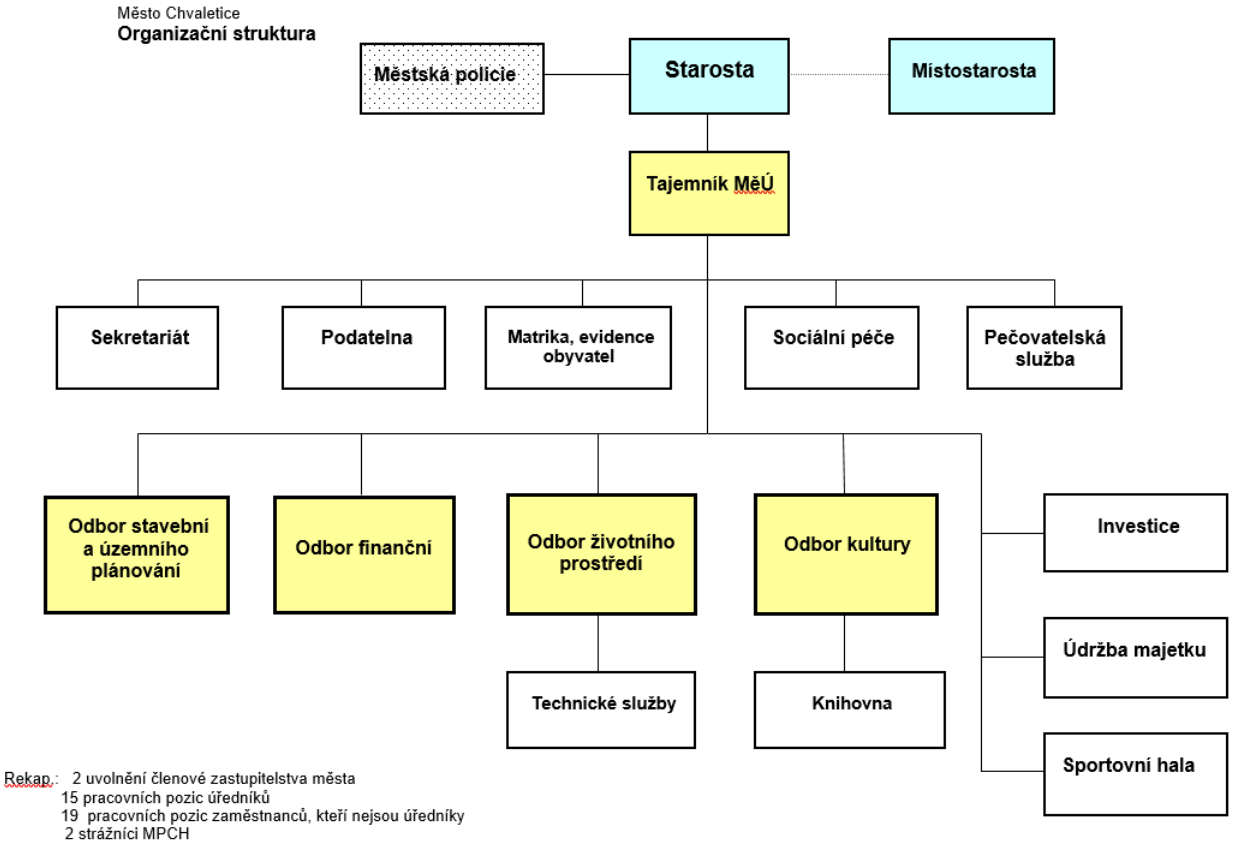
Proto je jistě důležité věnovat se problematice získávání zkušeností s tímto procesem v praxi různých původců. Tento příspěvek se soustředí na praktické zkušenosti Městského úřadu Chvaletice.

Obr. 1: Pohled na město Chvaletice, zdroj [4].

Město a Městský úřad Chvaletice

Město Chvaletice leží 25 km západně od Pardubic na rozhraní Chvaletické pahorkatiny a Pardubické kotliny v nadmořské výšce přibližně 260 m.n.m. V písemných zprávách se Chvaletice objevují poprvé v roce 1393, kdy byl dvůr s tvrzí u obce majetkem Hereše z Chvaletic. V 50. letech 20. století musela podstatná část obce ustoupit těžbě pyritové břidlice. Statut města získaly Chvaletice 1. ledna 1981. V současné době mají Chvaletice přibližně 3000 obyvatel. Ve městě je základní škola, mateřská škola, Střední odborné učiliště zemědělské a kulturní dům. Služby obyvatelstvu zahrnují poštu, lékárnu, knihovnu, zdravotní středisko apod. Své místo má ve městě i TJ Energetik, FK Baník, Taneční klub a Taneční škola. Město Chvaletice je známé elektrárnou o výkonu 4x200 MW vybudovanou v 70. letech s jedním z nejvyšších komínů v ČR, který měří 300 m. Více informací o městě a jeho okolí poskytují webové stránky města [4].

Městský úřad Chvaletice má 4 odbory, 8 úseků, 15 úředníků a 19 dalších zaměstnanců. Organizační struktura je znázorněna na Obr. 2.



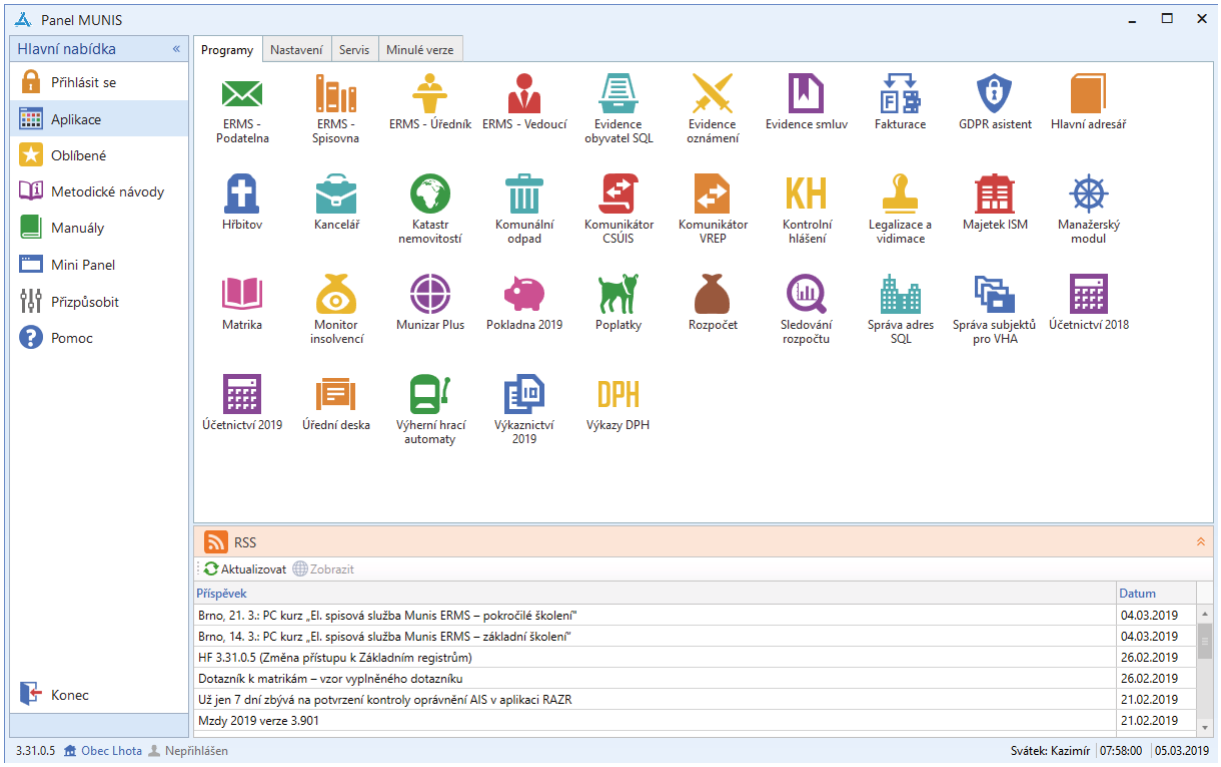
Obr. 2: Organizační struktura městského úřadu Chvaletice.

Městský úřad Chvaletice je pověřený obecní úřad a vykonává přenesenou působnost pro dalších 5 obcí. Správní obvod tak zahrnuje přibližně 6 tisíc obyvatel.

Spisová služba na MěÚ Chvaletice

Městský úřad Chvaletice si pro vedení spisové služby zvolil elektronickou spisovou službu Munis ERMS, která je součástí informačního systému Munis, jehož tvůrcem a dodavatelem je společnost Triada. Tento informační systém má moderní troj-vrstevnou architekturu, přičemž pro uložení dat je možné využít SQL server MS SQL nebo ORACLE ORACLE, ve Chvaleticích

je použit MS SQL server. Aplikační server využívá prostředí .NET 4.5 a pro připojení k SQL serveru má integrován vrstvu Entity Framework. I klientská aplikace využívá prostředí .NET 4.5, k čemuž přidává grafické komponenty WPF, které zajišťují vizuální atraktivitu výsledného produktu v souladu a moderními trendy ovládání aplikací. Aktuálně nabízí informační systém Munis více než třicet základních modulů a k tomu ještě mnoho servisních a konfiguračních aplikací. Ukázka aktuální základní nabídky modulů IS Munis je na Obr. 3.



Obr. 3: Vstupní nabídka modulů informačního systému Munis zobrazená v integračním nástroji nazvaném Panel Munis.

Elektronická spisová služba Munis ERMS je pro větší přehlednost uživatelů a jejich pohodlnější práci rozdělena do pěti aplikací: Podatelna, Úředník, Vedoucí, Spisovna a Nastavení. Licenčně však tvoří kompaktní celek zajišťující všechny potřeby vedení spisové služby od příjmu a tvorby dokumentů, přes jejich evidenci, vyřizování a tvorbu spisů, až po uložení dokumentů a spisů ve spisovně a následnou realizaci skartačního řízení jako posledního kroku životního cyklu dokumentů a spisů u původce.

Aplikace Podatelna slouží pro příjem všech typů dokumentů všemi možnými komunikačními kanály včetně informačního systému datových schránek a elektronické pošty. Přijaté dokumenty jsou zaevidovány a dále předávány k vyřízení vedoucím, nebo jiným pověřeným pracovníkům, jednotlivých odborů. Pro podporu předávání listinných dokumentů jsou tištěny předávací protokoly došlé pošty. Uvedené rozšíření je samozřejmě možné nastavit dle požadavků každého zákazníka. Dále řeší modul Podatelna celou výpravnu, a to opět jak pro listovní zásilky, tak pro elektronické zásilky posílané přes datovou schránku. Modul také eviduje všechny typy doručenek, které lze předávat obdobným způsobem jako dokumenty.

Aplikace Úředník je určena konkrétním pracovníkům pro přebírání a následné přerozdělování došlé pošty. V modulu lze také zaevidovat osobní podání, pokud se podatel dostaví přímo k úředníkovi. Aplikace dále slouží k vyřizování přijatých dokumentů včetně tvorby spisů, popř. typových spisů. V aplikaci Úředník lze vytvářet nové koncepty v mnoha podobách a využívat k tomu předpřipravené vzory, do nichž jsou příslušné údaje automaticky vpisovány. Podle nastavených pravidel jsou koncepty předávány ke schválení, přičemž při tom dochází k převodu digitálních dokumentů do výstupního datového formátu, k elektronickému podepisování kvalifikovaným podpisem podle nařízení eIDAS a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro

elektronické transakce, a k časovému razítkování. Dále lze v aplikaci Úředníky vytvářet zásilky, které jsou dále předávány k vypravení do aplikace Podatelna. V aplikaci Úředník se také připravují vyřízené dokumenty a uzavřené spisy, popř. uzavřené díly typových spisů k předání do spisovny. Při tomto procesu dochází ke všem potřebným kontrolám včetně případného převodu datového formátu podle zákona č. 499/2004 Sb.

Aplikace Vedoucí je speciální rozšíření určené pro uživatelé, kteří se spisovou službou pracují velmi výjimečně a v podstatě jen pro to, aby elektronicky podepsali (schválili) patřičné dokumenty. Cílená je tedy tato aplikace zejména na zastupitele a vedoucí představitele města. Základem přístupu aplikace Vedoucí je jednoduchost a přehlednost. V aplikaci vedoucí lze také kontrolovat činnost podřízených, vyhledávat dokumenty a spisy a zobrazovat různé statistiky.

Aplikace Spisovna zajišťuje celkovou evidenci spisovny a uložených dokumentů a spisů. Dále je v této aplikaci možné realizovat celé skartační řízení v elektronické podobě a odpovídajícím způsobem komunikovat s příslušným archivem. Výstupní SIP balíčky se samozřejmě hromadně generují v rámci daného skartačního řízení, ale je také možné je jednotlivě vytvořit kdykoliv dopředu během uložení dokumentu či spisu ve spisovně. Nejtypičtějším důvodem pro tento postup je ověření jejich kvality pomocí testovacího nástroje zveřejněného Národním archivem.

Aplikace Nastavení se využívá zejména v době konfigurace systému, popř. samozřejmě k dalším úpravám nastavení, pokud jsou v rámci změn u původce nebo v rámci vývoje právních předpisů potřeba. Lze v ní nastavit vše potřebné včetně automatického třídění dokumentů na podatelně, vzorů pro koncepty, schvalovacích procesů, parametrů pro plnotextové vyhledávání, pomocné číselníky metadat pro rychlejší zadávání údajů bez chyb apod.

Městský úřad Chvaletice využívá tuto spisovou službu již mnoho let, přičemž předtím využíval jejího technologického předchůdce, kterým byl modul Kancelář. Všechny dokumenty a spisy evidované v tomto předchůdci byly při změně modulu převedeny do nové elektronické spisové služby, takže úřad disponuje všemi potřebnými daty pro provedení elektronického skartačního řízení. Tab. 1 ukazuje počty čísel jednacích v posledních pěti letech a ilustruje tak rozsah využití spisové služby na úřadě.

Rok	Počet čísel jednacích
2014	5 043
2015	6 134
2016	5 766
2017	6 347
2018	5 723

Tab. 1: Počty čísel jednacích v posledních pěti letech ve spisové službě MěÚ Chvaletice.

Příprava na elektronické skartační řízení

Protože elektronické skartační řízení na rozdíl od řízení v původní listinné podobě vychází z předchozí evidence spisové služby, je základem kvalitní vedení spisové služby [5]. Předchozí postupy vytvářely určitou propast mezi vlastní evidencí dokumentů (v listinné podobě realizovanou v podobě podacího deníku) a skartačním řízením, pro které byly podklady sestavovány na základě oddělené evidence dokumentů a spisů uložených ve spisovně. Tato evidence se tvořila při předávání vyřízených dokumentů a uzavřených spisů do spisovny, přičemž byla oddělena od předchozího životního cyklu těchto entit natolik, že neznamenala žádnou kontrolu, zda v původní evidenci dokumentů je jejich vyřízení či uzavření vůbec vyznačeno.

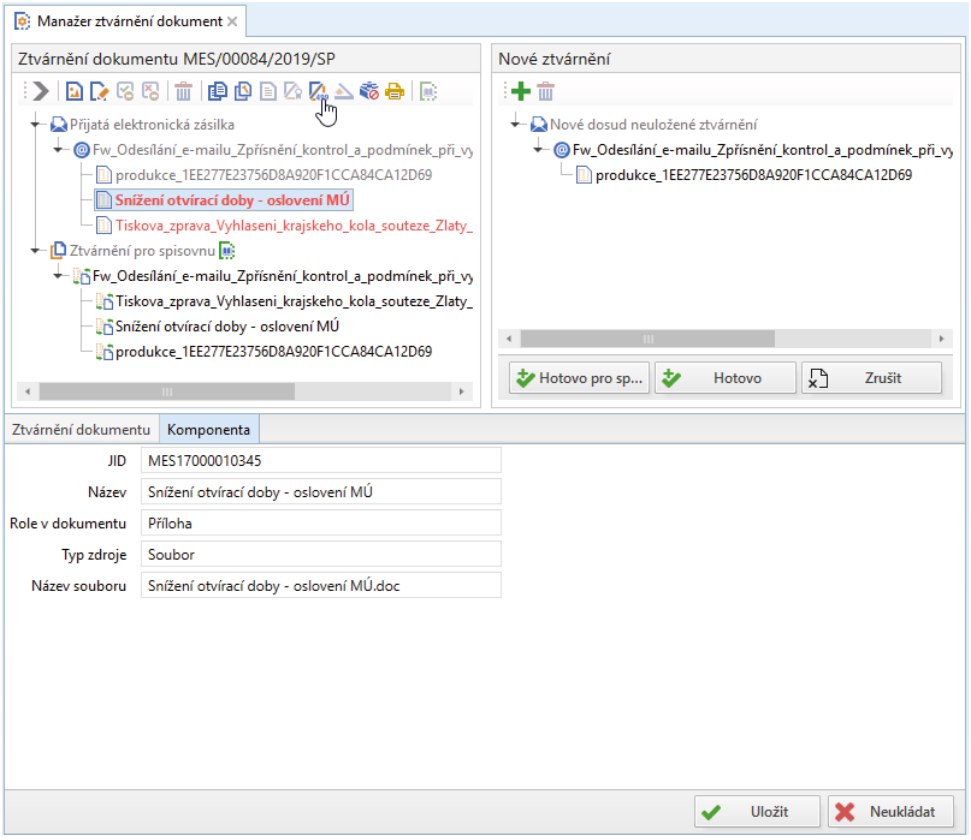
V případě vedení spisové služby v elektronické podobě se tato situace otáčí o „180 stupňů“, tedy skartační řízení je připravováno z dat, která vznikají z primární evidence dokumentů a spisů, jak ji vytvářejí všichni úředníci svou každodenní praxí. A proto je prvotní podmínkou, aby vůbec elektronické skartační řízení mohlo být realizováno, řádné proškolení všech úředníků a následná důsledná kontrola správného, úplného a přesného vedení spisové služby, do níž je třeba zaznamenat každý úkon provedený s dokumentem anebo spisem.

Městský úřad Chvaletice si důležitost školení jasně uvědomuje. Při zavedení spisové služby byly proškoleni všichni úředníci včetně vedení města a městské policie. Následně byly hloubkově proškoleny vybrané osoby, které dále prováděly opakovaná místní školení. Bez řádného opakování a pravidelných následných kontrol skutečného vedení spisové služby do všech důsledků, tedy včetně řádného vyřizování dokumentů, uzavírání spisů a zatřiďování těchto entit do věcných skupin, nemohou vzniknout kvalitní data a bez těchto kvalitních dat nemůže být nikdy realizováno skartační řízení v elektronické podobě.

Dalším významným krokem v přípravě na elektronické skartační řízení je naplnění dat spisovny. Jde o to, že v době oddělení spisové služby od evidence spisovny a následné elektronizaci v podstatě jen první části chybí v elektronickém systému spisové služby informace o uložení dokumentů a spisů ve spisovně. Reálně je tento krok spojen s kontrolami, které při uložení do spisovny musí být provedeny a vlastně by dle zákona měly být prováděny již v okamžiku vyřízení dokumentu a uzavření spisu. Ale praxe často takto důsledná bohužel není.

Zmíněné kontroly závisí na formě evidovaných entit. U listinných dokumentů a spisů je třeba zkontrolovat zejména úplnost, tedy zda evidované množství listů a příloh odpovídá skutečnosti. U digitálních entit je třeba zkontrolovat kvalitu datových formátů, popř. provést převod do výstupního datového formátu podle zákona č. 499/2004 Sb. Výstupní datové formáty jsou dány prováděcí vyhláškou k tomuto zákonu a v případě statických dokumentů je preferovaným datovým formátem PDF/A (blíže viz [1]). U hybridních entit je pak třeba provést kombinaci obou těchto kontrolních mechanismů.

Elektronický systém spisové služby Munis ERMS má tyto kontroly implementovány jako nedílnou součást procesu předání dokumentů a spisů do spisovny, přičemž se snaží uživatelům vycházet vstříc nabídkou různých hromadných procesů. Nicméně poslední slovo má a musí mít vždy úředník, který je zodpovědný za vyřízení dokumentu anebo uzavření spisu.



Obr. 4: Formulář tvorby ztvárnění, který umožňuje plně připravit dokument pro uložení ve spisovně. Všechny funkce pro listinné i digitální dokumenty jsou integrovány do jednoho komplexního formuláře.

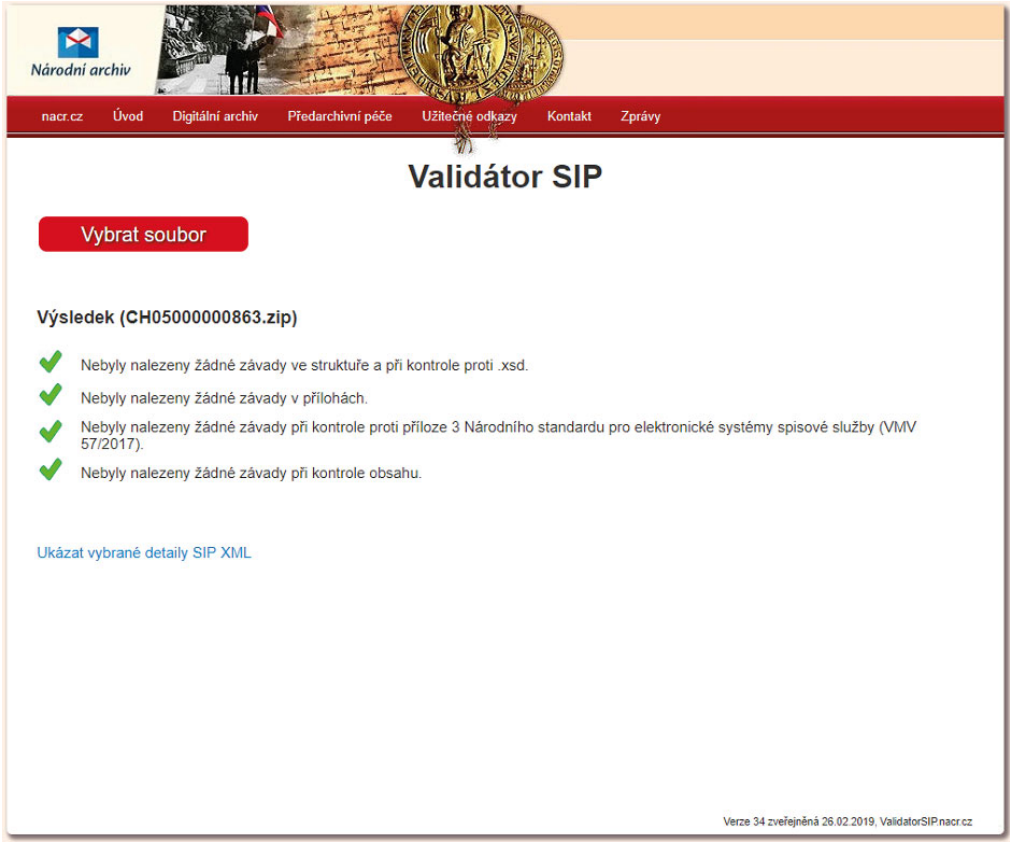
Zkušební elektronické skartační řízení

K otestování připravenosti úřadu na elektronické skartační řízení lze využít dvě cesty:

- Vygenerování SIP balíčků mimo skartační řízení a jejich ověření pomocí nástroje zveřejněného Národním archivem a aktuálně dostupného na adrese <https://validatorsip.nacr.cz/>.
- Vytvoření zkušebního skartačního řízení a využití testovacího národního archivního portálu dostupného na adrese <http://portaltest.nacr.cz/cs/prihlasit/>. Tato varianta samozřejmě již vyžaduje spolupráci archivářů z místně a věcně příslušného archivu.

Městský úřad Chvaletice využil postupně obě tyto varianty. Pro oba testy byla vybrána skupina deseti dokumentů, mezi kterými byly jak dokumenty čistě digitální, tak dokumenty analogové i jeden dokument hybridní. Zároveň byly vybrány zástupci všech tří skartační znaků A, S a V. U digitálních dokumentů byly vybrány, jak zástupci přijatých digitálních dokumentů, u kterých probíhal převod do výstupního datového formátu, tak vlastní „digital-born“ dokumenty, které byly rovnou na úřadě vytvořeny v datovém formátu PDF/A. Tím byly pokryty všechny různé možnosti a varianty, aby výsledný test byl co nejprůkaznější.

Výsledek prvního testu, který ověřoval kvalitu SIP balíčku vygenerovaného mimo skartační řízení, je pro první vybraný dokument na Obr. 5. Stejný výsledek platil i pro všechny další vybrané dokumenty.



Obr. 5: Výsledek kontroly SIP balíčku.

Při druhém testu bylo založeno zkušební skartační řízení, a to nejprve v elektronické spisové službě v aplikaci ERMS Spisovna, aby mohl být připraven zkušební skartační návrh, a posléze bylo toto řízení založeno také na testovacím národním archivním portálu. Přihlašovací údaje pro MěÚ Chvaletice vygeneroval Státní okresní archiv Pardubice, který aktivně a ochotně na celém testu spolupracoval, za což bychom rádi i touto cestou poděkovali.

Ve zkušebním skartačním řízení slouží jako skartační návrh seznam SIP balíčků, který elektronická spisová služba uloží do předem určené složky. Z ní jsou pak tyto soubory vybrány (nalistovány) z testovacího archivního portálu, který je po té načte a provede vstupní kontroly, včetně kontroly antivirové. Výsledky jsou průběžně uživateli zobrazovány. Následně je návrh uzavřen, čímž dojde k předání SIP balíčků příslušnému archiváři, který provádí další kontroly a hlavně vlastní výběr (detailní popis celého procesu je k dispozici na webu Národního archivu [6]). K tomu je vhodné dodat, že u elektronického skartačního řízení již nenavrhuje rozdělení skartačního znaku V na S a A původce, ale toto rozdělení řeší až v rámci vlastního výběru archivář. Ten může také požádat prostřednictvím portálu o předložení detailnějších informací nutných pro zodpovědné rozhodnutí.

Zpráva o schválení souboru	
Identifikátor:	CZNDA225202010ESK3887
Archiv:	Státní okresní archiv Pardubice
Původce:	Městský úřad Chvaletice, Pardubice, Česko
Archivář I:	
Původce I:	Renata Dymešová
Nahráno N souborů:	10
Schváleno O souborů:	10
Zamítnuto P souborů:	0
Nahrané soubory:	CH010000036930.zip; CH05000000863.zip; CH010000037079.zip; CH05000000866.zip; CH05000299389.zip; CH010000037061.zip; CH010000036495.zip; CH010000039772.zip; CH05000299293.zip; CH010000037326.zip

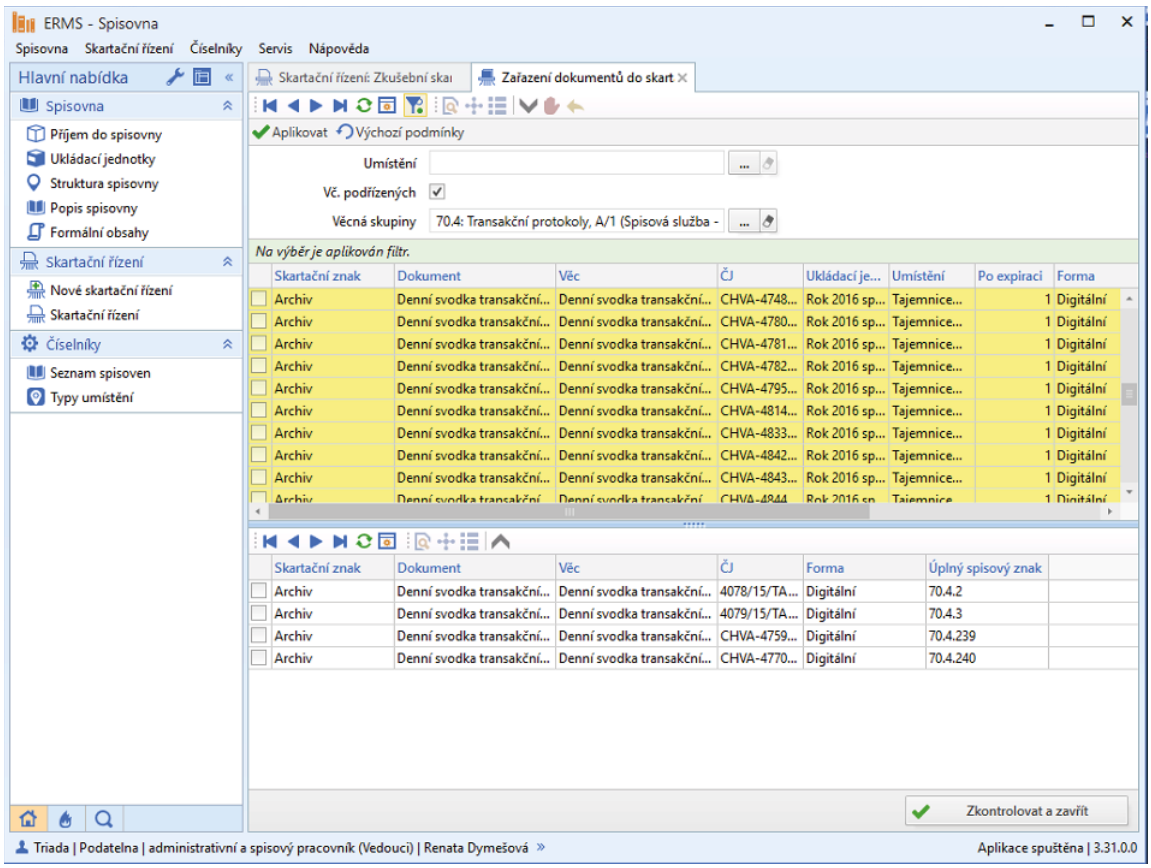
Název	Schváleno
CH010000036930.zip	**ANO**
Datum: čt 28. únor 2019 (09:52) **Velikost:** 11.03 KB **SHA512:** d296cbea5cc700f7a68540803ab923062a64ecfcaacfeb20840db5cef366762be55494d1c54b10f72b7bf816c90b7b8c3927b4b15cb93eaa7b9d5f22517deed2	
CH05000000863.zip	**ANO**
Datum: čt 28. únor 2019 (09:52) **Velikost:** 197.21 KB **SHA512:** f4f2302fbb6cc9cf0139ebd89063228a3f71e48882f68336f6fbca3oedd034a9e726aaa8c386598699e019bfe5b27f2bd47485ee00effaf662b8b5d9ad086fd8	
CH010000037079.zip	**ANO**
Datum: čt 28. únor 2019 (09:51) **Velikost:** 11.31 KB **SHA512:** 6863963994ec723c26b42cf107f096e4a3b6287bbc7e9e2b97072f54a6458e13bod6d75dcf3049cf76966ebe9b0542863ef16141bb0e0c82afbaf362aa537343	
CH05000000866.zip	**ANO**
Datum: čt 28. únor 2019 (09:51) **Velikost:** 111.74 KB **SHA512:** 516e798bb911c3476e1aba96cc3be6df9defa6e10b2c51b85c91dcffcfc699d58fbe6307e2d056e30b7bb797804ff42c5c0f9ae24370d8d50588ea2111706967	
CH05000299389.zip	**ANO**
Datum: čt 28. únor 2019 (09:51) **Velikost:** 283.95 KB **SHA512:** 5cb4cd8b9d15e07d8ca9fd8d08bfdfb3d4b2cb4433ec1dab284710e1febf291b892cc0805e00e37ee88d7b99301d8af62d870a1dfdcc4baab333031bb2756795	
CH010000037061.zip	**ANO**
Datum: čt 28. únor 2019 (09:51) **Velikost:** 11.31 KB **SHA512:** 64a7b465dfdb8420a05323717bd66b2a1bfd8f368769c57fc9ed03897cdf4f3c6729bdae15e3c8742fc790271d43bdd49b676d8741520aba5097fc7219802d68	
CH010000036495.zip	**ANO**
Datum: čt 28. únor 2019 (09:51) **Velikost:** 305.77 KB **SHA512:** ed7d04f70b10efc4de48b472659c9f6ecb7228b2781651cdc129e6fe32e495a8485265dceff0eec4924bfe322bd152ab77cf7d438fa3bde499ab60a00ceef424	
CH010000039772.zip	**ANO**
Datum: čt 28. únor 2019 (09:50) **Velikost:** 11.26 KB **SHA512:** 4ca84c931048d29c48c89cab841a8a5a6c6288400f764da7eb80e2e024281423ed8ed54e6a1cfab3fffbaae3f888a2d2d8954dea7b3c1e3cdef8782eed64222b	
CH05000299293.zip	**ANO**
Datum: čt 28. únor 2019 (09:50) **Velikost:** 334.06 KB **SHA512:** 2e04e9b70857bfca329a788a6eae6adcc6dc2da3db7f206cad85b20266a13f11a75e8e82f7a8748d1cc3e91e9b41c5963381360b3ed0319b8ed8e7dcc6964ad	
CH010000037326.zip	**ANO**
Datum: čt 28. únor 2019 (09:50) **Velikost:** 335.02 KB **SHA512:** 2d25793c617e452bb8de2696c107908bcf6f1a293f5fafe7e62f99e883fa6189822df1b9aa1a1a961ef898be4176166d5078bc921e79a85378896a31465caf29	

Obr. 6: Náhled na protokol o přijetí SIP balíčků do zkušebního skartačního řízení.

Obr. 6 ukazuje informace o výsledku přijetí deseti vybraných SIP balíčků do zkušebního skartačního řízení. Všechny SIP balíčky prošly technickou kontrolou, nicméně následně byly odhaleny některé nedostatky, např. z hlediska datace otevření věcných skupin. Je tedy třeba zdůraznit, že kontrolu archiváře nemůže nikdy žádný stroj plně nahradit, a proto nestačí jen formální test SIP balíčků pomocí nástroje zveřejněného Národním archivem, ale je třeba obou výše zmíněných postupů, aby se vše odladilo a připravilo na ostré skartační řízení v elektronické podobě.

Elektronické skartační řízení

Podmínkou pro provedení ostrého skartačního řízení je úspěšné projití předchozími testy. Pokud se vám toto podaří, máte dveře otevřené. V rámci skutečného elektronického skartačního řízení je třeba se zejména připravit na to, že jednotlivé kroky nějakou dobu trvají. Nějakou dobu trvá, než spisová služby vygeneruje stovky SIP balíčků, nějakou dobu trvá, než je archivní portál načte a zpracuje. Jednotlivé kroky samozřejmě není třeba po celou dobu sledovat, tedy mohou probíhat bez zásahu obsluhy pouze s průběžnou kontrolou. Ale je třeba si vyhradit příslušný čas a postupně posouvat krok za krokem celý proces ke zdárnému konci.



Obr. 7: Zařazení dokumentů do skartačního řízení.

Tyto kroky jsou:

1) Vytvoření elektronického skartačního řízení v elektronické spisové službě v aplikaci ERM Spisovna.
2) Výběr dokumentů a spisů s prošlou skartačního lhůtou a bez nastaveného příznaku pozastavení skartační operace (viz Obr. 7).
3) Vytvoření průvodního dopisu pro archiv (skartačního návrhu) včetně přílohy v podobě seznamu zařazených dokumentů a spisů.

4) Uložení odpovídajících SIP balíčků do určené složky.
5) Přihlášení na archivní portál a vložení souborů se SIP balíčky.
6) Uzavření skartačního návrhu na archivním portálu.
7) Následuje práce archiváře, která se samozřejmě také skládá z mnoha dílčích kroků, jejichž výsledkem je odpověď obsahující výběr archiválií. Před tento výsledek může být vložen dílčí mezikrok s žádostí po předání dalších informací k některým předkládaným dokumentům.
8) Zpracování (načtení) odpovědi archivu do spisové služby.
9) Předání vyžádaných listinných archiválií ve stejném režimu, v jakém probíhalo v původním schématu skartačního řízení.
10) Předání plných SIP balíčků digitálních archiválií.
11) Předání listinných dokumentů, které se mají zničit k trvalému protokolovanému zničení.
12) Smazání předaných digitálních dokumentů a smazání těch digitálních dokumentů, u nichž bylo povoleno zničení, z dokumentového úložiště elektronického systému spisové služby.

Shrnutí

Nezbytné podmínky pro úspěšné zvládnutí elektronického skartačního řízení jsou následující:

- poctivé vedení spisové služby všemi úředníky,
- důraz na školení a kontroly, protože bez nich nelze první podmínku splnit,
- komunikace s místně a věcně příslušným archivem a komunikace s dodavatelem elektronického systému spisové služby,
- naplnění dat spisovny, což vychází z procesů vyřizování dokumentů a uzavírání spisů a jejich kontroly,
- otestování vytvářených SIP balíčků jak po formální stránce pomocí nástroje zveřejněného Národním archivem,
- zkušební elektronické skartační řízení, během něhož jsou vytváření SIP balíčky zkontrolovány zkušeným pohledem archiváře a dalšími nástroji testovacího národního archivního portálu.

Pokud se těchto kroků budete držet, tak to také jistě zvládnete a množství provedených elektronických skartačních řízení dotažených až do úspěšných přejímek dokumentů bude narůstat.

Literatura

[1] Kunt, M., Lechner, T. *Spisová služba*. 2. aktual. vyd. Praha : Leges, 2017. 384 s. Praktik. ISBN 978-80-7502-233-2.

[2] Kunt, M. *Skartační řízení z elektronických evidencí dokumentů jako obraz elektronizace veřejné správy*. In Konference CNZ 2019. Dostupné na adrese <http://www.cnz.cz/wp-content/uploads/2018/10/CNZ2018_Kunt.pdf>.

[3] Výroční zpráva Moravského zemského archivu za rok 2017. Dostupná na adrese <http://www.mza.cz/sites/default/files/mza_vyrocni_zprava_za_rok_2017.pdf>.

[4] Oficiální webové stránky města Chvaletice dostupné na adrese <http://www.chvaletice.cz/>.

[5] Hottmarová, V., Jirásek, P, Rálišová, I., Lechner, T. *Elektronické skartační řízení v praxi*. In: Pánková, K. (ed.) ISSS 2017 – Internet ve státní správě a samosprávě. Hradec Králové, 3. 4. 2017–4. 4. 2017. Praha: Triada, 2017, s. 21-32. ISBN 978-80-904566-9-3.

[6] Stodůlka, Z., Kunt, M. *Národní archivní portal: Výběr ve skartačním řízení. Příručka pro původce.* Dostupné na adrese <http://www.nacr.cz/wp-content/uploads/2019/01/ESK_prirucka_puvodci_1_1.pdf>.

UTILITYREPORT – SNADNÉ, RYCHLÉ A ON-LINE VYJADŘOVÁNÍ K EXISTENCI SÍTÍ

Mgr. Lukáš Opat, ředitel marketingu a komunikace, HRDLIČKA spol. s r. o.

Společnost HRDLIČKA v minulém roce zcela přepracovala službu UtilityReport, která zjednodušuje proces vyjádření k existenci sítí na straně žadatele, příjemce žádosti i příslušného stavebního úřadu. Umožňuje snadné, rychlé a on-line odeslání hromadných žádostí dotčeným správcům sítí v místě plánované stavby, což žadateli šetří velké množství času i financí. Služba je podporována orgány veřejné moci a aktuálně je v ní zapojeno více než 500 měst a 8 krajů.

Proč tato služba?

Hromadná žádost o vyjádření k existenci sítí je vytvořena kompletně skrze webovou aplikaci zajišťující úplnost žádosti a zrychlení celého procesu vyjádření, čímž služba UtilityReport napomáhá k elektronizaci veřejné správy v procesu stavebního řízení, který je jedním z cílů eGovernmentu, za což získala v minulém roce speciální ocenění „The Best 2018“ v kategorii projekty měst.

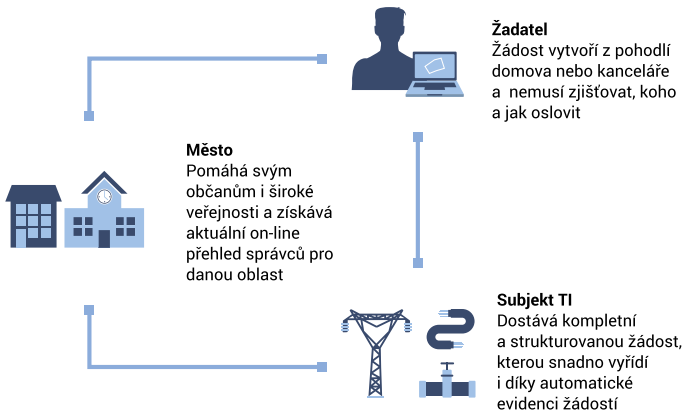
Služba funguje od roku 2010 a za tu dobu bylo skrze ni podáno více než 1,3 milionu žádostí. Aplikace je používaná nejen u nás, ale také na Slovensku, kde ji Ministerstvo hospodářství Slovenské republiky v roce 2018 ocenilo 1. místem v soutěži „Inovatívny čin roka“ v kategorii Inovace a služby.

Jak služba funguje?

Vytvoření žádosti skrze webovou aplikaci probíhá on-line ve čtyřech krocích interaktivního formuláře s integrovaným mapovým oknem, takže je celý proces velice jednoduchý, intuitivní a opravdu ho zvládne úplně každý.

Pro úspěšné podání žádosti stačí vyplnit informace o akci (stavbě), žadateli, investorovi a zakreslit zájmové území, pro které se následně vygeneruje seznam dotčených správců sítí a připraví plnohodnotné žádosti pro odeslání ve formátu PDF. Správcům, kteří přijímají žádosti elektronicky, se po dokončení procesu žádosti automaticky odešlou, ale zbývajícím správcům je zatím nutné žádosti doručit svépomocí.

Seznam správců sítí je pravidelně aktualizován a kontrolován ve spolupráci s příslušnými stavebními úřady, což z něj dělá nejaktuálnější dostupný seznam v České republice. V současné době obsahuje více než 7.900 registrovaných subjektů, kteří se aktivně vyjadřují k existenci svých sítí.



Pro koho je služba určena?

- stavebník / developer / projektant / úředník – podává žádost o vyjádření k existenci sítí
- vlastník / provozovatel / vyjadřující – dostává jednoznačnou strukturovanou žádost o vyjádření
- státní správa / samospráva – umožňuje bezplatné využití služby veřejnosti a získává on-line přehled správců sítí

Jaké jsou výhody služby?

Správcům sítí posíláte vždy úplnou žádost (údaje se vyplňují pouze jednou), a navíc jen těm, kterým je to skutečně potřeba, protože seznam správců je díky pravidelné aktualizaci a kontrole aktuální a díky tomu nikoho neopomenete.

Současná verze aplikace přináší video návody, průvodce a kontextovou nápovědu. Při vyplňování adres dochází k jejich našeptávání a zároveň k automatické kontrole. Přibyla také možnost přidávat různé přílohy k žádostem.

Registrovaní uživatelé mohou podávat žádosti po celém území České republiky a pro větší pořádek mají přehled o svých již odeslaných žádostech. Mohou si přednastavit celou řadu vstupních údajů nebo nahrávat zájmová území ve formátu JSON (odpadá tedy nutnost „ručně“ je kreslit v mapě).

TVORBA SPISOVÉHO ŘÁDU A REVIZE SPISOVÉHO A SKARTAČNÍHO PLÁNU

Tomáš Pitrocha, OÚ a DSO Domašov
Mgr. Tomáš Lechner, Ph.D., TRIADA, spol. s r. o.

Úvod

Každý původce, mezi které patří samozřejmě všechna města, obce, kraje, školy a další orgány veřejné moci, má právo upravit pravidla svého vnitřního fungování ve vnitřních směrnicích. Některé z těchto směrnic jsou navíc povinné, a tedy původce je musí vydat. Patří mezi ně také spisový řád, který původce vydává podle § 66 zákona č. 499/2004 Sb., o archivnictví a spisové službě, a podle § 110 zákona č. 128/2000 Sb., o obcích (blíže viz [2]) . V loňském roce významně obnovený zájem o oblast ochrany osobních údajů navíc stimuloval otázky kolem kvality a správnosti stěžejní přílohy jmenované směrnice, kterou je spisový a skartační plán. Tento plán definuje třídění dokumentů a spisů podle jejich obsahu do věcných skupin, přičemž každé věcné skupině přiřazuje skartační lhůtu (typicky v letech) a skartační znak.

Tvorba spisového řádu včetně všech jeho příloh není jednoduchou záležitostí, obzvláště pokud má být spisový řád funkčním předpisem a nejen formálním dokumentem uloženým na dně nějakého šuplíku. Proto společnost Triada přišla již v loňském roce s nabídkou služby celkové pomoci s přípravou této směrnice a identifikací slabých míst ve vedení spisové služby na úřadě. Tento příspěvek shrnuje dosavadní zkušenosti a na případové studii obce Domašov dokumentuje průběh tvorby nového spisového řadu.

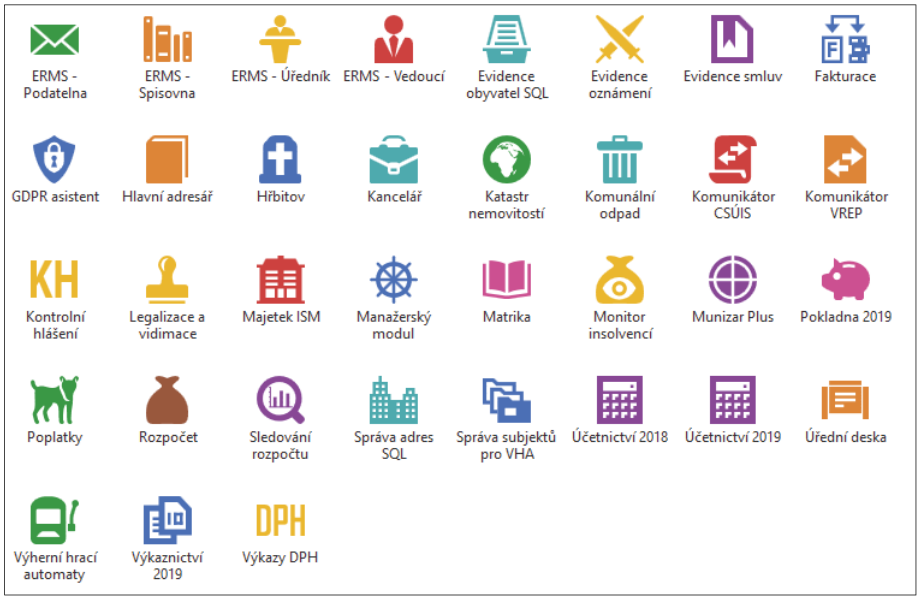
Role spisové služby v úřadování

Spisová služba je často úředníky vnímána negativním způsobem, neboť poměrně přísně formalizuje postupy a pravidla pro nakládání s dokumenty po celou dobu jejich životního cyklu u úřadu. Avšak toto precizní dodržování základních postupů úřadování a přesná evidence dokumentů je základem fungování veřejné správy již více než dvě stě let. Podle aktuálně platných předpisů je spisová služba odbornou správou 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 [§ 2 písm. l) zákona č. 499/2004 Sb.].

Spisová služba musí reflektovat vývoj společnosti směrem k celkové digitalizaci, a proto je již od roku 2012 preferovanou volbou (pro některé původce dokonce povinnou formou) elektronické vedení spisové služby. Má-li být elektronizace veřejné správy skutečně efektivní, musí být na vnější komunikační a informační nástroje e-Governmentu jako jsou datové schránky, aplikace CzechPOINT, základní registry apod. napojen v rámci vnitřního fungování úřadů výkonný systém, který přímočaře spojuje vnitřní a vnější procesy každodenního úřadování. Správně nastavený elektronický systém spisové služby je tak užitečným pomocníkem, který bdí nad dodržováním domluvených postupů a zajistí, aby evidence dokumentů byla úplná, aby elektronické dokumenty mohly být jednoduše přijímány a odesílány prostřednictvím elektronických komunikačních kanálů, aby nakládání s dokumenty a spisy bylo transparentní a průkazné, aby se ani listinné dokumenty neztrácely a aby byly dodržovány zásady ochrany osobních údajů včetně zásady omezeného uložení pouze po dobu nezbytně nutnou pro dosažení daného cíle zpracování (viz též [1]).

Jednou z možných elektronických systémů spisových služeb, která oplývá vysokou variabilitou a přizpůsobivostí pro úřady různých velikostí, je elektronická spisová služba Munis ERMS. Jedná se o jeden z modulů informačního systému Munis, jehož tvůrcem i dodavatelem je společnost Triada. Elektronický systém spisové služby Munis ERMS modul je pro přehlednost rozdělen do pěti aplikací: Podatelna, Úředník, Vedoucí, Spisovna a Nastavení. Avšak licenčně vždy tvoří nedělitelný celek podporující všechny funkce spisové služby včetně vedení spisovny a elektronického skartačního řízení.

Aplikace Podatelna slouží pro příjem všech typů dokumentů všemi možnými komunikačními kanály včetně informačního systému datových schránek a elektronické pošty. Dále aplikace Podatelna obsluhuje celou výpravnu, a to opět jak pro listovní zásilky, tak pro elektronické zásilky posílané přes datovou schránku, nebo e-mailovou výpravnou. Aplikace Úředník je určena konkrétním pracovníkům pro přebírání a následné vyřizování přijatých dokumentů včetně tvorby spisů. Dále umožňuje vytvářet nové koncepty v mnoha podobách a na základě nastavených schvalovacích procesů z nich dělat dokumenty s komponentami ve výstupním datovém formátu. V této aplikaci lze také připravovat zásilky následně předávané k vypravení do aplikace Podatelna. Aplikace Vedoucí je jednoduchou a přehlednou nadstavbou určenou pro snadné schvalování a elektronické podepisování konceptů. Je tak určena zejména starostům, místostarostům a dalším vedoucím pracovníkům. Aplikace Spisovna zajišťuje celkovou evidenci spisovny a uložených dokumentů a spisů. Dále je zde možné realizovat celé skartační řízení v elektronické podobě a odpovídajícím způsobem komunikovat s příslušným archivem. Aplikace Nastavení se využívá zejména v době konfigurace systému, popř. samozřejmě k dalším úpravám nastavení, pokud jsou v rámci změn u původce nebo v rámci vývoje právních předpisů potřeba.



Obr. 1: Přehled modulů informačního systému Munis, kde na prvním místě jsou vidět čtyři aplikaci elektronické spisové služby Munis ERMS.

Spisová služba má tedy hrát z hlediska informačního systému obce roli páteřní agendy, která zastřešuje celkovou evidenci dokumentů, navazuje na všechny vnitřní moduly, které s dokumenty pracují, podporuje všechny procesy úřadování a spojuje úřad s okolním světem prostřednictvím elektronických komunikačních nástrojů. Proto je důležité správné nastavení tohoto nástroje tak, aby přispíval k efektivitě fungování úřadu a zajišťoval naprosto přirozeně všechny potřeby. Můžeme si to ukázat na velmi jednoduchém příkladu:

Špatně: Úředník vyřizuje dokumenty, přičemž následně o tomto vyřízení zapisuje potřebné informace do spisové služby, aby naplnil literu zákona.

Dobře: Úředník vyřizuje dokumenty prostřednictvím spisové služby, která ho přehledně vede a zajistí, aby o provedených úkonech automaticky vznikaly všechny potřebné zápisy vyžadované právními předpisy.

Obecný proces tvorby spisového řádu

Spisový řád je vnitřní směrnicí vycházející zejména ze dvou základních zákonů upravujících fungování obecních a městských úřadů. Těmi jsou zákon č. 499/2004 Sb., o archivnictví a spisové službě, a zákon č. 500/2004 Sb., správní řád. Správná směrnice nemá opisovat zákon ani opakovat známá notorika, ale upřesňovat a specifikovat postupy, které jsou na úřadě skutečně

realizovány. Ač to může znít jednoduše, jedná se v případě spisového řádu o poměrně složitou a komplexní problematiku, jejíž zvládnutí vyžaduje nejen nezbytné znalosti, ale také řadu zkušeností.

Vlastní proces tvorby spisového řádu nabízený společností Triada se sestává z následujících kroků:

1. Dotazníkové šetření místních zvyklostí a reálných atributů vedení spisové služby. Dotazník spolu se všemi zaměstnanci vyplňuje řízeným způsobem pracovník společnosti Triada. Dotazník je samozřejmě připraven tak, aby pokrýval nejen elektronické (preferované) vedení spisové služby, ale byl použitelný i pro listinnou variantu. Jeho obecnost umožňuje, aby služba byla nabízena nejenom úřadům, které využívají informační systém Munis, ale všem obcím bez rozdílu vybraného provozovaného informačního systému. Pracovníci, kteří dotazník se zákazníkem vyplňují, již mají za dobu, po kterou je služba nabízena, praktické zkušenosti i s úřady, které využívají elektronické spisové služby jiných výrobců a dodavatelů.
2. Analýza stávajícího spisového řádu a porovnání jeho ustanovení s výstupy z dotazníkového šetření, která probíhá již mimo úřad. Během této doby samozřejmě může docházet ke komunikaci s úřadem pro upřesňování některých aspektů tvorby nového spisového řádu.
3. Kontrola spisového a skartačního plánu jako nezbytné součástí spisového řádu, a to jak po stránce formální a obsahové, tak také ve srovnání deklarované podoby ve směrnici a skutečně používaného číselníku věcných skupin v elektronickém systému spisové služby.
4. Sestavení nového spisového řádu na základě vzorů dodaných společností Triada, zpracování výstupů z dotazníku a výstupů z analýzy stávajícího spisového řádu úřadu. Při tomto sestavování jsou také identifikovány slabé stránky aktuálních postupů. Jde o to, aby výsledná směrnice reflektovala reálný stav, ale zároveň také plně respektovala povinnosti a pravidla stanovená aktuálními předpisy, zejména zákonem č. 499/2004 Sb., o archivnictví a spisové službě, vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby, a národním standardem pro elektronické systémy spisové služby.
5. Následuje předání výsledné směrnice a nových příloh úřadu. Přičemž se předpokládají ještě další následné kroky, jež jsou obsahem dalších bodů.
6. Navržení změn procesů, které jsou upraveny v nové směrnici a neodpovídají stávající praxi. Velice často jde např. o zpřesnění evidence kvalifikovaných certifikátů či úpravu podacího razítka tak, aby odpovídalo citované vyhlášce.
7. Seznámení všech zaměstnanců s novou směrnicí. Hodnotu školení není dobré podceňovat, protože bez tohoto seznámení nemůže být výsledná směrnice skutečně fungujícím a užitečným předpisem.

Obec a obecní úřad Domašov

Obec Domašov leží 25 km severozápadně od Brna v mírném údolí náhorní plošiny na pokraji Českomoravské vrchoviny. Nejstarší zmínka o Domašově pochází z roku 1048 z tzv. darovací listiny Břetislava I., který původní statek věnoval klášteru Rajhradskému. Obec se nacházela poblíže císařské silnice, nyní silnice č. II/602.

V současné době má obec něco přes 630 obyvatel a 239 čísel popisných. V obci se nachází základní škola pro první stupeň, kterou navštěvují i děti z Říček, Javůrku, Litostrova a Rudky, i mateřská škola, v budově obecního úřadu je obecní knihovna, vybudované zdravotní středisko je obsazeno pouze zubní lékařkou a pediatrickou poradnou, v obci je dále pobočka České pošty, soukromá prodejna potravin, cukrárna a tři restaurace. V obci úspěšně působí sbor dobrovolných hasičů.

Dále je obec součástí DSO Domašovsko, které spojuje obce Domašov, Rudka, Říčky, Javůrek a Litostrov za primárním účelem zásobování obcí pitnou vodou a provozování společné ČOV k čištění odpadních vod. Obec je také součástí mikroregionu Domašovsko. Více informací o obci lze najít na webových stránkách obce [3].

Obec má jedenáctičlenné zastupitelstvo. Je zřízen finanční, kontrolní a kulturně-sportovní výbor. Obecní úřad Domašov tvoří starosta, místostarosta a samostatný referent. Obecní úřad plní v oblasti samostatné působnosti úkoly, které mu uložilo zastupitelstvo obce, a pomáhá výborům v jejich činnosti. V oblasti přenesené působnosti obce vykonává státní správu s výjimkou věcí, které patří do působnosti zastupitelstva. Obecní úřad také rozhoduje o poskytování informací žadateli podle zvláštního zákona.

Obr. 2: Ilustrační foto obce Domašov, zdroj [3].

Případová studie aplikování služby na obci Domašov

Obecní úřad Domašov měl zpracován poměrně kvalitní spisový řád, avšak z roku 2007, což znamenalo, že vycházel ze situace listinného vedení spisové služby a nezohledňoval plně datové schránky a vývoj v oblasti ochrany osobních údajů. Spisový řád také neobsahoval všechny potřebné přílohy. Proto se obec rozhodla využít nabídku společnosti Triada a spisový řád plně aktualizovat.

Při vyplňování dotazníku se ověřilo, že úřad funguje adekvátně požadavkům daným platnými právními předpisy, aniž má uvedené postupy upřesněny v citované směrnici. Přesto došlo k identifikaci několika slabých míst, která byla v rámci diskuse nad vstupním dotazníkem ihned řešena.

V případě obce Domašov se tak v rámci tvorby nového spisového řádu zejména formalizovala zaběhnutá pravidla, což je ale podstatné zejména v případě jakýchkoliv personálních změn. Jde např. o pravidla elektronické podatelny, jejichž upřesnění je v kompetenci obce, přijímání podání na technických nosičích, pravidla oběhu dokumentů a rozhodování ve sporných otázkách vyřizujících osob apod.

Nový spisový řád obsahuje 16 článků a 12 příloh, které jsou následující:

- Spisový a skartační plán
- Otisk podacího razítka
- Vzor dokumentu „Obec Domašov“
- Vzor dokumentu „Obecní úřad Domašov“
- Potvrzení přijetí elektronického podání
- Plán zálohování Munis ERMS
- Průvodní dopis skartačního návrhu (vzor)
- Vzor soupisu dokumentů ve spisu
- Seznam samostatných evidencí dokumentů
- Seznam oprávněných zaměstnanců a jejich oprávnění pro specifické činnosti

- Seznam zkratek
- Vzory doložek pro převod podle § 69a zákona č. 499/2004 Sb.

Výsledný spisový řád včetně všech příloh byl předán v září 2018 a byl ihned schválen. Následně byl spisový řád zaslán ke kontrole a schválení včetně nového spisového a skartačního plánu do Státního okresního archivu Brno-venkov v Rajhradě.

Shrnutí

Jednou ze zásad zpracování osobních údajů podle GDPR je vytvoření a udržování odpovídající dokumentace všech procesů zpracování, ke kterým v organizaci dochází. Nedílnou součástí této dokumentace jsou z pohledu obcí vnitřní směrnice. Z hlediska spisové služby jakožto páteřní agendy a stěžejního nástroje evidence dokumentů je touto směrnicí spisový řád. Společnost Triada, která se specializuje na služby pro města a obce, proto nabízí obcím pomoc s tímto nesnadným úkolem, a to jak pro uživatele informačního systému Munis, tak pro úřady využívající elektronické spisové služby jiných dodavatelů. Výsledný spisový řád je nastaven tak, aby byl fungující směrnicí upřesňující každodenní chod úřadu.

Literatura

[1] Lechner. T. Důležitost spisového řádu pro kvalitní úřadování. *OBEC&finance* 2019, č. 5, s. 63.

[2] Kunt, M., Lechner, T. *Spisová služba.* 2. aktual. vyd. Praha : Leges, 2017. 384 s. Praktik. ISBN 978-80-7502-233-2.

[3] Oficiální webové stránky obce Domašov, dostupné na <http://obec.domasov.net/>.

INTEGROVANÁ SPRÁVA SÍTĚ JAKO SOUČÁST SOC STRATEGIE

Jindřich Šavel, Sales Director, Novicom, s.r.o.

Pouze dokonalá znalost a kontrola chráněného prostředí dává obráncům náskok před útočníky. Zvýšené nároky na ochranu kybernetického prostoru, osobních údajů, požadavky na efektivnější správu sítě, řízení přístupu do sítě a řešení bezpečnostních incidentů vedou organizace k nutnosti celkového zavedení pořádku v síti.

Zajištění kybernetické bezpečnosti je však dlouhodobá a nikdy nekončící úloha, která je jen velmi těžko zajišťována vlastními silami organizace. V této souvislosti se ukazuje jako **nejvhodnější řešení zavádění tzv. pokročilého modelu bezpečnosti**. Ten spočívá v přijetí problematiky v celé její šíři a rozdělení zodpovědnosti mezi interní IT a externí specializovanou organizaci.

Interní IT se tak může nadále věnovat již zvládnutým oblastem – zajištění provozních potřeb sítě, jako je základní správa stanic a sítě, běžná ochrana klientů (antivirus a antimallware) a perimetru (firewall), případně infrastrukturnímu monitoringu. K tomu by měly rovněž patřit pokročilé činnosti při správě interní sítě, jako je zajištění síťové visibility, kompletní správy IP prostoru (tzv. DDI – integrovaný DHCP, DNS a IPAM) a rovněž řízení přístupu do sítě (NAC). Tyto činnosti jsou poskytovány v běžnou pracovní dobu organizace (např. v režimu 9 až 17 hodin).

Ve spolupráci s poskytovatelem bezpečnostních služeb (tzv. MSSP – Managed Security Service Provider) jsou zajišťovány bezpečnostní potřeby sítě. Ty spočívají v pokročilém bezpečnostním monitoringu a neustálém vyhodnocování sítě a služeb pomocí nástrojů typu Log management, SIEM apod. Tyto činnosti zajišťuje vysoce kvalifikovaná obsluha Security Operation Centra (tzv. SOC) v režimu 24x7, která je speciálně trénovaná na identifikaci bezpečnostních hrozeb a provedení potřebných opatření (incident response).

Pro zajištění incident response v mimopracovní dobu chráněné organizace, tj. bez využití interních IT zdrojů organizace, je zapotřebí využívat plně integrované prostředí pro správu, zabezpečení a monitoring. V takovém případě je možné hovořit o tzv. **aktivním SOCu**.

Nesporné **výhody aktivního SOCu** si uvědomuje již celá řada MSSP poskytovatelů v ČR i v zahraničí a k zajištění aktivního SOCu si vybrali Novicom **řešení AddNet a BVS – Business Visibility Suite**.

Nástroj **Novicom BVS přináší přehled o komunikaci IT aktiv v síti**, včetně možnosti **modelování souvislostí business služeb s IT infrastrukturou**. Potřebné **změny infrastruktury pak zajišťuje unikátní integrovaný DDI/NAC nástroj AddNet**, který svým rozsahem funkcionality přesahuje hned do několika jinak samostatných tříd produktů (síťový monitoring, DDI, NAC) a umožnuje výrazně zefektivnit a zjednodušit síťovou správu. Jinými slovy, Novicom **AddNet dokáže** nejenom udělat **pořádek v síti** (IPAM) a spolehlivě provozovat základní síťové služby (DHCP/DNS), ale i **zajistit bezpečnost přístupu do sítě** včetně pokročilých síťových politik nebo **prevenci nákaz typu ransomware**. To vše integrované s dalšími provozními i bezpečnostními nástroji v rámci ucelené SOC strategie.

AddNet přináší robustnost, nadstandardní provozní spolehlivost, bezpečnost a flexibilitu nasazení. To všechno mu dávají **originální Novicom technologie**, jako je vlastní gridová platforma SGP, komunikační protokol SDP nebo systém vlastních Novicom appliancí. AddNet není jenom produkt, je to promyšlené know-how.

Novicom BVS nabízí následující dva funkční moduly:

1. **BVS Network Edition** – vizualizace aktuálního stavu IT infrastruktury a zachycení komunikací mezi IT zařízeními s uložením historie komunikací. Poskytuje představu o chování sítě – jaký typ provozu se v dané lokalitě vyskytuje.
2. **BVS Business Edition** – nadstavba nad síťovým modulem, která umožní modelování business služeb a jejich závislostí na IT infrastruktuře. Dává tak aktuální pohled na význam a kritičnost IT zařízení při provozování klíčových služeb pro koncové zákazníky.

To, jestli si organizace vybere standardní dodávku produktů AddNetu nebo BVS a jejich provoz si zabezpečí sama nebo bude **využívat AddNet či BVS formou služby od některého z partnerů**, závisí pouze na jejím přání.

NOVICOM – NETWORK MANAGEMENT HAS NEVER BEEN EASIER

VÝVOJ ZÁKLADNÍCH REGISTRŮ V ČESKÉ REPUBLICE A PROCES PROPOJENÍ OVM SE ZÁKLADNÍMI REGISTRY

Ing. Lenka Vaňková, Katedra práva, Národohospodářská fakulta,
Vysoká škola ekonomická v Praze

Úvod

Vytvoření centrálních registrů veřejné správy, které řeší potíže související s nejednotností, multiplicitou a neaktuálností klíčových databází, je jedním z pilířů elektronizace veřejné správy. Základní registry představují jeden z největších informatických projektů veřejné správy, jaký kdy byl v České republice realizován. Zároveň jde i o projekt s nejvíce pozitivním dopadem na veřejnou správu a komfort občanů a podnikatelů při kontaktu s ní [15].

Vytvoření základních registrů bylo zásadním krokem k nastartování efektivnějšího fungování veřejné správy. Před zavedením základních registrů si každá pobočka úřadu vedla v rámci své agendy svojí vlastní evidenci údajů, často v papírové podobě a neexistovala žádná kontrola úředníků a žádný záznam o tom, kdo, kdy a proč s těmito údaji zacházel. Vzhledem k tomu, že tato data nebyla právně závazná, musel každý občan vždy vyplnit formulář se stále stejnými údaji a jejich pravost stvrdit svým podpisem. V základních registrech jsou naopak všechny tzv. referenční údaje vždy aktuální a právně závazné. Pokud je úřady pro výkon své agendy potřebují, čerpají je přímo ze základních registrů. Pokud se některý údaj změní, všechny úřady připojené k základním registrům se tuto změnu dozví automaticky. K údajům v základních registrech má přístup pouze ten, kdo k tomu má zákonné oprávnění a každý přístup je navíc zaznamenán, takže naše osobní údaje jsou pod důkladnou kontrolou. V základních registrech jsou pak pouze aktuálně platné údaje bez historie. Díky základním registrům je výměna dat mezi orgány veřejné moci (OVM) od 1. července 2002 jednodušší. Díky nim se zrychlila a zjednodušila řada agend a občané a firmy získali důkladnou kontrolu nad tím, kdo, kdy a proč využívá naše osobní údaje [7].

Základní registry jsou ústředním informačním zdrojem pro informační systémy orgánů veřejné moci. Kromě toho jsou základní registry ústředním centrem pro výměnu dodatečných informací týkajících se informací uložených v základních registrech – např. registr vozidel, registr řidičů, atd. Informace, které jsou v základních registrech uložené, jsou průběžně kontrolovány a zlepšovány, integrací se odstraňují nesrovnalosti v datech. Příprava projektu základních registrů trvala v České republice poměrně dlouho. Jednotlivé orgány veřejné moci byly postupně propojeny se základními registry. Celý proces propojení orgánů veřejné moci se základními registry bude popsán v tomto článku.

Základní registry veřejné správy

Od 90. let 20. století začíná veřejná správa jako součást veřejného sektoru postupně využívat elektronické nástroje. Vlastní implementace informačních a komunikačních technologií ve veřejné správě je označována jako e-Government, který je vnímán jako, nyní již nedílná součást reformních procesů veřejné správy [2].

Cílem fungování základních registrů je zefektivnění a využití možností současných technologií pro online přístupy téměř kdykoli a odkudkoli. Současně by však základní registry měly splňovat a zajistit efektivní, bezpečnou a transparentní výměnu přesných a aktuálních tzv. referenčních údajů – státem garantovaných správných údajů obsažených v příslušném základním registru, který OVM využívá při své činnosti, a to aniž by ověřoval jejich správnost [10].

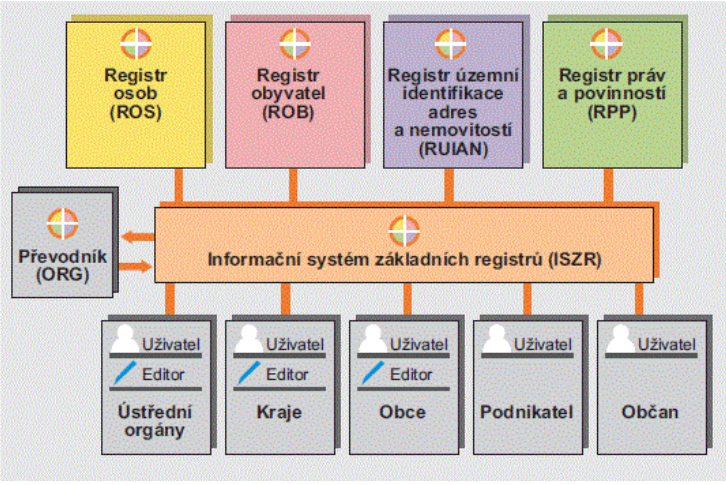
Příprava projektu základních registrů trvala v České republice poměrně dlouhou dobu. Jeden z prvních odkazů na základní registry byl v roce 2001 na mezinárodní konferenci ISSS [4]. Spuštění základních registrů bylo několikrát odloženo (změnou příslušného zákona), přičemž jedním z důvodů potřeby odkladů byla déletrvající příprava odpovídajících datových fondů v ta-

kové kvalitě, aby data mohla sloužit jako referenční údaje [9]. S tímto problémem se nepotýkaly pouze základní registry, nýbrž kvalita dat ovlivňuje celkovou výkonnost veřejné správy [1]. Základní registry veřejné správy byly spuštěny v České republice 1. července 2012.

Podnětem ke vzniku základních registrů bylo usnesení vlády č. 197 ze dne 28. února 2007, kterým vláda přijala „Strategii Efektivní veřejné správy a přátelské veřejné služby (Smart Administration) pro období 2007–2015. Obecným cílem vytvoření základních registrů veřejné správy bylo a je, aby orgány veřejné moci mohly data vedená v základních registrech efektivně a bezpečně sdílet. Právním základem vzniku systému základních registrů je zákon č. 111/2009 Sb., o základních registrech, v platném právním znění a Nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech. Zákon o základních registrech byl již jedenáctkrát novelizován, z toho třikrát dokonce ještě před nabytím účinnosti [3].

Rozvoj a rozšiřování využití základních registrů bylo naplánováno i v dalších letech (viz Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020), a to zejména při realizaci elektronické identity v návaznosti na implementaci nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES [3].

K údajům v základních registrech má přístup pouze ten, kdo k tomu má zákonné oprávnění a každý přístup je navíc zaznamenán, takže naše osobní údaje jsou pod důkladnou kontrolou. V základních registrech jsou pak pouze aktuálně platné údaje bez historie. Referenční údaje jsou uloženy ve čtyřech základních registrech a nad nimi funguje tzv. ORG – převodník identifikátorů, který jako jediný dokáže propojit data v jednotlivých registrech, přičemž pro zajištění maximální ochrany osobních údajů využívá vygenerovaný bezvýznamový identifikátor místo rodného čísla. Samotné sdílení dat zajišťuje Informační systém základních registrů, který zároveň kontroluje oprávnění k přístupu k datům. O provoz a bezpečnost základních registrů se stará Správa základních registrů [7]. Systém základních registrů obsahuje čtyři základní registry: Registr osob (ROS), Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (Registr obyvatel – ROB), Registr územní identifikace, adres a nemovitostí (RÚIAN), Registr agend orgánů veřejné moci a některých práv a povinností (RPP).



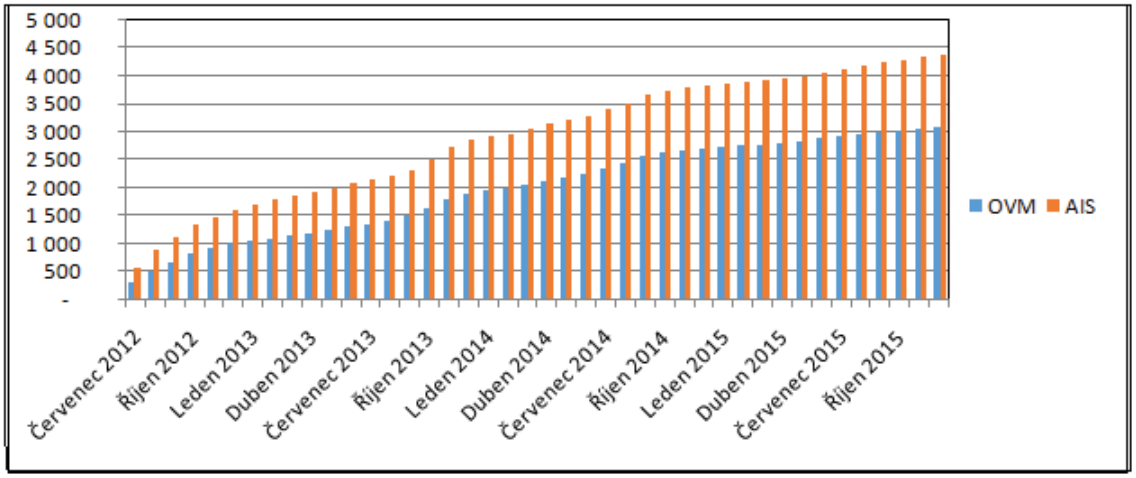
Obrázek 1 – Fungování systému základních registrů. Zdroj: http://www.szrcr.cz/informacni-system-zakladnich-registru, [Citace 25. 2. 2019].

Provoz základních registrů v průběhu let 2012 až 2015 – průběh připojování OVM a AIS

Ostrý provoz systému základních registrů byl zahájen, v souladu se zákonem č. 111/2009 Sb., o základních registrech, dnem 1. 7. 2012. Po prvních osmi měsících ostrého provozu, tedy ke dni 28. 2. 2013, Správa základních registrů eviduje 1 112 orgánů veřejné moci, které požádaly o připojení více než 1 796 agendových informačních systémů (AIS). Aktivně základní registry v této době využívalo 856 OVM, které za osm měsíců provozu uskutečnily celkem 108 241 327 transakcí. Z celkového počtu

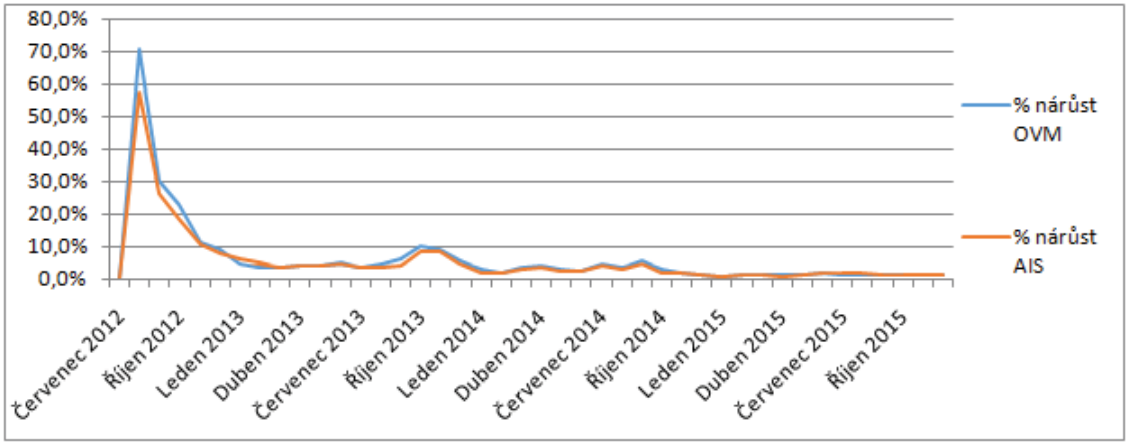
OVM, které evidují některý svůj AIS v informačním systému o informačních systémech veřejné správy (IS o ISVS), se základními registry spolupracovalo 65,33 % OVM, přičemž většina klíčových OVM se základními registry již spolupracovalo. Nové certifikáty do produkčního prostředí v únoru 2013 obdrželo Ministerstvo zdravotnictví, Státní veterinární správa a Ústavní soud. Krajské úřady a statutární města byla připojena v této době již všechna. Z pohledu Správy základních registrů (SZR) je zajímavé, že ve všech krajích se vyskytovaly OVM, které zaevidovaly svůj AIS do IS o ISVS, ale o certifikát umožňující přístup do základních registrů do této doby nežádaly [13].

Průběh napojování OVM k systému základních registrů je uveden na následujícím grafu. Jedná se o celorepublikový přehled o počtu připojených OVM a AIS k základním registrům.



Graf 1 – Přehled připojených OVM a AIS k základním registrům v letech 2012 – 2015. Zdroj: graf vlastní konstrukce, data: Správa základních registrů, 2012–2015 (Zprávy o stavu provozu).

Z výše uvedeného grafu 1 je patrné, že od počátku fungování základních registrů se počet připojených OVM a AIS zvyšuje. Proces připojování je na grafu zachycen v období od července 2012 do prosince 2015.

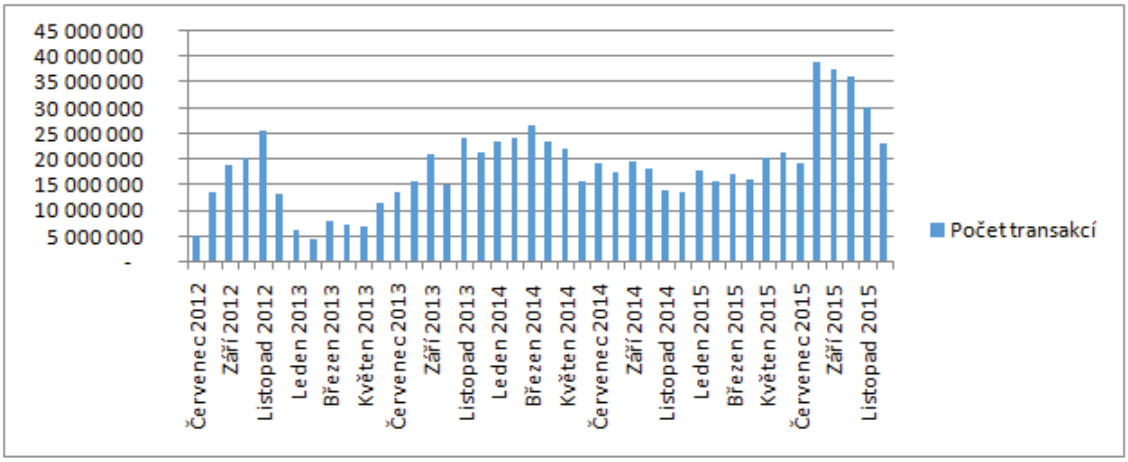


Graf 2 – Meziměsíční procentní nárůst připojených OVM a AIS k základním registrům v letech 2012–2015. Zdroj: graf vlastní konstrukce, data: Správa základních registrů, 2012–2015 (Zprávy o stavu provozu).

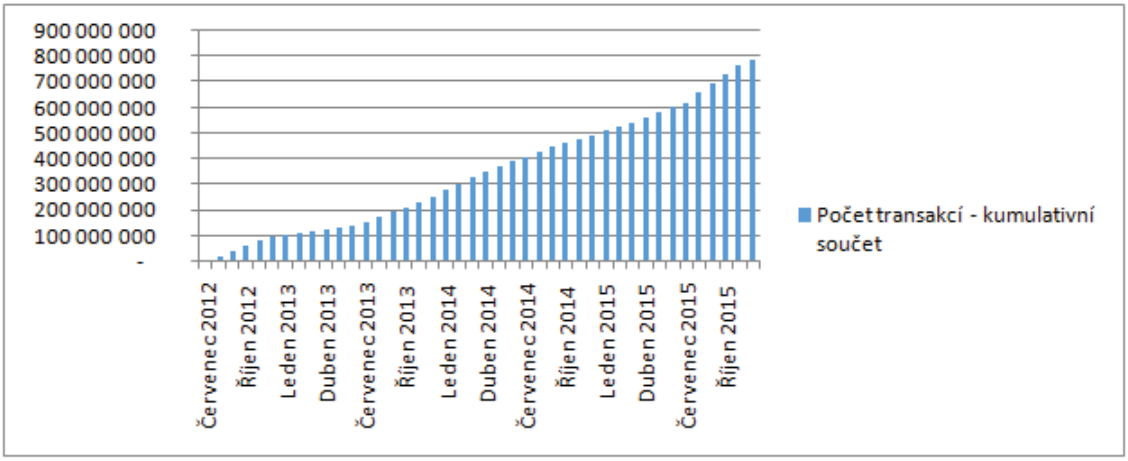
Největší nárůst je zaznamenán v prvních třech měsících v období od července 2012 do září 2012, kdy byly základní registry spuštěny a jednotlivé OVM a AIS se začaly připojovat k systému základních registrů v masovém měřítku (viz graf 2). V dalších

měsících je zřejmý poměrně pravidelný menší či větší nárůst počtu připojených OVM a AIS k základním registrům. Meziměsíční růst se začal zpomalovat v září 2012 a stabilizoval se v únoru 2013. Od března 2013 do září 2013 meziměsíční růst osciloval mezi 3–5 %. K většímu meziměsíčnímu nárůstu došlo opět na podzim 2013, od září do listopadu, kdy se růst pohyboval kolem 9 %. S výjimkou menších výkyvů v březnu, dubnu, červenci, srpnu a září 2014 následoval stabilní meziměsíční růst v rozmezí 1–2 %.

Průběh napojování OVM k systému základních registrů dokresluje ještě následující graf 3 a 4 o celkových počtech uskutečněných transakcí v produkčním prostředí. Vysoký počet transakcí uskutečněných v měsících říjen až listopad 2012 souvisí s tehdy probíhajícím ztotožňováním údajů v některých velkých AIS (s přidělováním agendových identifikátorů fyzických osob).



Graf 3 – Počet uskutečněných transakcí OVM v základních registrech v letech 2012–2015. Zdroj: graf vlastní konstrukce, data: Správa základních registrů, 2012–2015 (Zprávy o stavu provozu).



Graf 4 – Kumulativní součet počtu uskutečněných transakcí OVM v základních registrech v letech 2012–2015. Zdroj: graf vlastní konstrukce, data: Správa základních registrů, 2012–2015 (Zprávy o stavu provozu).

Kromě přístupu k referenčním údajům v základních registrech prostřednictvím svých AIS mohou jednotlivé OVM a dále i fyzické osoby nebo právnické osoby využívat další dva možné způsoby přístupů. Prvním z nich je přístup prostřednictvím informačního systému datových schránek. Jeho prostřednictvím bylo do 4. 3. 2013 zpracováno celkem 2 492 816 datových zpráv. Druhým možným způsobem přístupu k referenčním údajům je přístup prostřednictvím systému CzechPOINT. Na kontaktních místech bylo vydáno na žádost celkem 3 830 výpisů a úředníci pro plnění svých úkolů získaly ke stejnému datu prostřednictvím CzechPOINT@office celkem 177 509 výpisů [13].

V současné době, ke dni 4. 3. 2019, vykazuje Správa základních registrů od spuštění základních registrů, tj. od 1. 7. 2012, 2 099 939 230 transakcí. Od začátku letošního roku 74 469 014 transakcí, za posledních 24 hodin 1 052 044 transakcí. Údaje o celkovém počtu transakcí zahrnují: přijaté transakce[1], zamítnuté transakce[2] a odpovědi asynchronních transakcí ze strany ISZR (transakce, jejichž iniciátorem je ISZR).

Shrnutí

Základní registry se staly nedílnou součástí efektivního fungování veřejné správy. OVM by nemohly ověřit současný stav referenčních údajů bez dostupnosti základních registrů. Nebyly by schopni vydávat právně závazná rozhodnutí. Ve skutečnosti by to vedlo k narušení fungování veřejné správy. Kromě toho by nebyly občanům k dispozici jiné služby, jako je CzechPOINT [8].

Od počátku fungování základních registrů nedošlo k žádnému významnému výpadku systému a v základních registrech bylo uskutečněno téměř 2,1 miliardy počtu transakcí. Po prvních osmi měsících provozu základní registry používalo téměř 65 % všech OVM, přičemž většina klíčových OVM se základními registry již spolupracovalo.

V poslední době základní registry zaznamenaly další velký posun, kdy v polovině roku 2018 bylo konečně spuštěno řešení pro elektronickou identifikaci fyzických osob – v podobě Národního bodu pro identifikaci a autentizaci (NIA). Souběžně s tím začaly být vydávány nové občanské průkazy, tentokráte již skutečně elektronické a s možností využít je pro elektronickou identifikaci.

1 Přijaté transakce = korektní transakce, transakce s varováním (neobsahují žádná výstupní data), transakce s chybou

2 Zamítnuté transakce = transakce zamítnuté z bezpečnostních důvodů, transakce s výsledkem „nedefinováno“, nevalidní XSD požadavky (transakce bez správného vyplnění hlavičky a transakce prováděné nesprávným certifikátem).

Literatura

[1] KRÁL, J., ŽEMLIČKA, M. Kvalita dat a informací – základní omezení IT ve veřejné správě. In: POUR, V., VOŘÍŠEK, J. (Eds.) *Systems Integration* 2006. Praha: VŠE. pp. 215-222.

[2] LECHNER, T. Ekonomické dopady implementace ICT ve veřejné správě: důkazy z České republiky. *Politická ekonomie* 2013, Vol. LXI, No. 5, pp. 675-690.

[3] LECHNER, T., LECHNEROVÁ, R., SILVAROVÁ, L. Agendy a agendové činnostní role v základních registrech: promarněná příležitost. In: STEJSKAL, J., KŘUPKA, J. (eds.) *Sborník příspěvků z 11. mezinárodní vědecké konference "Veřejná správa 2016"*. Pardubice: Univerzita Pardubice, 2016. pp. 63-70. ISSN 978-80-7560-041-7.

[4] LECHNER, T., LECHNEROVÁ, R., SILVAROVÁ, L. Quality analysis of the basic register of rights and obligations. In: *Scientific papers of the university of Pardubice - Series D*, 2017, Vol. XXIV, No. 40 (2/2017), pp. 108-119. ISSN 1804-8048.

[5] MINISTERSTVO VNITRA. *Strategie realizace Smart Administration v období 2007–2015 – Efektivní veřejná správa a přátelské veřejné služby.* Dostupné na WWW: <www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx>. [Citace 2019-02-27].

[6] MINISTERSTVO VNITRA. *Strategický rámec rozvoje veřejné správy České republiky pro období 2014–2020.* Dostupné na WWW: <http://www.mvcr.cz/clanek/strategicky-ramec-rozvoje.aspx>. [Citace 2019-02-28].

[7] MINISTERSTVO VNITRA. Základní registry. Dostupné na WWW: <http://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry.aspx>. [Citace 2019-02-28].

[8] PEŠEK, M. Základní registry 2.0. In *Konference ISSS 2018*, 9.–10. dubna 2018, Hradec Králové. Dostupné na WWW: <https://www.isss.cz/archiv/2018/download/prezentace/mvcr_vrba-zr.pdf>. [Citace 2019-02-26].

[9] RIEGER, P., ŠTENCL, M. The new system of public registers in the Czech Republic. In: *Journal of Systems Integration*, 2010, Vol. 2, No. 1-2, pp. 23-32. ISSN 1804-2724.

[10] SILVAROVÁ, L. Diplomová práce. Dostupné na WWW: <https://insis.vse.cz/auth/lide/clovek.pl?id=79626;zalozka=7;zp=46618;studium=144836>. [Citace 2019-03-02].

[11] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Dostupnost základních registrů. Dostupné na WWW: <http://www.szrcr.cz/dostupnost>. [Citace 2019-02-20]

[12] SPRÁVA ZÁKLADNÍCH REGISTRŮ (2016). Měsíční statistiky provozu základních registrů. Dostupné na WWW: <http://www.szrcr.cz/pro-media/tiskove-zpravy>. [Citace 2019-02-20].

[13] SPRÁVA ZÁKLADNÍCH REGISTRŮ. Zpráva o stavu provozu základních registrů – osm měsí-ců ostrého provozu. Dostupné na WWW: <http://www.szrcr.cz/uploads/Dokumenty/ZPRAVA_SZR_20130318_na_web.pdf>. [Citace 2019-02-20].

[14] SPRÁVA ZÁKLADNÍCH REGISTRŮ (2012–2015). Zprávy o stavu provozu. Dostupné na WWW: <http://www.szrcr.cz/pro-media/tiskove-zpravy>. [Citace 2019-02-21].

[15] INSTITUT PRO VEŘEJNOU SPRÁVU PRAHA. Základní registry ve veřejné správě. Dostupné na www:<https://www.institutpraha.cz/obj/obsah_fck/egon/pdf_programy/zakladni_registry.pdf>. [Citace 2019-03-25].

Poděkování

Příspěvek je podporován grantem VŠE IGS F5/43/2018 „Analýza ekonomických, právních a dalších dopadů obecného nařízení o ochraně osobních údajů (GDPR)“.

partneři


ALEF


asseco


AUTOCONT


AV MEDIA
komunikace obrazem


DISK


FORTINET


GORDIC

ORACLE


paloalto
NETWORKS

záštity nad odbornými bloky a další odborní garanti

pořadatelé, spolupracující města, kraje, instituce

Sborník 22. konference ISSS
Editor: Kateřina Pánková
Vydavatel: TRIADA, spol. s r. o.
Rok vydání: 2019
ISBN: 978-80-907164-1-4

ISBN 978-80-907164-1-4