Materiál Ministerstva vnitra

Export z Národní architektury eGovernmentu ČR

Obsah

Pravidla pro funkční celky architektury jednotlivých úřadů 3
****Portály veřejné správy a soukromoprávních uživatelů údajů**** 3
Portál občana a portál veřejné správy 4
Agendový portál 4
Portál území 4
Portál soukromoprávního uživatele údajů 5
Elektronický systém spisové služby 6
Obecně o spisové službě 6
Řídící dokumenty 7
Architektura spisové služby 7
Architektura agendového informačního systému 8
Architektura provozních systémů 8
Přijímání a odesílání dokumentů 9
Další zdroje 9
Otevřená data 9
Možnosti přípravy IS pro otevřená data 10
Export dat nebo API v proprietárním formátu 11
Následná příprava dat k publikaci v podobě otevřených dat 11
Ochrana osobních údajů 11
Právní aspekty 12
Centrální místo služeb 12
Elektronická fakturace 14
Mandáty, role a práva v elektronické komunikaci 16
Propojený datový fond 18
Univerzální kontaktní místo 18
Elektronická identita 18

Pravidla pro funkční celky architektury jednotlivých úřadů

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

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

Portály veřejné správy a soukromoprávních uživatelů údajů

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

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

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

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

Portál občana a portál veřejné správy

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

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

Agendový portál

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

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

Portál území

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

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

Portál soukromoprávního uživatele údajů

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

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

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

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

Elektronický systém spisové služby

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

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

Obecně je nutno řešit a zajistit toto:

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

2. Zajistit integraci ESSL na úložiště digitálních dokumentů.

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

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

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

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

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

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

Obecně o spisové službě

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

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

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

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

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

Řídící dokumenty

V rámci výkonu spisové služby jsou řídícími drivery zejména:

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

Architektura spisové služby

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

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

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

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

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

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

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

a. elektronickým systémem spisové služby, nebo

b. informačním systémem, který plní funkci samostatné evidence

III. Se soubory v úložišti jsou oprávněny pracovat:

a. elektronický systém spisové služby, nebo

b. informační systém sloužící jako samostatná evidence, nebo

c. informační systém integrovaný na ESSL prostřednictvím ESSL

Architektura agendového informačního systému

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

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

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

Architektura provozních systémů

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

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

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

Přijímání a odesílání dokumentů

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

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

Další zdroje

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

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

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

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

Otevřená data

Otevřená data jsou:

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

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

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

Otevřenými daty zejména není:

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

Pro zajištění publikace otevřených dat z IS je třeba:

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

Možnosti přípravy IS pro otevřená data

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

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

Export dat nebo API v otevřeném formátu - preferované řešení

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

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

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

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

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

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

Export dat nebo API v proprietárním formátu

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

Následná příprava dat k publikaci v podobě otevřených dat

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

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

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

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

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

Ochrana osobních údajů

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

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

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

Právní aspekty

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

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

Centrální místo služeb

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

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

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

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

Komunikace mezi jednotlivými OVS je tak vedena výhradně prostřednictvím CMS.

CMS, popis zahrnutých služeb

Odbor Hlavního architekta eGovernmentu a Ministerstvo vnitra v rámci svých kompetencí požaduje od jednotlivých správců ISVS, aby služby těchto systémů publikovaly v rámci Centrálního místa služeb – CMS (služba CMS2 -02, CMS2 -04).

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

Služba CMS2 – 02 – Zveřejnění aplikace

Název parametru Vysvětlení

Kód služby CMS2-02

Název služby Zveřejnění aplikace

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

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

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

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

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

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

Služba CMS2 – 03 – Přístup k aplikaci

Název parametru Vysvětlení

Kód služby CMS2-03

Název služby Přístup k aplikaci

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

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

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

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

Přístup k aplikaci v síti Internet umožní subjektu připojení k aplikační službě zveřejněné v síti Internet na definovaných protokolech a portech. Cílovou aplikační službu v síti Internet je nutné definovat konkrétními IP adresami, protokoly a porty.

Služba CMS2 – 04 – Publikace AIS na eGSB

Název parametru Vysvětlení

Kód služby CMS2-04

Název služby Publikace AIS na eGSB

Popis služby Služba zajišťuje zpřístupnění publikačního agendového informačního systému (AIS) v rámci CMS a povolení síťové komunikace s rozhraním eGON Service Bus (eGSB)

Služba zajistí provozovateli publikačního agendového informačního systému (AIS) síťovou konektivitu mezi eGSB

(eGovernment Online Service Bus, tj. sdílená služba obecného rozhraní) a publikačním AIS na definovaných protokolech a portech. V rámci publikace jsou přiděleny privátní IP adresy z prostoru CMS (Konsolidované IP adresy).

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

Právní aspekty

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

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

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

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

Příkladem publikované služby - Centrální registr řidičů (CRŘ)

Elektronická fakturace

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

E-fakturace v kombinaci s řádně vedenou spisovou službou dle č.499/2004 Sb., zákona o archivnictví a spisové službě nabízí ekonomickým subjektům orgánů veřejné správy:

* * * * Ekonomické aspekty

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

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

Norma EN 169311:2017 a její pomocné normalizační výstupy umožní sémantickou interoperabilitu

elektronických faktur a pomohou odstranit bariéry na trhu a překážky v obchodu vyplývající z existence rozdílných vnitrostátních právních předpisů a norem – a přispějí tak k dosažení cílů stanovených Evropskou komisí.

Technické aspekty

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

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

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

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

Jakákoliv odchylka od tohoto pravidla by představovala porušení směrnice.

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

Právní aspekty

Implementace e-fakturace do prostředí veřejné správy České republiky je dána směrnicí 2014/55/EU, která nabyde účinnost 19. 4. 2018. K tomuto datu je také nutné mít ve svých spisových službách v rámci organizace nastavené technickoorganizační opatření, která budou v souladu s výše uvedenou směrnicí a technickými standardy z ní vyplívající. Směrnice byla inkorporována do české legislativy v rámci §221 zákona č. 134/2016, o zadávání veřejných zakázek. Zadavatel nesmí odmítnout elektronickou fakturu vystavenou dodavatelem za plnění veřejné zakázky z důvodu jejího formátu, který je v souladu s evropským standardem elektronické faktury.

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

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

Cílový adresáti

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

Odbor Hlavního architekta eGovernmentu Ministerstva vnitra

Ministerstvo vnitra je podle § 12 zákona č. 2/1969 Sb., kompetenčního zákona ústředním orgánem státní správy mj. pro oblast ISVS a plní též koordinační úlohu pro informační a komunikační technologie, jakož i obecně pro organizaci a výkon veřejné správy. Tyto kompetence jsou dále rozvedeny v ZoISVS, podle něhož se ministerstvo vnitra vyjadřuje k návrhům, projektům a investičním záměrům OVS v oblasti informačních a komunikačních technologií.

Na základě příslušných předpisů plní popsanou koordinační úlohu v oblasti informačních a komunikačních technologií Odbor Hlavního architekta eGovernmentu Ministerstva vnitra (OHA). OHA má nadresortní působnost, to znamená, že je pověřen a zodpovědný za koordinaci a vedení rozvoje eGovernmentu v celé veřejné správě. Samotný eGovernment zahrnuje nejen samotné informační technologie, ale také optimalizaci a zjednodušování služeb veřejné správy vázané na legislativní prostředí. Kromě zmíněných právních předpisů je OHA ke zmíněné koordinační úloze výslovně povolán též usnesením vlády ze dne 2. listopadu 2015, č. 889.

Mandáty, role a práva v elektronické komunikaci

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

1) Znalost typů mandátů při jednání s veřejnou správou

2) Jednoznačnou identifikaci a autentizaci klienta veřejné správy

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

4) Vlastní zajištění autorizace klienta veřejné správy

Mandáty pro jednání s veřejnou správou

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

1. Fyzická osoba

a. Jednající sama svým jménem

b. Jednající jménem jiné fyzické osoby ze zákona

i. rodič dítěte

ii. manžel/manželka

iii. registrovaný partner/partnerka

iv. opatrovník

c. Jednající jménem jiné fyzické osoby ze zmocnění

i. plná moc

ii. advokát

iii. zastupující FO

iv. jiný druh zmocnění

v. na žádost bez zmocnění

2. Fyzická osoba jednající za právnickou osobu

a. Jednatel právnické osoby

b. statutární zástupce právnické osoby (jedna FO)

c. Statutární orgán právnické osoby (více FO)

d. Insolvenční správce

e. Likvidátor

f. Jednající jménem zřizovatele právnické osoby

g. Pověřen k jednání za právnickou osobu

i. Veřejnoprávním titulem

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

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

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

* * * * * * Jednoznačná identifikace a autentizace klienta veřejné správy

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

„Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace.“

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vlastní zajištění autorizace klienta veřejné správy

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

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

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

Mandát plynoucí z veřejnoprávního nebo soukromoprávního titulu a to včetně plných mocí a dohod o zastupování při správním jednání s úřady patří mezi společné rozhodné skutečnosti, tak jak jsou zakotveny v souvisejících ustanoveních Správního řádu (zejména § 6 a § 50 a související). Proto je nanejvýš vhodné, aby příslušný orgán veřejné moci, pokud

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

Propojený datový fond

test

Univerzální kontaktní místo

Elektronická identita