Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Pravidla pro funkční celky architektury jednotlivých úřadů

Tato kapitola popisuje definované funkční celky v celé šíři (v celé architektuře) včetně pravidel, návodů a dobrých praktik k jejich správě a rozvoji. Jde o opačný přístup než v části Pravidla tvorby a údržby vlastní čtyřvrstvé architektury jednotlivých úřadů, kde se popisují jednotlivé vrstvy architektury úřadů.

Funkční celek je logická struktura obsahující všechny vrstvy architektury (primárně Byznys, Aplikace, Platformy, Komunikace), a který se nejčastěji tvoří kolem informačního systému veřejné správy. Typickým příkladem funkčního celku může být agendový informační systém typu spisová služba. Tento celek kromě samotného informačního systému obsahuje i procesy a služby v úřadu (skartační plán, příjem dokumentů atd.), potřebný HW a SW, komunikační propojení, bezpečnostní požadavky, standardy a pravidla a další.

Portály veřejné správy a soukromoprávních uživatelů údajů

Portál je vnímán jako celý funkční celek obsahující Front-end i Back-end realizující všechny typy služeb dle IKČR - Informační, Interakční, Integrační a Transakční. V oblasti informačních služeb poskytuje uživatelům přehled a veřejně dostupné informace z oblasti, kterou portál obsahuje včetně popisu životních situací. V informační části není potřeba řešit identifikaci, autentizaci a autorizaci uživatele. V oblasti interakčních služeb poskytuje uživatelům zpětnou vazbu mezi jeho konáním, a to včetně historie. Interakční služby vyžadují identifikaci, autentizaci a autorizaci uživatele. V oblasti integračních služeb poskytuje uživatelům sloučené služby z několika zdrojů, například různých agend. Integrační služby vyžadují identifikaci, autentizaci a autorizaci uživatele. V oblasti transakčních služeb poskytuje uživatelům zaručené služby jako úkony a podání se schopností předvyplnění všemi státu známými údaji. Transakční služby vyžadují identifikaci, autentizaci a autorizaci uživatele.

Portály tedy nemohou být samostatné a nepropojené aplikace, ale naopak musí se jednat o prostředek, který je integrován s informačními systémy v úřadu. Především s elektronickou spisovou službou, s agendovými informačními systémy, ale třeba i s ekonomickými systémy tam, kde se jejich prostřednictvím shromažďují údaje o výplatách či o poplatcích podle jednotlivých klientů. Portál má sloužit klientovi k získání informací, jako prostředek pro publikování otevřených dat, statistik a veřejných výstupů, pro elektronická podání a komunikaci klienta s úřadem apod. Nově musí portál sloužit i držitelům zaručené elektronické identifikace jako prostředek pro získání jejich údajů, pro různé notifikace, ale třeba i pro interaktivní podání žádostí, či podání žádostí o výpisy apod. Klientovi musí poskytnout též tzv. profil neboli personifikovanou část, kde si portál drží základní údaje o klientovi, které zná úřad a které chce klient sdělit sám.

Při provozování portálu je důležité zavést a změnit současné procesy orientované především na osobním kontaktu s klientem. Současné portály již musí disponovat funkcionalitou propojení se zaručenou identitou dle zákona 250/2017 Sb. a musí se umět přizpůsobit situaci, kdy klient veřejné správy bude komunikovat pouze elektronicky. Začíná se tedy samotným uživatelsky přívětivým prostředím, které musí být v souladu s **grafickým manuálem MVČR**. Dále je potřeba formulářový engine, který umožní nejen předvyplnit veškeré státu již známé údaje z **propojeného datového fondu** a **elektronické identity poskytnuté národní identitní autoritou**. V neposlední řadě je potřeba zajistit předávání všech podání učiněné v portálu do agendových informačních systémů, ve kterých se dle agendy podání řeší a zároveň do spisové služby úřadu. Při předávání podání z portálu je tak potřeba mít zajištěnou funkcionalitu, která z podání vytvoří "lidsky čitelný" a "strojově čitelný" formát v rámci jedné obálky, která je opečetěná a orazítkovaná portálem. Lidsky čitelný formát, typicky PDF, jde do spisové služby pro evidenci a strojově čitelný formát jde od agendového systému. Při provozu portálu nezáleží na technologiích, ani infrastruktuře. Není tedy preferované ani On Premise řešení, ani cloudové řešení, vše záleží na potřebách daného úřadu a možnostech, které technologie dokáží nabídnout. Je

vždy potřeba myslet na rozložení zátěže, například daňové přiznání z příjmu fyzických osob se podává 1x ročně a není proto nutné klást na infrastrukturu celoroční nepřetržitý provoz. Každé řešení však musí podporovat přístup k centrálním službám eGovernmentu a dalším službám veřejné správy skrze zabezpečenou infrastrukturu **referenčního rozhraní.**

Portál podporuje samoobslužného klienta, obsahuje jak přenesenou, tak samosprávnou působnost. Portál musí obsahovat popis situací, musí umět řešit mandáty v elektornické komunikaci.

Portál občana a portál veřejné správy

V případě Portálu občana v PVS stojí občan jako samoobslužný uživatel „vně" veřejné správy a portál mu poskytuje jedno univerzální vstupní místo dovnitř. Z toho důvodu jsou všechny věcné (agendové) a do budoucna i místní portály se svými službami federalizovány „pod" tímto ústředním portálem.

Portál občana pro svou funkcionalitu využívá služby propojeného datového fondu, stejně tak služby národní identitní autority. Z pohledu propojeného datového fondu je portál občana jedním ze čtenářských AIS, který má zmocnění dle agendy A344 zobrazovat subjektu údajů jeho informace, které o něm vede veřejná správa. Portál občana v tomto musí zajistit, aby agenda, dle které se řídí byla neustále aktualizovaná dle toho, jak se budou postupně rozšiřovat služby a portály poskytující údaje. Technicky je portál občana připojený jako čtenářský AIS na systém eGON Service Bus, skrze který čerpá autoritativní údaje pomocí publikovaných kontextů. V tomto musí portál občana pouze pravidelně aktualizovat čerpaný seznam kontextů jiných agend. Z pohledu národní identitní autority je portál občana poskytovatelem služeb čerpající zaručené služby identifikace a autentizace.

Agendový portál

Agednovým portálem je myšlen portál poskytující služby logicky centralizovaného systému pro jiné orgány veřejné správy. Typicky jde tedy o portál agendy v přenesené působnosti poskytovaný správcem (ohlašovatelem) agendy. Takový portál musí splnit několik podmínek:

- Musí být registrovaný jako informační systém veřejné správy v systému o informační systémech veřejné správy <yamdwe_nowiki>0</yamdwe_nowiki>
- Musí být federovaný do portálu občana
- Musí dle svého agendového zákona být schopný čerpat a poksytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako poskytovatel služeb <yamdwe_nowiki>1</yamdwe_nowiki>

Portál území

V případě portálů samospráv se předpokládají dva trendy: a) jednak budou lokální portály samospráv obsahovat obrácený směr navigace do Portálu občana, kde bude moci klient vyřídit vše ostatní ze státní správy, co případně nenašel v místním portálu a b) lokální portály budou moci být v dlouhodobé perspektivě nahrazovány místně přizpůsobenými službami centrálního Portálu občana v PVS. Takový portál musí splnit několik podmínek:

- Musí být registrovaný jako informační systém veřejné správy v systému o informační systémech veřejné správy <yamdwe_nowiki>2</yamdwe_nowiki>
- Musí dle svého agendového zákona být schopný čerpat a poksytovat údaje skrze systém eGON Service Bus
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako poskytovatel služeb <yamdwe_nowiki>3</yamdwe_nowiki>

Portál soukromoprávního uživatele údajů

V případě portálu soukromoprávního uživatele údajů (dále také jako SPUÚ) se jedná o situaci, kdy vlastník portálu není orgán veřejné moci, ale dle své povahy je podřízen zákonu 111/2009 Sb <yamdwe_nowiki>4</yamdwe_nowiki>. Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků, apod. Takový portál a jeho vlastník musí splnit několik podmínek:

- Musí mít zřízenou datovou schránku pro komunikaci s veřejnou správou
  - Právnické osoby mají datovou schránku zřízenou ze zákona
  - Zřídit datovou schránku je možné dle informací zde: <yamdwe_nowiki>5</yamdwe_nowiki> .
  - Datová schránka se může obsluhovat skrze webové rozhraní na adrese www.mojedatovaschranka.cz nebo mít funkcionality integrovány do vnitřních systémů organizace. Nejčastěji se jedná o elektronickou spisovou službu.
- Musí být ohlášen v rejstříku SPUÚ v registru práv a povinností. Zde je možnost kontroly https://rpp-ais.egon.gov.cz/AISP/verejne/katalog-spuu.
  - SPUÚ je podnikající fyzická osoba nebo právnická osoba, která není orgánem veřejné moci a je podle jiného právního předpisu oprávněna využívat údaje ze základního registru nebo z agendového informačního systému
  - Ohlášení do rejstříku SPUÚ probíhá pomocí agendového informačního systému působnostního viz https://rpp-ais.egon.gov.cz/AISP/. Do tohoto systému má přistup každý ohlašovatel agendy. Pokud má ohlašovatel agendy zároveň i možnost editace rejstříku OVM a SPUÚ, může SPUÚ přidat.
    - Pokud tedy existuje agenda, v rámci které je SPUÚ oprávněn čerpat údaje ze základních registrů nebo z agendového informačního systému, je třeba kontaktovat správce agendy a požadovat zavedení do rejstříku SPUÚ.
    - Pokud není soukromoprávní uživatel údajů ohlášen v AISP a správce agendy, ani jiné OVM, jej ohlásit nechce, musí SPUÚ kontaktovat správce Registru práv a povinností (pavel.kajml@mvcr.cz) se žádostí o ohlášení do rejstříku SPUÚ s těmito údaji (Název organizace, adresa organizace, IČO, DIČ, zákon a paragraf opravňující k přístupu do základních registrů nebo agendovému informačnímu systému, kontaktní osoba)
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb online služeb (dále též Service Provider). Více také zde https://www.eidentita.cz/Home/Ovm. Ohlášení může proběhnout automatizovaně skrze formulář, pokud to umožňuje typ zřízení datové schránky (typ 10, 14, 15, 16). Pokud nemáte takový typ, je nutné kontaktovat Správu základních registrů skrze datovou schránku napřímo s požadavkem obsahujíc všechny údaje, jako v případě automatizovaného způsobu:
  - Uživatel jako zástupce organizace požaduje po NIA Portálu, který je Service Providerem, službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů. NIA Portál kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).
  - Pro ověření uživatele pro registraci organizace či konfigurací jednotlivých Service Providerů je jako Identity Provider určen Informační systém datových schránek (ISDS). Národní identitní autorita provede přesměrování na přihlášení prostřednictvím datových schránek.
  - Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci či provést smazání již vytvořené registrace, musí být přihlášen prostřednictvím ISDS v roli Typ S - Oprávněná osoba se stavem datové schránky Stav schránky 1 - Přístupná a nesmí se jednat o datovou schránku fyzické osoby.
  - V případě, kdy je uživatel úspěšně ověřen, Informační systém datových schránek předá Národní identitní autoritě jako výsledek ověření autentizační token obsahující IČO a název subjektu, roli přihlašovaného uživatele a další atributy.
  - Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR) na jehož základě následně provede kontrolu existence IČO.
  - Národní identitní autorita předává NIA Portálu potřebné atributy z Informačního systému základních registrů a atributy přijaté v autentizačním tokenu z Informačního systému datových schránek, které jsou nutné ke zpracování formuláře pro registraci.

    - Na základě úspěšného splnění předchozích kroků umožní NIA Portál uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci.
    - Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).
    - NIA Portál zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci.
    - Uživatel provede konfiguraci Service Providera

- Musí umět přijímat a zpracovávat data pomocí standardů SAML2 nebo WS-Federation

Elektronický systém spisové služby

Tento dokument je určen jako soubor pro veřejnoprávní původce, kteří mají architektonicky řešit problematiku správy dokumentů, resp. výkonu spisové služby. Takové instituce musejí mít elektronický systém spisové služby (ESSL) a zajistit integraci svých informačních systémů, v nichž se spravují dokumenty (ISSD) na ESSL, nebo je zajistit jako samostatné evidence.

Legislativní rámec pro výkon spisové služby obsahuje zákon o archivnictví a spisové službě a vyhláška o podrobnostech spisové služby. Národní standard pro ESSL vydaný ministerstvem vnitra pak stanovuje podrobné technické požadavky na aplikační a byznysové funkce ESSL a ISSD systémů.

Obecně je nutno řešit a zajistit toto:

1. Mít v organizaci elektronický systém spisové služby, který splňuje požadavky Národního standardu.

2. Zajistit integraci ESSL na úložiště digitálních dokumentů.

3. Zajistit integraci všech svých IS pracujících s dokumenty na ESSL pomocí rozhraní stanoveného Národním standardem.

4. Zajistit řádné fungování modulu podatelny k roztřídění dokumentů do ESSL či příslušných IS.

5. Zajistit naplňování povinností spisové služby, včetně vedení transakčních záznamů k úlohám nad dokumenty a spisy.

6. Zajistit přípravu k realizaci elektronické skartace a elektronického skartačního řízení nejen u dokumentů v ESSL, ale i u dokumentů vedených a spravovaných v jiných IS.

7. Pravidelně aktualizovat svůj Spisový řád tak, aby odpovídal faktickému výkonu spisové služby a naopak.

8. Řešit spisovou službu a správu dokumentů jako obecnou schopnost úřadu.

Obecně o spisové službě

Orgány veřejné moci a další subjekty, které jsou podle příslušné legislativy zahrnuty do skupiny takzvaných “veřejnoprávních původců”, mají za povinnost realizovat správu svých dokumentů formou výkonu spisové služby. Spisovou službou se rozumí veškeré činnosti a procesy týkající se evidence, správy a vyřizování dokumentů. Jedná se o dokumenty v analogové podobě (například listinné dokumenty) a také v digitální podobě (například elektronické dokumenty).

U analogových dokumentů je hlavním cílem výkonu spisové služby evidence a správa metadat o těchto dokumentech a veškerých úloh a transakcí, které se s dokumenty činí. U digitálních dokumentů se pak jedná nejen o evidenci a správu metadat, ale také samotných souborů digitálních dokumentů, kterým se v odborné terminologii říká komponenty. Navíc obecně platí teze stanovená prováděcí vyhláškou o spisové službě, že

nebrání-li tomu nic podstatného, měly by se na vstupu do organizace analogové dokumenty digitalizovat a dále by se s nimi mělo pracovat jako s digitálními.

V úřadech se obecně dá správa dokumentů rozdělit podle účelu dokumentů takto:

- Obecné dokumenty úředního charakteru (evidují a spravují se v systému spisové služby)
- Agendové dokumenty (evidují a spravují se v agendových prostředcích integrovaných na spisovou službu)
- Ekonomické dokumenty (spravují se v ekonomickém systému integrovaném se spisovou službou)
- Dokumenty pracovní (neevidují se v této fázi v rámci spisové služby, ale je nutno je rozumně spravovat)
- Dokumenty vyňaté z evidence a ze spisové služby

Řídící dokumenty

V rámci výkonu spisové služby jsou řídícími drivery zejména:

- Legislativa
  - Zákon č. 499/2004 Sb., o archivnictví a spisové službě
  - Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
- Vnitřní řídící dokumenty úřadu
  - Spisový řád
  - Spisový plán
- Dokumentace k elektronickému systému spisové služby
  - Dokumentace k ESSL
  - Dokumentace k integracím ESSL
  - Dokumentace související s výkonem spisové služby

Architektura spisové služby

Spisovou službu považujeme za společnou schopnost na úrovni úřadu (capability), kde většina principů je shodných napříč celým úřadem (motivační vrstva, aplikační vrstva ESSL a integrace, byznysová vrstva procesů a funkcí a interakcí) a na úrovni jednotlivých agend se odlišuje dle výkonu dané agendy minimálně. Architekturu výkonu spisové služby tedy zahrneme do capability mapy úřadu a do architektury vykonávaných schopností.

Při zpracování Enterprise architektury úřadu i při zpracování a realizaci jednotlivých architektur týkajících se ať už agend nebo schopností, nebo řešení, je nutno zahrnout spisovou službu jako obecnou schopnost a správným způsobem řešit její realizaci. Je přitom nutno zvážit, do jaké míry je faktický i technický výkon spisové služby společný v rámci celé organizace a jestli a jakým způsobem se bude lišit v rámci jednotlivých agend či řešení. Jednoznačným doporučením je mít jeden elektronický systém spisové služby a u ostatních informačních systémů, včetně agendových informačních systémů a provozních informačních systémů, zajistit úkony spojené se správou dokumentů a výkonem spisové služby formou integrace na elektronický systém spisové služby předepsaným rozhraním.

Součástí architektury úřadu by tedy z pohledu spisové služby měly být vždy alespoň následující element:

Vzhledem k tomu, že legislativa obecně počítá s tím, že v rámci úřadu je jeden ESSL a ostatní agendové a provozní informační systémy jsou na něj integrovány a úkony spojené s dokumenty se realizují formou rozhraní ESSL, měla by v úřadu být implementována integrace všech informačních systému spravujících dokumenty s ESSL a samotný ESSL navázán na úložiště pro uchovávání komponent digitálních dokumentů. Na obrázku níže je znázorněn obecný stav pochopení integrace elektronického systému spisové služby za využití jednoho centrálního úložiště pro digitální dokumenty.

Hovoříme-li o integraci informačního systému s elektronickým systémem spisové služby a o správě úkonů spojených s dokumentem, může tato integrace být na úrovni byznysových objektu a jejich metadat řešena následujícími způsoby:

I. Digitální dokument, respektive jeho komponenty a datové soubory, jsou uloženy v úložišti digitálních dokumentů, které zajišťuje péči o digitální soubory

II. Metadata o dokumentu jsou spravována evidenčním nástrojem, tedy:

a. elektronickým systémem spisové služby, nebo

b. informačním systémem, který plní funkci samostatné evidence

III. Se soubory v úložišti jsou oprávněny pracovat:

a. elektronický systém spisové služby, nebo

b. informační systém sloužící jako samostatná evidence, nebo

c. informační systém integrovaný na ESSL prostřednictvím ESSL

Architektura agendového informačního systému

V rámci architektury každého informačního systému veřejné správy sloužícího pro podporu výkonu činností agendy veřejné správy je nutno myslet také na oblast výkonu spisové služby. Vzhledem k tomu, že prakticky v každé agendě veřejné správy se buď vytváří, nebo zpracovávají, nebo odesílají, nebo evidují dokumenty, anebo u ní dochází k zápisu záznamu do spisu (z pohledu legislativy týkající se spisové služby), je nutno zajistit úkony spojené se spisem a dokumentem. Vesměs existují dvě formy, jak zajistit povinnosti výkonu spisové služby v souvislosti s daným AISem, a to následující:

1. Integrovat AIS na ESSL prostřednictvím předepsaného rozhraní a zajistit, aby úkony spojené s dokumentem vykonával AIS prostřednictvím tohoto rozhraní.

2. Zajistit, aby daný AIS splňoval požadavky Národního standardu pro ESSL kladené na tzv. „samostatnou evidenci“ a vykonávat úkony spojené s dokumenty a všechny procesy týkající se výkonu spisové služby v samostatné evidenci tímto systémem.

Architektura provozních systémů

Velice často se zapomíná na to, že výkon spisové služby se týká všech dokumentů, a tedy nejen úředních dokumentů typu podání a rozhodnutí v rámci výkonu agend veřejné správy. U veřejnoprávních původců se jedná o evidenci a správu veškerých dokumentů (s výjimkou těch, které si daný původce odůvodněně vyňal z evidence ve svém spisovém řádu), a tedy je nutno zajistit výkon spisové služby v elektronické podobě také pro pracovní a provozní a neúřední dokumenty. To se týká jak dokumentů pracovního charakteru (zápisy z porad, organizační a řídící dokumenty, řídící akty, interní sdělení), tak ale také všech dokumentů ekonomického a

provozního charakteru (faktury, objednávky, smlouvy ekonomické doklady, personální dokumentace, žádanky, závěrky a výkazy apod.).

V případě provozních informačních systémů jednoznačně doporučujeme jejich integraci na elektronický systém spisové služby. Zejména u ekonomických informačních systémů, systému pro řízení personalistiky a mezd a zdrojů a dalších manažerských informačních systémů týkajících se různých žádanek, evidencí, a workflow procesů, se dost často na výkon spisové služby zapomíná. Zde je vhodná integrace na ESSL, neboť zajištění splnění všech požadavků Národního standardu na samostatné evidence pro tyto systémy by s sebou přineslo neúměrné finanční náklady spojené s pořízením a rozvojem těchto provozních IS. Integrací na ESSL se také zajistí řádné realizování skartačních řízení u těchto druhů dokumentů.

Přijímání a odesílání dokumentů

V souvislosti s architekturou a výkonem spisové služby připomínáme, že jednou ze zásadních úloh spisové služby je správa dokumentů jak přijatých, tak odesílaných. To se týká dokumentů vzniklých z vlastní činnosti i dokumentů jiných původců.

Při příjmu a odesílání dokumentů je třeba naplnit všechny povinnosti stanovené legislativou týkající se spisové služby, včetně jejich evidence v rámci podatelny a jejich následné evidence a zpracování buď v elektronickém systému spisové služby, nebo systému samostatné evidence splňujícím příslušné požadavky. To se týká i odesílání dokumentů. Mezi odesílané dokumenty patří dokumenty zveřejňované, a to včetně dokumentů zveřejňovaných na internetových stránkách. Také se to ale pochopitelně týká i elektronické úřední desky a na ní umisťovaných dokumentů.

Další zdroje

V souvislosti s výkonem spisové služby existuje celá řada dalších zdrojů informací a metodických dokumentů zejména Ministerstva vnitra a Národního archivu ČR. V rámci Ministerstva vnitra je gestorem Odbor archivnictví a spisové služby (OAS).

Mezodický návod pro kontrolu či sebekontrolu výkonu spisové služby v elektronické podobě je uceleným návodem a kontrolním seznamem pro všechny veřejnoprávní původce, aby si mohli zkontrolovat, zda jejich technické řešení ESSL splňuje potřebné technické a procesní požadavky a je také návodným dokumentem, co vyžadovat při technické implementaci ESSL a ISSD systémů v úřadu.

https://www.mvcr.cz/soubor/metodicky-navod-pro-kontrolu-vykonu-spisove-sluzby-vedene-prostrednictvim-elektronickeho-systemu-spisove-sluzby-u-verejnopravnich-puvodcu-pdf.aspx **Stanovisko MV ke správním deliktům a neúplnému vedení spisové služby** je základním stanoviskem, v němž OAS konsttuje, že i neúplné či nesprávné vedení spisové služby v elektronické podobě je porušením zákonných povinností.

https://www.mvcr.cz/soubor/stanovisko-spravni-delikt-podle-74-odst-9-pism-a-pdf.aspx

Otevřená data

Otevřená data jsou:

1. Volně přístupná na webu jako datové soubory ke stažení ve strojově čitelném a otevřeném formátu - CSV, XML, JSON, RDF a další formáty s otevřenou specifikací
2. Opatřená podmínkami užití neomezujícími jejich užití, viz návod na stanovení podmínek užití
3. Evidovaná v Národním katalogu otevřených dat (NKOD) jako datové sady opatřené přímými odkazy na

datové soubory, které je tvoří
4. Úplný obsah databáze nebo agregovaná statistika
5. Opatřená dokumentací
6. Připravena s cílem co nejsnazšího strojového zpracování programátory apod.
7. Opatřená kontaktem na kurátora pro zpětnou vazbu (chyby, žádost o rozšíření, apod.)
8. Jsou publikovány dle otevřených formálních norem ve smyslu § 4b odst. 1 zákona č. 106/1999 Sb. o svobodném přístupu k informacím.

Pokud vaše datová sada nesplňuje všechny uvedené podmínky, nejedná se o otevřená data české veřejné správy podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, který definuje otevřená data ve svém § 3 odst. 11.

Otevřenými daty zejména není:

1. odkaz na vyhledávací formulář určený pro koncové uživatele
2. odkaz na novou stránku s dalšími informacemi
3. odkaz na veřejné mapové rozhraní GIS
4. odkaz na API umožňující přístup k jednotlivým záznamům či vyhledávání záznamů, nikoliv export kompletních dat
5. datový soubor ve formátu PDF
6. datový soubor ve formátu XLS formátovaný pro tisk nebo obsahující výpočty
7. datový soubor v pseudo-CSV formátu (např. jiný oddělovač než “,”)

Pro zajištění publikace otevřených dat z IS je třeba:

1. Zajistit možnost získávání kompletních dat z IS v podobě datových souborů ve strojově čitelném a otevřeném formátu
2. Zajistit publikaci datových souborů na webu organizace nebo v jejím lokálním katalogu otevřených dat
3. Opatřit je lidsky čitelnou dokumentací a strojově čitelným schématem
4. Opatřit je otevřenými podmínkami užití
5. Zaregistrovat je v Národním katalogu otevřených dat (NKOD)

Možnosti přípravy IS pro otevřená data

Zásadní je mít přístup k datům IS. Provozovaný IS tedy musí:

1. umožňovat přístup k databázi nebo
2. mít možnost stahovat volitelně strukturovaná data (tabulky) z reportingového modulu systému nebo
3. nabídnout API, ze kterého se dají pravidelně získávat kompletní data v podobě datových souborů

Export dat nebo API v otevřeném formátu - preferované řešení

IS má rozhraní pro pravidelný export dat nebo neomezené API, které organizace může vytěžit a získat kompletní data v jednom z otevřených formátů.

- Pro tabulková data je to CSV
- Pro hierarchická data je to XML nebo JSON
- Pro grafová data je to RDF
- Pro geodata je to jeden z otevřených formátů pro geodata - GeoJSON, ESRI Shapefile, OGC GML, OGC GeoPackage.

Struktura dat je zdokumentována jednak lidsky čitelným dokumentem a jednak strojově čitelným schématem.

- Pro CSV je to schéma CSV on the Web
- Pro XML je to XML Schema
- Pro JSON je to JSON schema

- Pokud je použit vlastní slovník pro RDF, je popsán pomocí RDFS nebo OWL

V takovém případě jsou získaná kompletní data z IS připravena k publikaci formou otevřených dat.

Export dat nebo API v proprietárním formátu

Pokud se jedná o rozšíření existujícího IS, který neumožňuje export dat nebo nenabízí API ve strojově čitelném a otevřeném formátu a takovou úpravu nelze ve Vašem IS provést, využije se stávající export či API, které váš IS již umí (např. do MS Excel), a tento výstup se dále zpracuje do otevřeného formátu pomocí dalších nástrojů tak, aby bylo dosaženo stavu jako v případě přímého exportu do otevřeného formátu.

Následná příprava dat k publikaci v podobě otevřených dat

Data získaná z IS jedním z popsaných způsobů je následně třeba publikovat jako otevřená data. To znamená minimálně:

1. V případě API zajistit jeho vytěžení pro získání kompletních dat k publikaci (tj. případná přímá publikace API nenaplňuje podmínky otevřených dat)
2. Zajistit pravidelnou aktualizaci získaných dat (dle charakteru dat to může být ve frekvenci např. denně, měsíčně nebo ročně)
3. Publikovat získaná data na web ke stažení a následně publikovat každou jejich aktualizaci
4. Opatřit je dokumentací, podmínkami užití a kontaktem na kurátora
5. Katalogizovat je v Národním katalogu otevřených dat (NKOD)

K tomu lze využít nástrojů pro přípravu, publikaci a katalogizaci otevřených dat, jako je třeba LinkedPipes ETL.

Publikace otevřených dat by měla být zajištěna koncepčně na úrovni celé organizace. Kompletní postupy jsou k dispozici na Portálu otevřených dat, naleznete zde rovněž informace o školeních a workshopech, které Ministerstvo vnitra k této problematice poskytuje.

Pro příklad vhodného způsobu zveřejnění datové sady v lokálním katalogu se lze podívat na katalog České správy sociálního zabezpečení (ČSSZ).

Ochrana osobních údajů

Pokud jsou předmětem evidence informačního systému osobní údaje ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a nařízení (EU) č. 2016/679, Obecné nařízení o ochraně osobních údajů (GDPR), neznamená to, že nelze ze systému publikovat otevřená data. Ve formátu otevřených dat lze zveřejnit následující:

1. Pakliže se jedná o veřejnou evidenci či rejstřík a zvláštní právní předpis nařizuje zveřejnění informací, lze zveřejnit osobní údaje v podobě otevřených dat.
2. Anonymizace či Pseudonymizace. Z dat se odstraní osobní údaje a případně se nahradí bezvýznamovým umělým identifikátorem. Data bez osobních údajů se pak mohou zveřejnit v podobě otevřených dat. Ovšem pozor, v závislosti na charakteru dat je třeba zkontrolovat, zda data ve své kombinaci neumožňují identifikaci konkrétní osoby i po odstranění zjevných osobních údajů. Zejména se může jednat o kombinace jako město, věk a pohlaví nebo podobné.
3. Agregace. Data, která není možné nebo vhodné zveřejnit dle předchozího bodu, lze zveřejnit v agregované podobě. Tedy v podobě statistik. V případě zveřejnění statistik je žádoucí použít co nejjemnější možné členění.Tedy například počet přijatých podání uvádět raději po měsících namísto jen po letech.

Více informací naleznete na stránce o ochraně osobních údajů a GDPR ve vztahu k otevřeným datům.

Právní aspekty

Legislativní rámec otevřených dat v České republice tvoří jejich úprava obsažená v Zákoně č. 106/1999 Sb., o svobodném přístupu k informacím a v Nařízení vlády č. 425/2016 Sb., o seznamu informací zveřejňovaných jako otevřená data, které stanovuje vybraným orgánům veřejné správy povinnost zveřejňovat data z konkrétních jimi spravovaných informačních systémů ve formě otevřených dat.

Více informací o strategických dokumentech, akčních plánech a souvisejících předpisech ČR i EU naleznete na stránce věnované legislativnímu prostředí otevřených dat.

Veřejný datový fond

Veřejným datovým fondem (dále jen VDF) se rozumí celek datového fondu ČR, obsahující údaje zveřejňované orgány veřejné správy jako veřejné rejstříky a údaje zveřejňované jako otevřená data s podporou centrálního nástroje, kterým je Národní katalog otevřených dat (NKOD).

Veřejné rejstříky (VDF-VR)

Veřejnými rejstříky právnických a fyzických osob podle zákona č. 304/2013 Sb., Zákon o veřejných rejstřících právnických a fyzických osob (dále jen „veřejný rejstřík“), se rozumí:

- spolkový rejstřík,
- nadační rejstřík,
- rejstřík ústavů,
- rejstřík společenství vlastníků jednotek,
- obchodní rejstřík a
- rejstřík obecně prospěšných společností.

Do veřejného rejstříku se zapisují zákonem stanovené údaje o právnických a fyzických osobách (dále jen „zapsaná osoba“). Veřejný rejstřík je informačním systémem veřejné správy. Veřejný rejstřík je veden v elektronické podobě. Veřejný rejstřík vede soud (dále jen „rejstříkový soud“).

Ministerstvo financí uveřejňuje způsobem umožňujícím dálkový přístup informace o osobách zapsaných v České republice a údaje o tom, ve kterém veřejném rejstříku jsou tyto osoby zapsány. Ministerstvo financí umožňuje získat o údajích vedených ve veřejných rejstřících elektronický opis.

Údaje z Obchodního rejstříku společně s údaji z Registru živnostenského podnikání (RŽP) a Registru ekonomických subjektů (RES), Registru plátců spotřební daně (SD) a dalších zdrojů publikuje Ministerstvo financí prostřednictvím Administrativního registru ekonomických subjektů (ARES). ARES je IS, který zpřístupňuje veřejné údaje o ekonomických subjektech z informačních systémů (zdrojů) veřejné správy. Obsahuje údaje ze základních (majoritních) zdrojů, které jsou formou odkazů doplněny údaji z dalších zdrojů. Při zpracování se používají též kontrolní zdroje.

Veřejné rejstříky a vzdálený přístup k jejich údajům prostřednictvím ARES předcházely Základním registrům a musí být s nimi sladěny a integrálně nově zařazeny do celkové koncepce eGovernmentu. Koncepce rozvoje veřejných rejstříků a jejich IS musí tedy naplňovat přinejmenším následující požadavky:

1. Všechny rejstříky musí obsahovat ztotožněné údaje FO a PO, pokud je bylo proti čemu ztotožnit (u rezidentů).

2. Všechny rejstříky vedle toho, že jsou publikovány na internetu, musí být dostupné jako otevřená data. A to přímo, nebo prostřednictvím OD k ARES.
3. Všechny rejstříky musí být pro potřeby agend OVS dostupné přes eGSB, a to buď sdruženě, prostřednictvím ARES, nebo přímo, pokud jejich veřejné údaje nejsou v ARES zahrnuty.
4. ARES, jako klíčový veřejný rejstřík s velkým hospodářským dopadem, musí být být průběžně rozvíjen a inovován tak, aby odpovídal aktuálním potřebám občanské i podnikové veřejnosti ČR.

Otevřená data (VDF-OD)

Otevřenými daty se v rámci veřejného datového fondu se rozumí celek obsahující údaje zveřejňované orgány veřejné správy jako otevřená data a Národní katalog otevřených dat (NKOD).

NKOD je nástroj, ve kterém jednotlivé orgány veřejné správy katalogizují jimi zveřejňovaná otevřená data a jiné orgány veřejné správy a veřejnost v něm otevřená data vyhledávají a získávají k nim přístup.

Existence NKOD a povinnost jednotlivých orgánů veřejné správy v něm katalogizovat svá otevřená data je dána zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, který zavádí definici otevřených dat, NKOD a zmocňuje vládu vydat nařízení o seznamech, evidencích či registrech, jejichž veřejný obsah je povinně zveřejňován jako otevřená data, § 5 odst. 7 tohoto zákona pak zmocňuje orgány veřejné správy zveřejňovat i další informace jako otevřená data.

Nařízení vlády č. 425/2016 Sb. o seznamu informací zveřejňovaných jako otevřená data stanovuje, jaké informace mají být zveřejňovány orgány veřejné správy jako otevřená data povinně.

Pro naplnění závazků, které vyplývají ze strategických dokumentů, bude zveřejňování otevřených dat povinné pro všechny správce ISVS. Pro zamezení vytváření duplicitních informací ve veřejné správě, které mohou být zveřejňovány, bude zavedena povinnost orgánů veřejné správy je sdílet jako otevřená data.

Průběžná změna legislativního prostředí musí vést k postupnému rozšiřování povinností orgánů veřejné správy zveřejňovat informace reprezentované jako údaje evidované v ISVS, jejichž zveřejnění je možné, nebo jejich anonymizovanou podobu, souhrn či statistiku jako otevřená data s cílem dosáhnout plošné povinnosti. Je nutné výslovně zanést možnost zveřejňovat informace jako otevřená data do zvláštních předpisů upravujících zveřejňování údajů, v jejichž případě se postup podle zákona o svobodném přístupu k informacím nepoužije, např. do zákona o právu na informace o životním prostředí.

Je též nutné legislativně ukotvit povinnost orgánů veřejné správy využívat při výkonu svých agend otevřená data poskytovaná jinými orgány veřejné správy. To se týká především číselníků, kdy jsou stejné číselníky vytvářeny různými orgány veřejné správy.

Veřejný datový fond v současnosti tvoří otevřená data několika orgánů veřejné správy a NKOD. Různá kvalita otevřených dat komplikuje jejich opakovatelnou použitelnost. Je též téměř nemožné sdílet veřejné údaje mezi orgány veřejné správy jako otevřená data, neboť neexistují žádné garance dostupnosti. Pro zlepšení současného stavu se VDF stane virtuálním distribuovaným datovým prostorem, ve kterém orgány veřejné správy sdílí s veřejností i mezi sebou navzájem veřejné údaje evidované v jimi spravovaných ISVS v podobě kvalitních otevřených dat. VDF-OD bude mít následující součásti:

- *Sdílený veřejný datový fond (SVDF)* – bude podmnožinou otevřených dat, která je určena nejenom veřejnosti, ale slouží i ke sdílení veřejných údajů mezi orgány veřejné správy. Pro otevřená data v SVDF musí být zajištěna a garantována jejich dostupnost pro orgány veřejné správy, které je pro výkon svých agend využívají.
- *Národní katalog otevřených dat (NKOD)* – bude zvýšena jeho uživatelská přívětivost i na bázi sémantického slovníku pojmů. Bude podporovat standard DCAT-AP[1)].
- *Nástroj pro správu sémantického slovníku pojmů (NSSSP)* – umožní správu sémantického slovníku pojmů všemi orgány veřejné správy a popisovat jejich otevřená data za účelem sémantické harmonizace otevřených dat.
- *Katalog uživatelů otevřených dat (KUOD)* – bude evidovat, jaké orgány veřejné správy využívají jaká

otevřená data v SVDF.
- *Portál otevřených dat (POD)* – bude jednotný přístupový bod do VDF veřejně přístupný na adrese https://data.gov.cz.
- *5* (pětihvězdičkový) veřejný datový fond (5VDF)* – bude podmnožinou otevřených dat, které jsou zveřejněny jako propojená otevřená data. Jeho součástí bude index datových entit, který pro každou datovou entitu reprezentovanou v 5VDF poskytuje základní údaje z 5VDF a odkazy na různé její reprezentace v otevřených datech jednotlivých orgánů veřejné správy v 5VDF.

Budou zajištěny kapacity pro vytvoření nových komponent VDF-OD. Softwarové nástroje pro realizaci VDF budou vytvořeny jako open-source s maximálním využitím existujících open-source komponent.

SVDF bude naplňován postupně. Nejprve zde budou zveřejněny kompletní údaje evidované v základních registrech ROS, RÚIAN a RPP, statistiky vytvořené z údajů evidovaných v základním registru ROB a veškeré sdílené číselníky spravované orgány veřejné správy. Postupně pak budou v SVDF zveřejňovány i další sdílené veřejné údaje dle připravovaných projektů tvorby či zhodnocování jednotlivých ISVS tak, aby bylo dosaženo cílového stavu zveřejnění všech sdílených veřejných údajů v SVDF. V 5VDF budou zveřejněny údaje ze základních registrů a vybrané číselníky vybraných orgánů veřejné moci, které jsou potřebné pro propojování dat. V případě rozšiřování základních registrů budou též i v nich vedené údaje zveřejněny jako otevřená data ve SVDF a jako propojená otevřená data v 5VDF.

Bude vytvořeno HW a SW prostředí pro provoz komponent VDF-OD. Pro potřeby orgánů veřejné správy, které budou zveřejňovat otevřená data v SVDF bude vybudováno sdílené úložiště SVDF, které umožní zajistit a garantovat dostupnost pro ostatní orgány veřejné správy.

HW a SW prostředí pro VDF-OD bude zajištěno v NDC nebo eGovernment Cloudu. HW a SW prostředí sdíleného úložiště SVDF bude zajištěno v NDC nebo eGovernment Cloudu. Správcem vytvořených prostředí bude Ministerstvo vnitra.

Centrální místo služeb

CMS je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy s definovanou bezpečností a SLA parametry, tj. přístup ke službám eGovernmentu. CMS tak můžeme nazvat privátní sítí pro výkon veřejné

správy na území státu. CMS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do Internetu.

Centrální místo služeb v kombinaci s tzv. komunikační infrastrukturou veřejné správy (KIVS) nabízí pro jednotlivé OVS:

* * * * * * Připojení k CMS je možné realizovat jednou ze čtyř možností: 1. KIVS, 2. Krajský konektor, 3.IPsec VPN, 4. SSL VPN.

Komunikace mezi jednotlivými OVS je tak vedena výhradně prostřednictvím CMS.

CMS, popis zahrnutých služeb

Odbor Hlavního architekta eGovernmentu a Ministerstvo vnitra v rámci svých kompetencí požaduje od jednotlivých správců ISVS, aby služby těchto systémů publikovaly v rámci Centrálního místa služeb – CMS

(služba CMS2 -02, CMS2 -04).

Jednotliví uživatelé ISVS na úrovní státní správy a samosprávy služby těchto systémů konzumují, resp. k ISVS přistupují výhradně prostřednictvím CMS (služba CMS2 -03).

Služba CMS2 – 02 – Zveřejnění aplikace

Název parametru	Vysvětlení
Kód služby	CMS2-02
Název služby	Zveřejnění aplikace
Popis služby	Služba vytvoří prostředí pro publikaci aplikační služby informačního systému OVM. Varianty služby se liší podle cílového prostředí. Možné varianty jsou: 1. do sítě Internet 2. do sítě CMS 3. do sítě TESTA-ng 4. do Extranetu

Aplikační služba může být umístěna v infrastruktuře orgánu nebo v infrastruktuře Národního datového centra (NDC). Aplikační služba může být zveřejněna do více prostředí současně. Aplikační služba je zveřejněna na definovaných protokolech a portech.

Při zveřejnění aplikace do sítě Internet jsou aplikaci přiděleny veřejné IP adresy z prostoru CMS. Přístup ke zveřejněné službě může být omezen na definované zdrojové IP adresy.

Při zveřejnění aplikace do sítě CMS jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Službu je možné zveřejnit pro všechny ostatní subjekty připojené do sítě CMS (Veřejná služba) nebo pro definované subjekty a skupiny subjektů (Schvalovaná služba). O přístup ke Schvalované službě musí přistupující subjekty žádat prostřednictvím služby CMS203-1.

Při zveřejnění aplikace do sítě TESTA-ng (síť EU) jsou aplikaci přiděleny IP adresy z prostoru pro ČR v síti TESTA-ng. Přístup ke zveřejněné službě je omezen na definované zdrojové IP adresy. Zveřejnění aplikace musí být provozováno v souladu s provozními a bezpečnostními požadavky EU pro síť TESTA-ng.

Při zveřejnění aplikace do Extranetu jsou aplikaci přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy). Aplikační služba je zveřejněna do existujícího extranetu (extranet vytváří Správce CMS). Přístup k aplikaci v extranetu je umožněn všem uživatelům, kteří mají do daného extranetu přístup.

Služba CMS2 – 03 – Přístup k aplikaci

Název parametru	Vysvětlení
Kód služby	CMS2-03
Název služby	Přístup k aplikaci
Popis služby	Služba umožňuje zřizovat a rušit přístupy k aplikačním službám. Varianty služby se liší podle cílového prostředí. Možné varianty představují přístup: 1. k aplikaci v síti CMS 2. k aplikaci v síti TESTA-ng 3. k aplikaci v síti Internet

Služba umožňuje zřizovat, měnit a rušit přístupy subjektu k nabízené aplikační službě. Jednou žádostí lze zřídit přístup právě k jedné aplikační službě. Připojení je povoleno z definovaných IP adres v síti subjektu.

Přístup k aplikaci v síti CMS umožní subjektu připojení k aplikační službě zveřejněné jiným subjektem prostřednictvím služby CMS2-02-2 v síti CMS. Zřízení přístupu je podmíněno souhlasem vlastníka zveřejněné aplikační služby, které probíhá prostřednictvím portálu CMS.

Přístup k aplikaci v síti TESTA-ng umožní subjektu připojení k aplikační službě zveřejněné jiným státem Evropské unie v síti TESTA-ng. Připojení je povoleno na definovaných protokolech a portech. Přístup k aplikaci musí být provozován v souladu s provozními a bezpečnostními požadavky EU pro síť TESTA-ng.

Přístup k aplikaci v síti Internet umožní subjektu připojení k aplikační službě zveřejněné v síti Internet na

definovaných protokolech a portech. Cílovou aplikační službu v síti Internet je nutné definovat konkrétními IP adresami, protokoly a porty.

Služba CMS2 – 04 – Publikace AIS na eGSB

Název parametru	Vysvětlení
Kód služby	CMS2-04
Název služby	Publikace AIS na eGSB
Popis služby	Služba zajišťuje zpřístupnění publikačního agendového informačního systému (AIS) v rámci CMS a povolení síťové komunikace s rozhraním eGON Service Bus (eGSB)

Služba zajistí provozovateli publikačního agendového informačního systému (AIS) síťovou konektivitu mezi eGSB (eGovernment Online Service Bus, tj. sdílená služba obecného rozhraní) a publikačním AIS na definovaných protokolech a portech. V rámci publikace jsou přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy).

Ve výchozím stavu je komunikace mezi eGSB a publikačním AIS synchronní, volitelně lze zprovoznit komunikaci asynchronní.

Právní aspekty

S výjimkou tzv. provozních informačních systémů, které jsou uvedeny v § 1 odst. 4 písm. a) až d) zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS), je § 6g odst. 3 tohoto zákona správcům ISVS uložena povinnost poskytovat služby informačních systémů veřejné správy

prostřednictvím CMS. Organům veřejné správy je prostřednictvím § 6g odst. 4 ZoISVS uložena povinnost využívat sítě elektronických komunikací CMS.

Protože CMS je součástí tzv. referenčního rozhraní, definovaného v § 2 písm. j) ZoISVS, má vztah k CMS i povinnost uložená v § 5 odst. písm. d) ZoISVS, tj. povinnost správců ISVS zajistit, aby vazby jimi spravovaného ISVS na ISVS jiného správce byly uskutečňovány prostřednictvím referenčního rozhraní.

S ohledem na výše popsané vlastnosti CMS, jakož i s ohledem na výše popsané právní aspekty, lze také dodat, že využívání, popř. nevyužívání CMS je relevantním faktorem pro posuzování plnění souvisejících právních povinností, a to zejména povinností v oblasti kybernetické bezpečnosti nebo ochrany osobních údajů, jakož i povinnosti řádného a hospodárného nakládání s veřejnými finančními prostředky a povinnosti k předcházení vzniku škod.

Příkladem publikované služby - Centrální registr řidičů (CRŘ)

Elektronická fakturace

Elektronická fakturace (dále jen „e-fakturace“) je moderní prostředek, jehož primárním cílem je usnadnit a zefektivnit ekonomickým subjektům odesílání, příjem e-faktur a jejich následnou archivaci k dalšímu zpracování v rámci Evropské unie. E-faktura je dokumentem v digitální podobě (elektronickým dokumentem) podle ustanovení § 2 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů a nařízení eIDAS. Může být doručena ve strukturovaném nebo nestrukturovaném datovém formátu. Může být účetním záznamem podle zákona č. 563/1991 Sb., o účetnictví, daňovým dokladem podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, může sloužit i pro jiné účely (např. jako dodací list, záruční list, důkazní prostředek apod.)

E-fakturace v kombinaci s řádně vedenou spisovou službou dle č.499/2004 Sb., zákona o archivnictví a spisové

službě nabízí ekonomickým subjektům orgánů veřejné správy:

* * * *

Ekonomické aspekty

Evropská komise předpokládá, že „Masové přijetí elektronické fakturace v EU by vedlo k významným hospodářským přínosům a odhaduje se, že přechodem od papírových faktur k fakturám elektronickým se za období šesti let ušetří přibližně 240 miliard EUR.“1. Na základě tohoto zjištění „Komise chce, aby se elektronická fakturace stala převládající metodou fakturace v Evropě do roku 2020.

Jako prostředek k dosažení tohoto cíle má směrnice 2014/55/EU o elektronické fakturaci při zadávání veřejných zakázek za cíl usnadnit používání elektronických faktur hospodářskými subjekty, které dodávají zboží, práce a služby pro orgány veřejné správy (B2G), jakož i podporovat obchodování mezi samotnými hospodářskými subjekty (B2B). Vymezuje především právní rámec pro zavedení a přijetí evropské normy (EN) pro sémantický datový model vytvořený ze základních prvků elektronické faktury (EN 169311:2017).

Norma EN 169311:2017 a její pomocné normalizační výstupy umožní sémantickou interoperabilitu elektronických faktur a pomohou odstranit bariéry na trhu a překážky v obchodu vyplývající z existence rozdílných vnitrostátních právních předpisů a norem – a přispějí tak k dosažení cílů stanovených Evropskou komisí.

Technické aspekty

E-fakturaci je možné implementovat a realizovat ve svých organizačních jednotkách za dodržení jednoho z následujících technických standardů, který je v souladu se směrnicí 2014/55/EU:

* * * * Je třeba zmínit, že směrnice 2014/55/EU:

nepředepisuje, která syntaxe by měla být použita pro elektronickou fakturaci při zadávání veřejných zakázek. Pouze uvádí, které syntaxe jsou veřejní zadavatelé povinni akceptovat. Je zcela možné a velmi pravděpodobné, že jiné syntaxe, které nejsou uvedeny na seznamu výše, se budou i nadále používat, a to i pro přeshraniční výměny, zvláště tam, kde již existuje rozšířená národní nebo místní praxe;

neponechává veřejným zadavatelům žádný prostor pro volbu mezi syntaxemi, které jsou uvedeny na seznamu, jenž bude zveřejněn v Úředním věstníku Evropské unie, v návaznosti na článek 3 směrnice. Článek 7 jasně uvádí, že veřejní zadavatelé a zadavatelé v EU musí přijímat a zpracovávat elektronické faktury, které splňují normu a odpovídají kterékoli ze syntaxí uvedených na zveřejněném seznamu.

Jakákoliv odchylka od tohoto pravidla by představovala porušení směrnice.

To je případ českého formátu elektronické faktury ISDOC (Information System Document), verze 5.2 a vyšší (dle Usnesení vlády č. 347/2017 a vyhlášky č.194/2009 Sb), který není součástí výše uvedené směrnice, ale v rámci vnitřního trhu České republiky bude i nadále používán mezi ekonomickými subjekty.

Právní aspekty

Implementace e-fakturace do prostředí veřejné správy České republiky je dána směrnicí 2014/55/EU, která

nabyde účinnost 19. 4. 2018. K tomuto datu je také nutné mít ve svých spisových službách v rámci organizace nastavené technickoorganizační opatření, která budou v souladu s výše uvedenou směrnicí a technickými standardy z ní vyplívající. Směrnice byla inkorporována do české legislativy v rámci §221 zákona č. 134/2016, o zadávání veřejných zakázek. Zadavatel nesmí odmítnout elektronickou fakturu vystavenou dodavatelem za plnění veřejné zakázky z důvodu jejího formátu, který je v souladu s evropským standardem elektronické faktury.

Všechny veřejné zakázky, které jsou nadlimitní mohou být dodavatelem vyžadovány ve formě e-fakturace.

V neposlední řadě bylo schváleno Usnesení vlády č. 347/2017, které dává povinnost od 1. 1. 2019 Ústředním orgánům státní správy a jimi podřízeným organizačním složkám státu přijímat elektronické faktury ve formátech stanovených Evropskou směrnicí 2014/55/EU a dále ve formátu isdoc/isdocx (Information System Document) verze 5.2 a vyšší

Cílový adresáti

Dle zákona č. 134/2016, o zadávání veřejných zakázek se týká všech orgánů veřejné moci, kteří zadali k postoupení nadlimitní veřejnou zakázku a to od 1. 1. 2019 pro ústřední orgány moci a následně od 1.4.2020 pro uzemní samosprávu dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, §279 (5) b)

Mandáty, role a práva v elektronické komunikaci

Zajištění správné obsazení do role neboli autorizace, klienta využívajícího elektronické služby je jedním ze základních předpokladů jejího správného fungování. Různé role mají v rámci služby různá oprávnění a povinnosti a poskytovatel služby je povinen nabídnout klientovi veškeré role, do kterých se v rámci služby může pasovat, včetně rolí jako zástupce právnické osoby, zástupce nezletilého, registrující lékař pacienta a další. Tyto role s oprávněními vůči jiným klientům veřejné správy jsou mandáty. Aby proběhlo správné obsazení do role a zjištění mandátu, je pro poskytování elektronických služeb klientům veřejné správy nutné mít zajištěno několik základních náležitostí:

1) Znalost typů mandátů při jednání s veřejnou správou

2) Jednoznačnou identifikaci a autentizaci klienta veřejné správy

3) Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu

4) Vlastní zajištění autorizace klienta veřejné správy

Mandáty pro jednání s veřejnou správou

Při výkonu veřejné správy a to zejména při jakékoliv interakci a komunikaci s klientem veřejné správy je nutné, aby veřejná správa respektovala mandáty k zastupování jedné osoby druhou na základě různých titulů. Zjednodušeně se dá rozdělit forma mandátu zastupování takto:

1. Fyzická osoba

a. Jednající sama svým jménem

b. Jednající jménem jiné fyzické osoby ze zákona

i. rodič dítěte

ii. manžel/manželka

iii. registrovaný partner/partnerka

iv. opatrovník

c. Jednající jménem jiné fyzické osoby ze zmocnění

i. plná moc

ii. advokát

iii. zastupující FO

iv. jiný druh zmocnění

v. na žádost bez zmocnění

2. Fyzická osoba jednající za právnickou osobu

a. Jednatel právnické osoby

b. statutární zástupce právnické osoby (jedna FO)

c. Statutární orgán právnické osoby (více FO)

d. Insolvenční správce

e. Likvidátor

f. Jednající jménem zřizovatele právnické osoby

g. Pověřen k jednání za právnickou osobu

i. Veřejnoprávním titulem

ii. Soukromoprávním titulem (smlouva, plná moc, společenská smlouva, apod.)

Jak je zdůrazněno níže, při výkonu veřejné správy je nutné, aby příslušný orgán konající nějakou činnost v rámci dané agendy věděl, pro jakou formu zastupování je mandát umožněný nebo dokonce nutný. Zcela jiným způsobem se orgán veřejné moci bude chovat k mandátu plynoucímu z veřejnoprávního titulu rodičovství a jinak k mandátu plynoucímu ze soukromoprávního titulu plné moci.

Je také vhodné rozlišovat účel mandátu, tedy typ úkonů, které prostřednictvím zastupované osoby klient veřejné správy dělá. Ty je možno rozdělit do následujících skupin:

* * * * * *

Jednoznačná identifikace a autentizace klienta veřejné správy

Všechny subjekty povinné dle zákona č. 250/2017 Sb., o elektronické identifikaci mají povinnost dle §2 využívat k prokázání totožnosti při elektronickém kontaktu pouze kvalifikovaný systém, konkrétně:

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s

využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.“

Kvalifikovaný systém spravuje kvalifikovaný správce (státní orgán nebo akreditovaná osoba) a splňuje technické normy i specifikace Evropské unie a především je propojen s národním bodem pro identifikaci a autentizaci – tzv. Národní identitní autorita (NIA).

Identifikace a autentizace prostřednictvím NIA zajistí jen a pouze službu ověřené identity fyzické osoby, neboli každý systém čerpající služby NIA, se může spolehnout na to, že přihlášená fyzická osoba je skutečna ta, za kterou se vzdáleně a elektronicky vydává. Již se dále nezajišťují další služby typu autorizace.

Systém veřejné správy schopný komunikovat a získávat údaje z propojeného datového fondu

Systém poskytující elektronické služby veřejné správy musí být schopen komunikovat a získávat údaje z propojeného datového fondu. K tomu musí systém odpovídat předpisům:

* * Více o využívání údajů propojeného datového fondu a infrastruktuře referenčního rozhraní je napsáno v dokumentech: * eGovernment Online Service Bus * Centrální místo služeb

* Centrální sdílené služby eGovernmentu dokáží zajistit následující mandáty pro fyzické osoby, které se prokázaly u poskytovatele služeb svou zaručenou elektronickou identitou:

* o pro zajištění ověření, zda je fyzická osoba statutárním zástupcem

* o pro zajištění ověření, zda je fyzická osoba rodič nezletilého, který není svéprávný

o pro zajištění ověření, zda je fyzická osoba zákonným zástupcem jiné fyzické osoby

o pro zajištění ověření, zda je fyzická osoba opatrovníkem jiné fyzické osoby

o pro zajištění ověření, zda je fyzická osoba manžel/manželka

* o pro zajištění ověření, zda je fyzická osoba vlastníkem nemovitosti

* o Pro zajištění, zda je fyzická osoba pověřená k činění úkonů v ISDS vlastníkem datové schránky

Žádné další centrální služby ověření oprávnění/mandátů se v současné, ani dohledné době, neplánují. Proto je důležité, aby si každý poskytovatel elektronických služeb zajistit jiné typy mandátů sám.

Vlastní zajištění autorizace klienta veřejné správy

Každá vykonávaná agenda (výkon veřejné správy) může pro svoji potřebu vyžadovat jiné mandáty. Například mandát podání daňového přiznání za jinou fyzickou osobu, mandát nahlížení na zdravotnickou dokumentaci jiné fyzické osoby, nakládání s majetkem právnické osoby, u které nejsem statutární zástupce, či například mandát k zastupování při dědickém řízení.

Všechny tyto mandáty se musí řešit v rámci dané agendy a jako ideální řešení navrhujeme:

* * * * * Je důležité zdůraznit, že veřejná správa nemá rozlišovat formu komunikace a jednání s klientem. Tedy mandát obecně platící pro osobní jednání s úředníkem, nebo pro fyzické prováděné úkony na přepážce, musí mít klient umožněn využívat i při elektronické komunikaci a naopak. Také proto je nutné vést mandáty standardizovanou formou na jednom místě a využívat jich i při elektronické komunikaci klienta.

Mandát plynoucí z veřejnoprávního nebo soukromoprávního titulu a to včetně plných mocí a dohod o

zastupování při správním jednání s úřady patří mezi společné rozhodné skutečnosti, tak jak jsou zakotveny v souvisejících ustanoveních Správního řádu (zejména § 6 a § 50 a související). Proto je nanejvýš vhodné, aby příslušný orgán veřejné moci, pokud

* * * je zahrnul do rozhodných skutečností. Klient se totiž může odvolat na příslušná ustanovení správního řádu a neposkytovat zejména plné moci a další dokumenty, z nichž mandát plyne, úřadu opakovaně.

Zásadním požadavkem bezpečnosti a transparentnosti pro informační systémy veřejné správy je požadavek na jednotnou elektronickou identifikaci interních i externích uživatelů. Pro každou operaci je nutná znalost osoby, která tuto operaci provádí zvláště z hlediska nepopiratelné zodpovědnosti osoby.

Externí uživatelé (klienti) informačních systémů veřejné správy musí být jednoznačně identifikováni zvláště z důvodů ochrany osobních údajů a dále z procesního hlediska, jak předpokládá správní řád (jednoznačné prokázání totožnosti účastníků řízení).

Pro interní uživatele, pracující v informačním systému veřejné správy je nutnou podmínkou jednoznačná a nepopiratelná identifikace uživatele tak, aby bylo možné jednoznačně vyhodnotit oprávnění této osoby v rámci přístupu k údajům a službám informačních systémů a současně zpětně vyhodnotit činnost těchto osob dle záznamů v auditních systémech (logy).

Úloha správy přístupů se pro každý informační systém veřejné správy skládá z následujících kroků:

- **Identifikace –** jednoznačné a nepopiratelné určení fyzické osoby, která přistupuje k informačnímu systému veřejné správy
- **Autentizace** – prokázání, že přistupující osoba je tou osobou, za kterou se vydává. Autentizace probíhá předložením **autentizačních prostředků** (například uživatelské jméno a heslo, autentizační certifikát), které osobě přidělil správce informačního systému
- **Autorizace** – na základě údajů o identifikované a autentizované osobě a dalších údajů o této osobě (například zařazení na pracovní pozici) zařazení osoby do odpovídající role a z toho vyplývající vyhodnocení oprávnění na úkony a data v rámci informačního systému.

IKČR v této oblasti vyžaduje naplnění následujících principů pro všechny informační systémy veřejné správy:

1. Při tvorbě identitního prostoru si prvně udělat analýzu, zda nepostačuje již některý z federovaných identit v rámci NIA
2. Jakýkoliv nový identitní prostor musí být budován tak, aby byl federovaný v rámci NIA
3. Prostředky pro identifikaci a autentizaci jsou vždy vydány bezpečnou a jednoznačnou cestou identifikované osobě tak, aby byla zajištěna minimálně úroveň důvěry značná. O tomto vydání prostředků existuje trvalý záznam spolu s údaji, jak byla ověřena identita osoby
4. Osoba, jíž byly prostředky vydány, nedílně zodpovídá za ochranu těchto prostředků před odcizením a zneužitím
5. Osoba, jíž byly prostředky vydány, nese nedílnou zodpovědnost za všechny úkony, které byly v informačním systému provedeny při použití těchto prostředků
6. Věcný správce agend, které jsou vykonávány v rámci informačního systému, zodpovídá za obsazení osob do rolí (technicky vykonává technický správce informačního systému, vždy však na základě podkladů o věcných správců). Tuto svoji zodpovědnost může delegovat v rámci organizační struktury na více zodpovědných osob.

Jednotná elektronická identifikace klientů VS (NIA)

Pro jednoznačnou identifikaci, autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s IKČR a výše uvedenými požadavky bez nutnosti vytváření nákladných řešení a zvyšování administrativní zátěže.

Zákon č. 250/2017 Sb., o elektronické identifikaci, zavádí v §2 povinnost provádět prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.

Tento paragraf nabývá účinnosti 1. července 2020. Po tomto datu nebude možné pokračovat v praxi vydávání přístupových údajů klientů veřejné správy mimo systémy kvalifikovaného systému elektronické identifikace, pokud jiný zákon tuto cestu neumožnuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma **Národní identitní autority**, která vykonává činnosti Národního bodu dle § 20 a následujících a národního uzlu eIDAS pro spolupráci s oznámenými systémy elektronické identifikace dle nařízení Evropské parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

NIA zajistí OVS státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principy Single Sign-On. Žádné OVS si tedy již nemusí řešit přihlašovací identity pro své klienty samo! Toto platí pouze pro osoby uvedené v ROB nebo přihlašující se identitou v rámci eIDAS z členských států EU. V současném stavu ROB (stav As-Is) tedy pouze pro občany ČR a cizince s trvalým pobytem. V budoucím stavu (stav To-Be) pro občany ČR, cizince s trvalým pobytem a jiné fyzické osoby (EjFO), které mají k ČR právní či majetkový vztah (zahraniční vlastník nemovitosti, zahraniční lékař, zahraniční student, apod.).

Národní identitní autorita vytváří federativní systém, který se skládá z následujících komponent:

- **Národní bod** jako centrální bod federativního systému, který zajišťuje komunikaci a registraci účastníků federace. Tato komponenta zajišťuje současně vždy **jednoznačné ztotožnění** osoby, která prokazuje svoji totožnost předložením autentizačních prostředků
- **Kvalifikovaný správce,** který vydává jednoznačně identifikovaným fyzickým osobám prostředky pro vzdálenou autentizaci (prokázání totožnosti) a provádí veškeré činnosti spojené se správou těchto prostředků a prokazováním totožnosti fyzické osoby
- **Základní registry,** které poskytují jednoznačnou identifikaci osoby a zajištění vazeb této osoby vůči referenčním údajům o osobě
- **Národní uzel eIDAS,** který zajišťuje přijímání vzdáleného prokázání totožnosti z ohlášených systémů dle nařízení eIDAS a předávání vzdálené identifikace a autentizace z České republiky ostatním státům EU

Kvalifikovaný poskytovatel elektronických služeb **bude nadále zodpovědný** za řízení oprávnění (autorizaci) fyzické osoby, která prokázala takto svoji totožnost. Nadále tedy musí provádět správu oprávnění na základě údajů o osobě, které získá z propojeného datového fondu veřejné správy a vlastních údajů vedených v agendě.

Jednotný identitní prostor úředníků, autentizační informační systém (JIP/KAAS)

Jednotní identitní prostor (JIP) informačních systémů veřejné správy a Katalog autentizačních a autorizačních služeb (KAAS) je autentizační informační systém podle § 56a zákona o základních registrech a jeho správcem je Ministerstvo vnitra. Na základě znění zákona zavedení jakékoli osoby do tohoto autentizačního informačního systému vyžaduje její jednoznačné ztotožnění oproti základnímu registru obyvatel. Ministerstvo dále spravuje prostředky pro autentizaci, které vydává.

V rámci současného stavu (As-Is 2018) předpokládá co nejširší používání autentizačního informačního systému JIP/KAAS pro splnění zásadních podmínek pro identifikaci a autentizaci interních uživatelů informačních systémů veřejné správy. **Pro ty informační systémy, kde interní uživatelé informačního systému jsou zaváděni úřady, které nejsou správci tohoto informačního systému, je použití autentizačního informačního systému JIP/KAAS povinností.**

V rámci budoucího stavu (To-Be 2020) bude využití systému JIP/KAAS možné pouze v případě, že se stane jedním z poskytovatelů identity v rámci NIA (minimálně v úrovni značná) nebo se sám stane kvalifikovaným systém dle zákona 250/2017 Sb. Pokud nenastane ani jedna z podmínek výše, je potřeba zajistit identitní prostor úředníků jiným způsobem, například:

- Sekce pro státní službu na MV zajistí jednotný prostředek identity úředníka v rámci NIA.
- Jiný orgán veřejné moci zajistí vydávání profesních identit v rámci NIA z nichž požadavky na úřední

identitu (včetně zajištění finančních prostředků) sdělí Sekce pro státní službu na MV.
- Úředníkům bude uloženo využívat předem vybraný soubor federovaných identit v rámci NIA (například elektronický občanský průkaz).

Agendová mapa výkonu veřejné správy ČR

ke zvážení – spíše jde o celkový Meta-informační systém (Mapu) výkonu VS

Zákon 111/2009 Sb. O základních registrech zavedl jako jeden ze základních registrů Registr práv a povinností. Podle současného zění zákona je RPP zdrojem referenčních údajů o:

- Jednotlivých Orgánech veřejné moci a Soukromoprávních uživatelích údajů s veřejnoprávní působností
- Jednotlivých agendách a OVM v těchto agendách působících v definovaných činnostních rolích
- O právu jednotlivých agend resp. OVM v nich působících využívat údaje ze základních registrů
- O právu jednotlivých agend resp. OVM v nich působících vést údaje o evidovaných subjektech a objektech práva
- O právu jednotlivých agend resp. OVM v nich působících poskytovat jimi vedené údaje jiným agendám
- O právu jednotlivých agend resp. OVM v nich působících čerpat údaje z jiných agend

Pro ISVS podporující jednotlivé agendy tak RPP vytváří základní rámec oprávnění a povinností při sdílení údajů s jinými ISVS prostřednictvím referenčního rozhraní VS – definuje tedy základní pravidla interoperability ISVS v rámci VS ČR.

Z pohledu výkonu VS ČR definuje RPP kromě referenčního výčtu jednotlivých OVM také jejich působnosti v jednotlivých agendách, které definují zákonnou působnost OVM.

Zde ještě podrobněji rozvedeme:

- Věcnou a místní příslušnost
- Přenesená působnost

AIS Působnostní ve skupině systémů RPP, společně s Informačním systémem o ISVS (ISoISVS), Informačním systémem o datových prvcích (ISoDP) a s nově definovanými katalogy životních událostí, rolí subjektů práva, služeb a dalších objektů a katalogy jejich vzájemných vazeb tvoří tzv. Meta-informační systém veřejné správy, tedy systém informací o veřejné správě jako takové.

Úplné elektronické podání (ÚEP)

Tzv. úplné elektronické podání (ÚEP) je možné popsat tak, že klient, fyzická osoba (občan), ale i zástupce právnické osoby, má možnost vyřídit všechnu svou potřebnou agendu životní situace, tj. dosáhnout oprávněných požitků (nároků) nebo splnit povinnosti (závazky) plynoucí mu na základě jeho životní události z jeho změněné situace ve vztahu k veřejné správě, a to prostřednictvím elektronické interakce samoobslužně kdykoli a odkudkoli či asistovaně z kteréhokoli univerzálního kontaktního místa VS, bez nutnosti osobní návštěvy na příslušných úřadech, a následně možnost mít přehled o stavu a vývoji všech svých řešených životních událostí.

Všechny obslužné kanály veřejné správy musí být cílově vzájemně integrovány tak, aby mezi nimi bylo možno libovolně přecházet i v průběhu vyřizování podání a aby všechny informace byly zachovány, přenášely se do nich (mezi nimi).

Elektronické podání klienta vůči veřejné je dle této IKČR považováno za úplné, pokud splňuje všechny v úvodu této IKČR uvedené architektonické principy eGovernmentu, zejména pak:

- Podporuje princip Digital by Default tím, že je navrženo jako vnitřně plně digitální (nikdy se nemusí tisknout nebo osobně řešit), s tím, že ale podporuje asistovanými formami i tzv. elektronicky handicapované.
- Podporuje princip Whole-of -Government tím, že je dostupné rovnocenným způsobem ve všech elektronických kanálech eGovernmentu (samoobslužných i asistovaných), s upřednostněním univerzálních kontaktních míst (CzechPOINT a PO v PVS).
- Podporuje princip Once only tím, že pro předvyplnění formuláře i pro navigaci a volbu služby jsou využity všechny údaje o klientovi, které veřejná správa má a ze zákona je v dané situaci smí použít.
- Podporuje principy Interoperability by Default a Cross-border by default tím, že umožňuje elektronicky obsloužit všechny klienty, rezidenty ČR a EU, pro které je úkon relevantní, a to i vzdáleně ze zahraničí.

Dále ÚEP z hlediska front-office a klientů:

- Má služby agend v rámci ÚEP a jejich IT aplikace navrženy tak, aby služby bylo možno v obslužných kanálech kombinovat pro efektivním řešení životních událostí.
- Využívá jednotný identitní prostor (JIP) klientů a úředníků (JIP/KAAS).
- Umožňuje klientům sledovat průběh vyřizování jejich podání.

Z toho pro byznys, případně následnou aplikační architekturu úřadu plynou následující pravidla a požadavky IKČR:

1. Postupně všechna existující práva a povinnosti ze vztahu k VS budou doprovázena transakční službou (nejenom popisem návodu) v autentizované části portálu veřejné správy (PVS), a to v těch všech případech, kdy elektronická transakční služba bude proveditelná a bude odpovídat oprávněným zájmům klientů a současně i úřadů.
2. Stejnou službu lze získat off-line, pro jednotlivá (elementární, atomická) podání k nároku (právu) nebo závazku (povinnosti), tj. půjde stáhnout předvyplněný formulář na cokoli, off-line vyplnit, zaslat datovou schránkou nebo elektronicky podepsané doručit jakkoli jinak (i mailem, vložením do portálu), případně vložit do elektronické aplikace úřadu.
3. V případě menší četnosti podání stačí jeden z obou kanálů (on-line nebo off-line), musí však umožňovat dobrou (personalizovanou) navigaci ke službě a k jejímu předvyplnění.
4. Stejnou službu lze získat s pomocí služby úředníka na kterémkoli fyzickém kontaktním místě asistovanou formou. Pro typové a jednoduché elementární služby a z nich seskupené konfigurovatelné produkty pro řešení typových životních situací to takto bude možné na Univerzálních asistovaných kontaktních místech, nyní CzechPOINT.
5. Stojíce již mimo front-office eGovernmentu, zůstanou existovat tradiční kanály pro příjem listinných podání osobně, diktátem do protokolu nebo poštou – úřední přepážky a podatelny. Jejich úkolem ale bude obdržené vstupy neprodleně plně digitalizovat (s maximem OCR), aby celé další (následné) zpracování bylo jednotně plně elektronické.
6. Podnikatelé a organizace, mající ze vztahu k VS periodické a velmi informačně objemné povinnosti (jako například KV DPH, hlášení na SSZ a ZP atd.) budou využívat jejich další (a hlavní) kanál obsluhy, tzv. embedded systémy[2)] a A2A integrace jejich back-end a provozních systémů s API z AIS.
7. Nedílnou součástí řady podání je splnění finanční povinnosti (poplatku, daně) – IKČR předpokládá využívání elektronických platebních nástrojů, jejich postupnou centralizaci jako sdílené služby a vysokou míru automatizace návazných operací jakoje párování plateb a aktualizace stavu podání.
8. Elektronické samoobslužné služby pro občany (interakce) i pro organizace (integrace) musí být doplněny interaktivním podpůrným a poradenským kanálem (service-desk, call-me-back, apod.), tedy multikanálovým kontaktním centrem, které bude pomocí hlasu, chatu, SMS, mailu apod. pomáhat řešit situace klientů v samoobslužném webovém rozhraní nebo v integračním kanálu.
9. Služby a prostředky eGovernmentu musí být navrhovány a realizovány tak, aby služby zprostředkované třetími stranami (Service Broker) byly rovnocenným obslužným kanálem veřejné správy a součástí eGovernmentu. Za tím účelem bude třeba přinejmenším efektivně pracovat s elektronickými plnými mocemi a poskytovat služby AIS jako tzv. „otevřená API“ tak, aby je ověření partneři mohli zahrnout do svých nadstavbových aplikací.
10. Pro zajištění obsahu a postupu řešení služeb pro životní situace (události), napříč agendami a resorty, rovnocenně ve všech samoobslužných a asistovaných univerzálních klientských centrech, musí existovat,

nejlépe na MV nebo samostatně jako úřad, silné, kapacitně, znalostně a finančně dobře vybavené **Kompetenční centrum služeb veřejné správy.** To jediné dokáže naplnit služby pro ŽS obsahem napříč resorty, protože resorty samy to z legislativních i jiných důvodů udělat nemohou.

11. Pro individuální přizpůsobení (personalizaci) uživatelských rozhraní se budou využívat klientské profily. Cílově bude mít každý klient jenom jeden, celou veřejnou správou a všemi jejími obslužnými kanály sdílený osobní profil. Tento profil bude obsahovat výčet rolí, které již klient vůči veřejné správě hraje (v kterých agendách) a jaké údaje chce používat v jednotlivých rolí, nebo napříč všemi rolemi. Budou to údaje převzaté z propojeného datového fondu (jeho firmy, rodinní příslušníci, majetek apod.) a údaje doplněné klientem (preferovaný mail a telefon, preferovaný bankovní účet, apod.).

Kontaktní místa a obslužné kanály pro klienty VS

IKČR zdůrazňuje a rozvíjí tzv. Univerzální kontaktní místa. Ta představují obslužné kanály, tj. místa a prostředky, kterými klienti veřejné správy mohou realizovat služby veřejné správy, bez ohledu věcnou a místní příslušnost služby a služebního úřadu, a to jak samoobslužné (Portál občana v PVS), tak asistované (CzechPOINT).

Při rostoucí elektronizaci služeb klientům bude nezbytným dalším univerzálním kontaktním místem také multikanálové (hlas, mail, chat, SMS, ...) kontaktní centrum / Call-centrum, primárně určené na podporu uživatelů samoobslužných elektronických kanálů.

Portály pro externí klienty veřejné správy

Bude dále rozvedeno. Klíčové části:

- federalizace portálů jednotlivých resortů a území propojených jednou identitou občana,
- sdruženo pod Portálem občana,
- informační část a transakční část PVS,
- informuláře, používající identitu občana.

Asistovaná univerzální kontaktní místa - Czech POINT

Ministerstvo vnitra ČR vybudovalo Czech POINT (zkratka pro Český Podací Ověřovací Informační Národní Terminál) s cílem vytvořit univerzální podatelnu, ověřovací místo a informační centrum, kde by bylo možné na jednom místě **získat veškeré údaje**, opisy a výpisy, které jsou vedeny v centrálních veřejných evidencích a registrech, jakož i v centrálních neveřejných evidencích a registrech ke své osobě, věcem a právům.

S cílem vytvořit místo, kde je dále možné **ověřit dokumenty**, listiny, podpisy a také elektronickou podobu dokumentů, **učinit podání ke kterémukoli úřadu** veřejné správy, a konečně získat informace o průběhu řízení ve všech věcech, které stát k jeho osobě vede.

Aktuálně lze na pracovištích Czech POINT lze získat například výpis z katastru nemovitostí, obchodního rejstříku, rejstříku trestů.

Rozhraní **CzechPOINT@home** je určeno pro občany, kteří nechtějí pro výpis z rejstříku chodit na kontaktní místo Czech POINT a mají zřízenu vlastní datovou schránku fyzické osoby. Datová schránka žadatele slouží pro odeslání žádosti a pro doručení vystaveného výpisu z rejstříku nebo jiné odpovědi. Žadatel připravuje žádost o výpis či další podání pomocí webových formulářů CzechPOINT@home.

Výpisy z vybraných (zpoplatněných) rejstříků je možné získat prostřednictvím **e-shopu Czech POINT.**

Elektronické samoobslužné služby CzechPOINT postupně splynou s, respektive budou nahrazeny transakční

částí PVS.

Asistovaná kontaktní místa CzechPOINT budou naopak rozvíjena do té míry, že jejich prostřednictvím bude možné učinit zcela stejný rozsah podání a získat stejný rozsah informací jako v samoobslužném kanálu.

Propojený datový fond

IK ČR zavádí do architektury VS ČR pojem propojeného datového fondu (PPDF). Propojený datový fond je tvořen datovými fondy (zejména datovými kmeny a transakčními daty) jednotlivých ISVS, propojených referenčním rozhraním VS s datovými fondy jiných ISVS pomocí odkazů (referenčních vazeb) na referenční údaje o subjektech práva (fyzických osobách, právnických osobách a OVM) a referenční údaje o objektech práva - územních prvcích, vedených v základních registrech. Pro referenční vazby údajů o fyzických osobách se využívá Agendový identifikátor Fyzické osoby (AIFO), pro referenční vazby právnických osob Identifikační číslo osoby (IČO), pro referenční vazby územních prvků jejich příslušné identifikátory přidělené RUIAN.

Referenční rozhraní VS, pomocí něhož je PPDF zpřístupněn, je tvořeno Informačním systémem základních registrů a sběrnicí eGovernmentu, která je součástí CMS (eGSB).

Cílem rozvoje PPDF je publikovat jeho prostřednictvím nejen referenční údaje ze ZR a autoritativní (ze zákona vedené a spravované) údaje editorů ZR, ale také autoritativní údaje dalších agendových centralizovaně vedených ISVS.

Základními službami PPDF pro ISVS - čtenáře a uživatele údajů v PPDF jsou a budou:

- Ztotožnění (přidělení identifikátoru) subjektu resp. objektu práva v ISVS vedeném
- Výdej propojených údajů o subjektu/objektu práva v rozsahu oprávnění vedených v RPP pro příslušnou agendu podporovanou ISVS
- Notifikace o změnách referenčních a autoritativních údajů pro údaje v ISVS vedené
- Podpora reklamace chybných údajů
- Podpora pseudonymizace údajů o subjektech práva

Pro OVM a subjekty údajů to budou služby:

- Podpora vytváření výstupů z ISVS pro subjekty údajů
- Podpora vytváření autorizovaných výpisů z ISVS
- Podpora reklamace chybných údajů

PPDF je základním předpokladem pro naplnění principu Only Once a eliminace místní příslušnosti.

PPDF se skládá z následujících prvků eGovernmentu:

1. Základní registry (dále také ZR), publikované službami ISZR

Základní registry tvoří Základní registr obyvatel (též ROB), Základní registr osob (též ROS), Základní registr územní identifikace a nemovitostí (též RUIAN), Základní registr práv a povinností (též RPP), registr ORG a informační systém základních registrů (též ISZR).

1. Údaje editorů ZR publikované kompozitními službami ISZR

Kompozitními službami se rozumí služby ISZR, které poskytují údaje vedené v editorských systémech ZR s vazbou na referenční údaje vedené v ZR

1. Autoritativní zdroje publikované na eGSB

ISVS vedoucí evidence údajů ze zákona (autoritativní zdroj) publikují údaje pro potřeby jiných OVS nebo pro

klienty VS prostřednictvím CMS – eGSB.

ISZR a eGSB tvoří referenční rozhraní ve smyslu zákona o ISVS.

Autoritativní údaje veřejné správy

Jedním z principů, které chceme ve veřejné správě naplnit a pro které je projekt **Základní registry 2.0** zcela klíčový, je princip tzv. “autoritativních údajů” ve veřejné správě.

Cílem je, aby klienti veřejné správy nebyli nuceni dokládat skutečnosti, o kterých veřejná správa již ví, či které vznikly dokonce na základě rozhodnutí veřejné správy. Většina skutečností potřebných pro rozhodování veřejné správy je již někde evidována, a to formou údajů v informačních systémech veřejné správy. Tyto údaje mají svůj původ a v řadě případů je již nastavena i zodpovědnost za jejich správu v příslušném AISu (příkladem je oprávnění k řízení motorového vozidla, průkaz osoby se zdravotním postižením, status důchodce, potvrzení o bezdlužnosti apod.). Dále existují skutečnosti, které sice jsou na základě rozhodování veřejné správy, nicméně nejsou dosud vedeny v AIS jako údaje (příkladem je potvrzení o studiu, dohoda o chráněné dílně apod.). Zmapováním údajů v jednotlivých agendách, které probíhá nyní v rámci nových povinností ohlašovatelů vůči RPP je postupně zjištěna základní mapa údajů evidovaných, vyžadovaných a poskytovaných v rámci jednotlivých agend a to, kde a jakým způsobem jsou evidovány a v jakém AIS. Tím, jak již bylo popsáno výše, vznikne základní datová mapa veřejné správy, a je tedy možné ji zanalyzovat a identifikovat ty údaje a skutečnosti, které jsou používány ve více agendách.

Na referenčních údajích vedených v základních registrech (a na údajích vedených o fyzických osobách v systémech typu Evidence obyvatel) jsme si ověřili funkčnost principu, kdy tyto údaje a jejich změny klient nemusí dokládat, ale celá veřejná správa si tyto údaje získává prostřednictvím ISZR a na základě nich pak rozhoduje. Princip autoritativních údajů je pouze rozšířením tohoto funkčního celku i o další údaje.

V souvislosti s autoritativními údaji jsou obecně platné následující aspekty:

- Autoritativním údajem bude jen údaj vedený v AIS a vytvářený rozhodováním v rámci určité agendy veřejné správy.
- Autoritativním údajem bude údaj nebo soubor údajů, který dokládá nějakou skutečnost, jež je důležitou rozhodnou skutečností při rozhodování veřejné správy v rámci agendy či agend.
- U autoritativního údaje bude vždy jasné, jak vznikl, kdo je zodpovědný za jeho zápis, změny a správu, v jakém AIS je veden a jakým způsobem může být změněn či zrušen.
- Poskytovatelem autoritativního údaje bude vždy správce AIS, v němž je autoritativní údaje veden a evidován, a to vždy na základě zákonného zmocnění.
- Autoritativní údaj bude vždy vázán na subjekt práva, či objekt práva.
- Poskytování a využívání autoritativních údajů bude vždy logováno, podobně jako je tomu u údajů ze základních registrů.
- Technické řešení poskytování a využívání autoritativních údajů OVM bude realizováno prostřednictvím eGON service busu, a to vždy mezi jednotlivými AIS.
- Bude umožněno subjektu údajů si pořídit výpis autoritativního údaje jako výpis z informačního systému veřejné správy.

Protože cílem je efektivní a zároveň účelné propojování údajů především za účelem omezování nutnosti klienta dokládat skutečnosti, bude autoritativní údaj moci být orgánem veřejné moci získáván:

1. na základě souhlasu subjektu údajů (jménem subjektu údajů), nebo
2. na základě zákonného zmocnění (z moci úřední)

Na autoritativní údaje se budou vztahovat podobné principy jako na referenční údaje v ZR, a to zejména:

- Princip důvěryhodnosti: OVM bude takovému údaji důvěřovat, pokud se neprokáže opak;
- princip využívání: OVM bude muset takový údaj využít pro svoje rozhodování a nezatěžovat klienta jeho

doložením;
- princip reklamace: OVM, pokud zjistí nesoulad s autoritativním údajem, vznese jeho reklamaci a editor ji vyřídí;
- princip zpochybnění: autoritativní údaj, u nějž vznikne pochybnost, či který bude reklamován, bude vyznačen jako zpochybněný;
- princip notifikace a aktualizace: OVM budou získávat autoritativní údaje i s možností registrace notifikací o změnách, čímž se okamžitě dozví o změně údaje, a to zcela automaticky;
- princip zmocnění: subjekt údajů bude moci určit, které třeba i komerční subjekty mimo veřejnou správu budou získávat automaticky informace o změnách těchto údajů.

Pro vybudování a využívání autoritativních údajů je tedy nezbytné dobudovat potřebnou technickou infrastrukturu a nastavit principy a zajistit jejich dodržování, především pak vybudovat nástroje, s jejichž pomocí budou moci být informační systémy propojovány a autoritativní údaje využívány. K tomu je nezbytné realizovat projekt **Základní registry 2.0**, neboť dobudováním potřebných nástrojů a úpravou stávajících klíčových informačních systémů a jejich služeb bude moci být koncept autoritativních údajů realizován.

Pro rozběhnutí principu autoritativních údajů bude pochopitelně nutno také nastavit legislativní a technický rámec, to bude řešeno až v okamžiku, kdy budeme mít k dispozici potřebné nástroje. Oblast autoritativních údajů jako základní princip se ale již nyní přidává do Národní informační koncepce ČR, počítá s nimi koncept Digitálně přívětivé legislativy apod. Autoritativní údaje dále umožní naplňovat i cíle a zásady již v existujících strategií (kupříkladu “Strategie rozvoje ICT služeb ve veřejné správě”).

Autoritativní údaje se budou mezi jednotlivými informačními systémy předávat referenčním rozhraním. V naprosté většině to bude prostřednictvím EGON service busu, ale ne vždy, pokud již funguje a je využívána jiná cesta, která splní veškeré požadavky.

Obecné příklady

Autoritativní údaje budou vždy údaje vedené v informačním systému veřejné správy. Bude se jednat o údaje, které jsou v ISVS k dispozici a které je ISVS schopen publikovat (především prostřednictvím eGSB, ale nikoliv výhradně) a které jsou vázány na subjekt (tedy osobu) nebo na objekt (předmět evidence).

Příkladem podání autoritativního údaje jsou:

1. Oprávněný subjekt se dotazuje na řidiče
    1. Dotaz na subjekt v ROB - provazba přes AIFO tazatele
    2. Dotaz na autoritativní údaje o subjektu jako řidiči přes eGSB do systémů MD
    3. MD vrátí přes eGSB
2. Oprávněný subjekt se dotazuje na vlastníka a provozovatele vozidla
    1. Subjekt zná identifikátor objektu (SPZ vozidla)
    2. Dotaz přes eGSB na vozidlo podle SPZ a jeho atributy
    3. MD vrátí údaje o vozidle a
        1. údaje o vlastníkovi provázané přes AIFO
        2. údaje o provozovateli provazbou přes AIFO
3. Oprávněný subjekt se dotazuje na vozidla, která vlastní či provozuje subjekt
    1. Má ztotožněný subjekt přes AIFO (ROB) nebo IČ (ROS)
    2. Dotazuje se na vozidla vlastněná či provozovaná subjektem přes eGSB do systémů MD
    3. MD vrátí přes eGSB seznam vozidel s jejich identifikátory (SPZ) a jejich atributy
4. Oprávněný subjekt se dotazuje na to, zda je osoba v evidenci Úřadu práce
    1. Má osobu ztotožněnou v ROB přes AIFO
    2. Dotazuje se přes eGSB do systému JISPSV na MPSV
    3. MPSV/ÚPČR vrací údaje provazbou přes AIFO, nebo
    4. MPSV/ÚPČR vrací přes eGSB informaci, že osoba není v evidenci ÚP
5. Dotaz na děti subjektu
    1. Má ztotožněného rodiče v ROB přes AIFO

    2. Dotazuje se přes eGSB na děti rodiče
    3. MV/ISEO vrací přes eGSB AIFO dětí a případně údaje dětí (nemám vyjasněno)
6. Poskytování údajů pro výběr pokut Celní správou
    1. Subjekt má připravené údaje o udělené pokutě, včetně subjektu pokuty a jeho AIFO či IČ
    2. Oprávněný subjekt předá přes eGSB ticket k výběru uložené pokuty, včetně údajů o subjektu a číslo jednací rozhodnutí
    3. Celní správa si ticket převezme, zaeviduje do svého ISVS a koná
    4. Celní správa přes eGSB vrátí oprávněnému subjektu údaje o výběru pokuty s vazbou v původním ticketu

Potřebné rámcové kroky

Princip autoritativních údajů bude projednáván s orgány veřejné moci na různých úrovních, již dnes je ale jasné, že obecný rámcový další postup by měl být:

1. Zakotvit princip autoritativních údajů jako princip eGovernmentu (bude zakotveno v NIK)
2. Zanalyzovat údaje evidované v agendách podle ohlášení v RPP
3. Zanalyzovat potřeby vycházející ze seznamů rozhodných skutečností úřadů
4. Vydefinovat první skupiny adeptů na autoritativní údaje
5. Připravit obecný legislativní rámec pro využívání autoritativních údajů ve VS (pracuje se na principech legislativy)
6. Projednat a schválit legislativní rámec na obecné úrovni, nebo ověřit legislativou v určitých agendách
7. Dobudovat technickou infrastrukturu pro výměnu autoritativních údajů a jejich správu (projekt ZR2)
8. Vyzkoušet si AU na prvních druzích údajů
9. Postupně roztáhnout na další agendy

Sdílené agendové informační systémy (AIS)

Centrální IS pro agendy v přenesené působnosti

Sdílené agendové informační systémy pro agendy v přenesené působnosti, jako jsou např. Živnostenský rejstřík, Evidence obyvatel, Evidence řidičů a Registr motorových vozidel, budou rozšířeny tak, že pokud je někdo ohlašovatelem agendy s výkonem v přenesené působnosti, **musí** zajistit i centrální agendový informační systém (jeho Middle-Office a agendový portál) s možností integrace na lokální systémy úřadů v území.

Naproti tomu musí obce disponovat pouze odpovídajícím „zařizovacím standardem“ pro připojení na takové systémy a úřadování v nich.

Sdílené IS pro samosprávné agendy

IKČR navrhuje, aby OVS, které musí vybudovat podporovat IT podporu pro samosprávné agendy a mají pro to k dispozici potřebné zázemí (infrastrukturu, kapacity, znalosti), typicky ORP (zejména statutární města a bývalá okresní města) nebo kraje, poskytly tuto podporu v multitenantním režimu malým obcím (1. a 2. typu) ve svém správním území. A to za podmínek daných změnami legislativy, ke kterým bude muset pro plnou realizaci tohoto konceptu dojít.

Stejná forma sdílení je možná mezi těmito úrovněmi samosprávy i v případě spisové služby a provozních systémů, pokud malé obce nevyužijí možnosti sdílení centrálních služeb, budou-li k dispozici.

Cloud

Sdílený informační systém pro spisovou službu

Případně, pokud nebude uveden u elektronického úřadování.

Sdílené provozní informační systémy

Obecně chceme říci, že takové systémy budou přibývat tak, jak bude stát směřovat politicky a legislativně k centrům sdílených služeb pro oblast provozních procesů.

Centrální personální IS

- Informační systém státní služby ISoSS. Bude doplněno.

Centrální finanční plánovací a rozpočetnické IS (ERP)

Integrovaný informační systém Státní pokladny je účinný, transparentní, efektivní a centralizovaný nástroj pro řízení veřejných financí, centralizaci účetních informací státu, konsolidaci vybraných ekonomických ukazatelů za veřejnou správu a komplexní přesné a včasné výkaznictví za celý veřejný sektor v souladu s mezinárodními standardy.

Implementovaný informační systém integruje základní funkční bloky Státní pokladny zaměřené na řízení specifických procesů řízení a kontroly veřejných financí, kterými jsou:

- Rozpočtový informační systém (RISPR a RISRE)
- Centrální účetní systém (CSÚIS)
- Řízení státního dluhu (ŘSD)
- Platební styk (PS)
- Prezentační vrstva - Monitor Státní pokladny (Státní monitor, Krajský monitor a Obecní monitor)

Státní pokladna má před sebou několik možných směrů rozvoje, například integraci na nákupní řešení nebo controlling (nákladové, manažerské účetnictví) veřejné správy.

Monitor Státní pokladny je specializovaný informační portál Ministerstva financí, který umožňuje veřejnosti volný přístup k rozpočtovým a účetním informacím ze všech úrovní státní správy a samosprávy. Prezentované informace pocházejí ze systému Státní pokladny a Centrálního systému účetních informací státu a jsou čtvrtletně aktualizovány. Monitor zahrnuje grafickou webovou část, analytickou část a strojově čitelná zdrojová data.

Centrální registr administrativních budov (CRAB) má vyřešit dosavadní absenci aktuálního celostátního přehledu o administrativních objektech v majetku státu, o jejich obsazenosti a dislokaci státních zaměstnanců. Registr na základě získaných informací umožní maximální využití státních objektů. Ve své činnosti se opírá o Usnesení vlády České republiky ze dne 20. prosince 2012 č. 954 o Centrálním registru administrativních budov.

Informační systém CEDR jako celek je nástrojem zejména pro poskytování, evidenci a kontrolu dotací a pro výkon řady s tím souvisejících agend. Systém se skládá z řady vzájemně provázaných subsystémů, které jsou provozovány na MF- GFŘ, resortech, agenturách a územních orgánech finanční správy.

V informačním systému CEDR jsou shromažďovány údaje o všech dotacích a návratných finančních výpomocích ze státního rozpočtu, státních fondů, státních finančních aktiv a Národního fondu a jejich příjemcích na základě Usnesení vlády č. 584/1997Sb. (subsystém CEDRIII).

- **CEDR - resorty**: Údaje jsou do IS CEDR zaznamenávány buď pomocí subsystému CEDR - **resorty,** který mohou využívat všichni poskytovatelé dotací, nebo prostřednictvím jiných informačních systémů, ve kterých jsou všechny požadované údaje také shromažďovány (např. EDS/SMVS, MSC2007). Předávání údajů do IS CEDR ukládá zákon č. 218/2000 Sb., o rozpočtových pravidlech, §75. Lhůty pro předávání dat a povinné položky stanoví vyhláška č. 296/2005 Sb., o centrální evidenci dotací.
- **CEDR II - Kontrolní útvary FÚ** - Všechny údaje, shromážděné v **IS CEDR III,** jsou předávány do subsystému **CEDR II,** který využívají kontrolní útvary finančních úřadů. CEDR II proto obsahuje i moduly pro podporu evidence kontrol a vymáhání nedoplatků nebo částek, které mají být vráceny v případě zjištění porušení rozpočtové kázně. Informace o výsledcích provedených kontrol jsou na vyžádání zpřístupněny příslušným poskytovatelům dotací.
- **CEDR III - Veřejnost: Veřejné údaje z databáze CEDR** jsou zpřístupněny prostřednictvím subsystému CEDR – web na Internetu MF, který umožňuje i tvorby sestav a výběrů.

ISPROFIN-EDS/SMVS - Informační Systém PROgramového FINancování (ISPROFIN) je manažerský systém pro řízení a kontrolu čerpání položek státního rozpočtu. Dělí se na:

- EDS - Evidenční Dotační Systém eviduje a řídí poskytování návratných finančních výpomocí a dotací ze státního rozpočtu na pořízení nebo technické zhodnocení dlouhodobého hmotného a nehmotného majetku
- SMVS - Správa Majetku ve Vlastnictví Státu řídí poskytování prostředků ze státního rozpočtu na pořízení nebo technické zhodnocení hmotného a nehmotného dlouhodobého majetku státu.

Monit2014+ - Informační systém Monit2014+ je určen k procesnímu i datovému zabezpečení kompletního řízení a administrativních procesů nad projekty dotačních programů ze strukturálních fondů EU v České republice v programovém období 2014 - 2020.

Funkcionalita systému Monit2014+ pokrývá veškeré základní procesy životního cyklu dotačních programů i v rámci nich realizovaných konkrétních projektů.

Monit2014+ je napojen řadou rozhraní na desítky informačních systémů státní správy České republiky i Evropské unie podílejících se na implementaci dotačních programů EU.

Centrální systém práva - eSbírka/eLegislativa

Systém eSbírka se bude dělit na dvě části – na **portál**, kde se budou vyhlašovat závazná elektronická znění právních aktů vyhlašovaných ve Sbírce zákonů a mezinárodních smluv, včetně právně závazných úplných znění, a na **databázi informací o právních aktech**. Ta bude sloužit k pružné práci s aktuálními či minulými úplnými zněními právních předpisů, bude též obsahovat dokumenty související s právními předpisy, jako například výkladová stanoviska jednotlivých úřadů, umožní i vyhlašování závazné listinné podoby právního předpisu v textově zcela identické podobě elektronické. Vedle závazné podoby bude právní předpis v elektronické podobě zpřístupněn i v dalších formátech umožňujících následné využití dat v komerčních i neziskových projektech. Systém bude propojen se systémy Evropské unie EUR-Lex a N-Lex.

Systém eLegislativa představuje moderní nástroje pro tvorbu a projednání právních předpisů. Přináší významné změny do legislativní práce, zejména přípravu změn právních předpisů zápisem změn přímo do jejich úplného znění. Novely právních předpisů budou nově doprovázet jejich právně závazná úplná znění, což usnadní orientaci v častých změnách právního řádu. Zavedení eLegislativy přinese vyšší přehlednost tvorby, zejména projednání právního předpisu, a zároveň snížení počtu chyb v legislativním procesu a celkové zvýšení kvality a transparentnosti legislativního procesu.

Nová technická i legislativní podoba tvorby a publikace práva umožní, aby novely právního předpisu nově

doprovázela jejich právně závazná znění, obsahující aktuální znění předpisu ve znění přijatých změn. To usnadní orientaci v častých změnách právního řádu.

Vyplývat z toho bude povinnost připojit se k tomuto systému a současně zákaz nakupovat komerční databáze právních předpisů (výklady jsou dovoleny).

Centrální systém nákupu a veřejných zakázek

Národní elektronický nástroj (NEN), jako klíčový prvek soustavy Národní infrastruktury pro elektronické zadávání veřejných zakázek (NIPEZ), je komplexní elektronický nástroj pro administraci a zadávání veřejných zakázek a koncesí pro všechny kategorie veřejných zakázek a všechny kategorie zadavatelů, vč. sektorových. NEN podporuje všechny rozsahy elektronizace od evidence zadávacích řízení po plně elektronické postupy.

NEN umožní provázání (elektronickou procesní integraci) na interní systémy zadavatelů i dodavatelů či systémy eGovernmentu v ČR. Plně podpoří plánovací aktivity, neboť často bude využíván pro veřejné zakázky realizované v rámci dlouhodobých investičních projektů.

Pro operace relevantní pro Státní rozpočet musí být NEN integrován jak na lokální rozpočetnictví úřadů, tak zejména na RIS-PR a RIS-RE z IISSP.

Uživatelské rozhraní NEN musí být zařazeno do centrálního Portálu úředníka (PÚ), dostupného pro ty OVS, pro něž by bylo nehospodárné budovat svůj lokání PÚ. Dále musí být uzpůsobeno tak, aby jej ostatní OVS jako jednu z mnoha centrálních služeb mohly řady zařadit do svých lokálních Portálů úředníka (Intranet).

Uživatelé NEN se k němu musí přihlašovat pomocí JIP. To znamená klienti VS (dodavatelé) pomocí NIA a úředníci pomocí JIP/KAAS.

Jednotné obslužné kanály a uživatelská rozhraní úředníků

Ve shodě s cílem a s principy poskytnout úředníkům efektivní navigační a uživatelské prostředí pro elektronické úřadování, pro elektronickou správu zdrojů úřadu a pro zaměstnaneckou samoobsluhu je potřeba výrazně posílit a rozvinou, případně nahradit dosavadní možnosti sdílených služeb Portál úředníka a CzechPOINT@Office.

Portál úředníka

Aktuálně plní tuto roli pouze portál IS o Státní službě (ISoSS), který má dvě části - veřejnou a část pro služební úřady, s přístupem přes JIP/KAAS.

Veřejná část poskytuje 3 funkce:

- Přihlašování na úřednickou zkoušku
- Evidence obsazovaných služebních míst
- Evidence provedených úřednických zkoušek

Portál ISoSS v sekci pro služební úřady umožňuje:

- Vkládání návrhů na systemizaci pracovních míst (a dále také Vlastní kontrola návrhů, Úprava návrhů, Odesílání návrhů do schvalovacího procesu, Možnost vkládání odůvodnění k návrhu, Prohlížení postupu schvalovacího procesu návrhu)

Pro každého úřadníka bude v jeho „kmenovém“ úřadě poskytnuto jednotné univerzální vnitřní navigační prostředí a webové uživatelské pracovní prostředí.

Portál úředníka (PÚ) bude federativní (federalizovaný) obráceným způsobem než PVS. Tj. budou existovat jednotlivé centrální portálové služby (HR, vzdělávání, NEN, IISSP, ...), které budou připojovány do lokálního transakčního PÚ, do něhož by se měl postupně transformovat každý tzv. Intranet úřadu.

Vedlo toho se jeden z centrálních portálů VS, IKČR navrhuje, aby to byl personální portál ISoSS, rozšíří tak, aby pro úřední osoby a zaměstnance úřadů, pro něž je nehospodárné spravovat svůj vlastní PÚ, poskytl službu zprostředkování všech centrálních interních portálů na jednom místě.

Všechny funkce portálu úředníka, přesahující hranice „domovského“ OVS budou dostupné výhradně s využitím JIP/KAAS. Proto musí být i lokální IS dostupné se stejnou identitou nebo musí mít úřad pro Portál úředníka a do něj zařazené IS vybudovaný lokální Single-Sign-On řešení, integrované s JIP/KAAS.

CzechPOINT@Office

Jde o neveřejné pracoviště úřadu, kde úředník samostatně čerpá informace, ověřuje a předkládá podání v rámci k eGovernmentu. Je určeno pro úředníky orgánů veřejné moci, kteří ze zákona přistupují k rejstříkům nebo provádějí autorizovanou konverzi dokumentů z moci úřední. (Např. místo toho, aby občan nebo podnikatel dokládal Výpis z rejstříku trestů, úředník si pořídí nutný doklad pomocí Czech POINT@Office).

Jedná se o pracoviště na libovolném úřadě, s technickým vybavením stejným jako v případě veřejnosti přístupných pracovišť Czech POINT, tzn. standardní počítač s přístupem na internet, webový, formulářový a dokumentový prohlížeč, účet pro používání Czech POINT@Office (přístup pomocí dvojice certifikátů pro autentizaci a podpis žádostí).

Systém Czech POINT poskytuje rozhraní CzechPOINT@office, které je určeno pro orgány veřejné moci. Pomocí formulářů, dostupných v rozhraní CzechPOINT@office, mohou úředníci využívat pro výkon své působnosti. Jedná se zejména o:

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

Do oblasti nástrojů pro úředníky patří také podpora provádění autorizované konverze z moci úřední. K dispozici jsou dvě rozhraní systému CzechPOINT pro tuto úlohu:

- KzMU API 1
- KzMU API 2

CzechPOINT@Office bude postupně konvergovat k Portálu úředníka, splyne s ním nebo bude nahrazen a společně vytvoří jedno efektivní interní obslužné rozhraní.

Sdílené platformy a ICT infrastruktura VS ČR

Národní datová centra

Cílově jsou i NDC nadále nedílnou součástí IKČR, budou se rozvíjet vedle eGC a často dokonce ve stejných prostorách a se stejnými kvalitativními parametry, například bezpečnosti. Jejich role je pro řadu centrálních systémů eGovernmentu nezastupitelná.

Lze předpokládat, že bude společně s požadavky na parametry eGC definován povinný minimální standard pro NDC a že ještě několik resortních DC bude „povýšeno“ na NDC. Současně lze předpokládat, že části některých NSC se zapojí jako významné součásti státní části eGC a budou své služby nabízet vedle přímé dodávky „kmenovým klientům“ - organizacím svého zřizovatele, také volně, komukoli za podmínek eGovernment Cloudu.

Strategický rámec Národního cloud computingu – eGovernment cloud ČR

Cílem vybudování sdílených služeb eGovernment cloudu ČR (dále jen eGC) je významné zvýšení efektivity, flexibility a bezpečnosti a zároveň významné snížení pořizovacích a provozních nákladů provozu ISVS využitím sdílených cloudových služeb. eGC bude provozován jak státními, tak i komerčními provozovateli na základě společných standardů a pravidel.

Informační koncepce ČR zohledňuje základní cíle a koncepty eGC, stanovené usnesením Vlády ČR ve Strategickém rámci Národního cloud computingu (UV1499/16) a rozpracovávané v rámci projektu Příprava vybudování eGovernment cloudu, jehož výstupy dále upřesňovat standardy eGC a pravidla jeho provozu i využívání.

eGovernment cloud nabídne standardizované sdílené služby na úrovních IaaS (výpočetní výkon, datová úložiště, umístění v DC), PaaS (operační systémy, databáze, vývojová prostředí), SaaS (aplikační vrstva) a BPaaS (IT procesy, včetně jejich využití jako podpory k on-premise řešením). Z pohledu čtyřvrstvého modelu jsou služby IaaS a PaaS službami vrstvy IT technologické architektury, služby SaaS jsou službami vrstvy aplikační architektury a služby BPaaS službami vrstvy byznys - výkonu veřejné správy, její IT části.

Služby eGC budou definovány a popsány v centrálně řízeném Katalogu služeb eGC. Provozovatelé služeb eGC musí splňovat centrálně stanovované bezpečnostní a provozní podmínky. Splnění podmínek bude ověřováno atestačními středisky.

eGC bude poskytován jak formou centrálně řízeného nákupu služeb komerčních provozovatelů (tzv. komerční část eGC) pro ISVS s nižšími nároky na bezpečnost, tak i formou služeb provozovaných pod kontrolou státu (tzv. státní část eGC) pro služby s nejvyššími nároky na bezpečnost.

Aktuálně probíhající Projekt vybudování eGC analyzuje legislativní podmínky a připravuje definici právního rámce a nákupních procesů komerční i státní části eGC v souladu s platnou legislativou.

Služby eGC budou poskytovány ve čtyřech úrovních bezpečnosti, přičemž úrovně 1-3 budou poskytovány v komerční části eGC a úroveň 4 ve státní části. V rámci vybudování eGC vzniká i metodika hodnocení bezpečnostních dopadů ISVS pro určení příslušné úrovně bezpečnosti eGC.

Pro posouzení ekonomické výhodnosti služeb eGC vzniká metodika hodnocení celkových nákladů (TCO) porovnávající provoz on-premise proti využití služeb eGC.

V první fázi budování eGC bude využívání služeb eGC dobrovolné a zároveň proběhne sběr celkových kapacitních a finančních podkladů pro cílový rozsah eGC. V druhé fázi, po ukončení přípravy a schválení souvisejících legislativních změn, budou pro OSS uplatněny principy „cloud-first“ (povinné umístění ISVS do eGC, pokud dosavadní provoz nesplňuje požadavky bezpečnosti a spolehlivosti nebo když využití eGC je ekonomicky výhodnější než dosavadní provoz, nebo „cloud-only“ (pro systémy s nejvyššími nároky na bezpečnost).

Služby sdílených platforem a infrastruktury

Bude doplněno.

Komunikační infrastruktura

Zákon 365/2000 sb. v aktuálním znění zavedl povinnost publikovat služby ISVS jednotlivým uživatelům prostřednictvím Centálního místa služeb (CMS). V kombinaci s komunikační infrastrukturou veřejné správy zavádí CMS/KIVS pro jednotlivá OVS bezpečnou, od internetu oddělenou komunikační infrastrukturu, poskytující pro jednotlivá OVS:

- Bezpečný a spolehlivý přístup k aplikačním službám jednotlivých ISVS
- Bezpečnou a spolehlivou publikaci aplikačních služeb jednotlivých ISVS všem OVS působícím v daných agendách
- Bezpečný přístup do Internetu
- Bezpečný přístup k poštovním službám v internetu

Cílem je:

- publikovat bezpečným způsobem přes CMS/KIVS všechny aplikační služby centralizovaných ISVS se současným zajištěním bezpečného přístupu jednotlivých OVS k těmto službám při výkonu jejich působnosti.
- Umožnit bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě internet
- Zabezpečit bezpečné síťové prostředí pro zajištění interoperability v rámci EU

Centrální místo služeb (CMS)

CMS je systém, jehož primárním účelem je **zprostředkovávat řízené a evidované propojení informačních systémů subjektů státní správy ke službám** (aplikacím), které poskytují informační systémy jiných subjektů státní správy.

CMS jako součást „referenčního rozhraní„ je podrobně definováno zákonem č. 365/2000.

Službou se v tomto kontextu myslí služba nějakého informačního systému státní správy-ISVS (aplikace), který je připojen k CMS skrze KIVS, jedna aplikace službu poskytuje a jiné ji používají (konzumují).

Řešení CMS je z důvodu zajištění vysoké dostupnosti redundantní na úrovni lokalit a uzlů (dva plně vybavené uzly CMS ve dvou různých lokalitách, každý uzel z redundantních komponent, redundantní konektivita uzlů CMS).

Důsledná implementace zásad/principů/architektury CMS pro propojení informačních systémů subjektů státní správy současně účinně eliminuje negativní dopady aktuálních hrozeb a problémů veřejného internetu (výpadky DNS, latence, DoS, ...) na funkčnost ISVS.

Komunikační infrastruktura veřejné správy (KIVS)

Bude doplněno co to je, pro koho to je a jaká je leg. opora

Krajské konektory - ne (jenom) hvězda, ale sněhová vločka. , základní axiom je připojit krajskou síť jednou linkou na CMS.

Lze předpokládat změny, i legislativní, ve vztahu ke krajským sítím, vyplývající z architektonického požadavku,

aby se všechny kraje a jejich koncové body připojovaly k centrálním sdíleným službám eGovernmentu bezpečnými síťovými prostředky (KIVS a CMS), nikoli veřejným internetem.

Univerzální kontaktní místo

Elektronická identita

[1)]

https://joinup.ec.europa.eu/solution/dcat-application-profile-data-portals-europe

[2)]

viz zpráva OECD o rozvoji daňových řešení