Obsah

Způsoby využívání sdílených služeb, funkčních celků a tematických oblastí jednotlivými úřady

Tato kapitola popisuje způsoby využívání sdílených služeb, funkčních celků a tematických oblastí v celé šíři (v celé architektuře) včetně pravidel, návodů a dobrých praktik k jejich zanesení do informační koncepce a architektury úřadu. Jde o jiný přístup k popisu požadavků na využívání systémů a služeb eGovernmentu než v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury, kde se požadavky popisují skrze jednotlivé vrstvy architektury úřadu.

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 "správa dokumentů". Tento celek kromě samotného informačního systému typu elektronická spisová služba a důvěryhodné úložiště obsahuje i procesy a postupy v úřadu (skartační plán, příjem dokumentů atd.), potřebný HW a SW, komunikační propojení, bezpečnostní požadavky, standardy, pravidla a další. To, že se funkční celek popisuje skrze všechny vrstvy architektury ale neznamená, že jsou jeho nedílnou součástí. Například u vrstvy HW a SW vybavení se počítá s tím, že jde o sdílenou platformu, která není přímo součástí funkčního celku, ale využívá její služby.

Skladba této kapitoly odpovídá sdíleným službám, funkčním celkům a tematickým oblastem z části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR:

Tematické oblasti

- **Agendový model veřejné správy**
- **Identifikace klientů veřejné správy**
- **Propojený datový fond - PPDF**
- **Veřejný datový fond ČR - VDF**
- **Evidence subjektů**
- **Prostorová data**
- **Úplné elektronické podání - ÚEP**
- **Integrace informačních systémů**
- **Portály veřejné správy a soukromoprávních uživatelů údajů**
- **Přístupnost informací**
- **Elektronická fakturace - eFaktura**

Sdílené služby a funkční celky

- **Portál občana a portál veřejné správy - PO, PVS**
- **Národní identitní autorita – NIA**
- **Referenční rozhraní veřejné správy - ZR, ISZR, eGSB/ISSS, FAIS**
- **Univerzální kontaktní místo veřejné správy - CzechPOINT**
- **Systém správy dokumentů - eSSL**
- **Systémy a služby spojené s právním řádem a legislativou - eSeL**
- **Elektronické úkony a doručování - Datové schránky**

- **Jednotný identitní prostor veřejné správy – JIP/KAAS**
- **Jednotné obslužné kanály a uživatelská rozhraní úředníků**
- **Sdílené služby INSPIRE**
- **Sdílené agendové IS v přenesené působnosti**
- **Sdílené agendové IS pro samostatnou působnost územních samospráv**
- **Sdílené provozní informační systémy**
- **Sdílené statistické, analytické a výkaznické systémy**
- **eGovernment Cloud**
- **Národní datová centra**
- **Komunikační infrastruktura veřejné správy- KIVS/CMS**

Pravidla pro Agendový model veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci agendového modelu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k agendovému modelu VS popíše úřad do své informační koncepce.

Základní povinnosti ohlašovatele agendy

Ohlašovatel agendy je podle zákona č. 111/2009 Sb., o základních registrech zodpovědný za řádné ohlášení agendy a za aktualizace agendy, a především za správnost a pravdivost údajů uvedených v agendě. Zjistí-li kdokoliv nesoulad reality s údaji, měl by to jako u dalších referenčních údajů ohlásit ohlašovateli, a ten musí agendu upravit do souladu se skutečností. To se netýká jen základních informací, ale i všech dalších referenčních a nereferenčních údajů, jako jsou činnosti, působnosti OVM, údaje v agendě, agendové informační systémy apod.

Základními povinnostmi ohlašovatele jsou:

- Tam, kde je gestorem legislativy, dodržovat veškeré principy pro legislativu, včetně zásad Digitálně přívětivé legislativy
- Ohlásit agendu
- Ohlásit každou její změnu
- Ohlásit působnost všech OVM a definovat výkon jim svěřených činností
- Zajistit využívání údajů ze základních registrů a související oprávnění pro jejich využívání pro podporu výkonu agendy

- Ohlásit agendové informační systémy, které spravuje a které jsou poskytovány OVM působícím v agendě
- Ohlásit údaje v agendě vedených, čerpaných i poskytovaných
- K centralizovaným agendovým informační systémům vydávat provozní řád
- Metodicky řídit výkon agendy u OVM, který v agendě působí
- Spravovat, tzn. ohlašovat a udržovat aktuální, údaje v rejstříku OVM/SPUU. U SPUU se jedná o všechny subjekty, které jsou povinné dle právních předpisů spadající do agendy, jejichž je OVM ohlašovatel. Ohlašovat může ustanovit jiné OVM, které bude tyto úkony činit.

Základní povinnosti OVM působícího v agendě

V rámci agendy veřejné správy mohou veřejnoprávní činnosti vykonávat pouze ty orgány veřejné moci, které jsou v rámci ohlášení agendy vyznačeny jako orgány veřejné moci vykonávající působnost, a to v rámci konkrétních činností. To znamená, že po aplikaci principu referenčních údajů v Registru práv a povinností lze konstatovat, že pokud v rámci dané agendy vykonává veřejnoprávní činnost orgán veřejné moci, který nemá vyznačenou působnost, jedná se o porušení zákona a ohlašovatel agendy musí neprodleně toto napravit. To se týká nejen samotného seznamu působících orgánů veřejné moci, ale také přiřazení jejich činností. Výkon činnosti je byznysovou vazbou a odborně jej nazýváme "činnostní rolí".

Základními povinnostmi orgánů veřejné moci působících v agendě tedy jsou:

- Vykonávat činnosti dle ohlášení agendy
- Pokud OVM zjistí nesoulad skutečnosti a údajů v ohlášení agendy, je povinen požadovat po ohlašovateli nápravu.
- Pokud sám spravuje agendový informační systém pro výkon agendy (není poskytován centrálně), ohlásit tento systém do RPP jako ISVS.
- Pokud existuje centralizovaný agendový informační systém, tak tento využívat.
- Přistupovat k údajům v základních registrech a dalších ISVS výhradně na základě oprávnění ohlášeného v agendě.
- Spravovat jen ty údaje, které jsou ohlášeny v dané agendě.
- Pokud zjistí nesoulad referenčních údajů v jednotlivých základních registrech se skutečností, zahájit proces reklamace u příslušného editora.

Pravidla pro identifikaci klientů veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci identifikace klientů veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronické identifikaci klientů VS popíše úřad do své informační koncepce.

Fyzická identifikace

Fyzickou identifikací je myšlena situace, kdy klient veřejné správy je osobně přítomen v místě, kde je mu služba poskytována nebo je po něm vyžadována součinnost. K fyzickému prokázání totožnosti se používají identifikační doklady, které musí obsahovat:

- Aktuální a platné údaje o jeho držiteli
- Fotografii držitele

Jako identifikační doklad se používá **občanský průkaz** a **cestovní pas**. Identifikačním dokladem **není** řidičský průkaz, protože nesplňuje potřebné parametry při jeho vydávání, ačkoliv obsahuje například fotografii držitele.

Samotný občanský průkaz, který může sloužit i k elektronické identifikaci, lze použít k fyzické identifikaci na různé úrovni:

- Střední úroveň
  - Zjištění, zda nejde o padělaný občanský průkaz
    - Strojově čitelné občanské průkazy
    - Ostatní občanské průkazy
  - Zjištění, zda je předložený občanský průkaz platný
    - Seznam platných občanských průkazů
    - Seznam neplatných občanských průkazů
  - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
- Vysoká úroveň
  - Zjištění, zda nejde o padělaný občanský průkaz
    - Strojově čitelné občanské průkazy
    - Ostatní občanské průkazy
  - Zjištění, zda je předložený občanský průkaz platný
    - Seznam platných občanských průkazů
    - Seznam neplatných občanských průkazů
  - Kontrola fotografie a údajů na občanském průkaze proti klientovi, který jej předložil
  - Vyžádání si aktuálních údajů, včetně fotografie, o klientovi, který jej předložil a jejich kontrola

Elektronická identifikace

Elektronickou identifikací je myšlena situace, kdy klient veřejné správy není přítomen v místě poskytování služby. Identifikace tedy probíhá vzdáleně, bez fyzického kontaktu.

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy byl vytvořen technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy tuto činnost vykonávat v souladu s Informační koncepcí ČR a bez nutnosti vytváření vlastních 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 neumožňuje.

Podporu celého procesu elektronické identifikace prostřednictvím kvalifikovaného systému elektronické identifikace je vytvořena platforma Národní identitní autority (také jako NIA), 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.

Pravidla pro elektronickou identifikaci tedy primárně obsahuje Národní identitní autorita

Pravidla pro Propojený datový fond

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci propojeného datového fondu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k propojenému datovému fondu popíše úřad do své informační koncepce.

Údaje, dokumenty, výstupy a výpisy

Těžištěm pro správné využívání a pochopení smyslu propojeného datového fondu je porozumění rozdílu mezi **Poskytováním/Využíváním údajů, Poskytováním/Využíváním dokumentů, Výstupům z informačního systému a Výpisem z informačního systému**.

Poskytování / Využívání údajů

Na business vrstvě orgán veřejné moci, který provádí výkon veřejné správy, působí v agendě, kterou má řádně ohlášenou v RPP, má povinnost využívat pro tyto účely aktuální státem garantovaná data ze ZR a dále publikovat a čerpat agendové údaje přes eGon Service Bus / Informační systém sdílené služby. Soukromoprávní subjekt údajů (také jako SPUU) může také za dodržení zákonného zmocnění pro výkon veřejné správy a působení v určité agendě ohlášené OVM, čerpat údaje ze základních

registrů, ovšem výhradně přes AIS OVM nebo formuláře Czech POINT. V zákoně č. 111/2009 Sb. - Zákon o základních registrech, bude nově zakotveno globální zmocnění na čerpání údajů OVM ze ZR, přičemž RPP slouží jako zdroj informací pro informační systém ZR při řízení přístupu uživatelů k údajům v jednotlivých registrech a agendových informačních systémech. To znamená, že kdykoliv se daný subjekt pokusí získat určitý údaj, nebo ho dokonce změnit (editovat), systém posuzuje, zda subjektu bude dovolené na základě zákonného zmocnění pracovat s údaji poskytované veřejnou správou. V RPP jakožto metainformačním systému výkonu veřejné správy jsou uvedeny oprávnění v rámci agend pro čerpání údajů ze ZR, ale také veškeré údaje, které stání správa a samospráva publikuje za pomocí eGon Service Bus / Informační systém sdílené služby napříč veřejnou správou. Důležitým faktorem na business vrstvě v rámci čerpání údajů ze ZR a také publikování a čerpání údajů v rámci jednotlivých AIS OVM je mít řádně hlášenou agendu v RPP, což je nezbytnou podmínkou.

Seznam agend vedených v RPP je k dispozici na stránkách:
https://rpp-ais.egon.gov.cz/gen/agendy-detail/

Na aplikační vrstvě, prostřednictvím webových služeb jednotlivých referenčních rozhraní, ke kterým patří informační systém správy základních registrů, eGon Service Bus / Informační systém sdílené služby, služby Czech POINT a formulářového agendového informačního systému FAIS, má povinnost instituce čerpat referenční údaje ze ZR svými AIS a dále poskytovat a využívat údaje přes IeGon Service Bus / Informační systém sdílené služby napříč veřejnou správou. Dále je možné čerpat referenční údaje ze ZR i přes datové schránky.

Jedním z pravidel získávání referenčních údajů webovými službami je nejdříve ztotožnit svůj datový kmen vůči ZR a následně se přihlásit pro příjem notifikací o změnách. Další možností, ovšem v krajních případech, pokud datový kmen instituce není příliš rozsáhlý, je možné provádět pravidelnou aktualizaci údajů celého datového kmene pro ztotožnění subjektu údajů práva při výkonu veřejné správy.

Dalším pravidlem pro nakládání s osobními údaji je pseudonymizace údajů, což znamená uložení dat technikou oddělení agendových a identifikačních údajů a jejich propojení pomocí agendového identifikátoru fyzických osob (také jako AIFO), aby byly naplněny podmínky bezpečnosti a jednotlivých zákonů a nařízení, které z těchto okolností plynou. Získané AIFO nesmí za žádných okolností opustit AIS, které ho ze služeb ISZR získalo a při jeho předávání (za účelem předávání informací o fyzické osobě) se musí vždy použít služeb ISZR. Více informací o způsobu využití AIFO v rámci pseudonymizace je uvedeno zde.

- Informace ohledně ZR jsou k dispozici na stránkách: http://www.szrcr.cz/vyvojari
- Informace, jakým způsobem připojit svůj AIS nebo komunikační sběrnici do ISZR jsou k dispozici na stránkách: http://www.szrcr.cz/file/170/
- Informace, jakým způsobem využívat notifikace ze ZR je k dispozici na stránkách: http://www.szrcr.cz/spravny-postup-prace-s-notifikacemi-a-udrzovani-datoveho
- Informace k popisu služeb ZR: http://www.szrcr.cz/file/175/display/
- Podrobný popis služeb ZR: http://www.szrcr.cz/vyvojari/podrobny-popis-egon-sluzeb-zakladnich-registru

Z pohledu technologické vrstvy, je čistě na jednotlivé instituci, jakou si zvolí platformu v rámci vnitřního fungování úřadu a připojení se pro využívání služeb propojeného datového fondu, přičemž přistupovat do ZR je možné přes ISZR přímo AISem nebo komunikační sběrnicí.

Na komunikační vrstvě je povinnost instituce při výkonu veřejné správy využívat CMS. CMS je systém, jehož primárním účelem je zprostředkovávat řízené a evidované propojení informačních systémů

subjektů veřejné správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů veřejné 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 (také jako 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.

Poskytování / Využívání dokumentů

Dokumenty se přenáší skrze referenční rozhraní ve vazbě na subjekt či objekt údajů prostřednictvím eGON Service Bus / Informačního systému sdílené služby, nebo také prostřednictvím informačního systému datových schránek. Dokumenty se tvoří výstupem z informačního systému veřejné správy dle zákona č.365/2000 Sb.

Výpisy z informačního systému

Výpis z informačního systému je dokument, který má elektronickou podobu a vytváří se z veřejných evidencí. To znamená, výpis není personifikován pro konkrétní osobu a všechny obsažené informace jsou veřejné. Výpisy se tvoří dle zákona č. 365/2000 Sb.

Výstupy z informačního systému

Výstup z informačního systému je dokument, ať už v elektronické nebo listinné podobě, tvořený pro konkrétní osobu, přičemž obsahuje veřejné i neveřejné informace. Existuje i varianta ověřeného výstupu, která vznikla úplným převodem výstupu z informačního systému veřejné správy z elektronické do listinné podoby a obsahuje náležitosti dle zákona č.365/2000 Sb.

Pravidla pro Veřejný datový fond

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci veřejného datového fondu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k veřejnému datovému fondu popíše úřad do své informační koncepce.

VDF je tvořen otevřenými daty poskytovanými jednotlivými OVS za účelem sdílení s dalšími OVS a je podmnožinou všech otevřených dat VS. Je tedy nutné zajistit, aby všechny funkční celky architektury jednotlivých úřadů VS respektovaly a dodržovaly pravidla platná pro:

- otevřená data (legislativně podpořená zákonem č.106/1999 Sb.),
- data VDF - pravidla pro otevřená data navíc doplněná o další specifika odvozená od charakteristik VDF.

Otevřená data

Otevřená data jsou:

- Volně přístupná na webu jako datové soubory ke stažení ve strojově čitelném a otevřeném formátu - CSV, XML, JSON, RDF (JSON-LD, Turtle, …) a další formáty s otevřenou specifikací.
- Opatřená podmínkami užití neomezujícími jejich užití.
- Evidovaná v Národním katalogu otevřených dat (NKOD) jako datové sady opatřené přímými odkazy na datové soubory, které je tvoří.
- Opatřená úplnou dokumentací.
- Opatřená kontaktem na kurátora pro zpětnou vazbu (chyby, žádost o rozšíření, apod.).
- Jsou publikovány dle otevřených formálních norem ve smyslu § 4b odst. 1 zákona č. 106/1999 Sb. o svobodném přístupu k informacím.

Využívání otevřených dat při výkonu veřejné správy

Nejsou stanovené žádné požadavky na způsoby použití publikovaných otevřených dat, data lze libovolně importovat do vhodných aplikací a informačních systémů. Publikovaná data jsou zpřístupněna prostřednictvím NKOD (POD) a lze je získat jako soubory s datovými sadami. K datům lze také přistupovat s využitím aplikací třetích stran, které příslušné data využívají.

Publikace otevřených dat

Příprava ISVS pro export otevřených dat

Zásadní je zajištění přístupu k datům IS. Provozovaný IS tedy musí:

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

Vhodné otevřené formáty:

- tabulková data - CSV, XML, JSON, RDF (JSON-LD, Turtle, …),
- hierarchická data - XML, JSON, RDF (JSON-LD, Turtle, …),
- grafová data - RDF (JSON-LD, Turtle, …),
- geodata(prostorová data) - GeoJSON, ESRI Shapefile, OGC GML, OGC GeoPackage.

Struktura dat musí být zdokumentována lidsky čitelným dokumentem, ale také strojově čitelným schématem. Doporučené jazyky pro definici schémat schémata:

- CSV - schéma CSV on the Web,
- XML - XML Schema,
- JSON - JSON schema,
- RDF - RDFS, OWL, SHACL

Při dodržení výše uvedených bodů 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 v IS provést, využije se stávající export či API, které již systém nabízí (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.

Závěrečná 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 POD, včetně vyžadovaných standardů.

Data VDF

Otevřená data ve VDF

Ve VDF jsou poskytována otevřená data, která jsou určena mj. k využití jinými OVS při výkonu veřejné správy i mimo jejich rozsah práv a povinností zachycených v RPP. Nad rámec otevřených dat platí pro otevřená data ve VDF následující:

- Pokud OVS využívá data z VDF, považuje je za správná a nemusí ověřovat jejich správnost.
- Poskytovatel dat do VDF garantuje správnost, kvalitu, aktuálnost a pravidelnou aktualizaci údajů publikovaných ve VDF.

- Poskytovatel dat do VDF zajišťuje automatickou notifikaci všech změn v údajích publikovaných ve VDF zaregistrovaným zájemcům s využitím funkcionality Portálu otevřených dat.

Využívání otevřených dat z VDF při výkonu veřejné správy

Při výkonu veřejné správy může OVS potřebovat údaje jiných OVS, kterým ale nemá přístup v rámci rozsahu stanoveného v RPP. Pokud se jedná o veřejné údaje, přistupuje k nim prostřednictvím VDF. Jsou-li data ve VDF dostupná, není žádný jiný způsob přístupu k datům a sdílení dat povolen. Typicky jsou data z VDF využívána následujícím způsobem:

- ruční vyhledání potřebných datových sad v NKOD a zjištění odkazů ke stažení dat,
- nastavení skriptů k pravidelnému importu nalezených datových sad do vlastního IS ze zjištěných odkazů,
- import datových sad do IS VS,
- registrace v Notifikačním hubu k pravidelnému a strojovému získávání aktualizací,
- nastavení skriptů k importu změn získaných z Notifikačního hubu do IS VS.

Publikace otevřených dat do VDF

Pro publikaci otevřených dat do VDF platí stejná pravidla jako pro publikaci otevřených dat uvedená výše. Navíc musí být dodržená následující pravidla:

- Publikovaná data jsou popsána sémantickým slovníkem pojmů, který je vytvořen na základě údajů v RPP. Popis dat sémantickým slovníkem pojmů je vytvořen a publikován dle otevřené formální normy “Popis dat sémantickým slovníkem pojmů”. Sémantický slovník pojmů je tvořen a publikován dle otevřené formální normy “Sémantický slovník pojmů”.
- K identifikaci entit, o nichž jsou publikovány údaje ve VDF, jsou použita IRI dle otevřené formální normy “Propojená data”.
- V publikovaných datech se nepublikují duplicitní údaje s již publikovanými údaji ve VDF. V případě, že OVS publikuje údaje o entitě, o níž již publikuje ve VDF údaje jiný OVS, publikuje OVS pouze nové doplňující údaje k této entitě. V případě, že zavádí vlastní IRI k identifikaci entity než jiný OVS, propojí vlastní IRI s původním dle otevřené formální normy “Propojená data”.
- Souvislosti mezi entitami v datech stejného poskytovatele i různých poskytovatelů jsou reprezentovány dle otevřené formální normy “Propojená data”. Poskytovatel údajů ve VDF se snaží maximálně propojit entity, o nichž publikuje údaje, na entity, o nichž publikují údaje jiné OVS.

Údaje povinně zveřejňované ve VDF

Ve VDF jsou jako otevřená data povinně zveřejňovány následující údaje:

Poskytovatel zveřejňující údaje ve VDF	Zveřejňované údaje	Způsob zveřejnění
Český statistický úřad	Číselníky zavedené sdělením ve Sbírce zákonů	Dle OFN Číselníky

Poskytovatel zveřejňující údaje ve VDF	Zveřejňované údaje	Způsob zveřejnění
Ohlašovatel agendy ve smyslu § 48 písm. f) zákona č. 111/2009 Sb. o základních registrech	Číselníky kódující údaje uvedené v registru práv a povinností dle § 51 odst. 5 písm. h) zákona č. 111/2009 Sb., o základních registrech. Ohlašovatel agendy číselník zveřejňuje ve VDF, pokud již číselník nezveřejňuje Český statistický úřad nebo jiný ohlašovatel.	Dle OFN Číselníky

Společná pravidla pro otevřená data i data VDF

Organizační a procesní zajištění publikace dat

Zapojení VDF do výkonu veřejné správy vyžaduje publikaci skutečně právně závazných, platných a pravidelně aktualizovaných datových sad s jasně definovanou zodpovědností OVS za takové sady. Publikující organizace musí pro splnění uvedených požadavků realizovat vhodná organizační opatření, přiřadit pracovníkům příslušné procesní role a implementovat činnosti publikačních procesů do pracovních náplní pracovníků. Jako minimum je vyžadováno přiřazení těchto klíčových procesních rolí:

Koordinátor otevírání dat, do jehož kompetencí a povinností spadá:

- zajištění součinnosti a kontroly výstupů všech ostatních rolí, které se na otevírání dat podílejí,
- komunikace se všemi zapojenými pracovníky do publikace dat,
- externí komunikace s uživateli otevřených dat VS,
- komunikace a spolupráce s Národním koordinátorem otevřených dat,
- komunikace s Datovou kanceláří a s příslušným Chief data officer (CDO).

Kurátor dat - klíčová role pro:

- zajištění kvality, správnosti, aktuálnosti a tím i právní závaznosti dat konkrétní agendy,
- publikaci datových sad v souladu s platnými právními předpisy ČR a Standardy publikace a katalogizace otevřených dat VS ČR.

Kompletní doporučení, vhodné vzory interních dokumentů, všechny navržené procesní role a standardní publikační procesy jsou uvedeny na Portále otevřených dat.

Ochrana osobních údajů

Pokud jsou předmětem evidence informačního systému osobní údaje ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů a nařízení (EU) č. 2016/679, Obecné nařízení o ochraně osobních údajů (GDPR), neznamená to, že nelze ze systému publikovat otevřená data. V těchto případech platí následující doporučení.

1. V případě, že se jedná o veřejnou evidenci či rejstřík a zvláštní právní předpis nařizuje zveřejnění informací, lze zveřejnit osobní údaje v podobě otevřených dat.
2. Ochranu osobních údajů lze zajistit Anonymizací či Pseudonymizací. 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. V závislosti na charakteru dat je ale nutné zkontrolovat, zda data ve své kombinaci neumožňují identifikaci konkrétní osoby i po odstranění zjevných osobních údajů. Může se jednat o kombinace typu město, věk a pohlaví a podobné.

3. Data, která není možné nebo vhodné zveřejnit dle předchozího bodu, lze zveřejnit v agregované podobě. Tedy v podobě statistik. V případě zveřejnění statistik je ale žádoucí použít co nejjemnější granularitu dat a časové členění.

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. Podrobnější informace o strategických dokumentech, akčních plánech a souvisejících předpisech ČR i EU jsou k dispozici v aktualizované podobě na stránkách Portálu otevřených dat (POD).

Pravidla pro Evidenci subjektů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci agendového modelu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k agendovému modelu VS popíše úřad do své informační koncepce.

Principy pro využívání jednotlivých identifikátorů

Jako identifikátor fyzické osoby (a potažmo i právnické, protože za právnickou osobu vždy jedná fyzická osoba), se v různých agendách používají různé druhy identifikátorů, a to jak pro účely vnitřních procesů a služeb (uvnitř úřadu), tak i při výměně údajů (ven z úřadu). Identifikátory subjektů se využívají při úřední komunikaci a interakci s klientem, při evidenci údajů v příslušných informačních systémech a ve spisové dokumentaci a při výměně údajů s dalšími informačními systémy.

Při evidenci subjektů v datovém kmenu úřadu

Cílem PPDF a pseudonymizace je zavést jednotnou formu identifikace subjektu při jeho evidenci. Nelze nadále využívat dosud zneužívané persistentní identifikátory, ale je naopak nutné rychle se

přizpůsobit povinnostem pseudonymizace. Proto je nutno respektovat níže uvedené základní principy pro evidenci subjektů:

1. Identifikátorem pro komunikaci mezi jednotlivými agendovými informačními systémy je vždy AIFO (AIFO se překládá přes služby ISZR a ISSS).
2. AIFO se nikdy v systému nezobrazí a úředník k němu nesmí mít žádný přístup.
3. Úředním/klientským identifikátorem fyzické osoby nesmí být AIFO, ale vždy klientské číslo pro danou agendu, které přidělí správce dané agendy a které se využívá jako prezentovaný identifikátor v AISu a pro úředníka. Tento identifikátor musí být bezvýznamový, nelze tedy z něj odvodit další osobní údaje fyzické osoby. Agenda přidělující klientský identifikátor musí poskytovat služby pro jeho získání na základě stykového identifikátoru či AIFO a zpět. Současně řídí oprávnění k použití takové služby.
4. Při komunikaci s klientem (osobní jednání na přepážce i zpracování doručených dokumentů a zpráv) se využívají stykové identifikátory, jako jsou typ a číslo dokladu a využije se služba jednorázového překladu na AIFO a služby vydavatele klientského identifikátoru pro získání tohoto identifikátoru.
5. Stykové identifikátory si primárně neeviduji, leda by byly zároveň klientským číslem.
6. AIFO osoby se nikdy nesmí přímo poskytnout, vždy se využívá služeb překladu z mého AIFO na AIFO příjemce výměny údajů.
7. Pokud k tomu nejsou specifické důvody, tak při výměně údajů se vyměňuje pouze AIFO a nepřidávají se další identifikátory nebo údaje.

Služby pro překlad aktuálního stykového identifikátoru musí být poskytovány s úrovní dostupnosti kritická – jedná se o ztotožnění osoby. Vydavatel či správce stykového identifikátoru musí zajistit jeho historickou jednoznačnost a služby zajišťující překlad na AIFO i pro historické hodnoty identifikátoru (pro historické hodnoty je požadovaná úroveň dostupnosti – primární služba).

Při interakci s klientem

Při osobním jednání s klientem nebo při jeho prezenčním ztotožnění se využije typ a číslo dokladu, který klient předložil, nebo jinak ověřený stykový identifikátor.

- Klient předloží doklad s uvedeným identifikátorem, který je stykovým identifikátorem.
- Prostřednictvím daného AIS se zavolá služba jednorázového ztotožnění osoby přeložením stykového identifikátoru na dané AIFO v jeho agendě.
- Dále úředník pracuje v AIS podle AIFO subjektu (které sám na obrazovce nevidí), stykový identifikátor si dále neuchovává. Pokud existuje klientský identifikátor, ten při komunikaci uchovat může.
- Při komunikaci s ostatními AISy a ostatními agendami využije služby svého AISu (kdy AIS prostřednictvím ISSS zajistí výměnu údajů po překladu AIFO).

Při zpracování formulářů pak nastávají tyto tři situace a z nich plynoucí postupy:

1. Elektronický formulář: Formulář musí být vytvořen tak, aby umožňoval již přenos identity klienta, a při jeho zpracování provede AIS dohledání aktuálních údajů podle AIFO subjektů.
2. Listinný formulář: Na listinném formuláři se vyžaduje kombinace údajů křestní jméno, příjmení a typ a číslo dokladu, nebo jiný stykový identifikátor. Při zpracování formuláře se opět v AIS provede zavolání příslušné služby pro jednorázový překlad stykového identifikátoru na AIFO, a tím i ztotožnění subjektu pro daný AIS. V tomto případě se všechny údaje (včetně identifikátorů) pamatují z důvodu nutnosti uchovávání samotného formuláře.

3. Asistované podání: Při asistovaném podání na přepážce příslušný pracovník provede prezenční ztotožnění podle dokladu, a pokud na základě jednání na přepážce bude činit něco jménem subjektu, bude k tomu využívat příslušné služby. Pokud bude pak činit úkon jménem OVM, opět při zápisu do AIS tento AIS zavolá službu jednorázového překladu stykového identifikátoru na AIFO.

Pravidla pro Prostorová data a služby nad prostorovými daty

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k prostorovým datům a službami nad prostorovými daty popíše úřad do své informační koncepce.

Veřejná správa využívá prostorová data ve všech agendách (a jsou jejich nedílnou součástí), které zajišťuje, např. se jedná o agendy v oblastech dopravy, regionálním rozvoji, ochraně životního prostředí, územním plánování, stavební činnosti, zemědělství, lesnictví, při řešení daňových potřeb státu, v oblasti evidence a správy majetku, pro ochranu kulturního dědictví. Prostorová data mají mimořádný význam pro bezpečnost státu, ochranu obyvatelstva, pro předcházení haváriím a živelním pohromám a řešení mimořádných situací. Aktuální, jednotná a rychle dostupná prostorová data jsou nezbytná pro kvalitní operační a krizové řízení na všech úrovních.

Pro zajištění sdílení a efektivního využívání prostorových dat a informací je nezbytné vytvořit odpovídající soustavu zásad, znalostí, institucionálních opatření, technologií, dat a lidských zdrojů, která se označuje jako infrastruktura pro prostorové informace. V řadě zemí je národní infrastruktura pro prostorové informace (NIPI) upravena a definována, v České republice doposud ucelené, přehledné, systematické a formálně zakotvené stanovení NIPI schází, proto byla alespoň stanovena strategie rozvoje této infrastruktury, viz Strategie rozvoje infrastruktury pro prostorové informace v České republice do roku 2020.

Aby bylo možné NIPI efektivně budovat, je kromě centrálních prvků infrastruktury a sdílených služeb, vhodné definovat typovou funkcionalitu (na obecné úrovni) pro informační systém spravující prostorová data jako součást informačních systémů veřejné správy příslušného orgánu veřejné moci. Protože prostorová data a služby jsou pouhým nástrojem pro podporu výkonu agend veřejné správy, ať již na úrovni státní správy, tak i na úrovni samosprávy, je pro stanovení obecného modelu na

úrovni business architektury zásadní definovat klíčové konzumenty poskytovaných služeb ve formě agend a činností (dle terminologie základního registru agend orgánů veřejné moci a některých práv a povinností). Je zřejmé, že business vrstva bude odlišná pro jednotlivé segmenty, nicméně vykazuje určité společné rysy, zejména v řídících, podpůrných a provozních činnostech. Z pohledu podpory tzv. hlavních činností je důležitá vazba na Registr práv a povinností zakládající určité kompetence pro výkon konkrétních agend ve smyslu vazby na legislativu a jednotlivé aktéry (účastníky).

Uplatnění prostorových dat a služeb lze tedy fakticky nalézt ve všech oblastech, typicky, bez ohledu na konkrétní segment, při:

- formulování strategických dokumentů souvisejících zejména s rozvojem území, služeb a segmentů (např. zdravotnictví, školství, sociální služby) či správou zdrojů,
- podpoře výkonu agend veřejné správy související např. s územním plánováním, výstavbou, životním prostředím, dopravou, památkami, lesním hospodářstvím či integrovaným záchranným systémem,
- správě majetku, zejména při evidování, údržbě a opravě, investování (např. budovy, pozemky, komunikace, zeleň, infrastruktura),
- plánování kontrolních činností či řízení rizik v kontextu prostorových souvislostí.

Součástí business architektury je rovněž identifikace klíčových aktérů. Mezi externí lze zařadit veřejnost (fyzické osoby, fyzické osoby podnikající, právnické osoby), odbornou veřejnost, partnery a dodavatelé. Mezi interní patří např. politická reprezentace, vedení OVM, zaměstnanci vykonávající konkrétní agendy a činnosti a také zástupci ICT útvaru jako poskytovatelé ICT (GIS) služeb. Při popisu aplikační architektury je kromě vlastní funkcionality týkající se tvorby a správy prostorových dat potřebné se zaměřit také na sdílení dat nejen uvnitř vlastní organizace, ale také vůči ostatním informačním systémům veřejné správy.

Vlastní funkce systému pro správu prostorových dat tvoří na obecné úrovni zejména:

- tvorba a pořízení dat
- správa prostorových dat
- správa metadat
- transformace dat
- vizualizace
- analýzy
- workflow
- statistiky a reporting
- harmonizace dat INSPIRE
- tiskové úlohy
- opendata
- archiv

Pro publikaci a sdílení jsou klíčové služby vyhledávací služby, prohlížecí, stahovací, transformační a spouštěcí. Z pohledu vnitřního propojení s ostatními prvky ICT infrastruktury organizace jsou zásadní integrace na:

- Agendové informační systémy (např. stavební a územní řízení, státní správa lesů, památková péče), kde GIS pomáhá zejména s vizualizací agendových údajů v mapě, vizualizací souvislostí či trendů, s jejich tematizací.
- Elektronický systém spisové služby včetně spisovny; vztah mezi spisovou službu a digitální spisovnou a GIS není zpravidla realizován, přestože množství vstupů a výstupů z GIS má charakter dokumentu v kontextu zákona č. 499/2004 Sb. a národního standardu (NSESSS). GIS

se v takových případech chová jako samostatná evidence dokumentů, nicméně nerespektuje příslušné legislativní povinnosti. Jedním z možných řešení je realizace vazby právě na spisovou službu.
- Správa majetku a řízení investic, kdy majetek je primárně evidován a spravován v ERP (zpravidla v provázaných modulech evidence a údržby majetku a řízení investic s vazbou na účetní evidenci a rozpočet). Pro správu majetku jsou klíčová data katastru nemovitostí (vedená v ISKN) obsahující jak popisnou, tak i grafickou složku. Tato data ISKN jsou zpravidla v pravidelných intervalech dávkově aktualizována (lze však rovněž využít webových služeb dálkového přístupu katastru nemovitostí ČÚZK), přičemž dochází k často k duplicitní správě dat (včetně pravidelných aktualizací) rovněž v GIS. Optimální je zajistit společnou správu referenčních dat, zajistit jejich sdílení a vzájemnou iteraci na úrovni klientů.

Mezi klíčové, z pohledu vnější integrace na sdílené prvky eGovernmentu, patří:

- Registr územní identifikace, adres a nemovitostí
- Informační systém katastru nemovitostí
- Národní geoportál INSPIRE
- Digitální technická mapa ČR (IS DMVS)
- Informační systém identifikačního čísla stavby

Pravidla pro Úplné elektronické podání

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k úplnému elektronickému podání popíše úřad do své informační koncepce.

Úřad musí respektovat všechny návazné funkční celky jako např. propojený datový fond, portály veřejné správy či komunikační infrastrukturu veřejné správy a procesně zajistit zpracování podání tak, aby probíhalo elektronicky po celou dobu jeho životního cyklu.

Úřad pro splnění požadavků kladených na úplné elektronické podání musí splnit svými obslužnými kanály (např. portál):

- Využití Jednotného identitního prostor veřejné správy pro úřední osoby a Elektronickou identifikaci pro klienty veřejné správy.
- Předvyplnění podání všemi státu známými údaji klientovi po prokázání elektronickou identitou.

Zajištění tohoto požadavku se splní čerpáním údajů z Propojeného datového fondu.

- Má služby svých agend v rámci ÚEP a jejich IT aplikace navrženy tak, aby služby bylo možno v obslužných kanálech kombinovat pro efektivním řešení životních událostí.
- Umožňuje klientům učinit podání skrze různá elektronická rozhraní (webová stránka, formulář nebo asistovaná služba) a sledovat průběh vyřizování jejich podání skrze to samé rozhraní, přes které bylo podání realizované nebo jiné klientem určené.
- Postupně všechna existující práva a povinnosti ze vztahu k VS budou doprovázena transakční službou (nejenom popisem návodu) v Portálu občana, a to v těch všech případech, kdy elektronická transakční služba bude proveditelná a bude odpovídat oprávněným zájmům klientů a současně i úřadů.
- Elektronické podání formou ÚEP lze uskutečnit i papírově (off-line), tzn. půjde stáhnout předvyplněný formulář, ručně vyplnit, zaslat datovou schránkou nebo elektronicky podepsané doručit jakkoli jinak (i mailem, vložením do portálu), případně vložit do elektronické aplikace úřadu.
- 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.
- Stejnou službu lze získat s pomocí služby úředníka na kterémkoli fyzickém kontaktním místě asistovanou formou. Pro typové a jednoduché podání pro řešení typových životních situací to takto bude možné na Univerzálních asistovaných kontaktních místech.
- Zůstanou zachovány 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, aby celé další následné zpracování bylo jednotně plně elektronické.
- Nedílnou součástí řady podání je splnění finanční povinnosti (poplatku, daně). Platební brána tedy musí být součástí obslužného rozhraní. Pro agendy v samostatné působnosti je platební brána plně v zodpovědnosti koncového úřadu, pro agendy v přenesené působnosti musí o způsobu rozhodnout správce agendy.
- Elektronické samoobslužné služby pro klienty/občany i pro právnické osoby musí být doplněny interaktivním podpůrným a poradenským kanálem (service-desk, call-me-back, apod.).
- Podání nemusí vždy činit ta osoba, která je přihlášena elektronickou identitou, ale může se jednat o osobu zastupující jinou osobu. Úřad tedy musí zajisti správu mandátů.
- Pro individuální přizpůsobení uživatelského rozhraní musí úřad využívat tzv. klientské profily. Každý jedinečný a jednoznačně identifikovaný klient má profil jenom jeden. V tomto profilu jsou uchovávány osobní i agendové údaje ve shodě se pravidly správy údajů Právní aspekty pro pseudonymizaci.
- Podání zadané či zpracované v rámci řešení pro ÚeP musí být vždy přijímáno na podatelně a evidováno v systému eSSL nebo samostatné evidenci dokumentů v souladu se zákonem o archivnictví a spisové službě. Jejich přijetí musí být potvrzeno příslušnou odpovědní zprávou.

Pravidla pro Integraci informačních systémů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci úplného elektronického podání je popsán na samostatné stránce zde

nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k integraci informačních systémů popíše úřad do své informační koncepce.

Vnitřní integrace u jednoho správce či v jednom AIS

Integrace mezi informačními systémy jednoho správce je primárně zodpovědností a oblastí onoho správce. To neznamená, že taková integrace nepodléhá splnění EG principů, ale primárně se jí OHA nezabývá, dokud správce ISVS doloží soulad se zde uvedenými principy (jako je evidence subjektů, nebo propojený datový fond).

Technicky je doporučenou optimální metodou vybudovat jednu integrační platformu a integraci mezi jednotlivými informačními systémy zajistit formou služeb volaných a orchestrovaných v této integrační platformě. I při integraci (respektive výměně údajů mezi jednotlivými IS či agendami se musí ale myslet například na řádné logování transakcí a audit zpracování osobních údajů, zejména pokud se jedná o údaje o fyzických či právnických osobách.

Pro vnitřní integraci ale vždy platí následující:

- Jako identifikátor subjektu pro výměnu údajů i ve vnitřní integraci se využije AIFO, pokud se integrace zajišťuje překladem přes eGSB/ISSS.
- Pokud se integrace odehrává jen v perimetru správce, a tedy mimo překlad přes eGSB/ISSS, tak se jako identifikátor využije buď klientské číslo, nebo stykový identifikátor. To platí i v multiagendovém provozu, kdy jsou subjekty integrovány v jedné evidenci jednoho AIS sloužícího pro podporu více agend.
- Identifikátor AIFO se v žádném případě nevyužije při integraci AIS na provozní systémy, pokud tyto systémy nevyužívají AIFO v jejich agendě. V případě integrace subjektů mezi AIS a provozními systémy, které nemají pro subjekt přidělené AIFO v podporované agendě, se využije klientský identifikátor.
- AIFO se neeviduje a neposkytuje ve společných evidencích a v multiagendových AISech, AIFO se v takovém případě využije jen pro vnější integraci a pochopitelně pro ztotožnění a aktualizaci údajů pro konkrétní agendu. Mezi více agendami v jednom ISVS se pro propojení využije klientský identifikátor a AIFA jsou zapsána jen v komponentách AISu pro jednotlivé agendy, nikdy ve společné evidenci. Při vnější integraci pak volá AIS přes společnou evidenci službu eGSB/ISSS či ISZR prostřednictvím svého AIFO.

Vnější integrace na AIS jiného správce

Při vnější integraci se v maximální míře využívá referenční rozhraní, a to zejména eGSB/ISSS jako technický způsob výměny údajů o subjektech a objektech práva. Technická realizace integrace prostřednictvím eGSB/ISSS se řídí příslušnou provozní dokumentací eGSB/ISSS.

Při vnější integraci se využije:

- při výměně údajů o subjektu (fyzická osoba) překlad AIFO identifikátorů, nikdy se nevyužije přímá výměna prostřednictvím jiného identifikátoru,

- při výměně údajů o objektu (třeba vozidlo) jeho identifikátor (třeba RZ), ale je-li součástí i sada údajů o subjektu, pak se u fyzických osob (třeba vlastník vozidla) využije opět překlad AIFO mezi dvěma agendami.

Výměna údajů o subjektech při integraci IS

Jedním z důvodů integrace mezi více AIS je realizace propojeného datového fondu, tedy výměny údajů o subjektech a objektech práva.

Při vnitřní integraci u jednoho správce

Při vnitřní integraci mezi komponentami a systémy jednoho správce se primárně AIFO nevyužívá, protože se využije klientský identifikátor. Pomocí klientského identifikátoru a vazby všech údajů vedených o subjektu ve všech agendách (vždy přes jednotlivý AIS) se dá naplnit povinnost nevyžadovat již jednou vedené údaje a v kombinaci s jednotnou evidencí případů lze snadno zajistit povinnosti poskytnout subjektu údaje z ISVS a mít přehled o údajích, které o něm vedeme a o rozhodných skutečnostech, které se ho týkají.

Pokud se jedná o integraci mezi AIS a provozními informačními systémy, tak provozní IS kromě ESSL nevyužívají AIFO ve svých agendách. I proto je nutno využívat klientský identifikátor, nebo si na úřadě zavést jiný klidně i neveřejný identifikátor, kterým provážeme údaje vedené i v provozních systémech. V žádném případě k tomu nevyužíváme některý z AIFO identifikátorů, kterým bychom nahrazovali vlastní identifikátor v úřadu.

Při vnější integraci s IS jiného správce

Při výměně údajů v rámci propojeného datového fondu se vždy využije mechanismus výměny prostřednictvím překladu agendových identifikátorů (AIFO) přes ORG. Integrace se uskutečňuje prostřednictvím služeb eGSB/ISSS. I v situaci, kdy OVM vede některé další identifikátory o subjektu, vždy postupuje v souladu s § 8, odst. 3, zákona o základních registrech a využije volání služby poskytované agendovým informačním systémem poskytujícím údaje, službu volá přes eGSB/ISSS a volá ji s identifikací subjektu svým AIFO, kdy následně eGSB/ISSS zajistí překlad AIFO, poskytující AIS pak opět přes eGSB/ISSS zašle odpověď, a to zase s přeložených AIFO tazatele. Jiné identifikátory tedy nejsou nutné.

Obě strany integrace pochopitelně všechny transakce logují a samotné eGSB/ISSS uchovává informaci o využití služby.

Chce-li nějaké OVM získat z jiného AISu údaje o subjektu, musí si nejprve daný subjekt ztotožnit a mít k němu přidělené AIFO své agendy. Nezíská-li od poskytovatele údaje třeba proto, že nejsou správně nastavena oprávnění k údajům v RPP, nebo protože poskytovatel nemá řádně ztotožněný subjekt a nemá k němu AIFO, reklamuje to u poskytovatele jako porušení povinností podle zákona o základních registrech. Poskytovatel pak zjedná nápravu.

Pozor: U údajů takto získaných z jiných agend se jedná o údaje, které úřad vede (i když je technicky získal z jiného AIS), a tedy úřad musí postupovat podle paragrafu 6, odst. 2, Správního řádu a po subjektu je nevyžaduje a nepožaduje jejich doložení.

Pravidla pro Portály veřejné správy a soukromoprávních uživatelů údajů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci portálů veřejné správy a soukromoprávních uživatelů údaje je popsán na samostatné stránce zde nebo v rámci části Architektura sdílených služeb veřejné správy.

Využití a popis k přístupu k portálům VS a SPUU popíše úřad do své informační koncepce.

Úřad musí při provozování portálu zavést a změnit současné procesy orientované především na osobní kontakt 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.

Portál podporuje samoobslužného klienta, který obsahuje jak přenesenou, tak samosprávnou působnost a obsahuje popis životních situací, ve kterých se řeší mandáty v elektronické komunikaci. Pokud portál vykonává a podporuje agendu veřejné správy dle registru práv a povinností, musí se chovat jako jakýkoliv jiný agendový informační systém a pracovat dle definice agendy.

Při předávání podání z portálu je tak potřeba mít zajištěnou funkcionalitu, která z podání vytvoří "lidsky čitelné" a "strojově čitelné" informace v rámci jednoho dokumentu, typicky formátu PDF/A3 a vyšší. Tento „kontejnerový“ formát pak slouží jak pro plnění požadavku „čitelnosti“ tak i pro zajištění požadavku na automatizované zpracování dat (vložené XML s údaji pro automatizované zpracování). Dokument musí být dále pak opatřen náležitostmi dle zákona č. 297/2016 Sb., typicky elektronickým podpisem nebo elektronickou pečetí a časovým razítkem. 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 veřejné správy.

Agendový portál

Agendovým 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 informačních systémech veřejné správy
- Musí být federovaný do portálu občana
- Musí dle svého agendového zákona být schopný čerpat a poskytovat údaje skrze systém eGON Service Bus / Informační systém sdílené služby
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb
- Musí využívat stejnou strukturu katalogu služeb a životních situací, jaká je v RPP

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 pro každý úřad jeden - je na něm dostupné vše, v čem má úřad působnost
- Musí být registrovaný jako informační systém veřejné správy v systému o informačních systémech veřejné správy
- Musí být federovaný do portálu občana
- Musí dle svého agendového zákona být schopný čerpat a poskytovat údaje skrze systém eGON Service Bus / Informační systém sdílené služby
- Musí dle svého agendového zákona být schopný čerpat údaje z informačního systému základních registrů
- Musí být ohlášen jako kvalifikovaný poskytovatel služeb
- Musí využívat stejnou strukturu katalogu služeb a životních situací, jaká je v RPP

Portál soukromoprávního uživatele údajů

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

1. 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 na webu České pošty

    - 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.
2. 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.
    - 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 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, může SPUÚ kontaktovat správce Registru práv a povinností (posta@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)
3. 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 žadatel tento typ nemá, je nutné kontaktovat Správu základních registrů skrze datovou schránku napřímo s požadavkem obsahujíc všechny údaje, jako v případě automatizovaného způsobu:
    - IČO subjektu
    - Název kvalifikovaného poskytovatele (SeP)
    - Popis kvalifikovaného poskytovatele
    - URL adresa odkazující na úvodní webové stránk
    - URL adresa pro odeslání požadavků
    - Adresa pro příjem vydaného tokenu (URL)
    - URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu
    - Načtení certifikátu
    - Adresa pro načtení veřejné části šifrovacího certifikátu z metadat (URL). Touto veřejnou částí budou šifrována data v tokenu
    - Logo kvalifikovaného poskytovatele
4. Musí umět přijímat a zpracovávat data pomocí standardů SAML2 nebo WS-Federation

Postup ohlášení portálu jako kvalifikovaného poskytovatele služby

Následující kroky popisují jednotlivé části procesu, který je naznačen níže, na základě ověření přes ISDS. Aktuálně je registrace organizace prostřednictvím portálu národního bodu přístupná pouze pro orgány veřejné moci (OVM), ostatní subjekty musí provést registraci přímo u Správy základních registrů (viz krok 8). Kompletní příručka je dostupná zde.

1. Uživatel jako zástupce organizace požaduje po portálu národního bodu, který je Service Providerem, službu umožňující registraci dané organizace. Tato registrace umožní fungování dané organizace v NIA a vytváření jednotlivých Service Providerů.
2. Portál národního bodu kontaktuje Národní identitní autoritu, která ověření zprostředkovává, s požadavkem na ověření dané osoby (uživatele).
3. 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.

4. Uživatel provede ověření vlastní osoby přihlášením k datovým schránkám. Aby mohl uživatel registrovat organizaci na portálu národního bodu, musí být přihlášen prostřednictvím ISDS (v definované roli a typem schránky OVM). V případě, že organizace není OVM, je potřeba provést registraci u Správy základních registrů.
5. 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.
6. Národní identitní autorita provede sběr atributů v Informačním systému základních registrů (ISZR) na jehož základě následně provede kontrolu existence IČO.
7. Národní identitní autorita předává portálu národního bodu 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.
8. Na základě úspěšného splnění předchozích kroků umožní portál národního bodu uživateli službu registrace organizace (SeP) a zobrazí mu vyplněný formulář pro registraci. Toto platí pouze pro organizace, které jsou OVM. Není-li organizace OVM, jsou místo registračního formuláře zobrazeny podrobné informace o tom, jakým způsobem provést registraci přímo u Správy základních registrů.
9. Uživatel potvrdí správnost údajů a provedení registrace organizace (SeP).
10. Portál národního bodu zpracuje přijatý požadavek na registraci a po úspěšném zaregistrování umožní uživateli provést konfiguraci jednotlivých Service Providerů spadající pod danou organizaci (seznam konfigurací kvalifikovaných poskytovatelů).
11. Uživatel provede konfiguraci Service Providera zahrnující následující údaje:
    - IČO subjektu
    - Název kvalifikovaného poskytovatele
    - Popis kvalifikovaného poskytovatele
    - URL adresa odkazující na úvodní webové stránky kvalifikovaného poskytovatele
    - URL adresa pro odeslání požadavků
    - Adresa pro příjem vydaného tokenu
    - URL adresa, na kterou bude uživatel přesměrován při odhlášení z Vašeho webu
    - Načtení certifikátu
    - Adresa pro načtení veřejné části šifrovacího certifikátu z metadat
    - Zpřístupnění autentizace prostřednictvím brány eIDAS
    - Logo kvalifikovaného poskytovatele

Příklad pro poskytovatele zdravotních služeb

Poskytovatel zdravotních služeb není orgán veřejné moci, a proto je třeba zajistit kromě výše uvedeného postupu i následující kroky:

1. Požádat Ministerstvo zdravotnictví o zavedení do registru práv a povinností jako SPUÚ dle povinností vyplývající ze zákonů č. 250/2017 Sb. a č. 372/2011 Sb., ideálně pod agendou A1086
2. Na adrese https://www.eidentita.cz/Home/Ovm se přihlásit jako oprávněný uživatel datovou schránkou poskytovatele zdravotních služeb
    - Nově by se mělo nabídnout ruční zadání údajů s dalším postupem
    - Pokud se neobjeví, postupovat dle obecných bodů výše – poslání datové zprávy obsahující potřebné údaje (URL, logo….)
3. Upravit si svůj profil na https://www.eidentita.cz/Home/Ovm pro přístup jiných osob (IT oddělení např.) a správu svého profilu, konfigurovat pro Portál pacienta poskytovatele zdravotních služeb.

Pravidla pro Přístupnost informací

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci přístupnosti informací je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k přístupnosti informací popíše úřad do své informační koncepce.

Legislativní rámec pro přístupnost

Legislativní rámec pro povinnosti přístupnosti je poměrně široký. Níže jsou uvedeny pouze klíčové předpisy, které mají přímý vliv na přístupnost informací:

1. Obecná úroveň
    1. Mezinárodní přímo aplikovatelná Úmluva o právech osob se zdravotním postižením
    2. Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací
2. Úroveň základních služeb
    1. Procesně-správní předpisy, jako je Zákon č. 500/2004 Sb., Správní řád, apod.
    2. Zákon č. 155/1998 Sb., o komunikačních systémech neslyšících a hluchoslepých osob
    3. Nařízení EU č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (zejména článek 15)
    4. Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
3. Úroveň internetových stránek a mobilních aplikací
    1. Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací subjektů veřejného sektoru
    2. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (zejména § 5, odst. 2, písm. f), § 9, a další)
    3. Částečně legislativa ohledně spisové služby
4. Úroveň realizace veřejných zakázek
    1. Zákon č. 134/2016 Sb., o zadávání veřejných zakázek (zejména § 93)

Vesměs z legislativy plynou pro OZP následující práva a pro veřejnou správu povinnosti:

1. OZP musí mít možnost využívat všechny služby veřejné správy jako kdokoliv jiný
2. OZP musí mít možnost plnohodnotně využívat elektronické služby stát i elektronické služby subjektů veřejného sektoru
3. Existuje zde obecná absolutní povinnost přístupnosti výsledků všech veřejných zakázek či

zakázek podle legislativy k VZ, pokud jsou jejich výsledky určeny pro jakékoliv užívání fyzickými osobami, to se pochopitelně vztahuje i obecně na veškeré ICT zakázky.
4. Subjekty veřejného sektoru musejí mít svoje informace přístupné a to zejména na internetových stránkách a ve svých aplikacích
5. Přístupnost se vztahuje i na veškeré informační systémy pro zaměstnance, protože ani zaměstnanec s OZP nesmí být diskriminován tím, že není schopen pracovat se svým pracovním systémem

Standardy a metodiky

K dispozici jsou technické standardy a metodiky, které určují konkrétní technické postupy pro tvorbu a správu přístupného obsahu. Nejdůležitějšími v oblasti informačních systémů jsou následující:

- WCAG - Web content accessibility guidelines - Základní standard pro přístupnost obsahu
- WAI-ARIA: Standard Accessible Rich Internet Applications suite - Standard pro webové aplikace
- MAAP - Mobile accessibility applications principles - Soubor opatření pro přístupnost mobilních aplikací (přičemž pro jednotlivé platformy jsou opět k dispozici podrobné standardy)

Více o standardech a jejich realizaci se můžete dočíst třeba v sekci Standardy a normy na portálu pristupnost-informaci.cz

Architektonická řešení

Na obecné úrovni lze konstatovat, že přístupnost A to jak u internetových stránek tak ale třeba i u informačních systémů, je záležitostí dodavatele. Pokud je daná služba informační systém, aplikace, stránka poptávána jako dodávka v rámci veřejné zakázky, pak zde dopadají jednak obecné povinnosti stanovené v legislativě týkající se veřejných zakázek, jednak technické podrobnosti stanovené v legislativě týkající se přístupnosti internetových stránek a mobilních aplikací. Základním architektonickým řešením tedy je zahrnout potřebu přístupnosti a naplnění konkrétních technických norem jako nepřekročitelný požadavek v rámci architektury a v rámci požadavků na dodavatele. Je tedy nutno architektonicky a realizačně zajistit:

- Aby všechny internetové stránky (ať už veřejné či nikoliv) splňovaly požadavky na přístupnost.
- Aby všechny mobilní aplikace splňovaly požadavky na přístupnost.
- Aby všechny aplikace, systémy a informační systémy dodávané v jakékoliv formě veřejného investování také splňovaly požadavky na přístupnost.
- Aby byl elektronický systém spisové služby, agendové informační systémy a další aplikace a procesy nastaveny tak, aby digitální dokumenty odesílané organizací byly přístupné.
- Aby se požadavky na přístupnost staly nedílnou součástí požadavků na dodávky a veřejné zakázky i požadavků na interní vývoj.

Pravidla pro Elektronickou fakturaci

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích

vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci elektronické fakturace je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronické fakturaci popíše úřad do své informační koncepce.

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). Všichni povinní tedy musí kromě procesních změn zajistit i příjem a vydávání elektronických faktur dle evropských a českých pravidel.

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:

- Evropská norma pro elektronickou fakturaci EN 16931-1:2017 - otevřená a zdarma dostupná na této stránce
- Syntaxe dle Evropské směrnice 2014/55/EU čl. 3, odst. 2
- XML zprávu meziodvětvové faktury UN/CEFACT podle XML schémat 16B (SCRDM - CII)
- UBL zprávy faktury a dobropisu podle ISO/IEC 19845:2015

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

- nepředepisuje, která syntaxe by měla být použita pro elektronickou fakturaci v rámci veřejné 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. To je případ českého národního formátu elektronické faktury ISDOC (Information System Document), verze 5.2 a vyšší (který je definován vyhláškou č.194/2009 Sb a který musí být dle Usnesení vlády č. 347/2017 akceptován veřejnoprávními subjekty od 1.1.2019). Tento formát logicky není součástí výše uvedené směrnice, jakkoli je syntaxi UBL 2.1 velmi blízký, jelikož vychází z verze UBL 2.0. V rámci vnitřního trhu České republiky je formát ISDOC velmi široce rozšířen, zejména mezi soukromoprávními subjekty, které ve veřejné zakázce figurují v roli dodavatele, tedy vystavitele faktury.
- neponechává veřejným zadavatelům žádný prostor odmítnout fakturu ve kterékoliv ze syntaxí, 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.

Právní aspekty

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

Pravidla pro Portál občana a Portál veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci portálu občana a portálu veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k portálu občana a portálu veřejné správy popíše úřad do své informační koncepce.

Portál občana i portál veřejné správy jsou centrálně poskytované a provozované portály. Integrovat, či federovat služby úřadu lze přes vlastní řešení v podobě agendových portálů, portálů území či soukromoprávních uživatelů údajů. Integrace je celkem na 3 stupních:

1. Proklik na vlastní řešení s využitím Single Sign-On. Obsahuje pouze vlastní prostor na portálu občana, kde úřad zveřejní svou informační dlaždici, skrze kterou se klient dostane, s využitím principu Single Sign-On a zapojení do národního identitního prostoru, na vlastní řešení
2. Poskytování údajů do vlastního prostoru na portálu občana. Kromě možnosti prokliku na vlastní řešení zapojeného do národního identitního prostoru obsahuje i vždy aktuální údaje o klientovi poskytované skrze propojený datový fond
3. Kompletní vyřešení služby veřejné správy na portálu občana pomocí formulářového řešení se

všemi integracemi v bodech 1 a 2.

Přihlášení k portálu občana

Pro přístup na Portál občana je nutností přihlášení uživatele. Zvolený způsob přihlášení určuje i rozsah služeb, které jsou pro uživatele přístupné. Přihlašovací stránka Portálu občana je dostupná na adrese https://obcan.portal.gov.cz. Přihlášení je možné:

- prostřednictvím kvalifikovaného systému elektronické identifikace (NIA) v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci, a to s využitím občanského průkazu s elektronickou částí (pouze průkazy vydávané od 1. 7. 2018, nevyžadována registrace) nebo s využitím identifikačního prostředku Jméno, heslo a SMS (nutná registrace), příp. s využitím dalších prostředků identifikace.
- prostřednictvím autentizačního rozhraní Informačního systému datových schránek v souladu se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Přihlášení je umožněno pouze těmto typům subjektů – držitelů datových schránek:
  - fyzická osoba (FO)
  - podnikající fyzická osoba (PFO)

Přitom lze využít pouze datové schránky zřízené na žádost, nikoli ze zákona, tedy nikoli ty zřizované automaticky advokátům, statutárním auditorům, daňovým poradcům nebo insolvenčním správcům. Všechny možnosti přihlášení jsou na sobě nezávislé, ale pro plné využití všech služeb Portálu občana je doporučeno použít elektronický občanský průkaz a dále mít připojenou datovou schránku. V obou případech se jedná o přístup se zaručenou identitou v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, jinými slovy o přístup do informačního systému veřejné správy nebo elektronické aplikace s využitím prostředku pro elektronickou identifikaci, při jehož vydání nebo v souvislosti s ním anebo v souvislosti s umožněním jeho využití byla totožnost osoby ověřena státním orgánem, orgánem územního samosprávného celku nebo orgánem veřejné moci, který není státním orgánem ani orgánem územního samosprávného celku, nebo který byl vydán v rámci kvalifikovaného systému elektronické identifikace.

Evidence údajů

Portál občana uchovává perzistentně typově takovéto informace:

- BSI (bezvýznamové směrové identifikátory) – jde o celou sadu identifikátorů, které slouží ke komunikaci s okolními systémy (např. AIFO – ISZR, SePP – NIA atd.). Tyto identifikátory mají význam cizího klíče. Z jejich hodnoty (převážně jde o GUID) nelze přímo vyčíst žádné informace o uživateli. Tyto identifikátory neopouštějí perimetr PO jinak, než při komunikaci s dotčeným systémem.
- Nastavení – jde o informace ovlivňující zobrazené informace na Portálu občana (např. zobrazení dlaždic, nastavení notifikací apod.). Z jejich hodnot nelze přímo vyčíst žádné informace o uživateli.
- Dokumenty – jde o celou řadu „souborů“, které se vytvářejí v Portálu občana a nebo které si uživatel do PO nahrál. Jde například o tisknutelnou formu podání, archiv DZ apod. Tyto dokumenty se ukládají do speciální zabezpečené oblasti, která se „odemyká“ až při přihlášení uživatele. Tyto dokumenty mohou obsahovat i zvláštní kategorie osobních údajů (dříve jako citlivé údaje), ale z pohledu PO jsou „neviditelné“ (Portál občana neprovádí parsování těchto dokumentů).

- Komunikační atributy – v současné době jde o e-mail a telefonní číslo. Komunikační atributy neopouštějí přímo perimetr Portálu občana, ale slouží pouze pro navázání komunikace Portálu občana s uživatelem, resp. zasílání notifikací. Portál občana uživatele notifikuje pouze v případě jeho žádosti ve specifických případech (nastavení).

Transientně přes Portál občana prochází mnoho uživatelských informací. Jejich šíře se nedá přesně specifikovat – záleží, s jakým AIS uživatel prostřednictví Portálu občana komunikuje. Nicméně tyto informace se neukládají (jde pouze o on-line náhledy na informace). Co se týče notifikací změn údajů v základních registrech, proces je spouštěn v definovaných časech (konfigurace Portálu občana), Portál občana zjišťuje na základních registrech změnu přihlášených AIFO. Pokud taková změna proběhla a uživatel si nastavil notifikaci, PO vytvoří zprávu (podle nastavení uživatele) a uloží ji do fronty seznamu zpráv.

Komunikace s dalšími subjekty

Komunikace na úrovni frontend

Komunikací na úrovni frontend je míněno především sdílení společného prostoru kvalifikovaného systému elektronické identifikace (NIA). V tomto prostoru má uživatel možnost procházet přes jednotlivá portálová řešení a využívat tzv. principu „single sign-on“, tj. jednotného přihlášení sdíleného mezi všemi portály či aplikacemi. NIA se řídí ustanoveními zákona č. 250/2017 Sb., o elektronické identifikaci. V návaznosti na výše uvedené slouží tzv. statické dlaždice na Portálu občana pro přechod uživatele mezi Portálem občana a dalšími portály či aplikacemi bez potřeby další autentizace. Portál občany tedy z pohledu funkcionality statických dlaždic slouží jako rozcestník. V současné době si uživatel Portálu občana sám vybírá a aktivuje služby (v podání dlaždic) z katalogu. V dalších fázích rozvoje je uvažováno o nabízení relevantních dlaždic dle jejich obsahu a rolí, ve kterých uživatel bude vystupovat. Aktivní služby v podobě dlaždic jsou uživateli zobrazeny na dashboardu Portálu občana.

Komunikace na úrovni backend

Portál občana standardně napřímo komunikuje s jen omezeným množstvím systémů, a to centrálně sdílených služeb. Konkrétně jde o:

- Informační systém základních registrů prostřednictvím svých vlastních nebo kompozitních služeb,
- Informační systém datových schránek.

Pro komunikaci s ostatními systémy Portál občana výhradně využívá eGon Service Bus / Informační systém sdílené služby.

Komunikace prostřednictvím ISZR

- Čtení ze Základních registrů (ROB, ROS):
  - přístup k údajům v základních registrech probíhá v agendové činnosti (RPP), kterou použije čtenář;
  - činnost musí mít oprávnění na přístup k Základním registrům.

- Čtení přes kompozitní služby (AIS EO):
  - čtení přes kompozitní služby probíhá v agendové činnosti (RPP), kterou použije čtenář;
  - činnost musí mít oprávnění na čtení z AIS.
  - činnost musí mít oprávnění na čtení z ROB podle typu použité služby (ověření AIFO nebo referenčních údajů použitých pro vyhledávání).

Mezi napřímo volané služby patří např. E03 robCtiAifo (čtení referenčních údajů z registru ROB), E22 rosCtiPodleUdaju, E45 orgPrihlasAifo (zaevidování AIFO k notifikaci změn v ROB a ORG pro volající AIS), E98 iszrCtiSouborCiselniku, E106 rppVypisSeznamAgend, E153 iszrZpracujFormular, E181 robVypisSouhlasuPoskytnuti, E199 orgZjistiAis (zjištění kombinací AIFO / Agenda, ve kterých v ORG existuje AIFO odpovídající vstupnímu AIFO) nebo E226 eidentitaCtiAifo (převod bezvýznamového identifikátoru fyzické osoby na odpovídající AIFO AIS).

Komunikace prostřednictvím eGSB/ISSS

Pokud hovoříme o spolupráci přes back-end, je tím míněno napojení Portálu občana na publikační AIS a spolupracovat přes služby, které jsou vystaveny na eGSB/ISSS. Připojení publikačního AIS je z pohledu náročnosti poměrně složité a vyžaduje součinnost ze strany provozovatele eGSB/ISSS. Jeho vstupy jsou nezbytné zejména při definování kontextů (schémat datových zpráv), které jsou sice v kompetenci publikátora, ale pro zachování jednotného formátu přes všechny publikátory, je nutné schválení ze strany provozovatele eGSB/ISSS. Portál občana nekonzumuje veškerá data, která jsou publikována na eGSB/ISSS už i z toho důvodu, že ne vše je určeno pro uživatele – fyzickou osobu. Výběr toho, co a jak zobrazovat na Portálu občana, je tedy výsledkem konkrétní spolupráce gestora publikačního AIS a Portálu občana. Po shodě na rozsahu služeb postupují řešitelé Portálu občana v těchto krocích:

1. vývoj pro čtení dat (čtenářská aplikace),
2. oprávnění pro čtení a získání testovacích dat,
3. testování čtení dat.

Po ověření dostupnosti eGSB/ISSS si Portál občana z katalogu služeb stáhne potřebné WSDL a XSD definice služeb a kontextů pro dostupné publikační AIS. Na základě těchto souborů unikátních pro každý publikační AIS a obecného popisu služeb eGSB/ISSS popsaných v dokumentu „Využití služeb eGSB/ISSS čtenářskými AIS“ si Portál občana vytvoří vlastní klientské rozhraní webových služeb pro čtení dat pomocí eGSB/ISSS.

Pravidla pro Národní identitní autoritu

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Národní identitní autority je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a

tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k Národní identitní autoritě popíše úřad do své informační koncepce.

Úřad musí zajistit identifikaci a autentizaci klientů veřejné správy prostřednictvím kvalifikovaného systému elektronické identifikace (v současnosti pouze NIA) tam, kde ověření totožnosti vyžaduje právní předpis nebo výkon působnosti. Pro využití Národní identitní autority se musí organizace stát tzv. Kvalifikovaným poskytovatelem, dle postupu popsaném u Portálů veřejné správy a soukromoprávních uživatelů údajů.

Zásadním požadavkem bezpečnosti a transparentnosti pro informační systémy veřejné správy je požadavek na jednotnou elektronickou identifikaci 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).

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.

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

1. Každý úřad, který poskytuje své služby elektronicky a potřebuje pro ně ověřeného klienta, musí využít služeb kvalifikovaného systému elektronické identifikace (v současnosti pouze NIA)
2. Každý úřad musí akceptovat nejen identitu českého občana, ale kteréhokoliv občana Evropské Unie dle eIDAS.
3. Při tvorbě identitního prostoru si prvně udělat analýzu, zda nepostačuje již některý z federovaných identit v rámci kvalifikovaného systému elektronické identifikace (v současnosti pouze NIA)
4. Jakýkoliv nový identitní prostor musí být budován tak, aby byl federovaný v rámci kvalifikovaného systému elektronické identifikace (v současnosti pouze NIA)
5. 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
6. Osoba, jíž byly prostředky vydány, nedílně zodpovídá za ochranu těchto prostředků před odcizením a zneužitím
7. Osoba, jíž byly prostředky vydány, nese nedílnou zodpovědnost za všechny úkony, které byly v informačním systému provedeny při použití těchto prostředků
8. 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.

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 dle následující tabulky.

Typ subjektu	Mandát
Fyzická osoba	Jednající sama svým jménem
	Jednající jménem jiné fyzické osoby ze zákona: - rodič dítěte, - manžel/manželka, - registrovaný partner/partnerka, - opatrovník
	Jednající jménem jiné fyzické osoby ze zmocnění: - plná moc, - advokát, - zastupující FO, - jiný druh zmocnění, - na žádost bez zmocnění
Fyzická osoba jednající za právnickou osobu	Jednatel právnické osoby
	statutární zástupce právnické osoby (jedna FO)
	Statutární orgán právnické osoby (více FO)
	Insolvenční správce
	Likvidátor
	Jednající jménem zřizovatele právnické osoby
	Pověřen k jednání za právnickou osobu: - Veřejnoprávním titulem, - 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:

- Nahlížení na údaje subjektů údajů bez jakéhokoliv interaktivního využívání či zapisování údajů (informační účel).
- Přístup k údajům subjektů a jejich reklamace, nebo pokud je přímo umožněna editace klientům veřejné správy (transakční účel).
- Zmocnění k přístupu či využívání údajů subjektu údajů pro třetí strany, nebo poskytnutí údajů z ISVS třetím stranám (zmocňovací účel).
- Činění podání a úkonů vůči orgánům veřejné správy (účel úkonu).
- Využívání elektronických klientských služeb jako je objednání se k úředníkovi.
- Zápis, úprava a zrušení mandátu.

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:

- Zákon 365/2000 Sb., o informačních systémech veřejné správy. Systém klasifikovaný jako Informační systém veřejné správy (ISVS) využívající referenční rozhraní veřejné správy.
- Zákon 111/2009 Sb., o základních registrech. Systém klasifikovaný jako agendový informační systém (AIS) využívající údaje základních registrů a editorů základních registrů dle svého agendového zákona.
- Zákon 250/2014 Sb., o elektronické identifikaci. Systém, který vyžaduje ověření totožnosti
- Nařízení eIDAS

Více o využívání údajů propojeného datového fondu a infrastruktuře referenčního rozhraní je napsáno v kapitolách:

- eGON Service Bus/Informační systém sdílené služby
- Centrální místo služeb
- Propojenný datový fond

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

- eGON služba rosCtiPodleUdaju, rosCtiIco, rosCtiAifo (základní registr osob)
  - pro zajištění ověření, zda je fyzická osoba statutárním zástupcem
- eGON služba aiseoCtiPodleUdaju, aiseoCtiAifo (agendový informační systém evidence obyvatel)
  - pro zajištění ověření, zda je fyzická osoba rodič nezletilého, který není svéprávný
  - pro zajištění ověření, zda je fyzická osoba zákonným zástupcem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba opatrovníkem jiné fyzické osoby
  - pro zajištění ověření, zda je fyzická osoba manžel/manželka
- eGON služba isknCtiVlastniky (informační systém katastru nemovitostí)
  - pro zajištění ověření, zda je fyzická osoba vlastníkem nemovitosti
- Služba ISDS
  - 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:

- Zřídit buď v jednotlivých agendových informačních systémech, nebo v rámci centralizované správy subjektů mandátní registr.
- V rámci mandátního registru určit předem definované typy mandátů přípustné v dané agendě a způsob zápisu mandátů pro nahlížení a pro transakce ze strany klienta
- Povolit zapisovat všem klientům mandáty dle definovaných typů pod svou zaručenou elektronickou identitou.
- Umožnit klientům přidat mandát i offline, například na přepážce úřadu.
- Při každém přihlášení klienta kontrolovat kromě mandátů z centrálních sdílených služeb eGovernmentu i vlastní mandátní registr a dát vždy při přihlášení vybrat klientovi, v jaké roli a s jakým mandátem chce pracovat.

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

- využívá a buduje centrální evidenci subjektů,
- centrální evidenci rozhodných skutečností,
- skutečnosti o zapsaném anebo z něčeho plynoucím mandátu k zastupování,
- 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.

Pravidla pro Referenční rozhraní

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Národní identitní autority je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k Referenčnímu rozhraní popíše úřad do své informační koncepce.

Způsob získání referenčních údajů

Webové služby

Prostřednictvím webových služeb může subjekt čerpat referenční údaje ze ZR. Subjekt, který působí v agendě, má tuto agendu řádně ohlášenou v RPP, má zaregistrovaný svůj agendový informační systém (také jako AIS) a vydaný platný certifikát od správy základních registrů (také jako SZR), přičemž na čerpání údajů musí mít vlastní zákonné zmocnění ve svém zákoně a dle zákona č.111/2009 Sb., o základních registrech, je tento subjekt oprávněn čerpat referenční údaje ze ZR prostřednictvím vnějších služeb informačního systému správy základních registrů (také jako ISZR).

Pro získávání referenčních údajů webovými službami je nezbytné nejdříve ztotožnit svůj datový kmen vůči ZR a následně se přihlásit pro příjem notifikací o změnách.

- Informace ohledně ZR jsou na stránkách: http://www.szrcr.cz/vyvojari
- Informace, jakým způsobem připojit svůj AIS do ISZR: http://www.szrcr.cz/file/170/

- Informace, jakým způsobem využívat notifikace ze ZR je k nalezení zde: http://www.szrcr.cz/spravny-postup-prace-s-notifikacemi-a-udrzovani-datoveho
- Informace k popisu služeb ZR: http://www.szrcr.cz/file/175/display/
- Podrobný popis služeb ZR: http://www.szrcr.cz/vyvojari/podrobny-popis-egon-sluzeb-zakladnich-registru

Czech POINT

Zkratka Czech POINT znamená Český Podací Ověřovací a Informační Národní Terminál. Jde o kontaktní místo veřejné správy, které poskytuje občanům zejména ověřené údaje vedené v centrálních registrech, jako jsou rejstřík trestů, obchodní rejstřík nebo registr živnostenského podnikání. Kromě standardních služeb, lze využít výpisy ze základních registrů podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Občané tak mají možnost ověřit si údaje, které jsou o nich v registrech vedeny, úředníci pak mají prostřednictvím formulářů v části CzechPOINT@office přístup k referenčním údajům ze základních registrů.

Jedním z cílů zavádění je zrychlit, zpřístupnit a zefektivnit služby občanům a dalším subjektům. Czech POINT je tedy kontaktním místem veřejné správy, které umožňuje na jediném místě získávat výpisy nebo činit podání.

- Informace k Czech POINT naleznete na http://www.czechpoint.cz/public/

Informační systém datových schránek

Pomocí datových schránek je možné zasílat dokumenty v elektronické podobě orgánům veřejné moci a také je takto od nich přijímat.

Komunikace prostřednictvím datových schránek nahrazuje klasický způsob doručování v listinné podobě, protože zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, zrovnoprávňuje papírovou a elektronickou verzi zasílaného dokumentu. Orgánům veřejné moci a právnickým osobám jsou datové schránky zřízeny automaticky, všem ostatním na základě jejich žádosti. Požádat o výpisy může každý, kdo má zřízenou datovou schránku a je oprávněnou osobou podle § 8 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

- Informace k datovým schránkám naleznete https://www.datoveschranky.info/

Portál občana a portál veřejné správy

Fyzické osoby (občané) mají možnost žádat o výpisy ze základních registrů prostřednictvím datové schránky na svém personalizovaném účtu portálu občana, pokud mají na portálu občana zřízenou datovou schránku a připojenou do svého profilu. Do portálu občana je možné se přihlásit datovou schránkou, jménem – heslem – SMS nebo elektronickou občankou s čipem, vydávanou od 1. 7. 2018.

- Informace o způsobu přihlášení https://obcan.portal.gov.cz/prihlaseni
- Informace o elektronické identitě https://obcan.portal.gov.cz/prihlaseni
- Dále je možné požádat o výpis ze ZR přes portál veřejné správy.
- Odkaz na jednotlivé formuláře k nalezení zde: https://www.portal.gov.cz/obcan/formulare

Kdo může žádat o referenční údaje ze ZR

Webové služby

Subjekt státní správy svým AIS, který má zákonné zmocnění ve svém zákoně využívat referenční údaje ze ZR, působící v řádně ohlášené agendě v registru práv a povinností a má vydaný platný certifikát od správy základních registrů pro přístup do ZR. Dále soukromoprávní subjekt údajů zprostředkovaně přes AIS některého z orgánu veřejné moci, který má opět zákonné zmocnění využívat údaje ze základních registrů v rámci přidělené agendy řádně ohlášené v RPP.

Czechpoint

Na kontaktním místě, dle typu jednotlivých formulářů, které jsou v rámci Czechpoint k dispozici, může žádat fyzická, podnikající fyzická osoba i právnická osoba. Bližší informace, kdo může žádat u jednotlivého typu formuláře je k dispozici v sekci Typy žádostí pro získání referenčních údajů ze ZR.

Informační systém datových schránek

Informační systém datových schránek je prostředek pro získávání referenčních údajů ze základních registrů formou zaslání jednoho z formulářů v sekci Typy žádostí pro získání referenčních údajů ze ZR. Požádat o výpisy může každý, kdo má zřízenou datovou schránku a je oprávněnou osobou podle § 8 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů. Ostatní subjekty si mohou datovou schránku zřídit volitelně.

Portál občana a portál veřejné správy

Žádat o výpis údajů ze základních registrů v rámci portálu občana má možnost podat každá fyzická osoba (občan), která má na svém personalizovaném účtu portálu občana zřízenou datovou schránku připojenou ke svému profilu. V rámci portálu veřejné správy, má možnost podat žádost o získání referenčních údajů ze základních registrů každý subjekt, který je uveden v sekci Typy žádostí pro získání referenčních údajů ze ZR, dle typu žádosti.

Typy žádostí pro získání referenčních údajů ze ZR

Žádost o **výpis údajů z registru obyvatel** – dle § 58 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (fyzická osoba), o kterém jsou údaje vedeny.
- Za subjekt údajů podle § 58 odst. 9 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, může žádat jeho zákonný zástupce.
- Za subjekt údajů může žádat zmocněnec na základě plné moci s úředně ověřeným podpisem zmocnitele.

Žádost o **veřejný výpis údajů z registru osob** – dle § 61 zák. č. 111/2009 Sb., o základních

registrech, ve znění pozdějších předpisů.

- Žádost může podat jakákoliv fyzická osoba (nemusí být subjektem údajů).
- Žádat lze o poskytnutí údajů o jakékoliv podnikající fyzické osobě, právnické osobě nebo orgánu veřejné moci.
- Ve výpisu se objeví všechny údaje jako v neveřejném výpisu (viz níže) kromě osobních údajů osob, které jsou ve vazbě na registr obyvatel.

Žádost o **výpis (neveřejný) údajů z registru osob** – dle § 61 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (podnikající fyzická osoba nebo statutární orgán právnické osoby), o kterém jsou údaje vedeny v registru osob.

Žádost o **záznam o využívání údajů v registru obyvatel** – dle § 14 zák. č.111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (fyzická osoba), o kterém jsou údaje vedeny v registru obyvatel.
- V žádosti subjekt uvede období, za které má být záznam poskytnut.
- Každá fyzická osoba, která má zřízenu datovou schránku, obdrží vždy za uplynulý kalendářní rok bezplatně *Záznam o využívání údajů v registru obyvatel* automaticky do datové schránky, v souladu s § 14 odst. 4 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.
- Informace, jak číst záznam o využívání údajů naleznete v praktické příručce: viz http://www.szrcr.cz/obcan-a-podnikatel

Žádost o **záznam o využívání údajů v registru osob** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Žádost může podat subjekt (podnikající fyzická osoba nebo statutární orgán právnické osoby), o kterém jsou údaje vedeny.
- V žádosti subjekt uvede období, za které má být záznam poskytnut.
- Každá podnikající fyzická a právnická osoba, která má zřízenu datovou schránku, obdrží vždy za uplynulý kalendářní rok bezplatně *Záznam o využívání údajů v registru osob* automaticky do datové schránky, v souladu s § 14 odst. 4 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **změnu údajů při zjištění nesouladu v registru obyvatel** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- O změnu údajů při zjištění nesouladu v registru obyvatel může žádat subjekt údajů (fyzická osoba).
- Na základě žádosti dojde k podání **návrhu** na změnu referenčních údajů vedených o subjektu údajů v registru obyvatel.
- Dojde-li ke změně referenčního údaje, obdrží fyzická osoba, která má zřízenu datovou schránku, bezplatně *Výpis referenčních údajů* automaticky do datové schránky, v souladu s § 14 odst. 5 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **změnu údajů při zjištění nesouladu v registru osob** – dle § 14 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- O změnu údajů při zjištění nesouladu v registru osob může žádat subjekt údajů (podnikající fyzická osoba nebo statutární orgán právnické osoby).

- Na základě žádosti podává žadatel **návrh** na změnu referenčních údajů vedených o osobě v registru osob.
- O změnu údajů při zjištění nesouladu v registru osob může žádat podnikající fyzická osoba nebo statutární orgán právnické osoby.
- Dojde-li ke změně referenčního údaje, obdrží každá podnikající fyzická nebo právnická osoba, která má zřízenu datovou schránku, bezplatně *Výpis referenčních údajů* automaticky do datové schránky, v souladu s § 14 odst. 5 zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Žádost o **poskytnutí údajů z registru obyvatel třetí osobě** – dle § 58a zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Na základě žádosti poskytne subjekt údajů (fyzická osoba) své údaje jiné fyzické nebo právnické osobě.
- Těmto je možné poskytnout všechny nebo vybrané údaje vedené k Vaší osobě v registru obyvatel.
- Orgánu veřejné moci není nutné poskytnout Vaše údaje tímto způsobem, neboť tento má povinnost si referenční údaje zjistit.

Žádost o **odvolání poskytnutí údajů z registru obyvatel třetí osobě** – dle § 58a zák. č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

- Na základě žádosti přestanou být poskytovány Vaše údaje jiné fyzické nebo právnické osobě. Dojde k odvolání Vámi vybraných předchozích souhlasů s poskytnutím údajů třetí osobě učiněných žádostí výše.

Poplatky spojené s žádostmi o výpisy

- **Portál občana a portál veřejné správy** – podání žádostí datovou schránkou využitím formulářů uveřejněných na Portálu občana a portálu veřejné správy a vydání výpisů je **bezplatné**.
- **Czech POINT** – žádosti podané prostřednictvím kontaktního místa veřejné správy Czech POINT jsou zpoplatněny, avšak podání žádostí o změnu referenčních údajů a poskytnutí/odvolání poskytnutí referenčních údajů třetí osobě jsou **bezplatné**.

Povinnost využívat referenční rozhraní

Povinnost využívat referenční rozhraní pro uskutečňování takzvaných "vazeb" mezi jednotlivými informačními systémy veřejné správy ukládá zákon o informačních systémech veřejné správy. Tedy obecně platí, že pro sdílení údajů, výměnu údajů a propojování jednotlivých informačních systémů veřejné správy různých správců, má být primárně využíváno právě referenční rozhraní. U informačních systémů stejného správce toto nemusí platit vždy, pokud se nevyužívá překlad agendových identifikátorů při komunikaci o subjektu údajů vedené v rámci dvou nebo více agend.

Je nutné zdůraznit, že pouze využitím referenčního rozhraní je korektně prováděn překlad AIFO (AIFO jedné osoby v jedné agendě nesmí být poskytnuto jiné agendě). Pouze referenční rozhraní je napojeno na registr ORG a provádí překlad AIFO.

Možnost využívat referenční rozhraní

Mimo povinnost pro správce informačních systémů veřejné správy, je zde i možnost využití referenčního rozhraní, resp. služeb, které poskytuje, i pro jiné subjekty. Konkrétně jde o subjekty typu SPUÚ (Soukromoprávní uživatel údajů) dle zákona 111/2009 Sb., kteří pro využití služeb referenčního rozhraní potřebují zákonné zmocnění.

Užívání referenčního rozhraní při výměně údajů v rámci propojeného datového fondu

Výměna/sdílení údajů mezi jednotlivými informačními systémy veřejné správy se realizuje výhradně prostřednictvím referenčního rozhraní, a to konkrétně komponenty eGSB/ISSS. Jak se upřesňuje v části propojený datový fond, tak výměna údajů se realizuje vždy v rámci kontextu na subjekt práva.

Přístup ke službám referenčního rozhraní je na síťové úrovni možný pouze prostřednictvím Centrálního místa služeb (CMS), potažmo komunikační infrastruktury veřejné správy (KIVS), které můžeme nazvat privátní sítí pro výkon veřejné správy na území státu.

Správci agendových informačních systémů musejí realizovat napojení na referenční rozhraní, a to podle příslušných metodických dokumentů a provozních řádů:

- Provozní řád ISZR
- Podmínky pro připojení AIS k ISZR

Užívání referenčního rozhraní pro čerpání referenčních údajů

Správci agendových informačních systém se kromě provozních řádů řídí i dalšími postupy a to především legislativními. Současný stav (rok 2020) stále nutí k zákonnému zmocnění pro využívání referenčních údajů. V

Užívání referenčního rozhraní pro poskytování agendových údajů

Správci agendových informačních systémů poskytujících údaje z daných agend realizují napojení svých AISů na eGSB/ISSS v roli publikátora a kontrolu oprávnění k využívání údajů podle oprávnění v RPP. Pro výměnu údajů vybudují služby svého AIS tak, aby mohly být volány a zprostředkovány eGSB/ISSS.

Užívání referenčního rozhraní pro čerpání agendových údajů

Správci agendových informačních systémů využívajících údaje poskytované jinou agendou realizují volání služeb eGSB/ISSS (nemusí znát konkrétní AIS, požadují údaje od agendy), a to jen tehdy, pokud k tomu mají příslušné oprávnění zapsané u agendy poskytovatele v RPP.

Užívání referenčního rozhraní při zápisu a editace údajů v základních registrech

Editoři referenčních údajů v základních registrech realizují napojení svých editorských agendových informačních systémů na ISZR službami vnějšího rozhraní podle příslušné dokumentace Správy základních registrů a v případech, kdy agendové informační systémy nejsou též samostatnými evidencemi dokumentů, pak napojení těchto systémů na eSSL v rámci vnitřních vazeb. Pro editaci údajů a vyřizování reklamací údajů v základních registrech nevyužívají jiné rozhraní než právě ISZR.

Pravidla pro Univerzální kontaktní místo veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci univerzálního kontaktního místa je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k univerzálním kontaktním místům popíše úřad do své informační koncepce.

Úřad musí při tvorbě a správě svých služeb zohlednit možnost vyřízení služby jak samoobslužně, tak asistovaně. Primární odpovědnost za toto rozhodnutí nese věcný správce služby, což např. u služeb v přenesené působnosti není vždy daný úřad. Může však být dána určitá vlastní zodpovědnost za způsob, jakým je umožněno danou službu v přenesené působnosti vyřídit a pokud tuto možnost věcný správce poskytuje, je úřad povinen zohlednit všechny možnosti vyřízení. Nesmí také nastat situace, kdy služba veřejné správy, která je publikována pro samoobsluhu klienta nebude obsahovat všechny možnosti vyřízení, které má k dispozici v asistované formě.

Samoobslužná univerzální kontaktní místa

Aby se plně podporovala samoobsluha služby veřejné správy, musí splnit následující podmínky:

- Poskytování samoobslužných služeb pro klienta pod zaručenou elektronickou identitou
  - Všechny publikované samoobslužné služby jednotlivých úřadů musí mít možnost pracovat s klientem, který se prokazuje svoji zaručenou elektronickou identitou. Technicky to znamená soulad s pravidly a principy Národního identitního prostoru
- Federace pod Portál občana
  - Služby musí být federovány pod Portál občana / Portál veřejné správy v souladu s Národním identitním prostorem a plnit pravidla portálů veřejné správy a soukromoprávních uživatelů údajů

- Interaktivní uživatelské rozhraní
  - Formuláře a další služby pro klienta veřejné správy používající zaručenou elektronickou identitu a principy úplného elektronického podání.

Asistovaná univerzální kontaktní místa

Při provozování asistovaných univerzálních kontaktních míst je potřeba zajistit přidělení rolí v CzechPOINT pro pracovníky poskytující jeho služby skrze správce, tzv. lokálního administrátora.

V rámci asistovaných univerzálních kontaktních míst je nutné počítat s neustálým rozvojem a přidáváním služeb, které musí v co největší míře odpovídat těm samoobslužným. Žádná samoobslužná služby nesmí být bez své asistované varianty, která však může být řešena i v rámci úřadu, pokud tak vyžaduje její specifická náročnost (například daňové přiznání).

Pravidla pro Systém správy dokumentů

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci správy dokumentů je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k systémům správy dokumentů popíše úřad do své informační koncepce.

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 je třeba zahrnout do mapy schopností úřadu.

Při zpracování Enterprise architektury úřadu i při zpracování a realizaci jednotlivých architektur, týkajících se ať už agend nebo schopností, nebo jejich 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 (příloh k transakcím) a s 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 elementy:

- Elektronický systém spisové služby (splňující požadavky Národního standardu) včetně modulů podatelny a výpravny umožňující příjem a odesílání i digitálních dokumentů správnými komunikačními kanály
- Jmenný rejstřík (může být i samostatnou komponentou), nejlépe integrovaný na rejstřík kmenových dat klientů úřadu, notifikovaný ze základních registrů.
- Spisovna pro uchování uzavřených spisů a vyřízených digitálních dokumentů po dobu skartační lhůty
- Rozhraní ESSL zajišťující úkony spojené s dokumenty a procesy evidence dokumentů a správy jejich metadat v ESSL formou aplikačních služeb pro další informační systémy úřadu (agendové, provozní)
- Informační systémy spravující dokumenty integrované na rozhraní ESSL

Jelikož legislativa obecně počítá s tím, že v rámci úřadu je vždy provozován 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 systémů spravujících dokumenty (pokud nejsou samy samostatnou evidencí dokumentů v elektronické podobě) 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 objektů a jejich metadat řešena v souladu s následujícími pravidly:

1. Digitální dokument, respektive jeho komponenty a datové soubory, jsou uloženy v úložišti digitálních dokumentů, které zajišťuje péči o digitální soubory
2. Metadata o dokumentu jsou spravována evidenčním nástrojem, tedy:
    - Elektronickým systémem spisové služby, nebo
    - informačním systémem, který plní funkci samostatné evidence
3. Se soubory v úložišti jsou oprávněny pracovat:
    - elektronický systém spisové služby, nebo
    - informační systém sloužící jako samostatná evidence, nebo
    - informační systém integrovaný na ESSL prostřednictvím ESSL
4. Ve Jmenném rejstříku se vede evidence údajů o subjektech, jejichž se týkají dokumenty evidované ve spisové službě

Vazby na architekturu 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.

Vazby na architekturu 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.

Souvislosti s architekturou údajů o subjektech

Určení původci jež vykonávají spisovou službu v elektronické podobě musejí podle § 64, odst. 4 až 8, Zákona č. 499/2004 Sb., o archivnictví a spisové službě provozovat jako samostatnou komponentu takzvaný "Jmenný rejstřík", kam zapisují určené minimální údaje o všech subjektech, kterých se týkají jimi evidované dokumenty.

Realizace propojení jmenného rejstříku a ostatních komponent, respektive realizace procesů evidence subjektů je následující:

- V úřadu je u každého ESSL jako logická komponenta i Jmenný rejstřík. Funkce Jmenného rejstříku může za splnění všech dalších podmínek zastávat i zdroj evidence subjektů.
- Do jmenného rejstříku se evidují údaje o všech subjektech kterých se týkají evidované dokumenty a to s využitím AIFO fyzických osob v agendě spisové služby, nikoliv v agendách, ve kterých se o osobách úřaduje. Pro vazby jmenného rejstříku na eSSL a další evidence dokumentů je třeba využívat interní identifikátor, nikoliv AIFO.
- Evidence subjektů ve Jmenném rejstříku a evidence subjektů za účelem úřadování v agendě jsou dvě oddělené věci, proto je nutno dbát na správné postupy, viz související kapitoly k evidenci subjektů a identifikátorům.

Možné způsoby zajištění digitální kontinuity dokumentů

Je velmi důležité pamatovat na problematiku digitální kontinuity a o své elektronické dokumenty se aktivně starat. Veřejnoprávní původci musí zajistit evidenci dokumentů a to buď v systému spisové

služby, nebo v samostatných evidencích dokumentů. Oba výše uvedené způsoby pak musí splňovat požadavky Národního standardu pro elektronické systémy spisové služby v souladu se zákonem č. 499/2004 Sb. Zaměříme-li se na elektronické dokumenty ve smyslu nařízení eIDAS, pak budeme hovořit o elektronickém systému spisové služby a elektronických evidencích dokumentů. Jedním z klíčových požadavků Národního standardu je existence tzv. transakčního protokolu – zápisu provedených operací uskutečněných v rámci elektronického systému spisové služby nebo v rámci samostatné evidence dokumentů v elektronické podobě. Transakční protokol v případě elektronických dokumentů zajišťuje, že od okamžiku zaevidování dokumentu až do okamžiku jeho předání do archivu nebo okamžiku vyřazení a zničení je systematicky evidována jakákoliv operace týkající se evidovaného dokumentu. Tímto je zcela jednoznačně po dobu životního cyklu dokumentu zajištěno, že lze v rámci evidenčního systému garantovat určité vlastnosti elektronického dokumentu, zejména pak věrohodnost původu a neporušenost obsahu. U každého elektronického dokumentu musí být rovněž zajištěna po celou dobu životního cyklu jeho čitelnost, a to jak v technickém slova smyslu, tak z pohledu jeho uživatelsky vnímatelné podoby.

U veřejnoprávních původců je s ohledem na výše zmíněný požadavek prokázání věrohodnosti původu a neporušitelnosti obsahu dokumentu stanovena zákonná povinnost ověřování elektronických podpisů, elektronických pečetí a elektronických časových razítek, pokud je příchozí elektronický dokument obsahuje. Uvedení původci jsou ze zákona povinni výsledky ověření zaznamenat ve svých evidenčních systémech, které jak bylo uvedeno výše, musí splňovat zákonem stanovené požadavky, včetně požadavku na vedení transakčního protokolu. Proto není nutné po prvotním ověření u veřejnoprávních původců používat takové metody, jaké se používají běžně pro zajištění „věrohodnosti původu“ u soukromoprávních původců - například není nutné opětovně opatřovat elektronické dokumenty časovými razítky před jejich expirací a podobně - věrohodnost původu elektronických dokumentů je u veřejnoprávních původců zajištěna řádnou systematickou evidencí dokumentů v určených systémech, kde je navíc pomocí transakčního protokolu možné po celou dobu životního cyklu dokumentu prokázat veškeré operace, které se s evidovaným dokumentem uskutečnily - tj. pro prokázání věrohodnosti původu je zcela dostačující systematická evidence a transakční protokol.

Výše uvedené lze u veřejnoprávních původců i snadno ověřit – audit systémů zajišťujících vedení spisové služby je možné realizovat v průběhu času a každý veřejnoprávní původce má zákonem stanovenou povinnost kontroly těchto činností. Elektronické systémy spisové služby, ale i některé významné samostatné evidence dokumentů (typicky agendové informační systémy), splňují z pohledu zákona o kybernetické bezpečnosti charakteristiku tzv. významného informačního systému, neboť v případě jejich výpadku nebo nesprávného fungování by veřejnoprávní původci nemohli plnit řádně a souvisle svůj výkon. S ohledem na to by tyto měly být jako významné informační systémy identifikovány a oznámeny Národnímu úřadu pro kybernetickou a informační společnost procedurou dle kybernetického zákona. Tím se tyto systémy dostanou rovněž pod pravidelný dohled útvarů zajišťujících kybernetickou bezpečnost.

Elektronické systémy spisové služby a samostatné evidence dokumentů též zpracovávají osobní údaje fyzických osob, proto veřejnoprávní původci nad těmito systémy mají s ohledem na povinnosti vyplývající z obecného nařízení na ochranu osobních údajů a ze zákona o zpracování osobních údajů řadu povinností, které též zvyšují celkovou důvěryhodnost systémů, ve kterých veřejnoprávní původci evidují své dokumenty.

Výše uvedenými opatřeními lze u veřejnoprávních původců zcela spolehlivě prokázat věrohodnost původu a to i u přijatých dokumentů obsahující elektronické podpisy, elektronické pečetě a elektronická časová razítka a to bez nutnosti jejich opětovného opatřování časovými razítky nebo jinými autentizačními či autorizačními prvky.

Možné problémy

Možným rizikem zajištění digitální kontinuity založeného na základě transakčních protokolů eSSL je problematika kolizních dokumentů. Jedná se o situaci, kdy je do transakčního protokolu v souladu s NSeSSS poznamenán otisk (tzv. hash) dokumentu spolu s označení použitého hashovacího algoritmu, ovšem stejný hash může odpovídat i jiným dokumentům. Následně není možné, především u přijatých dokumentů, dovodit o jakém dokumentu (skrze jeho hash) transakční protokol pojednává, což výrazně komplikuje případné dosvědčení právní validity.

Pro eliminaci tohoto rizika, lze využít postupy, kterými se prodlužuje ověřitelnost podle standardu ETSI (The European Telecommunications Standards Institute) a který odpovídá předpisům eIDAS. Jde tedy o opakovaného přidávání kvalifikovaných elektronických časových razítek a validačních informací sloužící k prodlužování možnosti ověření platnosti podpisů a pečetí na elektronických dokumentech. Zjednodušeně lze říci, že tato opatření mají charakter nového elektronického podepsání, nového zapečetění či nového opatření kvalifikovaným elektronickým časovým razítkem. Tyto možnosti totiž znamenají, že se na autentizaci původního dokumentu použijí aktuálně dostatečně silné kryptografické postupy a algoritmy (konkrétně dostatečně robustní hashovací funkce a dostatečně velké klíče), a tím je – opět na určitou dobu – dostatečně ztíženo hledání kolizních dokumentů. Vzhledem k různým právním účinkům elektronických podpisů (představujících projev vůle), elektronických pečetí (představujících vyjádření původu) a časových razítek (představujících „fixaci v čase“) se v praxi, k prodloužení možnosti ověření platnosti původních podpisů a pečetí, využívají právě kvalifikovaná elektronická časová razítka. Důležité je, aby každý jednotlivý krok tohoto dlouhodobého procesu byl proveden včas. Tedy aby další časové razítko bylo přidáno ještě dříve, než zaúčinkuje tzv. časová pojistka (než skončí v čase omezená možnost ověření původního podpisu či pečeti). Případně promeškání nejzazšího okamžiku způsobí, že pozdě přidané časové razítko již nemá prodlužující účinek.

V praxi přitom není nutné (včas) přidávat časová razítka k jednotlivým dokumentům. Vhodnými postupy je možné minimalizovat spotřebu časových razítek, například společným umístěním více dokumentů (či pouze jejich otisků) do vhodného kontejneru (ASiC), a časovými razítky opatřovat pouze kontejner jako takový. Sdružování do kontejnerů je vhodné dle logického spojení dokumentů, například do úrovně spisů. Stejně tak není podstatné, kdo podniká výše naznačená opatření, nutná pro zajištění digitální kontinuity dokumentů.

Je však nutné konstatovat, že ač riziko kolizních dokumentů existuje, současné legislativní prostředí nedává veřejnoprávním původcům dostatečný prostor k rozhodnutí a vlastnímu zvážení rizik a dodatečné připojování elektronických pečetí či časových razítek by mohlo být v rozporu s péčí řádného hospodáře, neboť u nákladů na zajištění takového postupu by se mohlo jednat o neúčelně vynaložené prostředky veřejného rozpočtu.

Pravidla pro Systémy a služby spojené s právním řádem a legislativou

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci systémů a služeb spojených s právním řádem a legislativou je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k systémům a službám spojených s právním řádem a legislativou popíše úřad do své informační koncepce.

Míra možnosti a dokonce povinnosti využívat výše zmíněné informační systémy a jejich sdílené služby závisí na tom, v jakém postavení vůči konkrétní legislativě je příslušný úřad.

V tomto případě tedy můžeme rozdělit úřady do třech následujících kategorií:

- Gestor legislativy: Je zodpovědný za přípravu, provádění procesu připomínkování a projednání a následnou realizaci schválené legislativy. Gestor by také měl pravidelně provádět zhodnocení platné legislativy a na základě toho navrhovat její úpravy.
- Spolupracující subjekt: Jedná se o subjekt, který se aktivně podílí na spolutvorbě legislativy a je aktivně zapojen do procesu připomínkování a vyhodnocování daných návrhů
- Uživatel legislativy: Jedná se o subjekt, který se Danou legislativou řídí ať už v rámci veřejnoprávní činnosti jako výkon působnosti v dané agendě, nebo je pro něj příslušná legislativa jinou formou nějak závazná a ovlivňuje jeho činnost

V Každé z těchto třech základních rolí mohou být výše zmíněné informační systémy aktivně používány.

Nesmí se zapomínat ani na povinnosti výkonu spisové služby, ty se pochopitelně vztahují i na procesy návrhu a projednávání legislativy. Jsem-li tedy gestor za legislativu, především si zajistím integraci svých autorských systémů na ESSL a následně i integraci na závazně používané informační systémy (eLegislativa, ODOK, EKLEP, apod.).

Při vyhodnocování a následné přípravě návrhů na změnu jsou dvěma klíčovými zdroji platná legislativa (aktuální znění právních předpisů a jejich vazeb) a dopad na faktický výkon (zdrojem je RPP a agendový model a seznam úkonů v agendě). Pomocí vazeb s ostatními právními předpisy si také úřad zmapuje souvislosti na další schopnosti. Třeba u agendového zákona je třeba zohlednit i povinnosti spisové služby, povinnost nevyžadovat údaje, které již mám, apod. I s ohledem na to je vhodné jako zdroj mít vždy aktuální či očekávaná znění právních předpisů.

Při tvorbě architektury je pak nanejvýš vhodné mít prvky architektury s vazbou na příslušnou legislativu. Například pokud spravuji informační systém, tak ten slouží pro podporu procesu v zákoně. Tedy vím, že systém provozuji na základě zákona o ISVS a na základě příslušných agendových zákonů a požadavky na funkce musi zajistit realizaci příslušných procesů v jednotlivých zákonech.

Zdroje informací o právních předpisech a jejich promítnutí do agend veřejné správy se hodí i pro tvorbu a aktualizaci vnitřních směrnic a předpisů v organizaci. Kupříkladu, změní-li se legislativa k základním registrům či ke spisové službě, vím, že to bude mít dopad na moje procesy a tedy i na předpisy a směrnice jež procesy určují. Dojde tedy jistě ke změnám agendových procesních metodik, ke změně Spisového řádu, apod. K tomu také mám využívat výše zmíněné zdroje a zajistit jejich

integraci na komponenty, které využívám k udržování dokumentace.

Pokud daný úřad není gestorem za příslušnou legislativu, ale přesto je pro něj legislativa závazná, pak by měl také splnit některé z výše uvedených základních principů. Aktuální údaje o stavu právních předpisů včetně vazby mezi jednotlivými ustanoveními a jednotlivými právními předpisy musí sloužit jako základ pro byznysovou architekturu. Druhým zdrojem jsou pak údaje v registru práv a povinností.

Je vhodné tedy:

- Vybudovat a udržovat mechanismus, jak pokud možno automatizovaně zpracovávat dekomponované právní předpisy
  - Lze realizovat s využitím služeb ESbírky, či obdobného systému
  - Zajistit si notifikace o aktualizacích právních předpisů, jež mě zajímají a o aktualizacích vazeb z jiných právních předpisů na ně
- Vytvořit procesy a podporu pro sledování návrhů změn a stavu jejich projednávání
- Být schopen přiřadit klíčové elementy architektury ke konkrétním ustanovením či alespoň ke konkrétním právním předpisům
- Udržovat povědomost o všech právních předpisech, kterými se řídím

Z hlediska aplikační architektury očekává NAP následující změny na centrální i lokálních úrovních:

- Po dokončení systému eSbírka (a doběhnutí stávajících kontraktů nejpozději do 5 let - udržitelnost) přestanou úřady do svého portfolia zařazovat aplikace pro seznamování se s právem od komerčních dodavatelů a přejdou na eSbírku. Komerční aplikace s redukovanými licencemi mohou zůstat pro doplňkové služby jako jsou výklady práva, judikáty a další obsah, který ještě nebude zahrnut do eSbírky nebo si ponechá soukromoprávní (komerční) charakter.
- Po dokončení systému eLegislativa se změní úloha systémů EKLEP/VEKLEP. Jakmile eLegislativa přinese převážnou část potřebných funkcí, význam uvedených systémů se bude snižovat - o jejich pánu rozvoje/ ukončení ještě bude nutno jednat.
- Systém ODOK musí být integrován na systém eLegislativa.

Od okamžiku spuštění systému eSbírky a eLegislativy budou všechny úřady povinny ve svých systémech a propojených materiálech používat pouze odkazy do eSbírky a nikoliv textové vyjádření formou např. §1 zákona č. 100/2000 Sb.

Pravidla pro Elektronické úkony a doručování

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci elektronických úkonů a doručování je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k elektronickým úkonům a

doručování popíše úřad do své informační koncepce.

Úřadu je doporučeno využívat systém ISDS jako integrální součást své elektronické spisové služby. Úřady musí mezi sebou komunikovat prostřednictvím systému ISDS a svých datových schránek, pokud se jedná o výměnu dokumentů a jejich zaručeného doručení. Pokud se jedná o výměnu údajů mezi úřady, nevyužívají se datové schránky, ale propojený datový fond a jeho referenční rozhraní. Je nutné brát v potaz, že veškeré úkony činěné skrze datovou zprávu směrem do úřadu od klienta VS se pokládají za elektronicky podepsané a není potřeba po klientovi vyžadovat žádné další formy autorizace.

ISDS umožňují na vyžádání u věcného správce (Ministerstva vnitra) využívat identitní prostor datových schránek k přihlašování do vlastních řešení - typicky portálů. **Tento způsob identifikace a autentizace klienta VS bude umožněn pouze do 1.7.2020**, kdy vyprší přechodné ustanovení zákona 250/2017 Sb., které zavádí povinnost využívat systém Národní identitní autority .

Pro zajištění digitální kontinuity datové zprávy, podobně jako v části Systém správy dokumentů, je z pohledu uživatele (příjemce) nutné si vždy uložit nejen přijatý dokument, ale celou datovou zprávu (obálka + dokument). Tato celá datová zpráva lze kdykoliv zpětně věřit proti samotnému informačnímu systému datových schránek, samotný dokument však ne.

Pravidla pro Jednotný identitní prostor veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci jednotného identitního prostoru veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k jednotnému identitnímu prostoru popíše úřad do své informační koncepce.

Úřad musí zajistit propojení svého identitního systému (AD/LDAP/IDM) se systémem Jednotného identitního prostoru (také jako JIP/KAAS) pro tu část zaměstnanců, kteří se přihlašují k informačním systémům veřejné správy. Využití může být provedeno 2 druhy:

- Vytvoření vlastních aplikačních rolí pro systémy, jejichž je OVM správce
- Využití existujících rolí v registru práv a povinností

Pro uživatele, kteří nejsou pokrytí centrální licencí provozovatele, lze zakoupit licenci zvlášť. Cena

takovéto licence je pro 1 uživatele přibližně 2 000 Kč za první rok a 500 pro další roky.

Pravidla pro Jednotné obslužné kanály a uživatelská rozhraní úředníků

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci jednotných obslužných kanálů a uživatelských rozhraní úředníků je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k jednotným obslužným kanálům a UI úředníků popíše úřad do své informační koncepce.

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Pravidla pro Sdílené služby INSPIRE

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS v přenesené působnosti je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným službám INSPIRE popíše úřad do své informační koncepce.

Stručný přehled povinností pro naplnění technických požadavků INSPIRE (detailně viz Strategie implementace INSIRE):

1. vytvořit, zpřístupňovat a aktualizovat metadata dat a služeb INSPIRE (v souladu s nařízením (ES) č. 1205/2008); Metadata musí být zpřístupněna na Národní geoportál INSPIRE buď pomocí služby vytvořené nad katalogem každého poskytovatele nebo uložením metadat do katalogu geoportálu. Metadaty je možné popsat i aplikace využívající prostorová data.
2. zpřístupňovat vyhledávací a prohlížecí síťové služby (v souladu s nařízením (ES) č. 976/2009); Požaduje se vytvořit vyhledávací službu, která umožní vyhledat služby na základě specifikovaných vyhledávacích kritérií, a prohlížecí službu, která umožní datové sady zobrazit.
3. vytvořit a aktualizovat nově vytvořené nebo rozsáhle rekonstruované datové sady; Požaduje se publikovat prostorová data ve formátu GML dle datových specifikací maximálně do 6 měsíců od počátku jejich platnosti v produkčních databázích, sledovat jejich kvalitu a informace o ní zpřístupnit v metadatech.
4. zpřístupňovat stahovací a transformační síťové služby (mít je v souladu s nařízením (ES) č. 976/2009); Požaduje se umožnit stahování INSPIRE datových sad on-line (WFS) nebo tzv. předpřipravených datových sad off-line způsobem. Transformační služby musí umožňovat transformovat datové sady neharmonizovaných dat ve formátu GML do požadovaného geodetického referenčního systému. Je požadováno zajistit kvalitu služby a popsat ji v metadatech;
5. poskytovat přístup k datovým sadám a službám orgánům a subjektům Evropské unie (v souladu s nařízením (EU) č. 268/2010); Požaduje se poskytovat datové sady nebo služby orgánům a subjektům Evropské unie do 20 dnů od doručení žádosti s možností využití standardizované licence.
6. mít interoperabilní a harmonizované služby prostorových dat v souladu s nařízením (EU) č. 1089/2010; mít v souladu s novelizovaným nařízením (ES) č. 976/2009 služby umožňující spuštění služeb založených na prostorových datech; Požaduje zpřístupnit informace o kvalitě služeb a doplnit ke službám další operace zajišťující interoperabilitu (do října 2020).

Při implementaci technických požadavků Směrnice INSPIRE je nutné náročnosti jednotlivých činností poskytovatelů dat dále rozlišit podle role ve vztahu k tvorbě, správě a rozvoji infrastruktury INSPIRE. Zapojení všech dotčených subjektů do infrastruktury INSPIRE předpokládá jejich rozdělení do různých rolí ve vztahu k prostorovým datům, službám založených na prostorových datech, anebo aplikacím, které jsou nad daty nebo službami vytvořeny. Je samozřejmostí, že jeden poskytovatel může vystupovat ve více rolích:

- Povinný subjekt (definován v § 2 písm. b) zákona č. 123/1998 Sb.)
- Jiný poskytovatel (definován v § 11a odst. 3 zákona č. 123/1998 Sb.)
- Gestor národní datové sady INSPIRE – povinný subjekt odpovědný za konsolidaci a publikaci výsledné národní datové sady INSPIRE, pokud je jediným poskytovatelem pro dané téma příloh Směrnice INSPIRE. V opačném případě koordinuje spolugestory přispívající svými prostorovými daty do obsahu národní datové sady INSPIRE (přesně a úplně definován ve Strategii implementace INSPIRE)
- Spolugestor národní datové sady INSPIRE - Jeden či více povinných subjektů k danému tématu příloh Směrnice INSPIRE, který odpovídá za harmonizaci příslušné části NDSI (přesně a úplně definován ve Strategii implementace INSPIRE)

Tabulka uvádí základní přehled oblastí, které jsou pro jednotlivé role závazné:

Součást infrastruktury *(v závorce uvedeno číslo legislativního dokumentu, který povinnost ustanovuje)*	Povinný subjekt	Jiný poskytovatel	Gestor NDSI	Spolugestor NDSI	Zajištěné centrálně
Metadata (1205/2008/ES) *)	■	■	■	■	
Metadata kvality (1089/2010/ES)			■	■	
Datová sada v souladu (1089/2010/ES, 1253/2013/ES)			■	■	
Vyhledávací služby (976/2009/ES)					■
Prohlížecí služby (976/2009/ES)	■	■	■		
Stahovací služby (976/2009/ES)		■	■		
Transformační služby – souřadnice (976/2009/ES)					■
Transformační služby – datové formáty (1089/2010ES) **)			■		
Spouštěcí služby (noveliz. 1089/2010/EU a 976/2009/ES) ***)	■	■	■		
Sdílení (268/2010/ES)	■	■	■		
Monitoring a reporting (vyhláška č.103/2010 Sb.)	■	■	■		■
Koordinace (zákon 123/1998 Sb.)		■	■		■

**) zpřístupnění metadat lze zajistit uložením dat na Národní geoportál INSPIRE nebo vytvořením a registrací katalogové služby nad vlastním metadatovým katalogem taktéž na Národním geoportálu INSPIRE. Toto zajišťuje každý poskytovatel dat.*
***) transformace datových formátů není třeba provádět, pokud gestor národní datové sady INSPIRE zvolí cestu zpřístupnění datové sady v souladu s INSPIRE, tedy v souladu s 1089/2010/ES, 1253/2013/ES*
****) soulad s tzv. službami umožňujícími spouštění služeb založených na prostorových datech je povinný, pokud tyto služby poskytovatel provozuje*

Pravidla pro Sdílené agendové IS v přenesené působnosti

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS v přenesené působnosti je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným agendovým IS pro přenesenou působnost popíše úřad do své informační koncepce.

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Pravidla pro Sdílené agendové IS pro samostatnou působnost územních samospráv

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených agendových IS pro samostatnou působnost je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu sdíleným agendovým IS pro samostatnou působnost popíše úřad do své informační koncepce.

OVS, které musí vybudovat 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, mohou poskytnout podporu v 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.

NAP doporučuje municipalitám pro určitou dílčí sadu sdílených služeb použít jako základní prvek správní obvody ORP a vychází z následujících předpokladů:

- ORP jsou nejmenšími subjekty, které zpracovávají architektonický plán.
- Správní obvod ORP je jednoznačně dán a všechny subjekty, kterých se bude sdílení ve správním obvodě týkat, jsou známy.
- Poskytování služeb a dat je určeno standardy (např. u spisové služby).
- Tento model již v řadě ORP funguje.

Pro jiné sdílené služby (například dlouhodobé ukládání dokumentů v elektronických digitálních spisovnách) se mohou využít technologická centra krajů, neboť:

- Mají vybudovanou infrastrukturu
- Disponují IT kapacitami a kompetencemi

Pro další sdílené služby, například pro aplikační služby ekonomických systémů nebo spisových služeb, bude možné v dohledné době 3 let (2022) využít SaaS služby eGovernment Cloudu, protože:

- Procesy a o IT potřeby v těchto oblastech fungování samospráv jsou vysoce standardizované a opakovatelné, proto jsou velmi vhodné pro řešení v cloudu

- Tyto funkce a jejich podpora zůstávají v plné zodpovědnosti obcí, a proto tyto potřebují multi-tenantní řešení

Sdílené aplikační služby kraje

Doporučujeme, aby kraje pro obce zřídily a poskytovaly služby například informačního systému spisové služby.

Krajské sítě

Publikace služeb krajských center do krajské sítě a dále přes krajský konektor do CMS.

Sdílené aplikační, technologické a síťové služby ORP

Malé obce, typicky všechny obce prvního a druhého typu, provozující méně než 10 přístupových zařízení, jsou zproštěny povinnosti zajišťovat informatizaci svých služeb veřejné správy a svůj podíl na eGovernmentu vlastními silami.

Pravidla pro Sdílené provozní informační systémy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci sdílených provozních IS je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným provozním IS popíše úřad do své informační koncepce.

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Pravidla pro Sdílené statistické, analytické a výkaznické systémy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci Sdílených statistických, analytických a výkaznických systémů je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke sdíleným statistickým, analytickým a výkaznickým systémům popíše úřad do své informační koncepce.

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Pravidla pro eGovernment cloud

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci eGovernment Cloudu je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k eGovernment Cloudu popíše úřad do své informační koncepce.

Rozhodnutí o vstupu do eGC

Jedním ze dvou hlavních kritérií pro využití služeb Státní část eGovernment Cloudu (také jako SeGC) nebo Komerční část eGovernment cloudu (také jako KeGC) je úroveň bezpečnostních dopadů daného IS. SeGC zajistí maximální úroveň bezpečnosti a je určen pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická). KeGC je určen pro provoz služeb eGC bezpečnostních úrovní 1-3 (Nízká, Střední, Vysoká)

a v maximální míře umožňuje využití tržních mechanismů pro zajištění optimálních cen. Druhým rozhodujícím kritériem pro využití služeb eGC je kalkulace a porovnání nákladů vlastnictví (TCO) jednotlivých IS v modelu provozu on-premise (na vlastní infrastruktuře) a s využitím služeb eGC. K oběma způsobům stanovení bezpečnosti a ekonomické náročnosti vznikly metodické pomůcky dostupné na:

- Stanovení ekonomické náročnosti
  - Metodika
  - Pomocný excel
- Stanovení požadavků na bezpečnost
  - Metodika
  - Pomocný excel

Správce eGC zveřejní dynamický nákupní systém (také jako DNS) pro nákup eGC služeb vedených v jeho katalogu. Portál pro objednávání a správu služeb nebude spuštěn spolu s DNS, ale jeho spuštění se dá očekávat v první polovině roku 2020.

Každý úřad si také musí být vědom toho, že financování cloudových služeb se liší od provozu vlastního řešení. Při provozu a nákupu vlastních technologií jde o tzv. CAPEX, tedy kapitálové výdaje, a pořízené věci zůstávají v majetku úřadu. Naopak nákup cloudových služeb je tzv. OPEX, tedy provozní výdaje kdy úřadu v majetku nic nezůstává a platí si pouze službu. S tímto odlišným způsobem financování je třeba počítat při tvorbě rozpočtu a jeho čerpání, protože při využívání cloudových služeb pro celou infrastrukturu úřadu se razantně zvýší provozní výdaje a sníží investiční.

Přístup správců ISVS k eGC

Každý správce centralizovaného poskytovaného agendového informačního systému by měl postupně činit při správě a rozvoji svých informačních systémů takové kroky, aby oddělil infrastrukturu od samotné technologické a aplikační vrstvy příslušných informačních systémů. To znamená, že by se svými postupnými kroky měl připravit na to, že od určité Doby bude provozovat svoje centralizované agendové informační systémy v cloudu a měl by postupně omezovat svoji závislost na vlastních datových centrech a pouze jím provozovaných technologických platformách.

V následující fázi budování eGC, dlouhé zhruba dva roky, bude umísťování IS do eGC (využívání služeb eGC) dobrovolné. Dlouhodobě bude uplatněn princip cloud-first – povinné umístění IS do eGC, pokud kalkulace TCO neprokáže nákladově efektivnější provoz onpremise.

Povinnosti komerčních poskytovatelů služeb eGC

Konkrétní povinnosti stanoví Řídící orgán eGovernment Cloudu. Již nyní však platí pravidla pro nutnost připojení skrze infrastrukturu CMS/KIVS a tím i respektování

katalogového listu služby připojení přes IPSec

Pravidla pro Národní datová centra

Popis architektury úřadu a veřejné správy ČR po jednotlivých

vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci národních datových center je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu k národním datovým centrům popíše úřad do své informační koncepce.

NAP nestanovuje v této verzi pro tento funkční celek či tematickou oblast žádná pravidla.

Pravidla pro komunikační infrastrukturu veřejné správy

Popis architektury úřadu a veřejné správy ČR po jednotlivých vrstvách architektury a zapracování požadavků do informační koncepce a architektury úřadu je popsán v části Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury.

Popis centrálně poskytovaných systémů a jejich služeb, funkčních celků a tematických oblastí v rámci komunikační infrastruktury veřejné správy je popsán na samostatné stránce zde nebo v rámci části Popis sdílených služeb, funkčních celků a tematických oblastí veřejné správy ČR.

Využití a popis k přístupu ke komunikační infrastruktuře veřejné správy popíše úřad do své informační koncepce.

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

- Bezpečný a spolehlivý přístup k aplikačním službám jednotlivých ISVS
- Bezpečnou a spolehlivou publikaci aplikačních služeb jednotlivých ISVS
- Bezpečný přístup do internetu
- Bezpečný přístup k poštovním službám v internetu
- Zabezpečuje bezpečné síťové prostředí pro zajištění interoperability v rámci EU
- Umožňuje bezpečný přístup k aplikačním službám ISVS určeným pro koncové klienty VS ze sítě

internet

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, jakožto součást komunikační infrastruktury veřejné správy, 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.

Připojení k CMS

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.

Připojení k CMS je možné realizovat prostřednictvím:

1. Neveřejného KIVS operátora (Krajské sítě, Metropolitní sítě, ITS Ministerstva vnitra a další)
2. Veřejného KIVS operátora (Soutěž KIVS operátora přes centrálního zadavatele MVČR)
3. IPsec VPN
4. SSL VPN

Pro OVS jsou přípustné pouze první 2 varianty - Neveřejný a veřejný KIVS operátor, komunikace mezi jednotlivými OVS je tak vedena výhradně prostřednictvím KIVS/CMS, tzn. jednotlivé OVS mají povinnost přistupovat k informačním systémům veřejné správy (ISVS) pouze prostřednictvím KIVS/CMS.

IPsec a jeho úskalí

Ačkoliv jsou pro OVS přípustná jen připojení pomocí KIVS, existují úřady využívající připojení IPsec, který se ovšem nehodí pro kritické služby a funkce úřadování. Nevhodné je toto připojení např. pro systém CDBP (systém sběru žádostí o vydání občanského průkazu nebo cestovního dokladu občana České republiky), kdy mohou nastat následující rizika:

1. Spojení realizovaná prostřednictvím kryptografických prostředků přes veřejný internet nejsou vhodná jako primární způsob čerpání služeb, které mají mít garantovanou funkčnost a dostupnost. Systém CDBP je koncepčně založen na předpokladu provozu na vyhrazené síti, která je zcela oddělena od běžného internetového provozu a tomu odpovídá i úroveň jeho zabezpečení.
2. V rámci spojení realizovaných prostřednictvím veřejného internetu není možné dostatečným

způsobem garantovat následující:
- požadavek na dostupnost, protože internet není zaručeně garantované přenosové prostředí s definovanými SLA,
- požadavek na propustnost, protože systém CDBP využívá na ORP "těžkého" klienta se vzdálenou správou; nezbytná je tedy komunikace oběma směry (centrum systému CDBP – ORP a ORP – centrum systému CDBP) pro instalací nových verzí aplikace pomocí "balíčků" o velikosti cca 500 MB/PC a pro stahováním logů z PC o velikosti cca 100 MB/PC,
- požadavek na fungování protokolu WoL, který umožňuje dálkové „probouzení“ jednotlivých pracovních stanic systému CDBP bez zásahu obsluhy, je nezbytný z důvodů distribuce nových verzí SW, stahování logů či jiných činností souvisejících s provozem Systému CDBP.

3. Na základě výše uvedeného reálně hrozí, v případě využití IPsec, riziko výpadků spojení při pořizování žádostí o občanské průkazy a cestovní pasy, což může vést ke zpomalení nebo úplné nedostupnosti pracovišť systému CDBP. V případě, že by v důsledku užívání IPsec, nebylo možné dálkově nainstalovat na koncová pracoviště systému CDBP aktualizace, bude nezbytné, aby instalaci provedl technik při výjezdu, který by úřad musel uhradit.

CMS, popis zahrnutých služeb

Odbor Hlavního architekta eGovernmentu a Ministerstvo vnitra v rámci svých kompetencí požaduje od jednotlivých správců ISVS, aby služby ISVS 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/ISSS

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

Služba zajistí provozovateli publikačního agendového informačního systému (AIS) síťovou konektivitu mezi eGSB/ISSS (eGON Service Bus / Informační systém sdílené služby, 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/ISSS 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 skrze CMS se publikují služby 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 CMS.

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.