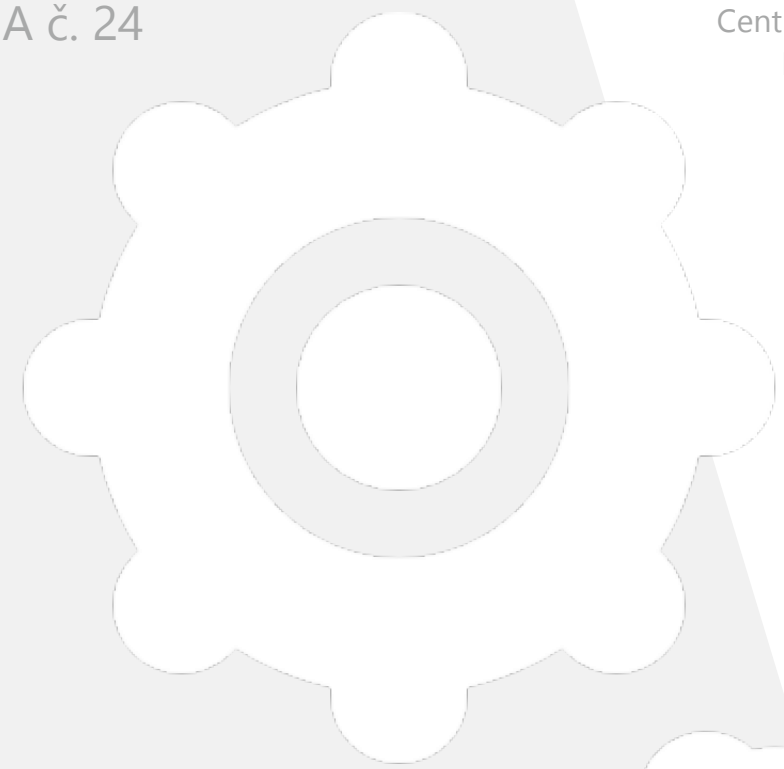
Společný Metodický pokyn

CHJ a OHA č. 24

Centrální harmonizační jednotka
Ministerstvo financí ČR



Digitalizace úřadu

v souladu s cíli, principy a zásadami českého eGovernmentu

Příručka pro ICT odbory, kontrolory a auditory

Verze 1.0

Vydáno dne 8. 11. 2022

Obsah

1 Úvod

Tato příručka vznikla ve spolupráci Centrální harmonizační jednotky Ministerstva financí ČR, Odboru Hlavního architekta eGovernmentu Ministerstva vnitra ČR, Ministerstva pro místní rozvoj ČR a Odboru Kabinetu místopředsedy vlády pro digitalizaci Úřadu vlády ČR.

Příručka je určena primárně pro útvary úřadů, které jsou věcnými správci ICT[1], útvary úřadů, které jsou zodpovědné za provoz a podporu ICT a také pro zaměstnance v organizacích veřejné správy, kteří zjišťují a vyhodnocují rizika nehospodárného, neefektivního a neúčelného výkonu veřejné správy, informují o výskytu závažných nedostatků, případně přijímají nebo navrhují opatření k nápravě nedostatků (včetně kontrolorů, interních a externích auditorů).

Úřady, které hospodaří s veřejnými prostředky, mohou na základě informací uvedených v této metodice zjistit, zda plní všechny zákonné požadavky v oblasti digitalizace veřejné správy a také identifikovat, v jakých oblastech je potřeba se zlepšit. Hlavním cílem tohoto metodického pokynu je napomoci úřadům plnit požadavky Informační koncepce ČR, která je, včetně jejích navazujících dokumentů, základním dokumentem v oblasti digitalizace. Digitalizace ve veřejné správě je často označována pojmem eGovernment, který lze chápat jako správu věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější. V tomto metodickém pokynu je kladen důraz na maximální využívání centrálních sdílených služeb eGovernmentu, ale i na doporučení a rady při tvorbě a správě ICT. Na konkrétních případech je ilustrováno, jak lze pohlížet na vybrané oblasti digitalizace úřadu, jak zjistit, zda je určitá centrální sdílená služba eGovernmentu využívána správně, zda existuje v úřadu dostatečná podpora ICT, či zda je úřad připraven na budoucí rozvoj.

Účelem této příručky naopak není a nemůže být poskytnutí závazného vyčerpávajícího výkladu k příslušným ustanovením relevantních zákonů, které se dotýkají digitalizace, případně které se dotýkají veškerých procesů souvisejících například s kybernetickou bezpečnostní, ochranou osobních údajů či právem subjektů na informace.

Základními právními předpisy, které definují povinnosti v oblasti digitalizace, jsou:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (dále „zákon č. 365/2000 Sb.“)
- Zákon č. 111/2009 Sb., o základních registrech (dále „zákon č. 111/2009 Sb.“)
- Zákon č. 12/2020 Sb., o právu na digitální služby (dále „zákon č. 12/2020 Sb.“)
- Zákon č. 250/2017 Sb., o elektronické identifikaci (dále „zákon č. 250/2017 Sb.“)
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím (dále „zákon č. 106/1999 Sb.“)
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (dále „zákon č. 300/2008 Sb.“)

Pro upřesnění je důležité zmínit, že zákon č. 181/2014 Sb., o kybernetické bezpečnosti včetně jeho doprovodných právních předpisů, není obsahem této metodiky a informace a podporu v oblasti kybernetické bezpečnosti doporučujeme hledat na stránkách Národního úřadu pro kybernetickou a informační bezpečnost https://nukib.cz/.

[1] Informační a komunikační technologie (angl.. Information and communication technology). Pro účely této metodiky se bude jednat nejen o informační systém, ale například i licence, HW, SW, apod. Neboli vše, co přímo souvisí s tím, že mám určitou činnost nebo proces podporovanou informační technologií.

Ač výše zmíněné právní předpisy pracují s různou definicí povinných subjektů, pro účely této metodiky bude používán souhrnně pojem úřad, který zastřešuje hlavní dvě skupiny subjektů definované dvěma hlavními výše zmíněnými zákony zabývající se digitalizací:

1. Orgány veřejné moci (dle § 2 odst. 1 písm. c) zákona č. 111/2009 Sb.), tedy státní orgány, územní samosprávné celky, fyzické nebo právnické osoby, byla-li jí svěřena působnost v oblasti veřejné správy, notáři, soudní exekutoři a archivy.
2. Orgány veřejné správy (dle § 1 odst. 1 zákona č. 365/2000 Sb.), tedy státní orgány a orgány územních samosprávných celků.

Digitalizace je dnes součástí všech oblastí působnosti úřadů a jejich agend. V každé agendě se shromažďují a sdílejí informace a většina agend realizuje služby veřejné správy, například vydávání řidičských průkazů, poskytnutí příspěvku na živobytí, dodání hlasovacích lístků voličům. Díky využití ICT se data již nemusí evidovat v šanonech v papírové podobě a služby poskytovat v úředních hodinách v budově úřadu. Digitalizace veřejné správy umožňuje poskytovat vybrané služby online v jakoukoli denní hodinu a jednoduše sdílet data mezi jednotlivými úřady.

Výstupem digitalizace by neměl být jen např. informační systém, ale také změna procesů, která povede k efektivnějšímu nakládání s veřejnými prostředky díky úspoře lidských kapacit, času či lépe poskytovaným službám. Úřad by měl při digitalizaci svých procesů zohlednit především potřeby klientů. Využití ICT k další digitalizaci veřejné správy je zdrojem mimořádných příležitostí k dramatickému zvýšení výkonnosti veřejné správy na všech jejích úrovních – a to jak prostřednictvím zvyšování její uživatelské přívětivosti, dostupnosti a rychlosti poskytování služeb veřejné správy občanům, tak také cestou ke snižování „provozních“ nákladů na tyto služby na straně občanů a samozřejmě veřejné správy. Bohužel běžnou praxí je často digitalizace izolovaných procesů bez návazností na související procesy nebo absence systému řízení úřadu, který by formalizoval vazby procesů na výkony agend v souladu se zákonnými zmocněními.

Aby mohlo být dosaženo hospodárnosti prostředků vynakládaných na digitalizaci, je nezbytné dodržet stanovené cíle digitalizace veřejné správy v odpovídající kvalitě za co nejnižší cenu. Nápomocnými, a zároveň neopominutelnými materiály při zavádění digitalizace v odpovídající kvalitě jsou vydané principy eGovernmentu popsané v Informační koncepci ČR[2], přičemž je potřeba dodržovat Národní architektonický plán[3]. Zákonné požadavky v oblasti digitalizace společně s obecnými architektonickými principy definovanými v Informační koncepci ČR lze využít také jako kritéria pro účelnost vynakládaných prostředků. Účelnost, efektivnost a hospodárnost (tzv. 3E)[4] je vymezena v zákoně č. 320/2001 Sb., 219/2000 Sb. a 218/2000 Sb. Více k souladu se 3E je uvedeno například v metodice „Správa majetku v souladu s principy 3E“[5].

Úřad musí mít schopnost porozumět postupům a procesům realizovaným pomocí ICT, a to jak z pohledu potřeb jejich pořízení, tak správy, údržby a podpory. Aby mohla tato schopnost v úřadu být, je nutné budovat vnitřní znalosti nejen formou lidských zdrojů, ale i například dostatečné dokumentace ICT. Dokumentace ICT slouží pro ulehčení souvislostí a pochopení situace jak lidem a útvarům uvnitř úřadu, tak externím entitám (např. dodavatelům).

---

[2] Online: https://archi.gov.cz/ikcr
[3] Online: https://archi.gov.cz/nap_dokument
[4] Účelnost (z angl. Effectiveness) je takové použití veřejných prostředků včetně nefinančních, které zajistí optimální míru dosažení cílů veřejné správy. Hospodárnost (z angl. Economy) je takové využití veřejných prostředků, jež zajistí s jejich co nejnižším využitím dosažení stanovených cílů veřejné správy v odpovídající kvalitě. Efektivnost (z angl. Efficiency) je takové využití veřejných prostředků, jimž bude dosaženo nejvýše možného rozsahu, kvality a přínosů k dosažení cílů veřejné správy ve srovnání s vynaloženým objemem těchto prostředků.
[5] Online: https://www.mfcr.cz/cs/legislativa/metodiky/2021/metodicky-pokyn-chj-c-15-40927

Stručný obsah jednotlivých kapitol

Tato příručka uvádí v jednotlivých kapitolách zásady rozvoje a správy digitalizace, které jsou publikovány v dokumentu **Klíčové oblasti architektury [Architektura eGovernmentu ČR].** V jednotlivých kapitolách jsou popsány povinnosti a pravidla, které mají úřady dodržovat, jsou definovány otázky k ověření žádoucího stavu a současně i příklady dobré a špatné praxe.

Kapitola č. 2 uvádí cíle a principy rozvoje eGovernmentu a vyjmenovává relevantní a nadřazené dokumenty se kterými úřad pracuje při formování své informační koncepce a strategie rozvoje úřadu.

Kapitola č. 3 se týká architektury úřadu a popisuje nutnost vést a spravovat celkový popis úřadu ve formě, kterou je možné komunikovat nejen dovnitř úřadu, ale i vně úřadu. Dovnitř úřadu je tato komunikace potřebná především pro rozhodování o změnách a investicích a vně úřadu pro komunikaci s centrálními úřady státní správy nebo dodavateli a jinými partnery.

Kapitola č. 4 se věnuje oblasti dat a jejich sdílení. Popisuje správu dat v informačních systémech, jejich kategorizaci, centrální evidenci, a jakými způsoby by měla být veřejná či neveřejná data sdílena.

Kapitola č. 5 popisuje pravidla a povinnosti při kontaktu s klientem úřadu, uvádí možné tzv. obslužné kanály veřejné správy a zmiňuje plán digitalizace služeb veřejné správy.

Kapitola č. 6 popisuje způsoby identifikace klientů veřejné správy a také identifikaci uživatelů interních systémů spravovaných úřadem.

Kapitola č. 7 se zaměřuje na elektronický oběh dokumentů a pravidla při práci s dokumentem, který je reprezentovaný elektronickou formou.

Kapitola č. 8 popisuje, jak má být zajištěna bezpečná a spolehlivá komunikace s využitím komunikační infrastruktury veřejné správy.

Kapitola č. 9 se věnuje cloudovým službám, které umožňují úřadu čerpat služby, které mohou naplňovat potřeby úřadu z hlediska principů 3E.

Základní pojmy a zkratky frekventované v tomto dokumentu[6]

AIFO - Agendový identifikátor fyzické osoby, neveřejný identifikátor, který je jednoznačně přiřazen záznamu o fyzické osobě v agendovém informačním systému nebo základním registru v rámci příslušné agendy, je užíván výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen

AIS – Agendový informační systém

Autentizace – proces ověření totožnosti, prokázání, že osoba/aplikace/technický prostředek, je skutečně tou identitou, za kterou se prohlašuje nebo je prohlašován. Jedná se o poskytnutí záruky, že prohlašovaná charakteristika je správná

Byznys služba – služba úřadu publikovaná prostřednictvím jednoznačně definovaného rozhraní a je jednoznačně formálně řízena organizací (například má SLA smlouvu)

DŘ – Dlouhodobé řízení

[6] Nejdůležitější pojmy vyskytující se v českém eGovernmentu (jak v právních předpisech, tak v odborné terminologii) jsou uvedeny ve Slovníku pojmů eGovernmentu. Online: https://archi.gov.cz/slovnik_egov

eIDAS – Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu

eSSL - elektronická spisová služba

ICT – Informační a komunikační technologie

IK – Informační koncepce

IK ČR – Informační koncepce České republiky

ISDS - Informační systém datových schránek

ISVS – Informační systémy veřejné správy jsou určeny k podpoře výkonu veřejné moci, tj. zejména v případech, kdy orgán veřejné moci (např. orgán obce) zasahuje do právních poměrů jiných osob (fyzických nebo právnických) nebo poskytuje digitální služby, ale ne pro podporu provozních činností úřadu jako např. správa majetku obce, personalistika atd. Práva a povinnosti související s ISVS jsou upraveny v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy

KII - Kritická informační infrastruktura

KIVS/CMS – Komunikační infrastruktura Informačních systémů veřejné správy, centrální místo služeb

PPDF - Propojený datový fond je primárním zdrojem platných a právně závazných neveřejných údajů pro subjekty práva i pro všechny orgány veřejné moci při výkonu jejich působnosti. PPDF vede k náhradě manuálních interakcí mezi úřady pomocí automatizované výměny údajů

NKOD - Národní katalog otevřených dat je informační systém veřejné správy přístupný způsobem umožňujícím dálkový přístup a sloužící k evidování informací zveřejňovaných jako otevřená data

VDF - Veřejný datový fond je základní metoda pro sdílení veřejných informací mezi veřejnoprávními subjekty navzájem i pro sdílení veřejných údajů mezi veřejnoprávní a soukromoprávní sférou v ČR

OHA – odbor Hlavního architekta eGovernmentu MV ČR

RPP – Registr práv a povinností

Určený informační systém - pojem je definován v § 2 písm. v) zákona č. 365/2000 Sb., podle něhož se jedná o takový informační systém veřejné správy, který využívá služby tzv. referenčního rozhraní nebo mu poskytuje služby

2 Koncepce a strategie

Digitalizace úřadu by měla probíhat dle nastavených principů a zásad v nadřazených strategiích a v souladu s:

- Informační koncepcí ČR včetně jejích navazujících dokumentů.
- Informační koncepcí úřadu.
- Strategií rozvoje úřadu / systémem řízením kvality ve služebních úřadech.
- Provozních dokumentací informačních systémů veřejné správy.

Zásadním dokumentem pro formulaci záměrů digitalizace je **Informační koncepce úřadu (IK).**

IK je strategický dokument, který slouží ke stanovení směru rozvoje a správy ICT. Informační koncepci povinně vede každý orgán veřejné správy, dobrovolně pak ostatní úřady. Informační koncepce úřadu nemá jít do hloubky, identifikuje cíle a oblasti rozvoje a správy informačních systémů a rámcově určuje parametry realizačních projektů ve vazbě na dosažení cílů stanovených úřadem. Zároveň je nutné ji pravidelně aktualizovat a nechat odsouhlasit nejvyšším vedením. IK má svou povinnou strukturu a obsah danou vyhláškou č. 529/2006 Sb., mimo tu může samozřejmě úřad IK rozšířit o potřebné informace.

Informační koncepce ČR stanovuje principy a zásady, které jsou rozpracovány v navazujících dokumentech, a určují směr digitalizace celé veřejné správy. Definuje celkem 6 cílů, které jsou následně děleny do podcílů. Navazující principy a zásady vždy směřují k naplnění některého z cílů:

1. Uživatelsky přívětivé a efektivní „on-line“ služby pro občany a firmy.
2. Digitálně přívětivá legislativa.
3. Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu.
4. Zvýšení kapacit a kompetencí zaměstnanců ve veřejné správě.
5. Efektivní a centrálně koordinované ICT veřejné správy.
6. Efektivní a pružný digitální úřad.

Legislativní proces nemusí vždy odpovídat reálnému stavu, to se bohužel projevuje i v požadavcích na IK, kdy vyhláška neobsahuje potřebné údaje k splnění souladu s IKČR, proto doporučujeme využít znalostní bázi s texty k IK a souladu IK s IKČR.

IK ČR stanovuje v oblasti koncepcí a strategií dosažení následujících cílů a podcílů:

- Zvýšení kapacit a kompetencí zaměstnanců ve veřejné správě (všech 8 podcílů).
- 5.01 Implementace procesu řízení IK ČR.
- 5.12 Zajištění zpětné vazby realizace IKČR.
- 6.03 Zavedení nových metod řízení a sdílení služeb.

Strategie rozvoje úřadu / systém řízení kvality ve služebních úřadech je především procesně a službově orientovaná strategie, která má za cíl nastavení měření a vyhodnocování jejich kvality vůči klientům. Informační koncepce je s touto strategií komplementární a popisuje potřebu ICT jakožto nezbytné součásti pro poskytování kvalitních služeb klientům. Strategii rozvoje služebního úřadu, měly úřady zpracovat dle metodického pokynu pro řízení kvality ve služebních úřadech do 30. 6. 2021.

Vnímáme jako podstatné, aby strategie rozvoje úřadu a strategie ICT byly provázané dokumenty.

Provozní dokumentace je nedílnou součástí ICT, bez kterého je informační systém veřejné správy jen tzv. černá skříňka – blackbox. Provozní dokumentace zajišťuje organizaci provozuschopnost informatiky a popisuje systém její správy, rozvoje a údržby. Vyhláška č. 529/2006 Sb. stanovuje i strukturu a obsah provozní dokumentace. Provozní dokumentace by měla popisovat funkční a technické vlastnosti

informačního systému veřejné správy a blíže rozpracovávat oprávnění a povinnosti jeho správce, provozovatele a uživatele. Povinně ji vede každý orgán veřejné správy, dobrovolně ostatní úřady.

Legislativa je středobodem pro fungování úřadu a určuje mantinely, v nichž se může pohybovat. Problém nastává ve chvíli, kdy zákon přímo předjímá určité řešení, které je zamýšleno pro „papírový“ proces a z hlediska digitalizace není optimální či jí výslovně znemožní (např. Zákon vyžaduje podání listinnou formou, nebo dodání přílohy, které nelze zaslat elektronicky, vyžaduje povinné údaje, které lze získat ze základních registrů atd.)V horších případech zákon předjímá (byť většinou ne explicitně) způsob nakládání s podáním atd. V ideálním případě by zákon měl být technologicky neutrální, a natolik obecný, aby nepředjímal jakékoliv technické řešení, a ani mu nebránil. V praxi to však není vždy možné.

Ideálem je vznik právního předpisu a jeho digitalizačního řešení ruku v ruce, jako vzájemně optimálně sladěných. Jak toho dosáhnout?

- **Na přípravě zákona by se měli podílet také IT odborníci.**

  Je zvykem, že na přípravě zákona spolupracuje věcný gestor s legislativním útvarem. Pokud se již v této fázi zapojí i IT analytici, IT architekti a lídři digitální transformace úřadu, je možné řadu nedostatků odchytit již v zákoně, a napsat jej tak, aby budoucí IT řešení bylo snadné, levné a propojitelné se zbytkem systémů úřadu i veřejné správy jako celku.

- **Součástí přípravy musí být zamyšlení nad klientskou orientací, přívětivostí a procesní optimalizací služeb.**

  Je třeba odstranit či maximálně upozadit konkrétní procesní kroky, které zbytečně předpokládají fungování procesu. Slovní spojení jako „písemné podání“, „přítomnost klienta“ či „žadatel doloží“ již předpokládají, že nebude konat úřad, ale druhá strana.

- **Legislativa funguje jako celek a musí se navzájem doplňovat.**

  Řadu systémů a služeb není třeba stavět od základů. Pokud už existují sdílené systémy a služby, je vhodné je využít. Již není potřeba popisovat a vyžadovat registraci či ověření totožnosti klienta s českým občanstvím nebo např. povinnost informování o změnách údajů. Na toto už existují centrální služby, které jsou pro veřejnou správu bez poplatku a garantují správnost pro zamezení chybného úředního postupu.

  A platí to i obráceně – systém může nabídnout své služby zbytku veřejné správy.

2.1 Popis optimálního stavu, základní principy a pravidla

Optimální stavem v této oblasti je dlouhodobé řízení informačních systémů veřejné správy v souladu s výše uvedenými dokumenty:

- Informační koncepcí ČR včetně jejích navazujících dokumentů.
- Informační koncepcí úřadu.
- Strategií rozvoje úřadu / řízení kvality ve služebních úřadech.
- Provozní dokumentací informačního systému veřejné správy.

Povinnosti úřadu ve vztahu k organizační jednotce odpovídající za rozvoj a koordinaci eGovernmentu při Ministerstvu vnitra (dále OHA – útvar hlavního architekta eGovernmentu):

1. Spolupracovat s OHA při plnění jeho úkolů. Tato povinnost se využívá pouze na žádost ministerstva vnitra při potřebě konzultací nebo dalšího směřování dlouhodobého řízení ISVS.
2. Předložit OHA k vyjádření návrhy dokumentací programů obsahujících pořízení nebo technické zhodnocení určených informačních systémů. Tato povinnost se plní standardními formuláři Ministerstva financí.
3. Předložit OHA k vyjádření investiční záměry akcí pořízení nebo technického zhodnocení určených informačních systémů. Tato povinnost se plní standardními formuláři Ministerstva financí.
4. Předložit OHA k vyjádření projekty určených informačních systémů. Tato povinnost je základním stavebním kamenem schvalování všech projektů, které mají dopad do fungování eGovernmentu. Z povinnosti jsou vyjmuty systémy samospráv sloužící výlučně k samostatné působnosti.
5. Předložit OHA k posouzení před zahájením poskytování služby informačního systému veřejné správy provozní dokumentaci určeného informačního systému. Tato povinnost může být i vyžádána útvarem OHA a má zabránit spuštění služby, která by byla v rozporu s dlouhodobým řízením ISVS a podmínkami ve stanoviscích odboru OHA.

Veškeré povinnosti dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy jsou uvedeny v následující tabulce, kde by si každý úřad měl zjistit, kdo je na jeho straně odpovědný za danou povinnost.

Část zákona č. 365/2000 Sb.	**Téma**	**Věcná odpovědnost**	**Oblast**	**Odpovědnost na straně OVS**
§ 4 odst. 1 písm. a)	Národní architektura eGovernmentu	Ministerstvo ve spolupráci s orgány veřejné správy	Vyhledávání, zpracovávání, ukládání a vytváření nových informací, které jsou znalostní základnou pro kvalitní vytváření a rozvoj informačních systémů veřejné správy	
§ 4 odst. 1 písm. b)	Národní architektura eGovernmentu	Ministerstvo ve spolupráci s orgány veřejné správy	Zpracovávání návrhů strategických dokumentů v oblasti informačních systémů veřejné správy, a to i z hlediska bezpečnosti těchto systémů, a předkládání těchto dokumentů vládě, sledování a analýza informační potřeby veřejné správy a stavu informačních systémů veřejné správy	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
§ 4 odst. 1 písm. c)	Tvorba a údržba ISVS	Ministerstvo ve spolupráci s orgány veřejné správy	Příprava nebo koordinace přípravy záměrů pro budování nebo přetváření informačních systémů veřejné správy spravovaných státními orgány nebo informačních systémů veřejné správy spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu přenesené působnosti, vyvolané společnou potřebou více správců informačních systémů veřejné správy	
§ 4 odst. 1 písm. d)	Tvorba a údržba ISVS	Ministerstvo ve spolupráci s orgány veřejné správy	Příprava nebo koordinace přípravy záměrů pro budování nebo přetváření informačních systémů veřejné správy spravovaných státními orgány nebo informačních systémů veřejné správy spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu přenesené působnosti, vyvolané potřebou spolupráce a koordinace na mezinárodní úrovni	
§ 4 odst. 1 písm. e)	Návrhy dokumentací programů	Ministerstvo ve spolupráci s orgány veřejné správy	Vyjadřování se k návrhům dokumentací programů obsahujících pořízení nebo technické zhodnocení určených informačních systémů vypracovaných podle zvláštního právního předpisu. Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele dokumentace programu a k potřebám zajištění řádného výkonu veřejné správy	
§ 4 odst. 1 písm. f)	Národní architektura eGovernmentu	Ministerstvo ve spolupráci s orgány veřejné správy	Zajištění tvorby metodických pokynů pro výkon odborných činností spojených s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
§ 4 odst. 1 písm. g)	Národní architektura eGovernmentu	Ministerstvo ve spolupráci s orgány veřejné správy	Koordinace a vytváření podmínek pro činnost veřejné správy prostřednictvím veřejně přístupných informačních systémů veřejné správy, včetně dálkového přístupu	
§ 4 odst. 1 písm. h)	Kontaktní místo veřejné správy	Ministerstvo ve spolupráci s orgány veřejné správy	Koordinace a vytváření podmínek pro činnost kontaktních míst veřejné správy.	
§ 4 odst. 2 písm. a)	Kontrola a vydávání stanovisek	Ministerstvo	Kontroluje u orgánů veřejné správy dodržování povinností stanovených zákonem č. 365/2000 Sb.	
§ 4 odst. 2 písm. b)	Kontrola a vydávání stanovisek	Ministerstvo	Vyjadřuje se k investičním záměrům akcí pořízení nebo technického zhodnocení určených informačních systémů. Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele investičních záměrů akcí a k potřebám zajištění řádného výkonu veřejné správy	Je zodpovědné MVČR
§ 4 odst. 2 písm. c)	Kontrola a vydávání stanovisek	Ministerstvo	Vykonává působnost stanovenou tímto zákonem v oblasti akreditace a atestací	
§ 4 odst. 2 písm. d)	Referenční rozhraní	Ministerstvo	Stanoví a spravuje referenční rozhraní a ve Věstníku ministerstva zveřejní pravidla užívání referenčního rozhraní	
§ 4 odst. 2 písm. e)	Kontrola a vydávání stanovisek	Ministerstvo	Ukládá správní tresty za přestupky	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
§ 4 odst. 2 písm. f)	Kontrola a vydávání stanovisek	Ministerstvo	Ukládá opatření směřující k nápravě nedostatků	
§ 4 odst. 2 písm. g)	Kontrola a vydávání stanovisek	Ministerstvo	Vyjadřuje se k projektům určených informačních systémů spravovaných státními orgány nebo určených informačních systémů spravovaných orgány územních samosprávných celků, které slouží k výkonu přenesené působnosti	
§ 4 odst. 2 písm. h)	Kontrola a vydávání stanovisek	Ministerstvo	Posuzuje, zda informační systémy veřejné správy splňují požadavky kladené na ně právními předpisy upravujícími informační nebo komunikační technologie, informační koncepcí orgánu veřejné správy a provozní dokumentací, a jde-li o informační systémy veřejné správy spravované orgány veřejné správy, pro něž jsou závazná usnesení vlády, rovněž informační koncepcí České republiky a jinými usneseními vlády týkajícími se informačních nebo komunikačních technologií	
§ 4 odst. 2 písm. i)	Kontrola a vydávání stanovisek	Ministerstvo	Vydává Věstník ministerstva, v němž uveřejňuje metodické pokyny, seznam atestačních středisek, udělení osvědčení o akreditaci a udělení atestů a další dokumenty vztahující se k informačním systémům veřejné správy. Vydávání Věstníku ministerstva zabezpečuje ministerstvo prostřednictvím portálu veřejné správy	
§ 4 odst. 2 písm. j)	Kontrola a vydávání stanovisek	Ministerstvo	Konzultuje návrhy metodických pokynů zejména s dotčenými osobami nebo jejich součástmi formou veřejné konzultace, jejímž cílem je získání stanovisek a	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
			připomínek dotčených osob nebo jejich součástí k předmětnému návrhu, a za tímto účelem zřídí a spravuje informační systém, kde způsobem umožňujícím dálkový přístup uveřejňuje návrhy metodických pokynů, umožňuje předkládání připomínek a uveřejňuje výsledek konzultace	
§ 4 odst. 2 písm. k)	Kontrola a vydávání stanovisek	Ministerstvo	Kontroluje výkon působnosti kontaktních míst veřejné správy	
§ 4 odst. 2 písm. l)	Centrální místo služeb	Ministerstvo	Spravuje centrální místo služeb	
§5 odst. 1	Tvorba a údržba ISVS	Orgán veřejné správy	Orgány veřejné správy v rozsahu své zákonné působnosti provádějí výběr technických a programových prostředků a dalších produktů pro provoz jimi vytvářených a spravovaných informačních systémů veřejné správy; to neplatí, předpokládá-li informační koncepce České republiky užití produktu určitých vlastností.	
§ 5 odst. 2 písm. a	Kontrola a vydávání stanovisek	Orgán veřejné správy	Spolupracovat s ministerstvem při plnění jeho úkolů	
§ 5 odst. 2 písm. b	Kontrola a vydávání stanovisek	Orgán veřejné správy	Předložit ministerstvu k vyjádření návrhy dokumentací programů obsahujících pořízení nebo technické zhodnocení určených informačních systémů vypracovaných podle zvláštního právního předpisu a investiční záměry akcí pořízení nebo technického zhodnocení určených informačních systémů. Povinnost podle věty první se nevztahuje na	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
			technické zhodnocení určeného informačního systému spočívající jen ve změnách nemajících vliv na vnitřní vazby tohoto určeného informačního systému nebo na vazby na jiné informační systémy veřejné správy	
§ 5 odst. 2 písm. c	Kontrola a vydávání stanovisek	Orgán veřejné správy	Předložit ministerstvu před zahájením poskytování služby informačního systému veřejné správy jimi spravovaným určeným informačním systémem nebo na žádost ministerstva provozní dokumentaci určeného informačního systému k posouzení, zda určený informační systém splňuje požadavky kladené na něj právními předpisy upravujícími informační nebo komunikační technologie, informační koncepcí orgánu veřejné správy a provozní dokumentací, a jde-li o informační systém veřejné správy spravovaný orgánem veřejné správy, pro něhož jsou závazná usnesení vlády, rovněž informační koncepcí České republiky a jinými usneseními vlády týkajícími se informačních nebo komunikačních technologií; část věty před středníkem se použije pouze v případě určených informačních systémů spravovaných státními orgány nebo určených informačních systémů spravovaných orgány územních samosprávných celků, které slouží k výkonu přenesené působnosti,	
§ 5 odst. 2 písm. d	Tvorba a údržba ISVS	Orgán veřejné správy	Zajistit, aby vazby jimi spravovaného informačního systému veřejné správy s výjimkou provozního informačního systému na informační systémy veřejné správy jiného správce byly uskutečňovány prostřednictvím referenčního	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
			rozhraní. Toto ustanovení se nevztahuje na vazby mezi jimi spravovanými informačními systémy veřejné správy a informačními systémy veřejné správy vedenými zpravodajskými službami,	
§ 5 odst. 2 písm. e	Kontrola a vydávání stanovisek	Orgán veřejné správy	Odstranit zjištěné nedostatky ve lhůtě stanovené ministerstvem,	
§ 5 odst. 2 písm. f	Kontrola a vydávání stanovisek	Orgán veřejné správy	Předložit ministerstvu k vyjádření a v případě určených informačních systémů spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu samostatné působnosti, na vědomí projekty určených informačních systémů; část věty před středníkem se nepoužije v případě technického zhodnocení určeného informačního systému spočívajícího jen ve změnách nemajících vliv na vnitřní vazby tohoto určeného informačního systému nebo na vazby na jiné informační systémy veřejné správy,	
§ 5 odst. 2 písm. g	Kontrola a vydávání stanovisek	Orgán veřejné správy	Uskutečnit programy obsahující pořízení nebo technické zhodnocení určených informačních systémů, jejichž návrhy dokumentace jsou povinny předložit ministerstvu k vyjádření, investiční záměry akcí pořízení nebo technického zhodnocení určených informačních systémů, které jsou povinny předložit ministerstvu k vyjádření, a projekty určených informačních systémů, které jsou povinny předložit ministerstvu k vyjádření, až po souhlasném vyjádření ministerstva nebo souhlasném rozhodnutí vlády	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
§ 5 odst. 2 písm. h	Kontrola a vydávání stanovisek	Orgán veřejné správy	Oznámit ministerstvu zahájení zkušebního provozu určeného informačního systému souvisejícího s jeho pořízením nebo technickým zhodnocením před tím, než tato skutečnost nastane, vést záznam o průběhu zkušebního provozu a zpřístupnit záznam ministerstvu dálkovým přístupem; část věty před středníkem se nepoužije v případě zkušebního provozu souvisejícího s technickým zhodnocením určeného informačního systému spočívajícím jen ve změnách nemajících vliv na vnitřní vazby tohoto určeného informačního systému nebo na vazby na jiné informační systémy veřejné správy,	
§ 5 odst. 2 písm. i	Kontrola a vydávání stanovisek	Orgán veřejné správy	Zahájit poskytování služby informačního systému veřejné správy jím spravovaným určeným informačním systémem až po vyjádření ministerstva, že určený informační systém splňuje požadavky kladené na něj právními předpisy, informační koncepcí orgánu veřejné správy a provozní dokumentací, a jde-li o informační systém veřejné správy spravovaný orgánem veřejné správy, pro něhož jsou závazná usnesení vlády, rovněž informační koncepcí České republiky a jinými usneseními vlády týkajícími se informačních systémů veřejné správy; část věty před středníkem se nepoužije na službu informačního systému veřejné správy, která se týká výlučně výkonu samostatné působnosti,	
§ 5 odst. 2 písm. j	Tvorba a údržba ISVS	Orgán veřejné správy	Provádět hodnocení ekonomické výhodnosti způsobu provozu jimi spravovaných informačních systémů veřejné správy,	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
§ 5 odst. 2 písm. k	Tvorba a údržba ISVS	Orgán veřejné správy	Provádět před pořízením informačního systému veřejné správy nebo v rámci technického zhodnocení anebo rozvoje jimi spravovaného informačního systému veřejné správy hodnocení ekonomické výhodnosti jeho provozu.	
§ 5 odst. 3	Kontrola a vydávání stanovisek	Ústřední správní úřady	Ústřední správní úřady zveřejňují věstníky vydávané ve své působnosti na portálu veřejné správy	
§ 5 odst. 7	Tvorba a údržba ISVS	Orgán veřejné správy	Orgány veřejné správy mohou při zkušebním provozu informačního systému veřejné správy využívat v nezbytném rozsahu údaje, které se v informačním systému veřejné správy vedou nebo povedou nebo které jsou nebo budou v souvislosti s poskytováním služby informačního systému veřejné správy využívány.	
§ 5a odst. 1	Dlouhodobé řízení ISVS	Ministerstvo	Ministerstvo vytváří a předkládá vládě ke schválení informační koncepci České republiky. Informační koncepce České republiky stanoví cíle České republiky v oblasti informačních systémů veřejné správy a obecné principy pořizování, technického zhodnocení, vytváření, správy, provozování, užívání a rozvoje informačních systémů veřejné správy v České republice na období 5 let.	
§ 5a odst. 2	Dlouhodobé řízení ISVS	Orgán veřejné správy	Orgány veřejné správy vytvářejí a vydávají informační koncepci orgánu veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. V informační koncepci orgánu veřejné správy orgány veřejné správy stanoví své	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
			dlouhodobé cíle v oblasti řízení spravovaných informačních systémů veřejné správy a vymezí obecné principy pořizování, technického zhodnocení, vytváření, správy, provozování, užívání a rozvoje svých informačních systémů veřejné správy. V případě orgánů téhož územního samosprávného celku se vytváří jedna informační koncepce pro všechny orgány územního samosprávného celku. Orgány veřejné správy předkládají informační koncepci orgánu veřejné správy do 3 měsíců ode dne jejího vydání nebo aktualizace ministerstvu. Strukturu a náležitosti informační koncepce orgánu veřejné správy, jakož i postupy orgánů veřejné správy při jejím vytváření, vydávání a při vyhodnocování jejího dodržování, požadavky na řízení informačních systémů veřejné správy, včetně bezpečnostních úrovní a dekomponování informačních systémů veřejné správy, technické požadavky na informační systémy veřejné správy, pravidla pro strukturování dat v informačních systémech veřejné správy a bezpečnostní požadavky na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy spravovaných orgány veřejné správy, které nejsou orgány nebo osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti podle zákona upravujícího kybernetickou bezpečnost, stanoví prováděcí právní předpis.	
§ 5a odst. 3	Dlouhodobé řízení ISVS	Orgán veřejné správy	Na základě vydané informační koncepce orgánu veřejné správy orgány veřejné správy vytvářejí a vydávají provozní dokumentaci	

Část zákona č. 365/2000 Sb.	Téma	Věcná odpovědnost	Oblast	Odpovědnost na straně OVS
			k jednotlivým informačním systémům veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. Strukturu a náležitosti provozní dokumentace stanoví prováděcí právní předpis.	
§ 5a odst. 4	Dlouhodobé řízení ISVS	Orgán veřejné správy	Orgány veřejné správy si zajistí atestaci dlouhodobého řízení informačních systémů veřejné správy s výjimkou provozních informačních systémů a prokáží splnění povinností atestem dlouhodobého řízení informačních systémů veřejné správy. Rozsah provozní dokumentace předkládané při atestaci stanoví prováděcí právní předpis. Povinnost podle věty první se nevztahuje na obce, které vykonávají přenesenou působnost pouze v základním rozsahu.	
§ 5b odst. 1	Dlouhodobé řízení ISVS	Orgán veřejné správy	Orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.	
§ 5b odst. 2	Dlouhodobé řízení ISVS	Orgán veřejné správy	Orgány veřejné správy při využívání cloud computingu postupují podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost.	

Obecně musí úřad strategicky řídit rozvoj a provoz svých ICT v souladu s plánovaným rozvojem eGovernmentu a proto je předkládá připravené projekty k vyjádření odpovědnému orgánu. OHA rovněž povoluje spuštění služby na základě žádosti úřadu.

Poznámka: Ve všech krocích může mít útvar OHA připomínky či jiné poznámky, které je úřad povinen reflektovat a odstranit.

Informační koncepce:

Úřady vytvářejí a vydávají informační koncepci orgánu veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. V informační koncepci orgánu veřejné správy orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení spravovaných informačních systémů veřejné správy a vymezí obecné principy pořizování, technického zhodnocení, vytváření, správy, provozování, užívání a rozvoje svých informačních systémů veřejné správy.

► § 5a odst. 2 zákona č. 365/2000 Sb. o informačních systémech veřejné správy

► Aktuální znění Informační koncepce ČR vychází z usnesení vlády č. 644 ze dne 15. června 2020.

IKČR definuje celkem 34 principů a zásad, které jsou uvedeny s vysvětlujícími odkazy níže. K naplnění jednotlivých principů směřují povinnosti dle Národního architektonického plánu a naplnění jednotlivých zásad popisují Metody řízení ICT veřejné správy.

Principy IKČR	**Zásady IKČR**
Standardně digitalizované	Na prvním místě je klient
Zásada „pouze jednou“	Standardy plánování a řízení ICT
Podpora začlenění a přístupnost	Strategické řízení pomocí IK OVS
Otevřenost a transparentnost	Řízení architektury
Přeshraniční přístup jako standard	Řízení požadavků a změn
Interoperabilita jako standard	Řízení výkonnosti a kvality
Důvěryhodnost a bezpečnost	Řízení zodpovědnosti za služby a systémy
Jeden stát	Řízení katalogu služeb
Sdílené služby veřejné správy	Udržení interních kompetencí
Připravenost na změny	Procesní řízení
eGovernment jako platforma	Řízení přínosů a hodnoty
Vnitřně pouze digitální	Řízení kapacit zdrojů
Otevřená data jako standard	Nezávislost návrhu, řízení a kontroly kvality
Technologická neutralita	Vztah informatiky a legislativy

Uživatelská přívětivost	Řízení financování ICT
Konsolidace a propojování informačních systémů veřejné správy	Využívání otevřeného software a standardů
Omezení budování monolitických systémů	Podpora vyváženého partnerství s dodavateli

Provozní dokumentace

Na základě vydané informační koncepce orgánu veřejné správy orgány veřejné správy vytvářejí a vydávají provozní dokumentaci k jednotlivým informačním systémům veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. Strukturu a náležitosti provozní dokumentace stanoví prováděcí právní předpis.

► § 5a odst. 3 zákona č. 365/2000 Sb. o informačních systémech veřejné správy

Projekty určených informačních systémů

Orgány veřejné správy jsou v rámci informačních systémů veřejné správy povinny předložit ministerstvu k vyjádření a v případě určených informačních systémů spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu samostatné působnosti, na vědomí projekty určených informačních systémů; část věty před středníkem se nepoužije v případě technického zhodnocení určeného informačního systému spočívajícího jen ve změnách nemajících vliv na vnitřní vazby tohoto určeného informačního systému nebo na vazby na jiné informační systémy veřejné správy,

► § 5 odst. 2 písm. f) zákona č. 365/2000 Sb. o informačních systémech veřejné správy

Atestace

Orgány veřejné správy si zajistí atestaci dlouhodobého řízení informačních systémů veřejné správy.

► § 5a odst. 4 zákona č. 365/2000 Sb. o informačních systémech veřejné správy

2.2 Klíčové otázky

1)	**Má úřad platnou informační koncepci a je schválená nejvyšším vedením úřadu?** *Je potřeba si vyžádat dokument Informační koncepce a zjistit, kdo a jak ji schválil.*
2)	**Je informační koncepce v souladu se systémem řízení kvality úřadu?** *Je potřeba si vyžádat dokumenty Informační koncepce a Strategie rozvoje úřadu / systém řízení kvality ve služebních úřadech a zjistit, zda jsou tyto dokumenty v souladu. Tedy zda na sebe vzájemně odkazují, zda mají nastaveny mechanismy aktualizací a zda pracují se stejnými rozvojovými aktivitami.*
3)	**Vede úřad evidenci svých ISVS a vede k nim provozní dokumentaci?** *Je potřeba si vyžádat dokument Informační koncepce a porovnat seznam informačních systémů v ní vedený se stavem ohlášení v registru práv a povinností na adrese*

	https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs a zde ke každému systému existuje provozní dokumentace splňující požadavky vyhlášky k zákonu č. 365/2000 Sb.
4)	**Existuje atest dlouhodobého řízení informačních systémů veřejné správy v rámci úřadu?** *Je potřeba si vyžádat dokument Atestace dlouhodobého řízení ISVS a zjistit, zda je stále platný.*
5)	**Má úřad vnitřní pokyn, který stanoví uplatňování informační koncepce v praxi včetně pravidelného hodnocení stanovených cílů?** *Je potřeba si vyžádat dokument interní akt řízení, případně organizační řád, který popisuje a stanoví práva a povinnosti v podobě správy Informační koncepce.*
6)	**Předkládá úřad informační koncepci do 3 měsíců ode dne jejího vydání nebo aktualizace odboru OHA?** *Je potřeba si vyžádat dokument interní akt řízení, případně organizační řád a zjistit, kdo je zodpovědný za procesy týkající se Informační koncepce. Následně zjistit, zda byla splněna povinnost předložení této koncepce zodpovědným útvarem.*
7)	**Je informační koncepce úřadu pravidelně aktualizovaná a v souladu s Informační koncepcí ČR?** *Je potřeba si vyžádat dokumenty Informační koncepce a atestace dlouhodobého řízení ISVS a zjistit, zda je Informační koncepce aktualizovaná a zda obsahuje provazbu na Informační koncepci ČR, což je povinnost dle Čl. 2 bod 2. zákona č. 104/2017 Sb.*
8)	**Existují souhlasná vyjádření odboru OHA ke všem projektům určených informačních systémů?** *Je potřeba si vyžádat dokumenty Informační koncepce a Stanoviska OHA a porovnat, zda plánované projekty a záměry z informační koncepce byly realizovány a existují k nim souhlasná stanoviska OHA.*
9)	**Eviduje úřad harmonogram náprav nedostatků, které OHA odhalilo v rámci posuzování projektů, informační koncepce, provozní dokumentace, dokumentace programů či investičních záměrů úřadu a provádí jejich nápravu?** *Je potřeba si vyžádat dokumenty Stanoviska OHA a zjistit, zda jsou ve stanoviscích vyžadovány některé nápravy, které má úřad povinnost odstranit dle § 5 odst. 2 písm. e) zákona č. 365/2000 Sb. Následně zda existuje zodpovědný útvar, který eviduje a kontroluje nápravu těchto nedostatků.*
10)	**Vede úřad evidenci všech ICT projektů, ve které je zřejmé, v jaké je projekt fázi?** *Je potřeba si vyžádat dokument organizační řád a zjistit, kdo je zodpovědný za projektové řízení. Následně si vyžádat výstup z evidence projektů, které se zabývají ICT. Tento výstup se dá použít pro porovnávání dle otázky č. 8.*

2.3 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Dlouhodobé řízení ISVS – obec s rozšířenou působností

Vzhledem k potřebě usnadnit občanům obce komunikaci s úřadem (OVS), bylo rozhodnuto zahájit digitalizaci služeb úřadu. Před zahájením každého projektu byla konfrontována informační koncepce a strategie rozvoje úřadu. Zjistilo se, že poslední změna informační koncepce proběhla před 2 lety a nepočítala s takovýmto rozhodnutím.

Úřad zajistil aktualizaci informační koncepce, aby reflektovala i požadavky informační koncepce ČR a předložil ji Ministerstvu vnitra (OHA).
Na základě aktualizace informační koncepce byly vybrány projekty, které je nutné zrealizovat pro dosažení požadovaného cíle. Projekty, které byly výlučně v samostatné působnosti, úřad odeslal Ministerstvu vnitra pouze pro informaci, ostatní byly zpracovány jako plnohodnotná žádost o stanovisko OHA. Po obdržení souhlasného stanoviska OHA se začalo s výběrem dodavatele a realizací projektu.
V průběhu realizace dodavatel implementoval nové služby a připravil je k uvedení do běžného/rutinního provozu. Úřad požádal ministerstvo vnitra o stanovisko ke spuštění těchto služeb do běžného/rutinního provozu a současně se žádostí předložil provozní dokumentaci těchto služeb. Obec zahájila provoz služeb po obdržení souhlasného stanoviska Ministerstva vnitra.

Protože obec plánovala projekty dle své informační koncepce, nemohlo se stát, že by se realizovaly projekty, které by nezapadaly do celkové architektury a vize obce.
Protože obec od začátku konzultovala projektový záměr s ministerstvem vnitra a realizaci projektu zahájila až po obdržení kladného stanoviska, byl projekt realizován v souladu s architektonickými principy Národního architektonického plánu a do řešení byly zahrnuty všechny požadované centrální sdílené služby eGovernmentu.
Obec využitím centrálních sdílených služeb uspořila část nákladů, neboť nemusela samostatně řešit jejich implementaci, ale využila již hotové řešení.

▸ Příklad špatné praxe

Dlouhodobé řízení ISVS – ústřední správní úřad

Ústřední správní úřad dostal dle legislativní změny povinnost implementovat nový informační systém pro podporu sběru požadavků od občanů. Jelikož se jednalo o legislativní požadavek, neposuzoval úřad soulad se svou informační koncepcí a pustil se rovnou do realizace projektu.
Úřad připravil zadávací dokumentaci a uskutečnil výběrové řízení, na jehož základě vybral vítězného uchazeče. Ten zahájil implementaci požadovaného řešení. V půlce realizace obdržel úřad dotaz od vlády na postup projektu a dodržování stanoveného harmonogramu, načež byl konfrontován, zda má na projekt souhlasné stanovisko ministerstva vnitra.
Úřad toto souhlasné posouzení neměl, a tak kontaktoval ministerstvo vnitra s žádostí o dodatečné posouzení. Ministerstvo vnitra této žádosti vyhovět nemohlo, protože byl porušen nastavený postup schvalování, nicméně připustilo dodatečné konsultace. Při dodatečných konzultacích bylo nalezeno několik nedostatků v původním návrhu, které nakonec znamenaly výrazné zásahy do projektu, jeho prodražení a prodloužení. Jednalo se například o nedodržení povinnosti čerpání údajů o fyzických osobách z registru obyvatel.

Protože úřad mylně vycházel s předpokladu, že legislativní povinnost realizovat změnu jej vyvazuje z jiné zákonné povinnosti vůči rozvoji ISVS, unikly mu při realizaci projektu podstatné skutečnosti, které by byly odhaleny, pokud by postupoval v souladu s pravidly dlouhodobého řízení ISVS.

3 Architektura úřadu

Tato kapitola se zabývá postavením a významem architektury v úřadu a jejím praktickým uplatněním. Architektura je často mylně vnímána jako nadbytečná zátěž úřadu, její složitost k tomu vybízí. Nicméně úřad odpovídá za kvalitu výkonu svých služeb a orientaci na služby klientům.

Architektura úřadu je nápomocná při pochopení fungování služeb úřadu občanům, způsobu využívání a dostupnosti těchto služeb a nakonec i vnitřního uspořádání organizace, jeho agend, odpovědností a způsobu informatické podpory až do úrovně technologií.

Aby byl úřad úspěšný při naplňování cílů digitalizace veřejné správy, musí vědět, jak funguje, co hodlá zlepšit, a jak toho chce dosáhnout. Proto by měl mít povinně strategii rozvoje úřadu / systém řízení kvality ve služebních úřadech a také informační koncepci úřadu. Informační koncepce ČR definuje cíle a principy, které vymezují povinnosti úřadu ve vztahu k digitalizaci a optimalizaci fungování veřejné správy, prostřednictvím architektury úřadu.

Předpokladem pro začátek tvorby architektury je, že úřady znají strukturu svých informačních aktiv a také svých agend, procesů a vnitřní organizaci. Tedy znají jednotlivé prvky, které tvoří architekturu úřadu. Úřad by ji měl řádně popsat, doplnit souvislosti a vazby jednotlivých prvků s využitím nástroje a metodik k tomu určených a publikovaných v metodických pokynech Národní architektury eGovernmentu.

Architektura úřadu
Architektura úřadu jako manažerská metoda je prostředkem celostního poznávání organizace na podporu rozhodování, zejména při plánování strategických změn, ale také na podporu řízení výkonnosti, kvality a zodpovědnosti.
Představuje popis struktury a chování úřadu (kdo jsme), plánovaných změn (odkud a kam jdeme) a jejich informatické podpory (k čemu nám je a má být ICT jako celek a jednotlivé informační systémy veřejné správy). Základními vodítky a nadřazenými strategiemi jsou:
► Národní architektonický rámec, navazující dokument IKČR dle usnesení vlády ČR ze dne 3. října 2018 č. 629
► Národní architektonický plán, navazující dokument IKČR dle usnesení vlády ČR ze dne 3. října 2018 č. 629

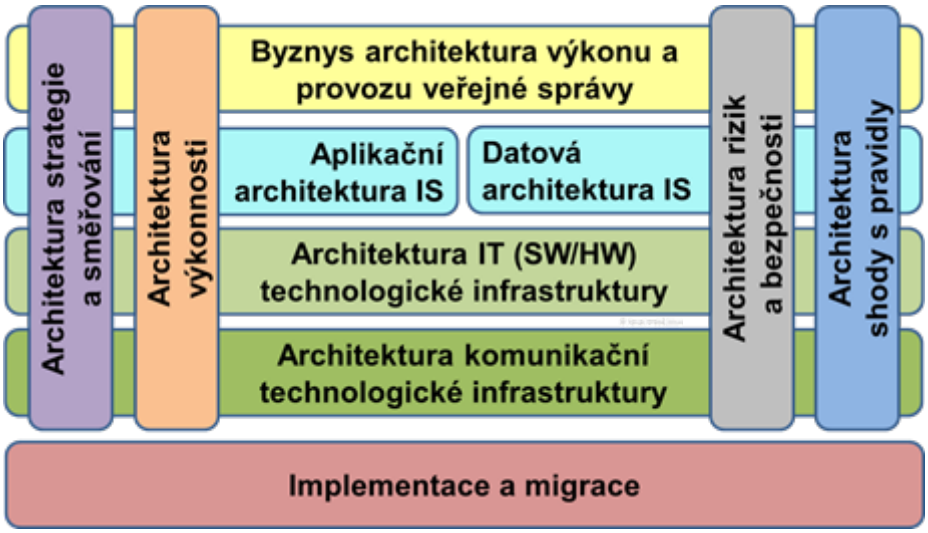
K čemu může úřad využít zpracovanou architekturu úřadu:

- Rozhodování o prioritách digitalizace úřadu při vědomí všech souvislostí a znalosti zdrojů a relevantních nákladech.
- Podpora zavádění systému řízení úřadu (systém řízení kvality ve služebních úřadech). Architektura popisuje toky dat, vazby agend na informační systémy, komunikace úřadu s veřejností, apod.
- Kvalifikované zdůvodnění žádostí o investiční záměry.
- Řízení změn – architektura zná všechny souvislosti při zavádění změn a odhalí skryté náklady, nebo rizika.
- Odůvodnění žádostí při povinném posuzování odborem Hlavního architekta eGovernmentu.
- Zásadním významem je strukturovaný přehled o všech níže uvedených vrstvách architektury a jejich provázaností. Na jeho základě lze zpracovávat povinnou provozní dokumentaci, vypisovat specifikaci výběrových řízení a stanovat optimální způsoby řízení a správy ICT.
- Srozumitelně zpracovaná architektura slouží jako prostředek pro komunikaci s vedením úřadu ale i nastavení informačních vazeb s jinými úřady.

- Architektura odhalí skryté vazby a zabrání nehospodárnému vynakládání prostředků. Úřady mají tendenci řešit projekty ICT izolovaně, což často vede k více nákladům vzniklým požadavky na dopracování.

Význam a užití jednotlivých vrstev architektury

Architektura úřadu dle Národního architektonického rámce[7] se člení do jednotlivých domén, které popisuje následující obrázek. Následující popisy domén jsou uváděny v přehledové úrovni, smyslem je pochopení jejich účelu v kontextu digitalizace úřadu-



Horizontální (hlavní, klíčové) **domény, vrstvy,** architektury úřadu vyjadřují všechny základní prvky existence organizace, tj. její fungování a její zdroje (zde stále zaměřené převážně na ICT zdroje). Tedy koncepty poskytující odpověď na otázku **Co tvoří naši organizaci?** Těmito koncepty jsou:

- Byznys architektura – popisuje služby, procesy, organizaci úřadu s přiřazením rolí a zodpovědností. Odpovídá zejména na otázky: Co náš úřad dělá? Jaké agendy a činnosti vykonává? Jaké poskytuje služby? Kdo má jaké role a odpovědnosti? Kdo má s kým komunikovat?
- Architektura informačních systémů, členěná na:
    - Informační (datovou). Odpovídá zejména na otázky: Jaká data úřad zpracovává? V jakých informačních systémech jsou data zpracovávána? Jak jsou data klasifikována? Odkud data pochází? Komu je úřad poskytuje?
    - Aplikační architekturu. Odpovídá zejména na otázky: Jaké informační systémy (IS) úřad spravuje? Jak jsou IS klasifikovány? Kdo IS spravuje a provozuje? Jaké funkce IS vykonává a jak jsou vázány na procesy a služby úřadu? Jaký je systém identifikace v IS? Kdo má k IS a datům přístup a jaký? Jaké licence úřad užívá a vlastní?
- Technologická architektura, členěná na:
    - Architekturu IT technologií – popisuje jednotlivé IT platformy hardwarového a softwarového vybavení včetně vazeb na jednotlivé aplikace. Odpovídá zejména na otázky: Jaké služby platformy poskytují? Jaké politiky platformy musí splňovat? Kdo platformy spravuje a provozuje a kde jsou umístěny?

[7] Architektura úřadu v kontextu veřejné správy a jejích vrstvách architektury – uvádí popisy pravidel jednotlivých vrstev architektury.

- Architekturu komunikační infrastruktury – popisuje služby a strukturu komunikačních sítí a technických prostředků včetně technologických center. Odpovídá zejména na otázky: Jaké komunikační služby úřad využívá? Jaké politiky platformy musí splňovat? Kdo sítě provozuje a jaká jsou komunikační rozhraní. Jaká je dostupnost komunikační infrastruktury?

Vertikální domény motivační architektury, aspekty, doplňují a protínají horizontální architektury vrstev a poskytují odpovědi na otázku ***Proč je naše organizace taková, jaká je?,*** respektive ***Proč by měla být jiná než je?*** Těmito aspekty jsou:

- Architektura strategie a směrování, původně také zvaná jenom motivační architektura. Odpovídá zejména na otázky: Proč je potřeba změna? Jaké jsou cíle změny? Komu je změna určena? Kdo jsou zainteresované osoby? Jaká jsou omezení či potřeby změny?
- Architektura výkonnosti, měřící dosahování strategie i provozní efektivity. Odpovídá zejména na otázky: Je řešení hospodárné, efektivní a účelné? Jaké jsou metriky?
- Architektura rizik a bezpečnosti – postihující specifické bezpečnostní aspekty napříč doménami. Odpovídá zejména na otázky: Jaká jsou rizika? Jak se na bezpečnostní události a incidenty reaguje?
- Architektura shody s pravidly, standardizace a dlouhodobé udržitelnosti.

IK ČR stanovuje v oblasti architektury úřadu dosažení následujícího cíle:

- 5.03 Zavedení principů a postupů „Enterprise architektury“

3.1 Popis optimálního stavu, základní principy a pravidla

Úřad zpracovává architekturu úřadu dle Národního architektonického plánu a v souladu s cíli a principy Informační koncepce ČR. Pro naplnění této povinnosti je potřeba, aby úřad ustanovil odpovědný útvar za rozvoj architektury úřadu a zajistil kompetence a výkon rozdílných a vzájemně se doplňujících rolí (některé role lze zajisti externě):

- Správce architektury úřadu a to ve všech čtyřech úrovních (byznys, aplikační, datová i technologická). Odpovídá za tvorbu a aktualizaci centrálních sdílených (nebo jednotných) služeb a centrálních sdílených (nebo standardizovaných) informatických služeb úřadu.
- Metodik tvorby architektur (přirozený vzor a leader) v jednotlivých organizacích v úřadu, tj. věcný komunikátor s vedením úřadu a správci jednotlivých agend, případně s garanty jednotlivých informačních systémů. Tato role zajišťuje propojení s informační koncepcí úřadu, systémem řízení kvality úřadu a také zajišťuje soulad s nadřazenými strategiemi eGovernmentu. Zajišťuje tvorbu metodik, správu korporátních sdílených znalostí (vzory, návody, referenční modely a praktické příklady)
- Správce prostředků pro sdílení architektonických modelů, obecně architektonických znalostí (architektonické úložiště, portál, wiki, diskusní fóra…).
- Lokální (interní) architekti úřadu odpovídající za svěřenou vrstvu architektury.

Povinnosti úřadu vztahující se ke zpracování architektury úřadu

- Zpracovat informační koncepci úřadu dle § 5a odst. 2 zákona č. 365/2000 Sb. o informačních systémech veřejné správy a s tím související dokumenty.

- Předkládat žádosti o stanovisko na odbor Hlavního architekta eGovernmentu (včetně řešení architektury) - dle zákona č. 365/2000 Sb. a usnesení vlády ze dne 27. 1. 2020 č. 86.
- Vést provozní dokumentaci dle Vyhlášky č. 529/2006 Sb.

Lze očekávat, že předmětem kontrol budou vybrané předkládané ICT projekty a naplnění zásad Národního architektonického plánu a vyhlášeným standardům architektury řešení.

Úřad by měl vést a pravidelně aktualizovat povědomí o úrovni vyspělosti řízení informatiky a jeho vazby na systém řízení kvality úřadu. Tato příručka předkládá návod hodnocení úrovně vyspělosti úřadu měřené z pohledu architektury. (Výchozí zdroj The OpenGroup) Výstup hodnocení slouží jako podklad pro vedoucího ICT nebo Metodika tvorby architektury nebo Digitálního zmocněnce při jednání s vedením úřadu při dokladování dosahování cílů digitalizace úřadu a příležitostí ke zlepšení.

Úrovně vyspělosti architektury úřadu	
Úroveň 1)	Neexistuje architektura úřadu nebo základní vize řízení ICT úřadu. 1. Vedení úřadu nemá povědomí o tom, co je to architektura úřadu a proč by ji měl udržovat a jakou vazbu má na systém řízení kvality úřadu. Úřad nemá vizi rozvoje svých informačních systémů, pouze operativně obnovuje stávající stav ICT dle technologické obnovy nebo legislativních požadavků.
Úroveň 2)	Neformálně řízená architektura úřadu. 1. Řízení ICT na úřadě je závislé na několika jedincích. Neexistuje systematická správa architektury. 2. Úřad disponuje zaměstnanci, kteří mají povědomí o architektuře IS. 3. Nejsou stanoveny architektonické principy, a standardy vedení dokumentace. Standardy jsou vedeny neformálně. 4. Vedoucí pracovníci ICT a vrcholové vedení úřadu není zapojeno do procesu správy architektury úřadu.
Úroveň 3)	Probíhá zavádění procesů správy architektury. 1. Dokumentace ICT je udržovaná, jsou definovány procesy ICT. 2. Architektonická vize a principy jsou definovány. 3. ICT projekty procházejí standardizovaným procesem.
Úroveň 4)	Definovaná architektura 1. Architektura je základně definována a komunikována mezi všemi ICT rolemi na všech vrstvách architektury úřadu. 2. Architektonické principy a zásady jsou stanoveny v souladu s IK ČR. 3. Správa architektury je formalizována a jsou nastaveny odpovědné role za její správu. 4. Rozdílová analýza a plán migrace jsou definovány. Jsou definovány cíle, metody, nástroje k dosažení cílů úřadu v oblasti digitalizace. 5. Informační koncepce a dokumentace se pravidelně aktualizuje a je zveřejněna dle pravidel interních politik.

Úroveň 5)	Řízená a měřitelná architektura úřadu 1. Úřad architekturu využívá jako zažitou součást kultury úřadu. 2. Architektura se pravidelně aktualizuje. Business, aplikační, datová a technologická vrstva je definována. 3. Veškeré ICT investiční záměry úřadu jsou podloženy výstupy z architektury. 4. Finanční plánování a investiční kontroly jsou sestaveny na základě zpětných vazeb a poučení z krizových scénářů architektury úřadu. Proces plánování počítá se začleněním výstupů architektury.
Úroveň 6)	Proaktivní architektura 1. Informační koncepce úřadu a architektonická dokumentace se používá a zohledňuje v celé organizaci v rámci rozhodovacích procesů životního cyklu ICT projektu. 2. Zaměstnanci mají zájem na digitalizaci úřadu a jsou si vědomi významu a přínosů architektury při optimalizaci pracovních procesů. 3. ICT odbor aktivně sbírá a vyhodnocuje business požadavky od koncových klientů (občanů, zaměstnanců úřadů), s technickým správcem a architektem předkládají návrhy na řešení IS. 4. Vrcholové vedení úřadu má přehled o aktuálním stavu informačních systémů na úřadě, na základě business, technických a legislativních požadavků předkládá vedení úřadu finanční plán alokací na zajištění provozu a rozvoje ICT úřadů vyplývající z informační koncepce úřadu.

3.2 Klíčové otázky

1)	**Jak je organizačně zajištěn výkon rolí odpovídající za správu architektury úřadu?** *Je potřeba si vyžádat dokument organizačního řádu úřadu a zjistit, zda je přidělena odpovědnost za architekturu úřadu.*
2)	**Jakou formou spolupracuje vedení úřadu s osobou odpovědnou úřadu za informační koncepci a architekturu? Využívá tyto kompetence vedení úřadu k rozhodování?** *Je potřeba si vyžádat dokument Informační koncepce a organizační řád úřadu a zjistit, zda mají zainteresované strany dostatečná práva a povinnosti.*
3)	**Má úřad zpracovanou architekturu úřadu?** **Je architektura úřadu aktuální/pravidelně aktualizována?** *Je potřeba si vyžádat dokument Informační koncepce úřadu a zjistit, zda je architektura popsaná a jak je nastaven proces její údržby a správy.*
4)	**Existuje záměr posílit využívání architektury vyjádřený v informační koncepci?** *Je potřeba si vyžádat dokumentu Informační koncepce a zjistit, jak a zda je popsána strategie v oblasti architektury.*
5)	**Je architektura úřadu v souladu se systémem řízení kvality ve služebních úřadech?** **Je zajištěn soulad s právními předpisy?** *Je potřeba si vyžádat dokument Strategie rozvoje úřadu / systém řízení kvality ve služebních úřadech a zjistit, zda je v souladu s právními předpisy. Tento dokument je popsán v kapitole 1.*

6)	**V jaké úrovni vyspělosti úřad spravuje a používá architekturu?** *Je potřeba vyhodnotit, ideálně z dokumentu Informační koncepce, v jaké úrovni popsaných v předcházející tabulce se nachází architektura úřadu.*

3.3 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Architektura úřadu - tvorba plánu investic

Vzhledem k potřebě vytvořit plán investic na další rozpočtové období je potřeba nejen prioritizovat projekty z pohledu uživatelských potřeb, dopadů na ICT z hlediska rozsahu změn, jejich proveditelnosti a konečně i nákladů.
Útvar zodpovědný za správu architektury úřadu vypracoval na základě seznamu investičních akcí zprávu o dopadu na současné ICT úřadu a náklady zavádění změn a:

- zpřesnil investiční záměr z hlediska finančního krytí, a dopadů záměru na jiné procesy informační záměry;
- navrhl postup prací tak, aby nebyly dotčeny služby úřadu vůči klientům i vnitřním uživatelům např. z důvodu kolizních požadavků na infrastrukturu.

Útvar architekty byl následně připraven vytvořit kvalifikované podklady pro zadávací dokumentace jednotlivých ICT projektů a přesně specifikoval zadání vůči dodavatelům.

▸ Příklad špatné praxe

Architektura úřadu – žádost o stanovisko odboru Hlavního architekta eGovernmentu

Úřad v rámci svého rozpočtu plánoval investici do ICT. Jelikož úřad nemá organizačně zajištěno interní zpracování architektury, byl upozorněn až svým ekonomickým útvarem, že vydat prostředky na tuto investici lze až po souhlasném posouzení odborem Hlavního architekta eGovernmentu.
Úřad následně zjišťoval, jaké jsou podmínky a náležitosti žádosti, přičemž jedna z nich je i předaná architektura řešení projektu.
Z důvodu neexistence vlastního architekta, byl nucen si najmout externí společnost, která požadovanou architekturu řešení dodala. Při tvorbě a komunikaci s odborem Hlavního architekta eGovernmentu se přišlo i na několik chybějících komponent a propojení, které vyžadují právní předpisy a Národní architektonický plán.
Po souhlasném posouzení a vydání stanoviska nebyl úřad schopen jakkoliv dále užívat výstupy od externí společnosti, nebyl schopen přebrat dodané know-how a architektura řešení časem zastarala. Stala se tak investicí, kterou úřad svým jednáním částečně zhatil.

4 Data a jejich sdílení

Každý informační systém obsahuje data a informace. Ať už se jedná o agendová či neagendová data, vždy platí, že data představují cennou informační hodnotu. Aby bylo možné s daty pracovat maximálně efektivně, musí si úřad vlastnící informační systém zajistit přístup ke všem datům, a to v otevřeném a strojově čitelném formátu, bez dodatečných nákladů a s možností libovolně s daty nakládat. To je podmínkou nejen pro efektivní výkon veřejné správy, ale také pro sdílení dat. Úřady spravují data v informačních systémech v rámci svých činností při výkonu agend. Stejně jako úřad eviduje svůj majetek s péčí řádného hospodáře prostřednictvím karet majetku, měl by evidovat i svá data. Úřad by měl mít přehled, jaká data ve svých agendách vede a co data znamenají (tj. jaký je jejich význam).

Nástrojem pro evidenci dat je datový model úřadu, který obsahuje konceptuální datové modely pro jednotlivé agendy. Generováním schémat a dokumentací z modelů úřad zajistí standardizaci a interoperabilitu dat. Díky tomu může data pochopit kdokoli a správně je využít. Vytvořením modelu tak úřad přispívá k naplnění architektonických principů Interoperabilita jako standard, Připravenost na změny a Konsolidace a propojování informačních systémů veřejné správy.

Naplnění principů a zásad eGovernmentu vyjádřené v IK ČR

Všechna agendová data musí být zaregistrována v Registru práv a povinností (RPP), který dává informaci, jaká data se ve veřejné správě vedou, jaká data jsou vymezena číselníky, zda jsou data veřejná či neveřejná a jak je lze získat. RPP je jedním ze základních registrů, které jsou základním (referenčním) datovým zdrojem údajů o subjektech a objektech ve veřejné správě a také metainformačním systémem o výkonu veřejné správy. Základním registrem je také Registr obyvatel (ROB), Registr osob (ROS) a Registr územní identifikace, adres a nemovitostí (RÚIAN).

Úřad by měl svá data sdílet a využívat sdílená data, čímž dodrží architektonický princip Zásada „pouze jednou“, Otevřenost a transparentnost, Jeden stát a Sdílené služby veřejné správy. Přistupovat ke stejným datům umožňuje více subjektům současně referenční, sdílené a bezpečné rozhraní informačních systémů veřejné správy (tzv. Referenční rozhraní veřejné správy). V rámci tohoto rozhraní lze přistupovat například k datům ze základních registrů, které jsou nezbytným podpůrným nástrojem pro výkon většiny konkrétních agend ve veřejné správě v ČR. Prostřednictvím referenčního rozhraní úřad přistupuje k tzv. Propojenému datovému fondu (PPDF) a Veřejnému datovému fondu (VDF), což mu umožňuje získat potřebné údaje pro výkon agend. Jiným způsobem by data pro výkon agend úřad neměl získávat. Díky těmto datovým fondům si mohou úřady (resp. jejich informační systémy) vyměňovat údaje se zaručenou garancí, v PPDF neveřejné údaje (vč. údajů ze základních registrů) a ve VDF veřejné údaje. Kromě úřadů mohou údaje v PPDF a VDF využít i tzv. soukromoprávní uživatelé údajů, tj. osoby oprávněné podle nějakého právního předpisu využívat takové údaje (např. zdravotní pojišťovny).

V budoucnu je plánován přístup k neveřejným údajům pro kohokoli, kdo se identifikuje a splní stanovené podmínky, skrze tzv. řízený přístup. V této oblasti je připravován samostatný zákon o správě dat veřejného sektoru, který by měl definovat pravidla pro přístup k neveřejným datům za účelem výzkumů, statistických šetření apod.

V souladu s architektonickým principem Otevřená data jako standard by mělo být maximum údajů zveřejněno také jako otevřená data, aby je kromě úřadů mohli využít i komerční subjekty a veřejnost. Všechna otevřená data lze vyhledat na jednom místě, a to v Národním katalogu otevřených dat (NKOD).

IK ČR stanovuje v oblasti strukturovaných dat v informačních systémech a jejich sdílení dosažení následujících cílů:

- 1.05 Zlepšení národního katalogu otevřených dat.
- 3.04 Zkvalitnění, aktualizace a validace obsahu Registru práv a povinností.
- 3.07 Vytvoření základních služeb.
- 5.07 Podpora sdílení údajů agendových systémů pro výkon agendy státní správy v přenesené působnosti.
- 5.09 Propojený datový fond.
- 5.10 Veřejný datový fond.
- 5.11 GeoInformace.

Základní otázky pro tuto kapitolu:

- Je zajištěn přístup k datům?
- Je zřejmé, jaká data jsou vedeny a k čemu jsou potřeba?
- Jsou agendová data úřadu evidována v Registru práv a povinností?
- Jsou sdílena agendová data úřadu a využívána sdílená data z datových fondů?

4.1 Popis optimálního stavu, základní principy a pravidla

Předpokladem pro sdílení dat je zajištění přístupu k datům vedeným v informačních systémech úřadu bez dodatečných finančních nákladů a s možností s daty libovolně nakládat (s výjimkou omezení definovaných právními předpisy). Úřad by měl mít zajištěn přístup k veškerým datům vedeným v databázích ve strojově čitelném a otevřeném formátu, a to prostřednictvím alespoň jedné z následujících možností:

- rozhraní (API), které úřad může kdykoliv využívat alespoň k tomu, aby pomocí sady požadavků získal veškeré údaje ze všech databází ve strojově čitelném a otevřeném formátu ve smyslu § 3a odst. 1 a 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. K API musí mít úřad k dispozici vždy aktuální a kompletní dokumentaci popisující syntaxi a sémantiku jeho datových struktur a syntaxi, sémantiku a způsob přístupu k operacím, které API nabízí.
- export kompletního obsahu databází na požádání nebo v pravidelných intervalech ve strojově čitelném a otevřeném formátu ve smyslu § 3a odst. 1 a 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Datový fond úřadu

Všechny údaje spravované v informačních systémech úřadu, tvoří tzv. datový fond úřadu. Základní jsou údaje o subjektech (klientech, dodavatelích, zaměstnancích, apod.) a o objektech práva (evidovaná vozidla, kulturní památky, hospodářská zvířata, vl. majetek úřadu, apod.), které představují tzv. datový kmen úřadu.

Údaje o řízeních (operacích, úkonech) se subjekty nebo nad objekty veřejné správy se nazývají transakční data úřadu. Údaje o subjektech a objektech úřady využívají při výkonu agend (například agenda občanských průkazů, agenda ochrany veřejného zdraví, atd.). Všechny údaje vedené v určité agendě dle § 51 zákona č. 111/2009 Sb., o základních registrech musí být zapsány v Registru práv a povinností (RPP). Díky tomu má kdokoli přehled o tom, jaké údaje se v agendě vedou z hlediska právního vymezení a jak je k nim možné přistoupit.

Přehled údajů evidovaných v agendách lze dohledat v rozcestníku (listu „údaje“ u dané agendy) nebo v otevřených datech z RPP. V RPP je veden také rejstřík informačních systémů veřejné správy (ISVS), který poskytuje seznam informačních systémů a jejich vazeb na agendy. Úřady, které jsou správcem informačního systému, mají povinnost, dle § 52c zákona č. 111/2009 Sb., zapisovat údaje o spravovaném informačním systému do rejstříku ISVS a ohlašovat změny údajů vedených v tomto rejstříku.

Základní povinnosti úřadu k evidenci údajů ve svých agendách

Úřady mají povinnost v RPP odlišit veřejné a neveřejné údaje vedené v agendě, jak vyplývá z § 51 odst. 6 písm. k zákona č. 111/2009 Sb. (účinnost od 1. 2. 2022). Úřady evidují údaje prostřednictvím agendového IS RPP Působnostní (část VI. Údaje agendy) a musí při evidenci údajů v RPP postupovat dle metodiky definice údajů vedených v agendě ve vazbě na subjekty a objekty práva. Tato metodika vychází z principů modelování dle významu dat, který je definován v legislativě či jiných dokumentech.

Pro popis údajů je proto vhodné pro danou agendu vytvořit konceptuální datový model dle významu dat a udržovat jej aktuální ve vazbě na platnou legislativu. Konceptuální datový model poskytuje úřadu přehled, jaké údaje ve svých agendách vede a co údaje znamenají. Díky tomu, že je konceptuální datový model vázán na pojmy v legislativě, umožňuje rychleji reagovat na případné změny legislativy a udržuje know-how nezávisle na personálním obsazení úřadu.

Tvorba konceptuálního datového modelu

Proč by měl úřad popisovat význam a jaké nástroje je možné pro tvorbu modelu využít, se mohou úřady dozvědět na specializovaném školení, které je poskytováno zdarma. Z principů modelování vychází i metodika pro definici údajů za účelem jejich evidence v Registru práv a povinností.

► Metodika definice údajů vedených v agendě
► Školení Modelování významu dat ve veřejné správě

Využívání údajů datového fondu ČR

Z konceptuálního datového modelu agendy vyplývá i vazba na údaje, které vedou jiné úřady. Pokud úřad nebo soukromoprávní uživatel údajů identifikuje potřebu využívat veřejné i neveřejné údaje jiných úřadů v rozsahu potřebném k provedení úkonu pro výkon agendy, může dle § 5 a § 5a zákona č. 111/2009 Sb. požádat v agendovém IS RPP Působnostní (část VII. Oprávnění k údajům a VIII. Využití veřejných údajů) o využívání údajů vedených v základním registru nebo agendovém informačním systému (AIS).

Neveřejné údaje (tj. údaje, jejichž neveřejnost vyplývá z nějakého právního předpisu) se sdílí v rámci Propojeného datového fondu, konkrétně údaje ze základních registrů skrze Informační systém základních registrů (ISZR) a údaje z AIS prostřednictvím Informačního systému sdílené služby (ISSS). Údaje z PPDF úřad vždy čerpá ve vztahu ke konkrétnímu subjektu či objektu práva. Je žádoucí, aby každý AIS, který vede údaje o osobách (fyzických či právnických) a adresách byl napojen na ISZR a čerpal údaje ze základních registrů včetně notifikací o změnách. Díky tomu může úřad udržovat svůj datový kmen agendy aktuální. Dodržování tohoto principu je vyžadováno při schvalování žádostí.

Ochrana osobních údajů je v základních registrech zajištěna převodníkem agendových identifikátorů fyzických osob, díky němuž není možné při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v jiné agendě. Úřad by měl dodržovat pravidla evidence subjektů a zajistit pseudonymizaci v rámci výkonu veřejné správy. Jako identifikátor by úřad neměl používat ani rodné číslo, jelikož zakládá možnost snadného zneužití údajů. Úřady, které nemají vlastní AIS, mohou získat údaje ze základních registrů pro výkon agendy prostřednictvím formuláře na Portálu veřejné správy či aplikace CzechPOINT@office (blíže viz Portál veřejné správy).

Propojený datový fond

Propojený datový fond (PPDF) je primárním zdrojem platných a právně závazných neveřejných údajů pro subjekty práva i pro všechny orgány veřejné moci při výkonu jejich působnosti. Tak vede PPDF k náhradě manuálních interakcí mezi úřady pomocí automatizované výměny údajů.

► Globální architektura propojeného datového fondu

Ke každé definici údaje subjektu či objektu agendy v RPP z hlediska právního vymezení ***musí úřad v RPP*** vyplnit i odpovídající technickou definici tohoto údaje subjektu či objektu práva, označovanou jako Technická specifikace údaje agendy (TSÚA). Právě tato technická specifikace údaje umožní definovat tzv. kontext pro subjekt či objekt, prostřednictvím kterého úřad poskytuje definované údaje jiným úřadům přes ISSS. Pokud má úřad vytvořen konceptuální datový model agendy, může z něj automaticky vygenerovat datovou strukturu potřebnou pro sdílení dat.

Pokud jsou možné hodnoty údaje vymezeny číselníkem, musí úřad uvést odkaz na existující číselník v RPP, případně vytvořit číselník postupem podle otevřené formální normy pro číselníky a nahrát jej do RPP. Kromě číselníků by měl úřad zpřístupnit jiným úřadům i ostatní veřejné údaje skrze Veřejný datový fond. U veřejných údajů vedených v agendě musí úřad v RPP vyplnit odkaz na datovou sadu v NKOD, ve které je údaj publikován.

Veřejný datový fond

Veřejný datový fond (VDF) tvořený publikovanými veřejnými údaji veřejné správy je základní metodou pro sdílení veřejných informací mezi veřejnoprávními subjekty navzájem i pro sdílení veřejných údajů mezi veřejnoprávní a soukromoprávní sférou v ČR. VDF se od pouhé publikace automatizovaně čitelných otevřených dat posune též k publikaci právně závazných, platných a pravidelně aktualizovaných datových sad s jasně definovanou zodpovědností úřadu za takové sady.

► Globální architektura veřejného datového fondu
► Metodika poskytování dat ve veřejném datovém fondu
► Školení Veřejný datový fond (VDF) v architektuře veřejné správy

Za předpokladu, že všechny úřady správně popisují své agendy, může jakýkoliv jiný úřad v RPP zjistit, jaké údaje včetně číselníků může využít z jiných agend a jakým způsobem může k datům přistoupit. Přístup k datům, znalost významu dat a správná evidence v RPP jsou tak předpokladem pro sdílení a využívání dat. Výhodou sdílení dat prostřednictvím datových fondů je možnost propojení údajů o subjektech a objektech práva napříč agendami, garantovaná správnost a aktuálnost údaje a možnost získání notifikací o změnách údajů.

Výhodou publikace údajů do PPDF, namísto přímého napojení na AIS jiného úřadu, je např. to, že úřad nemusí ověřovat zdroj dotazu (Agenda, Orgán veřejné moci, Informační systém či přímo tázající se osoba), nezodpovídá za ztotožnění subjektu údajů (za přesné určení osoby AIFO je zodpovědný tazatel), nemusí udržovat jedno či více rozhraní směrem k velkému počtu tázajících se informačních systémů a publikační rozhraní má zajištěnou kybernetickou ochranu. Současně dojde ke snížení nákladů na zajištění sdílení údajů s ostatními úřady.

Podmínky pro využívání údajů z datového fondu ČR

Aby mohl úřad využívat neveřejné údaje skrze PPDF, tzn. propojit svůj AIS s ISZR či ISSS, musí splňovat několik podmínek:

- Správce AIS musí mít v RPP ohlášenou působnost v agendě, kterou tímto AIS bude vykonávat.
- Správce AIS musí mít svůj AIS ohlášen v rejstříku ISVS v Registru práv a povinností.
- Správce AIS musí připojit AIS na příslušný přístupový bod (KIVS nebo CMS).
- Správce AIS musí v RPP definovat požadavek na přístup k jiným agendám.
- Správce AIS musí vyplnit formulář Registrační autority základních registrů (RAZR).
- Správce AIS musí certifikovat AIS pro přístup k ISZR a ISSS (viz postup pro vytvoření žádosti).
- Správce AIS musí do AIS implementovat volání služeb ISZR dle provozní dokumentace, tj. volání, konzumace a využívání webové služby vnějšího rozhraní ISZR.
- Správce AIS musí realizovat napojení na ISSS pro publikaci údajů ostatním úřadům (publikační konektor) a také pro čtení jednotlivých údajů od ostatních úřadů.

Aby mohl úřad prostřednictvím svého AIS získat využívat veřejné údaje prostřednictvím veřejného datového fondu (VDF), musí splňovat několik podmínek:

- Správce AIS musí mít v RPP ohlášenou působnost v agendě, kterou tímto AISem bude vykonávat.
- Správce AIS musí mít svůj AIS ohlášen v rejstříku ISVS v Registru práv a povinností.
- Správce AIS musí připojit AIS na příslušný přístupový bod (KIVS nebo CMS).

Veřejné údaje z VDF nemusí úřad číst prostřednictvím AIS, každý zaměstnanec si může stáhnout příslušnou datovou sadu údajů. Na rozdíl od získání údajů skrze PPDF nevyžaduje VDF kladné stanovisko k využití údajů a není zatížen žádnou administrativní procedurou. Využívání veřejných údajů je tak spojeno s nižší administrativní zátěží. Oproti výměně údajů přes PPDF umožňuje VDF dávkovou výměnu údajů v podobě celého obsahu datových sad s údaji bez vazby na konkrétní subjekt práva. Dle principů VDF jsou údaje dostupné ve VDF v totožné podobě také povinně publikovány jako otevřená data.

Otevřená data

Formou otevřených dat úřad poskytuje údaje veřejnosti. V souladu s principem Otevřená data jako standard by jako otevřená data měly být zveřejněny veřejné údaje kompletně a neveřejné údaje v anonymizované podobě, jako souhrn nebo statistika, nebo v obdobné formě, pokud může mít význam pro uživatele těchto dat. V návaznosti na obecný princip jsou definovány konkrétní povinnosti publikace otevřených dat v zákoně č. 106/1999 Sb. a dalších zákonech (např. č. 123/1998 Sb., č. 332/2020 Sb., č. 256/2000 Sb., atd.). Úřady publikují otevřená data správně, tj. v souladu s § 3a odst. 5 zákona č. 106/1999 Sb., pouze v případě, že informace zveřejňují způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, neomezí způsob ani účel následného využití a evidují je v národním katalogu otevřených dat (NKOD). V opačném případě se nejedná o publikaci otevřených dat.

Povinnost publikovat otevřená data

Úřady mají povinnost zveřejnit jako otevřená data:

1) informace z jimi vedených registrů, evidencí, seznamů nebo rejstříků obsahující informace, které jsou na základě zákona každému přístupné *(u nově vznikajících registrů a registrů uvedených dříve v nařízení vlády č. 425/2016 Sb. platí povinnost již nyní, u existujících registrů musí být zveřejněno nejpozději do 31. 12. 2023)*

2) metadata informací zveřejněných způsobem umožňujícím dálkový přístup na svých úředních deskách a metadata těchto úředních desek *(musí být zveřejněno nejpozději od 1. 2. 2022)*

3) dynamická data, která nejsou obsažená v registrech a jejichž poskytnutí není zákonem omezeno, a to prostřednictvím rozhraní pro programování aplikací jako otevřená data bezprostředně po jejich shromáždění, případně bez zbytečného odkladu tak, aby nedošlo k nepřiměřenému narušení jejich využitelnosti

4) datové sady s vysokou socio-ekonomickou hodnotou (tzv. HVDs) dle předpisu Evropské unie vydaného podle čl. 14 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2019/1024

► § 5a a § 5b zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Pro správnou a pravidelnou publikaci otevřených dat by úřad měl mít přijatou interní směrnici nebo jiným způsobem vymezit role v publikaci a katalogizaci otevřených dat (např. role koordinátor otevírání dat, kurátoři dat a správce katalogu otevřených dat). Úřad by měl zároveň rozhodnout o způsobu katalogizace otevřených dat, vytvořit publikační plán a pravidelně jej aktualizován, komunikovat s uživateli a monitorovat využívání dat uživateli. Co jsou otevřená data, proč se mají publikovat, jak identifikovat datové sady pro publikaci a jak analyzovat přínosy a rizika jejich publikace je podrobně vysvětleno v e-learningovém kurzu Co jsou otevřená data a kurzu Publikační plán a publikace dat.

Dle § 4b zákona č. 106/1999 Sb. musí úřad při publikaci otevřených dat splňovat datové standardy tzv. otevřené formální normy (OFN). Jedná se o technická doporučení zaměřená na vybrané datové sady, která zajišťují, že stejná data publikovaná různými poskytovateli budou interoperabilní. Schopnost posoudit možnost/nutnost využití otevřených formálních norem a výhody aplikace OFN v rámci organizace otevírající svoje data mohou úřady získat v e-learningovém kurzu Úvod do otevřených formálních norem.

V Národním katalogu otevřených dat jsou evidována všechna otevřená data, resp. jejich metadata (tj. data popisující souvislosti, obsah a strukturu zaznamenaných informací a jejich správu v průběhu času). Povinné položky metadat, které musí být registrovány v NKOD, definuje otevřený formát dat OFN pro rozhraní katalogů otevřených dat. Jedná se například o název datové sady, popis či periodicitu aktualizace. Samotná data jsou volně přístupná na webu úřadu jako datové soubory ke stažení a právě odkaz na soubor je jednou z položek metadat.

Kromě souborů ke stažení lze v NKOD registrovat i datovou službu zpřístupňující data datové sady. Katalogizaci do NKOD může úřad provést přímo přes formulář, ale vhodným řešením pro publikaci většího množství otevřených dat nebo častou aktualizaci metadat je využití lokálního katalogu otevřených dat (LKOD). Příkladem jednoduchého LKOD, který mohou úřady snadno a levně využít je referenční implementace LKOD. Výhodou minimalistické verze LKOD je zejména to, že úřad nemusí opětovně posílat datové zprávy pro vytvoření, editaci či mazání datových sad. Prostřednictvím datové zprávy úřad pouze zaregistruje LKOD a zbytek změn dělá již bez datové schránky. Chytřejší LKOD umožní automatizovat procesy tvorby/editace metadat, opět již bez datové schránky. LKOD může být i součástí datového portálu úřadu, kde kromě dat budou dostupné i různé články a analýzy. Proces katalogizace je návodně popsán v e-learningovém kurzu Katalogizace otevřených dat.

Úřady zodpovídají za kvalitu svých dat i svých katalogizačních záznamů, proto by měli na kvalitu svých dat dbát, pravidelně ji sledovat a dělat kroky k nápravě zjištěných nedostatků. Na Portálu otevřených dat v sekci Datová kvalita si může každý úřad zkontrolovat kvalitu metadatových záznamů i dostupnost v denně počítaných statistikách NKOD a dashboardech jednotlivých poskytovatelů. Zároveň by se měl každý úřad vyvarovat příkladům špatné praxe. Přehled o technologiích a technických postupech používaných v otevřených datech může úřad získat také v e-learningovém kurzu Technické aspekty otevřených dat.

Kde se dozvědět více o oblasti dat?

Na webu archi.gov.cz či na Portálu otevřených dat, kde najdete:

► Online školení
► E-learning
► Články
► Výroční zprávy o stavu otevřených dat

Dílčí konzultace přes email archi@mvcr.cz nebo otevrenadata@mvcr.cz

4.2 Klíčové otázky

1)	**Má úřad zajištěn přístup ke všem datům ze svých informačních systémů, a to v otevřeném a strojově čitelném formátu, bez dodatečných nákladů a s možností libovolně s daty nakládat?** *Je potřeba si vyžádat smlouvy k informačním systémům a posoudit, zda ustanovení smlouvy neomezují přístup k datům. Přístup k datům lze ověřit také vyžádáním konkrétních dat z informačního systému a ověřením, že při procesu získání dat nevznikly žádné náklady a bylo možné získat libovolná data a dále využít.*
2)	**Má úřad v Registru práv a povinností u agendy ohlášeny všechny údaje vedené v agendě?** *Je potřeba zjistit, s jakými daty úřad pracuje ve svých agendách a v Registru práv a povinností ověřit, že jsou v něm tato data evidována.*
3)	**Má úřad v Registru práv a povinností u agendy odlišeny veřejné a neveřejné údaje?** *Je potřeba ověřit, že v Registru práv a povinností je u údajů vyplněna veřejnost údaje a že u neveřejných údajů je uveden odkaz na konkrétní ustanovení právního předpisu, které definuje neveřejnost.*
4)	**Má úřad v Registru práv a povinností u agendy uvedeno, které údaje v agendě jsou kódovány číselníky i s odkazem na číselník?** *Je potřeba ověřit, že v Registru práv a povinností jsou nahrány jednotlivé číselníky a označeno, hodnoty, kterých údajů jsou vymezeny číselníky. Je možné si vyžádat seznam číselníků využívaných v konkrétních agendových IS a ověřit jejich existenci v Registru práv a povinností.*
5)	**Má úřad pro konkrétní agendu vytvořen konceptuální datový model a udržuje ho aktuální?** *Je potřeba si vyžádat konceptuální datový model agendy nebo celého úřadu. Je vhodné ověřit, že model vychází z platné legislativy a zda jsou nastaveny procesy pro údržbu modelu. Je vhodné ověřit, že je model dále využíván, např. pro aktualizaci evidence údajů v Registru práv a povinností, pro automatické generování datových struktur, atd.*
6)	**Odděluje úřad u fyzických osob agendové a identifikační údaje a využívá k jejich propojení tzv. Agendový identifikátor fyzické osoby (AIFO)?** *Je možné si vyžádat provozní dokumentaci jednotlivých IS, ve kterých jsou vedeny informace o fyzických osobách a ověřit, zda jsou IS připojeny na základní registry a odebírají notifikace o změnách.*
7)	**Definoval úřad v Registru práv a povinností tzv. kontexty pro subjekty a objekty práva a publikoval je do Informačního systému sdílené služby?** *Je vhodné si vyžádat seznam neveřejných údajů subjektů a objektů práva, které jsou vyměňovány mezi informačním systémem úřadu s informačními systémy jiných úřadů (kromě*

	základních registrů). Je potřeba posoudit, zda pro tyto neveřejné údaje úřad publikoval kontext pro subjekt/objekt práva v informačním systému sdílení údajů.
8)	**Využívá úřad pro výkon agend dostupné údaje z datových fondů?** *Je vhodné posoudit, zda informační systémy úřadu čerpají neveřejné údaje jiných úřadů prostřednictvím informačního systému základních registrů nebo prostřednictvím informačního systému sdílené služby (lze ověřit v RPP záložka oprávnění k údajům). Je vhodné ověřit, zda úřad eviduje, jaké využívá veřejné údaje (lze ověřit v RPP záložka veřejné údaje).*
9)	**Plní úřad povinnosti publikace otevřených dat alespoň v minimálním rozsahu dle § 5a a § 5b zákona č. 106/1999 Sb.?** *Je vhodné si vyžádat seznam registrů, rejstříků, evidencí a seznamů vedených ze zákona s datem jejich vzniku. Je vhodné si vyžádat seznam dynamických dat, která nejsou obsaženy v registrech a jejichž poskytnutí není zákonem omezeno. Je potřeba ověřit, zda úřad spravuje data s vysokou socio-ekonomickou hodnotou (tzv. HVDs) vyplývající z předpisu Evropské unie vydaného podle čl. 14 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2019/1024. Je potřeba ověřit, že jsou nastaveny procesy ke zveřejnění dat z těchto seznamů tak, aby byl dodržen termín stanovený zákonem a docházelo k pravidelné aktualizaci.*
10)	**Plní úřad povinnosti publikace otevřených dat vyplývající z jiných zákonů než ze zákona č. 106/1999 Sb.?** *Je potřeba ověřit, že jsou nastaveny procesy ke zveřejnění dat tak, aby byl dodržen termín stanovený zákonem a docházelo k pravidelné aktualizaci. Je potřeba ověřit, zda jsou publikovány formou otevřených dat všechny veřejné údaje a neveřejné údaje v anonymizované podobě, jako souhrn nebo statistika, nebo v obdobné formě.*
11)	**Publikuje úřad otevřená data v odpovídající kvalitě a podle vydaných otevřených formálních norem?** *Je potřeba ověřit, že zveřejněné datové sady/datové služby splňují všechny zákonné požadavky publikace otevřených dat (umožnění dálkového přístupu, strojově čitelný a otevřený formát, neomezená licence, evidence v Národním katalogu otevřených dat) a u HVDs též požadavky vymezené přílohou předpisu Evropské unie vydaného podle čl. 14 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2019/1024 v dané kategorii. Dále je vhodné ověřit datovou kvalitu, zejména dodržení otevřených formálních norem (lze využít validátor schémat), vyplnění povinných metadat a dostupnost datových souborů/služeb (lze využit dashboardy) a vyvarování se příkladům špatné praxe.*
12)	**Má úřad nastaveny procesy pro publikaci otevřených dat?** *Je potřeba si vyžádat interní směrnici publikace a katalogizace otevřených dat nebo jiné dokumenty, ve kterých jsou vymezeny role v této oblasti. Je potřeba ověřit, zda je stanoven koordinátor otevírání dat, kurátoři dat, bylo rozhodnuto o způsobu katalogizace otevřených dat, existuje publikační plán a je pravidelně aktualizován, bylo rozhodnuto o způsobu komunikace s uživateli a o monitoringu kvality metadat a využívání dat uživateli.*

4.3 Příklady dobré a špatné praxe

▶Příklad dobré praxe

Identifikace fyzických osob

Úřad vede ve své agendě informace o fyzických osobách tak, aby zajistil oddělení agendových a identifikačních údajů (tzv. pseudonymizaci údajů). Úřad vede ve svém informačním systému u fyzických osob agendový identifikátor fyzické osoby (AIFO) a čerpá referenční údaje ze základních registrů. Dále používá interní technické bezvýznamové identifikátory a bezvýznamový

klientský identifikátor. Díky identifikaci přes AIFO úřad pracuje s aktuálními a garantovanými údaji.

Vzhledem k tomu, že úřad neeviduje rodná čísla ani jiné významové či obecné identifikátory, snižuje rizika neoprávněného nakládání s osobními údaji a neoprávněného spojování osobních údajů.

▶ Příklad dobré praxe

Publikace a čtení agendových údajů

Ministerstvo spravedlnosti publikovalo do ISSS kontext Výpis údajů z Rejstříku trestů (A483.1). Datový obsah kontextu je k dispozici na portálu CMS v rámci sítě KIVS (odkaz nefunguje v běžném internetu) a díky tomu mohou kontext automatizovaně číst jiné úřady a již nemusí mít své informační systémy napojeny přímo na Rejstřík trestů. Například ministerstvo průmyslu a obchodu v roce 2022 připravovalo projekt na čtení kontextu, aby mohlo automatizovaně ověřit bezúhonnost osob v případě ohlášení živnosti a nemuselo mít propojen Registr živnostenského podnikání přímo s Rejstříkem trestů. Díky tomu, že tento kontext bude číst i CzechPoint a Portál občana, mohou výpis z Rejstříku trestů jednoduše získat i občané. Dalším dobrým příkladem z praxe je policie ČR, která publikuje údaje o osobách v pátrání (kontext 418.1). Datový obsah kontextu je také k dispozici na portálu CMS v rámci sítě KIVS a díky tomu mohou kontext číst jednotlivé městské policie ČR, jejichž strážníci kontrolují jednotlivé osoby v terénu a mohou na dálku zjistit, zda kontrolovaná osoba není náhodou v pátrání a podle toho dále podnikat další kroky.

▶ Příklad dobré praxe

Publikace úřední desky jako otevřená data

Město Trutnov k datu 1. 2. 2022 plnilo povinnost publikovat metadata informací zveřejněných způsobem umožňujícím dálkový přístup na svých úředních deskách a metadata těchto úředních desek. Město Trutnov plnilo povinnost tím, že v NKOD publikovalo datovou sadu úřední deska dle datového standardu Otevřená formální norma pro úřední desky (OFN) a vyplnilo metadata datové sady včetně položky specifikace, kde odkázalo na příslušnou OFN. Město Trutnov nastavilo aktualizaci datové sady s denní periodicitou. Město Trutnov také splňuje všechny povinné položky metadat dle ukazatele datové kvality Q3. V rámci datové sady publikovalo město Trutnov konkrétní distribuci, která odkazovala na konkrétní soubor s daty. Tento soubor byl validní podle JSON schématu v OFN a byla podporována k tomu určená technika (Cross-Origin Resource Sharing CORS), která umožňuje data využít i ve webových aplikacích. Všechny tyto informace se dají ověřit v testovací aplikaci, kde jsou popsány nejčastější chyby při zveřejňování úředních desek a vysvětleno, jak problémy řešit.

Zda konkrétní organizace publikuje nějakou datovou sadu lze zjistit přímo v NKOD nebo přes rozhraní do NKOD (tzv. SPARQL endpoint), kde lze dotaz specifikovat i na konkrétní OFN. Dotaz v jazyce SPARQL identifikující datové sady dle OFN pro úřední desky lze jednoduše upravit pro zjištění datových sad dle jiných OFN, a to úpravou odkazu na danou OFN na řádku 12 dotazu.

▶ Příklad dobré praxe

Způsob publikace otevřených dat

Ministerstvo financí (MF) publikuje otevřená data v souladu s platnými standardy, má datový portál, jehož součástí je i lokální katalog otevřených dat, s návody a analýzami ke svým datům a komunikuje s uživateli dat různými způsoby, např. sbírá podněty na nové datové sady, poskytuje individuální konzultace a komunikuje na Twitteru. MF má schválenou interní směrnici pro publikaci otevřených dat i publikační plán, zástupci ministerstva se pravidelně účastní konference otevřená data a školení v oblasti otevřených dat, což podporuje systematickou a správnou publikaci otevřených dat.

▶ Příklad špatné praxe

Nezajištění přístupu k datům

V roce 2017 prováděl Nejvyšší kontrolní úřad (NKÚ) kontrolní akci u ministerstva a zjistil, že ministerstvo nemělo zajištěn přístup ke všem údajům o veřejných zakázkách. Přestože je ministerstvo správcem Informačního systému o veřejných zakázkách, mělo přístup pouze k dílčím údajům prostřednictvím nastavených sestav. Pro získání datové sestavy obsahující jiné, resp. všechny povinně zadávané údaje bylo ministerstvo závislé na poskytnutí služeb provozovatele za úplatu ve výši cca 150 tis. Kč. NKÚ konstatoval závislost na dodavateli (tzv. vendor lock-in) i to, že omezený přístup ministerstva k datům vedl v konečném důsledku k nepředávání informací dalším úřadům, které by mohly tyto údaje využít.

▶ Příklad špatné praxe

Špatné nakládání s daty úřadu

Co často úřady opomínají provádět při získávání údajů ze základních registrů, je přihlášení se k notifikacím, aby nedocházelo k přílišnému zatěžování základních registrů díky opakovanému stahování velkého množství údajů v rámci svého datového kmene bez využívání notifikací např. z ROB.
Dále úřady nedostatečně správně pracují s ostatními identifikátory uvnitř úřadu tzv. interními (resortními) identifikátory. V tomto směru platí jednoduché pravidlo, interní identifikátor úřad využívá uvnitř úřadu, při komunikaci mezi OVM využívá identifikátorů AIFO k identifikaci fyzické osoby a IČO k identifikaci právnické osoby a pro komunikaci s klientem může použít klientský identifikátor.
Velkým kamenem úrazu u většiny úřadů je řízení přístupu k jejich datům a nakládání s nimi. Úřady nedoceňují význam datového modelu úřadu u jeho udržování.

Důsledkem je absence neohlášených údajů v RPP u drtivé většiny agend a také velmi malé množství kontextů k dispozici pro publikaci údajů ostatním úřadům v rámci výměny údajů mezi jednotlivými AIS úřadů.

▶ Příklad špatné praxe

Nepochopení principu otevřených dat

Státní zemědělský intervenční fond (SZIF) má dle § 12 odst. 6 a 7 zákona č. 256/2000 Sb. zveřejňovat informace o poskytnutých dotacích jako otevřená data. SZIF sice data publikuje na svých webových stránkách, ale nesplňuje podmínky pro označení dat jako „otevřená data“. Dle § 3 odst. 11 zákona č. 106/1999 Sb. se otevřenými daty rozumí informace zveřejňované způsobem

umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není omezen a které jsou evidovány v Národním katalogu otevřených dat.
K datu 1. 2. 2022 nepublikoval SZIF v NKOD žádnou datovou sadu a tudíž nepublikoval žádná otevřená data.

Datové sady konkrétního poskytovatele lze jednoduše filtrovat přímo v NKOD nebo je možné využít rozhraní do NKOD (tzv. SPARQL endpoint). Dotaz v jazyce SPARQL lze jednoduše upravit na jakéhokoli poskytovatele, a to úpravou IČO poskytovatele na řádku 14 dotazu.

▶ Příklad špatné praxe

Omezující podmínky využití otevřených dat

Ministerstvo spravedlnosti publikovalo k datu 1. 2. 2022 informace z Informačního systému veřejných rejstříků. V licenčních podmínkách bylo uvedeno, že uživatel smí výstupy, údaje, data a informace šířit (tj. kopírovat, distribuovat a sdělovat veřejnosti), využívat a citovat a využívat pro nekomerční použití. Z toho vyplývá, že data nemohou být použita pro komerční užití. Vzhledem k tomu, že dle definice otevřených dat v § 3 odst. 11 zákona č. 106/1999 Sb. nesmí být omezen způsob ani účel následného využití, MSp nepublikovalo informace jako otevřená data.

Podmínky užití by měly být specifikovány u každé distribuce datové sady v Národním katalogu otevřených dat. Pokud nejsou podmínky užití uvedeny, taktéž se nejedná o otevřená data. Poskytovatele, kteří nemají stanoveny podmínky užití, eviduje ukazatel datové kvality Q2. Způsob správného stanovení podmínek užití je popsán v modulu č. 7 e-learningového kurzu Publikační plán a publikace dat.

▶ Příklad špatné praxe

Chybějící povinné položky metadat a nedostupnost otevřených dat

Ministerstvo zdravotnictví mělo ke dni 1. 2. 2022 v NKOD evidováno 106 datových sad, přičemž u žádné datové sady nebyly vyplněny povinné položky metadat dle otevřené formální normy pro rozhraní katalogů. U datových sad nebylo vyplněno například téma, periodicita aktualizace, klíčová slova a v některých případech dokonce ani podmínky užití. Nedostatečné vyplnění metadat v tomto případě souvisí i se špatným způsobem katalogizace. Ministerstvo zdravotnictví totiž využívalo nevyhovující rozhraní lokálního katalogu, které již není od 11. 1. 2021 podporováno. Ministerstvo zdravotnictví též mělo problém s dostupností distribucí datových sad, k datu 1. 2. 2022 bylo nedostupných 5 %.

Počet datových sad nesplňujících povinné položky metadat dle jednotlivých poskytovatelů otevřených dat zobrazuje ukazatel datové kvality Q3, počet datových sad s nespecifikovanými podmínkami užití dle poskytovatele ukazatel datové kvality Q2 a nedostupnost distribucí dle poskytovatele ukazatel datové kvality A1.1. Způsob registrace datových sad prostřednictvím nevyhovujícího lokálního katalogu je vidět ve třetím sloupci této statistiky.

5 Obslužné kanály veřejné správy

Obslužné kanály veřejné správy lze chápat jako způsoby či prostředky komunikace mezi klientem veřejné správy a veřejnou správou. Obslužné kanály jsou klíčovým aspektem, který zajišťuje poskytování služeb klientům veřejné správy. Úřady by se měly snažit o zajištění tzv. úplného elektronického podání, díky kterému občan digitálně kdykoli a odkudkoli či prostřednictvím univerzálního kontaktního místa vyřídí celou svou životní situaci. Přehled údajů o službách veřejné správy, úkonech a jejich obslužných kanálech je uveden v tzv. katalogu služeb veřejné správy.

Dále uvádíme je obslužné kanály digitální, neuvádíme tradiční komunikační kanály, jako je osobní komunikace klienta s úředníkem a doručování prostřednictvím zprostředkovatele jako je pošta.

Jednou z možností, které obslužné kanály nabízejí, je možnost učinit tzv. digitální úkon. Právo činit digitální úkon a využívat digitální služby je zakotveno v zákoně č. 12/2020 Sb.

> ►Základní právní oporou pro obslužné kanály je § 4 odst. 1 zákona č. 12/2020 Sb. o právu na digitální služby, ze kterého plyne právo uživateli služby (klientovi veřejné správy) činit úkony prostřednictvím různorodých kanálů.

Příklady obslužných kanálů pro klienty

Portál veřejné správy s Portálem občana - hlavní samoobslužný kanál veřejné správy je webovým portálem, který umožňuje centralizovaný přístup k individualizovaným informacím a digitálním službám. Aby se klient/občan mohl do portálu přihlásit, musí disponovat tzv. zaručenou elektronickou identitou, přihlášení je tedy umožněno přes kvalifikovaný systém elektronické identifikace.

V současnosti jsou nástroje identifikace sdruženy v Národní bodu pro identifikaci a autentizaci, zvaném historicky také NIA – Národní identitní autorita popsaná v kapitole č. 6. Národní bod nabízí klientům celou škálu prostředků pro prokázání identity. Od elektronického občanského průkazu s čipem, přes mobilní klíč eGovernmentu až po nově implementovanou bankovní identitu a také autentizační rozhraní Informačního systému datových schránek (předpokládá se zrušení tohoto nástroje identifikace).

Portál občana umožňuje různě pokročilé propojení (federace) portálů či systémů veřejné správy.

V oblasti centralizovaných webových portálů by měl v budoucnu vzniknout např. Portál podnikatele, který lze vedle Portálu občana chápat jako další rozšíření Portálu veřejné správy, obsahově zaměřené na podnikatele a zástupce organizací.

Agendové portály, portály úřadů. Většina centrálních úřadů buduje interaktivní weby s charakterem portálů (MOJE daně, Jednotný portál práce a sociálních věcí (MPSV/ČSSZ) a další), které nabízejí příslušnou podmnožinu digitálních služeb pro klíčové agendy a stále více pro celé úřady nebo resorty. Je správné a žádoucí, aby digitální služby a úkony poskytované portály úřadů byly dostupné také na Portálu občana.

Takto státní správa vyjde vstříc občanům, kteří se těžko orientují v roztříštěné nabídce služeb VS. Zároveň tím úřady naplní principy IK ČR, např.:

- P8: Jeden stát.
- P9: Sdílené služby veřejné správy.
- P11: eGovernment jako platforma.

V souladu s principem *P1: Standardně digitalizované* musí úřady udržovat otevřené i další kanály pro ty, kteří nemohou buď z vlastního rozhodnutí, nebo z technických důvodů využívat digitální služby. Listinná či asistovaná podoba služby by však měla být odvozena od její podoby digitální, ne naopak.

Portály území - typicky portály krajů, obcí, měst či městské části. Portál může obsahovat kromě nabídky samosprávných služeb, jako je např. správa místních poplatků, i služby přenesené působnosti. Nicméně neměla by nastat situace, kdy je služba přenesené působnosti vytvořena jen pro portál území. Je zodpovědností věcného správce portálu, aby vytvořil centrální prostředí pro vyřizování služeb přenesené působnosti, které portál území využije, ale nevytváří. Z hlediska uživatelského komfortu je nutné řešit i možnost přesměrování/přechodu mezi portály. Takovéto chování musí být intuitivní a nerušivé.

Portály soukromoprávních uživatelů údajů (SPUÚ). Může se jednat o portály poskytovatelů zdravotních služeb, soukromých pojišťoven, bank, státních podniků aj. Tyto portály poskytují služby, které mohou být propojeny (federovány) do Portálu občana, avšak pouze za předpokladu, že SPUÚ (soukromoprávní uživatel údajů) je ohlášen v Informačním systému registru práv a povinností (rejstříku) dle § 52a zákona č. 111/2009 Sb. a má povinnost elektronicky ověřovat totožnost klienta.

Mobilní samoobslužné kanály. Stejně jako to již stalo u Portálu občana, je žádoucí, aby všechny výše uvedené kategorie samoobslužných portálových řešení měly i svůj ekvivalent pro mobilní telefony. Tam se bude průběžně přesouvat těžiště vývoje digitálních služeb. Je možné je účinně kombinovat s tzv. Mobilní identitou.

Centrálním asistovaným obslužným kanálem je Czech POINT (Český Podací Ověřovací Informační Národní Terminál), který má více než 6000 územních pracovišť, zvaných KMVS (Kontaktní místa veřejné správy), převážně na poštách a obecních úřadech. Do budoucna je plánováno postupně rozšiřovat množství služeb dostupných asistovaně v síti Czech POINT.

Vedle asistovaných přepážek KMVS by v rámci Czech POINT mělo v blízké době vzniknout i tzv. Kontaktní centrum VS (KCVS), tedy multikanálové Call-centrum[8].

Jednotná informační a znalostní základna. Všechny centrální obslužné kanály se plně doplňují a vzájemně se propojují, s mírnými omezením se propojují i kanály centrálních a samosprávních úřadů. Informace o nabídce služeb pro řešení životních situací a znalosti o průběhu obsluhy jednotlivých klientů v jednotlivých kanálech jsou potom jednotně využívány ku prospěchu klientů.

Příklady obslužných kanálů pro úředníky

Za zmínku stojí též jednotné obslužné kanály úředníků. I úředníci totiž musí mít přístup ke všem informacím Jednotné informační znalostní základny, aby mohli klienty efektivně obsloužit.

Základním nástrojem přístupu úředníků k informacím je tzv. Czech POINT@Office a postupně budované funkce Portálu úředníka. Tento portál úředníka se bude skládat z rostoucí množiny centrálních sdílených služeb pro úředníky, ať již z oblastí výkonu služeb veřejné správy nebo z provozních oblastí (nákup, vzdělávání, personalistika, správa nemovitostí). Tyto centrální funkce budou v každém většímu úřadu kombinovány v transakční části Intranetu úřadu s webovými uživatelskými rozhraními klíčových

[8] Primární úlohou Call centra bude technicky i věcně podporovat uživatele samoobslužných kanálů, tedy portálů a webových nebo mobilních forem digitálních služeb státu. V nabídce KCVS budou postupně také některé úkony, vykonatelné hlasem po telefonu, s odpovídajícími způsoby ověření identity klienta - ty však zatím nejsou zvoleny, uzákoněny ani implementovány.

IS, do nichž mají úředníci úřadu přístup tak, aby každý úředník měl jednotnou pracovní plochu a nemusel své aplikace nikde shánět.

Motivace k využívání obslužných kanálů

Klienti obslužných kanálů jsou v některých případech motivováni k jejich využívání jednodušším a návodným vyplňování elektronických formulářů. Další motivací je poskytnutí slevy na správním poplatku za předpokladu splnění uvedených podmínek. Viz ustanovení § 9 zákona č. 634/2004 Sb. o správních poplatcích.

> ►Ustanovení § 9 zákona č. 634/2004 Sb. o správních poplatcích motivuje klienty veřejné správy, aby svá podání činili s využitím elektronických formulářů. Správní úřad sníží poplatek o 20%, maximálně však o 1000 Kč, pokud klient využije k podání elektronický formulář, publikovaný podle zákona o právu na digitální služby. Toto neplatí pouze v případě, že jediným způsobem, který služba umožňuje je podání elektronickým formulářem.

Vazba katalogu služeb na obslužné kanály pro digitální úkony.

Katalog služeb poskytuje přehled o jednotlivých službách, které úřady poskytují svým klientům. Každá služba může obsahovat jeden i více úkonů, přičemž tyto úkony mohou být vykonávány s využitím jednoho nebo i více obslužných kanálů. ***Katalog služeb tak eviduje obslužné kanály.*** Zákon o právu na digitální službu je ultimativním motivačním nástrojem s povinností postupné digitalizace služeb, potažmo vede k využívání obslužných kanálů (datová schránka, podání s uznávaným podpisem).

> ►Přechodné ustanovení § 14 odst. 4 stanoví povinnost provést postupně digitalizaci služeb a úkonů obsažených v katalogu služeb všem ohlašovatelům agendy, pokud to povaha služby nebo úkonu nevylučuje. Postupná digitalizace je prováděna v souladu s harmonogramem, který vydala vláda.

Úřad se může při přípravě investičních záměrů na obslužné kanály opřít IK ČR a dosažení následujících cílů:

- 1.01 Vytvoření národního katalogu a vyhledávače služeb veřejné správy.
- 1.02 Centrální informační služby nové generace.
- 1.03 Rozvoj sdílených služeb univerzálních obslužných kanálů.
- 1.04 Rozvoj on-line „front-office“ služeb jednotlivých rezortů.
- 1.06 Zavedení rolí v OVS, zodpovědných za elektronickou obsluhu klientů, napříč agendami, a stanovení správců služeb.
- 1.07 Vytvoření systému zpracování podnětů a návrhů veřejnosti na zlepšování služeb.
- 1.08 Zařazení metodik UX/UI do tvorby informačních systémů.
- 6.01 Efektivní a uživatelsky přívětivá IT podpora práce úředníků.

Předpoklady využívání obslužných kanálů

Předpokladem jednotného, efektivního a přívětivého poskytování služeb klientům v obslužných kanálech VS a jejich využívání klienty je vybudování tzv. ***Jednotné informační a znalostní základy.***

Základem těchto znalostí je vedle anonymních informací z příslušné části Katalogu služeb VS zejména existence jednotného tzv. ***datového kmene klientů*** úřadu napříč agendami a obslužnými kanály. Údaje v tomto kmenovém registru jsou identifikovány Klientským identifikátorem úřadu (KID), jsou ztotožněny vůči základním registrům a pravidelně z nich notifikovány a slouží jako centrální evidence osobních údajů pro agendové IS a jako předloha pro tzv. klientské účty v IS pro saldokontní správu pohledávek a závazků klientů. Tyto systémy si každý zvlášť vedou ke svému identifikátoru KID své AIFO, ale osobní údaje si neukládají, dle potřeby je na vyžádání vyžadují z kmene.

Více o identifikaci subjektů také v následující kapitole 6.

V následujících kapitolách uvádíme popisy obslužných kanálů tvořící základní služby eGovernmentu.

Obslužné kanály vyžadující fyzickou přítomnost klienta	**Obslužné kanály umožňující provedení úkonu klienta vzdáleným přístupem (korespondenčně nebo interaktivně)**
Asistovaná přepážka úřadu	Datová schránka
Kontaktní místo veřejné správy (Czech POINT)	Agendové portály jednotlivých úřadů umožňující podat úplné elektronické podání
	Elektronická komunikace (prostřednictvím sítě elektronických komunikací) - zaslání elektronického dokumentu podepsaného uznávaným elektronickým podpisem
	Jiný způsob, pokud tak stanoví právní předpis. Řada úřadů má vyvinuty individuální digitální nástroje, které budou využívány, dokud se zájem klientů nepřesune z nich do kanálů nově propagovaných.

5.1 Asistovaná přepážka úřadu

Základním obslužným kanálem byla v minulosti asistovaná přepážka úřadu (dále také „asistovaná přepážka“), vyžadující fyzickou přítomnost klienta. Asistovaná přepážka má i v dnešním způsobu poskytování služeb veřejné správy stále své místo a řadu let ještě bude, neboť existuje stále velký počet klientů, kteří digitální technologie neovládají, nebo potřebují asistenci.

Nejčastěji využívána při žádosti o občanský průkaz, při registraci nově zakoupeného vozidla nebo při žádosti o cestovní doklad. V případě asistované přepážky tak jde o poskytování specializovaných služeb. Poskytování služeb na asistované přepážce probíhá tak, že klient osobně dorazí na přepážku se svým požadavkem a pracovník na přepážce jej obslouží. Často je klient povinen zaplatit příslušný správní poplatek. Správní poplatek je možné zaplatit v hotovosti na pokladně úřadu, přičemž jednotlivé úřady stále více umožňují hradit poplatek i platební kartou. Pokladní poté vystaví potvrzení o zaplacení příslušného správního poplatku.

Podání klienta učiněné prostřednictvím asistované přepážky jej však nevyřazuje z elektronického světa zcela, neboť úřad by měl klientovi umožnit sledovat životní cyklus jeho podání (začátek, vyřízení apod.) formou elektronických nástrojů. Tedy i úkony provedené na přepážce by měly být součásti Jednotné informační a znalostní základy a odtud dostupné k přístupu ostatními obslužnými kanály. Jinými slovy klientovi musí být umožněno se do portálu úřadu, resortu nebo do Portálu občana přihlásit se zaručenou identitou.

►Zákon o právu na digitální služby ve svém ustanovení § 4 odst. 2 uvádí, že nestanoví-li zákon závaznou podobu úkonu, má právo jej uživatel učinit jako digitální úkon. Docházíme tedy k závěru, že pokud existuje potřeba, aby byl určitý úkon činěn standardní fyzickou cestou (tedy nikoliv digitálně), musí mít taková podoba úkonu nesporný materiální důvod (jako je odběr biometrických údajů) a musí být výslovně vymezena v zákoně.

5.2 Kontaktní místo veřejné správy (Czech POINT)

Czech POINT (Český podací ověřovací informační národní terminál) je českou veřejností využíván stále častěji. Ve své podstatě se toto kontaktní místo veřejné správy příliš neliší od asistované přepážky, ovšem je zde podstatný rozdíl. Tento rozdíl spočívá především v tom, že prostřednictvím kontaktního místa jsou poskytovány univerzální služby (různé výpisy, potvrzení apod.), zatímco v případě asistované přepážky jde o poskytování vysoce specializovaných služeb (např. finanční úřady – daňová přiznání). Klient, který se na kterékoli kontaktní místo osobně dostaví, je obsloužen pracovníkem kontaktního místa, který přistupuje k centrálním sdíleným systémům eGovernmentu a poskytuje mu službu bez ohledu na věcnou a místní příslušnost.

Kontaktní místa veřejné správy jsou hustě rozmístěna po území celé České republiky. Služby kontaktních míst nabízejí např. držitelé poštovní licence (Česká pošta), obecní úřady, notáři nebo někteří advokáti. Na kontaktním místě může klient získat výpis z registru obyvatel, katastru nemovitostí, případně využít další služby, jako je například reklamace svých údajů v základních registrech, nebo elektronická konverze dokumentů. Pracovníci kontaktního místa jsou na jeho obsluhu speciálně vyškoleni. Za poskytnutí služby prostřednictvím kontaktního místa následně klient zaplatí poplatek v závislosti na druhu poskytnuté služby. Poplatek je nejčastěji možné hradit přímo v hotovosti, popřípadě platební kartou.

Kontaktní místo je však pouze jednou z možností, jak vyřídit potřebný úkon a jeho největší benefit spočívá v asistenci vyškoleného pracovníka, který klientovi v případě potřeby poradí. Kontaktní místo slouží především k vyřizování jednodušších úkonů (získávání výpisů, podání apod.). Veškeré služby nabízené kontaktním místem je také možné vyřídit samoobslužně.

►Právní oporou je zde § 4 odst. 1 písm. b) zákona o právu na digitální služby. Zákon o právu na digitální služby tudíž počítá s kontaktním místem veřejné správy jako s jedním z obslužných kanálů.

5.3 Datové schránky

Datová schránka je základním nástrojem pro elektronickou komunikaci s orgány veřejné správy, **jejíž využití je povinné z pohledu úřadů** pro všechny případy, ve kterých adresát či jiný právní předpis neuvedl jinak. Jedná se o korespondenční komunikační kanál sloužící k učinění podání vůči orgánům veřejné správy a doručování písemností od těchto orgánů. Hlavní devizou datové schránky je, že klient může své podání realizovat prakticky kdykoliv a odkudkoliv, kde je přístup k internetu, aniž by musel osobně na poštu či na úřad v úředních hodinách.

Zasílání zpráv orgánům veřejné správy z datové schránky je zdarma. Mít datovou schránku je navíc pro klienta výhodné v tom ohledu, že orgány jsou ze zákona povinny pro doručování písemností využít přednostně datovou schránku. Klient tak má jistotu, že se dozví o všech důležitých písemnostech, které pro něj často mohou mít nezanedbatelné právní důsledky.

Založení datové schránky lze provést na některém z kontaktních míst veřejné správy (Czech POINT). Založení schránky je zdarma. Pro fyzickou osobu samozřejmě není povinné datovou schránku mít, nicméně pro některé z dalších subjektů definovaných v zákoně je její vlastnictví nutností. Důležitým právním předpisem, který upravuje datové schránky, jejich užití a práva a povinnosti z toho plynoucí je zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů.

Za poskytnutí některých služeb iniciovaných úkonem v Datové schránce může být vybírán správní poplatek. Úřad má volbu způsobu úhrady správního poplatku. Úřad proto nejčastěji na základě podání zašle klientovi výzvu k uhrazení správního poplatku, přičemž pokud klient poplatek ve stanovené lhůtě nezaplatí, je řízení zastaveno. Výzva obsahuje číslo účtu, variabilní symbol a výši poplatku, který má klient uhradit. Po zaplacení poplatku řízení pokračuje a klientovi je poskytnuta příslušná služba.

U podání učiněného vůči úřadu platí tzv. fikce podpisu. To znamená, že takové podání se považuje za vlastnoručně podepsané. Tento mechanismus tak kromě ostatních výhod rovněž usnadňuje úřední styk.

> ►Právo učinit digitální úkon prostřednictvím datové schránky plyne z § 4 odst. 1 písm. a) zákona o právu na digitální služby.

5.4 Agendové portály jednotlivých úřadů umožňující podat úplné elektronické podání

Pro autentizovaného klienta je pohodlné využívání služeb veřejné správy prostřednictvím informačních systémů, zejména samoobslužných portálů. Takto může učinit úplné elektronické podání odkudkoli a většinou kdykoli.

Aby bylo zajištěno, že služba je poskytována konkrétnímu klientovi, je nutné jej elektronicky identifikovat s využitím tzv. národního bodu pro identifikaci a autentizaci (NIA). Jiný způsob není umožněn. Viz kap č. 6.

Formuláře, které uživatel v informačním systému vyplňuje, by již měly být předvyplněny všemi dostupnými údaji o klientovi, které má veřejná správa k dispozici. Klient nesmí být nucen znovu vyplňovat data, která o něm veřejná správa již eviduje, což zajišťuje pohodlnost tohoto způsobu podání. Úřad je povinen zajistit technické řešení propojením na tzv. referenční rozhraní veřejné správy, které je legislativně ukotveno v zákoně č. 365/2000 Sb. o informačních systémech veřejné správy.

Jelikož takové podání bude často podléhat správnímu poplatku podle zákona č. 634/2004 Sb. o správních poplatcích, ***musí úřad vyřešit placení těchto poplatků,*** aniž by musel být klient fyzicky přítomen. Jen tak lze zajistit opravdu úplné elektronické podání bez nutnosti fyzické přítomnosti klienta.

Je tedy potřebné, aby úřad zajistil implementaci platební brány do obslužného rozhraní a následného řešení pro procesy zpracování přijatých plateb.

> ►Právo učinit digitální úkon s využitím informačního systému za předpokladu prokázání identity prostřednictvím národního bodu je zakotveno v § 4 odst. 1 písm. d) zákona o právu na digitální služby.

5.5 Elektronická komunikace (prostřednictvím sítě elektronických komunikací) - zaslání elektronického dokumentu podepsaného uznávaným elektronickým podpisem

Klienti, kteří nedisponují datovou schránkou nebo nejsou schopni využít samoobslužné kanály, mohou zaslat dokument podepsaný uznávaným elektronickým podpisem.

Tento způsob je možný ze zákona, přičemž orgány veřejné správy mají ze zákona povinnost zveřejňovat adresu elektronické podatelny (§ 5 odst. 1 písm. i zákona č. 106/1999 Sb., o svobodném přístupu k informacím).

Pravidla elektronických podpisů upravuje zákon 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce. Zde je ovšem třeba rovněž věnovat pozornost evropskému nařízení eIDAS (nařízení 910/2014), které je přímo účinné ve všech členských státech EU včetně České republiky a má přednost před národními předpisy.

> ►Právo učinit digitální úkon prostřednictvím sítě elektronických komunikací s využitím písemnosti podepsané uznávaným elektronickým podpisem je zakotveno v § 4 odst. 1 písm. c).

5.6 Jiný způsob, pokud tak stanoví právní předpis

Je zcela legitimní, že mnohé úřady na základě svých agendových právních předpisů v minulosti vybudovaly řešení a technická zařízení pro tzv. přístup dálkovým způsobem, která neodpovídají ani jednomu z výše uvedených čtyř typových obslužných kanálů.

Úřady mohou tato specializovaná řešení nadále využívat, pokud umožní, aby v nich učiněné úkony a poskytnuté informace byly nadále součástí jednotné informační a znalostní základny úřadu a byly dostupné subjektu práva i v dalších obslužných kanálech. To znamená mimo jiné, že úkony učiněné v těchto řešeních se musejí opírat o jednotný datový kmen klientů, ztotožněný vůči ZR.

Pro úplnost doplňujeme i standardní komunikační kanály jako je podání učiněné v listinné formě prostřednictvím zprostředkovatele poštovních služeb, osobně na podatelně nebo ústně do protokolu. Objem podáních učiněných těmito kanály by se měl snižovat, a to ve prospěch kanálů digitálních.

5.7 Kontaktní centrum úřadu

Úřad může zřídit další asistenční kanál, který má klientům veřejné správy pomoci v situaci, kdy si neví rady, jaký obslužný kanál k poskytnutí služby využít nebo jak jej využít a jak služby čerpat. V tom případě hovoříme o multikanálovém kontaktním centru, zjednodušeně o Call-centru, případně o centru péče o klienty[9] nebo centru podpory klientů[10]

Kontaktní centrum nebo centrum podpory klientů nelze (dosud, zatím) samo o sobě považovat za digitální obslužný kanál podle zákona. Nicméně se jedná o využívaný prostředek, který za určitých podmínek umožňuje i podání nebo poskytování osobních informací.

[9] z angl. Customer Care
[10] z angl. Service Desk, Support Desk nebo Help Desk, vše víceméně synonyma.

Podstatným účelem kontaktních center je ale poskytovat podporu klientů, kteří se snaží obsloužit v samoobslužných kanálech a narážejí na nějaké potíže, například pokud obslužný kanál nepracuje jak má nebo nefunguje vůbec. Úřad si sám nastaví podpůrné procesy na řešení hlášení a poruch (nefunkčnost aplikace, nemožnost přihlášení apod.). Nemá jít jenom o podporu technickou (ICT), ale i o podporu obsahovou, podpora při řešení životní situace (výkonu agendy), a tomu je nutné centrum podpory přizpůsobit.

Formy kontaktních center

Je žádoucí, aby kontaktní centrum úřadu bylo jednotné a multikanálové, tj. aby nad údaji o službách a o klientech nabízelo pomoc ve všech obslužných kanálech. Ať již jako asistence v portálu, hlasem nebo chatem, ale i osobní asistencí na přepážce. Tento požadavek se jeví jako nadbytečný, vždyť přepážky byly výše uvedeny samostatně. Ale je žádoucí, aby kontaktní centra měly stejné informace a používaly stejný podpůrný software jako při asistenci na webu nebo po telefonu.

Podpora klientů tedy může mít mnoho podob, respektive může být dostupná v řadě komunikačních kanálů. Většině klientů veřejné správy bude nejznámější helpdesk ve formě asistenta na telefonu. Klient na portále, zajišťujícím poskytování samoobslužné služby, často nalezne telefonní kontakt, na který může v případě problémů zavolat nebo si nechá zavolat asistentem zpět[11]. Na druhém konci telefonu je asistent, který klienta navede, případně mu poradí s dalšími kroky. Výhodou tohoto způsobu je přímá interakce mezi klientem a asistentem na druhém konci telefonu. Nevýhodou je, že asistent nemusí znát řešení všech problémů, a poté je třeba situaci řešit jinak. Vyšší vývojový stupeň helpdesku umožňuje asistentovi i sdílet obrazovku klienta a pracovat s ním společně[12].

Telefon je v dnešní době asi nejsnazší, ale nikoliv jediná forma kontaktního centra. Vedle telefonního kontaktu však existují i další formy komunikace. K aplikacím poskytujícím služby jsou často zveřejňovány i emailové adresy, na které se může klient při potížích obrátit. Na emailový dotaz pak odpovídá příslušná osoba, vyhrazená na řešení těchto problémů. Výhodou podpory prostřednictvím emailu je, že klient může precizněji popsat svůj problém. Nevýhodou je, že klient musí disponovat emailovou schránkou a odpověď na dotaz může trvat déle než je tomu v případě podpory po telefonu, respektive nejedná se přímou interakci.

Nejmodernějším způsobem, který se však v současnosti stále více objevuje, je implementace ***chatu v reálném čase,*** který klientům umožňuje pokládat otázky prostřednictvím chatovacího rozhraní. Často však na druhé straně není osoba, nýbrž expertní systém, který obsahuje databázi nejčastějších dotazů a odpovědí na ně. Člověk nastupuje až v případě, kdy klient na svůj dotaz nedostane odpověď nebo je problém složitý. Výhodou této formy je opět přímá interakce klienta s expertním systémem a následně člověkem, pokud je problém obtížnější. Na straně poskytovatele je výhoda také v tom, že jednodušší dotazy a problémy klientů odfiltruje implementovaný expertní systém a člověk nastupuje až v případě, že problém je složitější a nelze ho jednoduše vyřešit. Tím je šetřen čas pracovníků a náklady na případné experty. Nevýhodou může být delší čas vyřizování v případě, že problém je složitý.

Nelze přesně říci, že jeden způsob podpory je horší než ostatní, a proto byly u každého uvedeny jeho výhody a nevýhody. Vždy samozřejmě záleží na poskytovateli, které komunikační kanály pro centrum podpory implementuje. Je ale strategií eGovernmentu ČR, aby těchto kanálů bylo vždy více, a je pak na klientovi, kterou formu podpory si vybere.

---

[11] z angl. funkce „Call-me-Back“
[12] z angl. Co-Browsing

Do budoucna vize obslužných kanálů eGovernmentu předpokládá, že klienti se pro řešení svých životních situací a při potížích v univerzálních obslužných kanálech budou obracet na ústřední Kontaktní centrum veřejné správy (KCVS), které bude poskytovat služby podpory 1. úrovně[13].

Toto centrum bude real-time komunikačními i datovými prostředky integrováno s lokálními kontaktními centry velkých úřadů, zejména ministerstev, která budou poskytovat agendově specifickou podporu[14] a umožní případné předání podnětu až na odborného gestora předmětné služby nebo předmětného ICT řešení.

5.8 Popis optimálního stavu, základní principy a pravidla

Doporučením pro úřady lze obecně formulovat tak, aby při digitalizaci svých agend důsledně využívaly a realizovaly výše zmíněné obslužné kanály s maximální ohledem na přívětivost služeb pro koncového klienta.

► Základní právní oporou pro obslužné kanály je § 4 odst. 1 zákona č. 12/2020 Sb. o právu na digitální služby, ze kterého plyne právo uživateli služby (klientovi veřejné správy) činit úkony prostřednictvím různorodých kanálů.

5.9 Klíčové otázky

1)	**Může klient využívat všechny druhy obslužných kanálů (pro agendy úřadu uvedené v katalogu služeb), které uvádí zákon o právu na digitální služby?** *Je potřeba si vyžádat přehled obslužných kanálů pro agendy, které úřad uvedl v katalogu služeb veřejné správy https://archi.gov.cz/nap:katalog_sluzeb a zkontrolovat jaké kanály úřad využívá. Zároveň je potřeba vyžádat plán zavádění digitalizace agend, nejlépe obsažený v informační koncepci úřadu a provést kontrolu, zdali úřad splnil závazek zavádění obslužných kanálů.*
2)	**Má úřad plán zavádění digitalizace agend a realizace příslušných obslužných kanálů?** *Dle § 14 odst. 4 zákona 12/2020 Sb. je stanoven termín digitalizace ohlášených agend. Je potřeba vyžádat tento plán nebo informační koncepci úřadu, kdy by měl být uveden a provést kontrolu realizačních opatření, např. dokumentaci přípravných nebo realizačních projektů nebo příslušný investiční plán.*
3)	**Může klient zaplatit správní poplatek elektronicky prostřednictvím platební brány?** *Je potřeba zkontrolovat funkcionalitu portálu úřadu, na kterém je příslušná služba publikována.*
4)	**Může klient v případě potřeby využít služeb helpdesku nebo jiných služeb kontaktního centra úřadu?** *Je potřeba vyžádat dokumentaci (provozní pokyny) k těmto kanálům a zkontrolovat dostupnost služby deklarovanou v dokumentaci.*
5)	**Má úřad ustaveného správce Katalogu služeb a jejich rozvoje na základě zpětné vazby klientů?** **Plní tento pracovník i roli správce obslužných kanálů úřadu, má dostatečnou pravomoc sjednocovat obsluhu klientů úřadu napříč jednotlivými agendami?** *Je potřeba si vyžádat dokumentaci (rozhodnutí, řídicí akt, popis pracovní pozice) deklarující pravomoci této role.*

[13] angl. First Level Support
[14] angl. Second Level Support

6)	**Udržuje úřad jednotnou informační a znalostní základnu pro obsluhu klientů, zejména pak centrální datový kmen klientů úřadu?** *Je potřeba si vyžádat dokumentaci k vedení datového kmene klientů, a posoudit způsob vedení záznamů komunikace s klientem v obslužných kanálech. Je potřeba zkontrolovat jaké jsou závazky úřadu v informační koncepci ve vztahu k obsluze klientů.*

5.10 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Portál Moje daně.

Úřad na svém portálu publikoval online služby finančního úřadu, kde klient najde daňovou informační schránku a její modernizovanou verzi, která přináší zjednodušení, zrychlení a vyšší komfort elektronické komunikace s Finanční správou.
Daňový subjekt může prostřednictvím daňové informační schránky získávat informace shromažďované ve spisu a na osobním daňovém účtu. Může získávat také informace o svých právech a povinnostech a činit podání s využitím vybraných informací, které o něm správce daně zpracovává.

▸ Příklad dobré praxe

Integrovaný systém plnění ohlašovacích povinností (ISPOP) a Centrální registr životního prostředí (CRŽP).

Oba systémy představují základ nové architektury informačních systémů rezortu životního prostředí, přes které mj. firmy a další subjekty hlásí institucím veřejné správy informace o vlivu jejich ekonomické činnosti na životní prostředí.
Pro uživatele systémů ministerstvo ve spolupráci s externí agenturou zajišťuje pomoc při práci prostřednictvím call centra – tel.: 490 522 536, každý pracovní den od 9:00 do 15:00 – a elektronického písemného helpdesku.

▸ Příklad dobré praxe

Komplexní portály MPSV a ČSSZ

Úřady přistoupily k řešení komunikace s klienty velkoryse a zejména proto, že obsluhují značnou část populace.
Na portálech jsou uvedeny online služby, informace a formuláře pro řešení životních situací pojištěnců, zaměstnavatelů a OSVČ.

▸ Příklad dobré praxe

Obecné využití různorodých obslužných kanálů

Úřad umožňuje pro klienty využití relevantních obslužných kanálů veřejné správy.
Úřad si tímto opatřením zvýšil efektivitu práce a zároveň zmírnil problémy s personálními zdroji.
Úřad využil externí organizace při realizaci centrálních služeb veřejné správy, protože má omezené kvalifikované zdroje.
Úřad rovněž zpracoval realistický plán postupné digitalizace agend a prodiskutoval s OHA architekturu řešení a možnosti využívání potřebných dat vedených v datovém fondu ČR a zároveň technické řešení a kapacity přenosu dat.

▸ Příklad špatné praxe

Osobní přítomnost klienta na přepážce

Úřad při vyřizování žádostí vyžaduje, aby se klienti dostavili osobně na přepážku. Podoba tohoto úkonu navíc vůbec není zakotvena v legislativě. Úřad nemá v plánu realizaci obslužných kanálů, prostřednictvím kterých může klient svoji životní situaci vyřídit bez nutnosti fyzické přítomnosti.

- Tento přístup značně omezuje práva klientů činit digitální úkony.
- Vyřizování takových požadavků zbytečně maří čas pracovníků na jednoduchých úkonech, které by mohly být realizovány plně elektronicky.
- Klienti, kteří disponují potřebnými nástroji (datová schránka, prostředek pro elektronickou identifikaci) jsou tak zbytečně omezeni ve svých právech činit digitální úkony. Musí se dostavit osobně na přepážku, což je stojí nemálo času. Poskytování služeb takovým způsobem je pro ně značně nepohodlné.

▸ Příklad špatné praxe

Potíže s placením

Úřad vyžaduje po klientech zaplacení správního poplatku za provedené úkony nebo jiné platby, ale nabízí pouze platbu v hotovosti, popřípadě převodem na účet. Klient tedy nemůže při poskytnutí asistované služby zaplatit kartou, protože úřad nedisponuje platebním terminálem. Je tak nucen u sebe mít hotovost a zaplatit příslušný poplatek na pokladně. Pokud klient platí například více správních poplatků nebo jinou platbu o vyšší částce, musí při sobě mít dostatečnou hotovost.

Klienti využívající samoobslužnou formu poskytování služeb pak nemohou platit kartou a jsou nuceni platit převodem z účtu. Musí vyplnit a zkontrolovat všechny údaje (č. účtu, variabilní symbol…) a často ztrácejí kontrolu nad procesem podání.

6 Identifikace subjektů v informačních systémech

V této kapitole budeme rozlišovat popis identifikace státních zaměstnanců včetně pracovníků veřejné správy (typicky agendových IS s uživateli v pozici úředníků, gestorů a správců) a klientů veřejné správy – občanů. Klienty VS jsou i právnické osoby (PO), nicméně i za ně vždy jedná fyzická osoba (FO), resp. oprávněná fyzická osoba. Obecně je potřeba rozlišovat identifikaci a identifikátory subjektů práva (FO i PO), tj. uživatelů služeb dle zákona č. 12/2020 Sb. a identifikaci konajících osob (vždy jen FO) a jejich oprávnění jednat za subjekt práva.

Identifikace je běžnou součástí poskytování služeb a má zajistit, že je služba poskytována konkrétnímu klientovi. Při fyzickém styku je identifikace prováděna vizuálně, tedy klient přijde na přepážku úřadu pro vyřízení služby a jeho identifikace proběhne pomocí dokladu totožnosti typu občanský průkaz. Podobně jako jde o automatickou činnost při poskytování služeb při fyzickém styku, je potřeba přistupovat k identifikaci i ve vzdáleném (elektronickém) styku.

Elektronická identifikace přináší řadu možností nad rámec fyzické identifikace a proto se celý proces prokazování a ověřování totožnosti rozpadá na 3 základní kroky:

1. Identifikace.
2. Autentizace (někdy označované také jako autentizace či autentifikace).
3. Autorizace.

V prvním kroku jde vždy o prokázání totožnosti, neboli předání takových údajů, které mají zaručeně ukázat pouze na jednoho konkrétního klienta. Typickým příkladem může být set údajů jméno+příjmení+datum narození nebo číslo občanského průkazu. Za identifikaci se dá ale považovat i zadání uživatelského jména na portálu či klientského identifikátoru (např. číslo pojištěnce).

V druhém kroku jde o ověření totožnosti, neboli na základě prokazované totožnosti z prvního kroku úřad zjišťuje, zda jde skutečně o toho klienta, za kterého se vydává. V řadě elektronických služeb jsou tyto dva kroky sloučené pomocí například znalosti nejen uživatelského jména, ale i hesla. Zde se uplatňují i principy více faktorové autentizace, kdy kromě hesla je nutné využít další faktor, například kód z SMS nebo potvrzení v mobilní aplikaci.

Poslední krok je přidělení role ověřené identitě. Jakmile je úřadu známa totožnost a je i ověřena, může se této identitě přiřadit oprávnění. Oprávnění mohou být různého charakteru i členění dle potřeb informačního systému. Nejčastější jsou role čtenář, editor, schvalovatel, atd. Pro potřeby zastupování a mandátů se ovšem musí uvažovat i role statutární zástupce, rodič, zákonný zástupce, zmocněnec, atd.

Povinnost elektronické identifikace

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

► § 2 zákona č. 250/2017 Sb., o elektronické identifikaci.

Kvalifikované systémy elektronické identifikace jsou dostupné a poskytované skrze Národní bod pro identifikaci a autentizace (známý také jako NIA)

Národní bod pro identifikaci a autentizaci (NIA) je centrální bod federativního systému, který zajišťuje komunikaci a registraci účastníků (v této federaci pouze pro občany ČR a cizince s trvalým/přechodným pobytem evidované v základním registru obyvatel). Tato komponenta zajišťuje současně vždy

jednoznačné ověření totožnosti osoby, která prokazuje svoji totožnost s využitím autentizačních prostředků (prostředků pro elektronickou identifikaci). Je definován v zákoně č. 250/2017 Sb. jakožto informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace. Zajišťuje úřadům státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principy Single Sign-On.

IK ČR stanovuje v oblasti identifikace v informačních systémech dosažení následujících cílů:

- 1.04 Rozvoj on-line „front-office“ služeb jednotlivých rezortů.
- 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.
- 6.01 Efektivní a uživatelsky přívětivá IT podpora práce úředníků.

6.1 Identifikace klientů veřejné správy

Pro jednoznačnou elektronickou identifikaci a autentizaci klientů veřejné správy Česká republika vytvořila technický a právní rámec, který umožňuje všem správcům informačních systémů veřejné správy vytvářet vzdálené přístupy ke svým službám s použitím prostředků identifikace schválených státem. Úřad musí postupovat při zavádění způsobu identifikace klientů v souladu s Informační koncepcí ČR a bez nutnosti vytváření vlastních nákladných řešení a zvyšování administrativní zátěže.

Elektronickou identifikací ve smyslu zákona č. 250/2017 Sb., o elektronické identifikaci, který je spolu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce promítnutím Nařízení Evropského parlamentu a rady EU č 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. Zároveň se zde omezíme pouze na část elektronické identifikace a s ní spojenými tématy, ačkoliv vlastní nařízení je podstatně širší (pečetě, certifikáty, důvěryhodnost dokumentů apod.).

Proč vlastně chceme elektronickou identifikaci?

Tak, jako se musíme na úřadech prokázat platným průkazem totožnosti, aby bylo jasné, s kým daný úředník hovoří, tak i v online komunikaci s různými portály musíme svoji identitu prokázat. Je to stejné, jen s tím rozdílem, že na druhé straně není úředník, ale různé informační systémy.

Průkaz totožnosti v elektronickém světě - **elektronický identifikační prostředek (eID)**. Ten může mít různé způsoby použití a také různou úroveň důvěry (zcela odlišná je pro identifikaci v knihovně při zapůjčení knihy a pro identifikaci osoby na katastru nemovitostí, kde jde o nakládání s majetkem – zde musí být dostatečně zaručena její pravost a správnost údajů.

Způsoby zřízení identity pro komunikaci s veřejnou správou

Občan ČR si musí pro tento účel pořídit identifikační prostředek, který ČR uznává a to vydávaný státem, nebo soukromoprávními poskytovateli.

Klíčovým systémem pro zajišťování komunikace s veřejnou správou je ***Národní identitní autorita***. Ta vytváří federativní systém zajišťující orgánům veřejné správy státem garantované služby identifikace a autentizace, který se skládá z následujících komponent:

- ***Národní bod pro identifikaci a autentizaci*** jako centrální bod federativního systému, který zajišťuje komunikaci a registraci účastníků federace. Tato komponenta zajišťuje současně vždy jednoznačné ztotožnění osoby, která prokazuje svoji totožnost s využitím autentizačních prostředků (prostředků pro elektronickou identifikaci). Je definován v zákoně č. 250/2017 Sb. jakožto informační systém veřejné správy podporující proces elektronické identifikace

a autentizace prostřednictvím kvalifikovaného systému elektronické identifikace. Zajišťuje orgánům veřejné správy státem garantované služby identifikace a autentizace včetně federace údajů o subjektu práva ze základních registrů a možnost předávání přihlašovací identity dle principy Single Sign-On.

- ***Kvalifikovaný správce,*** který vydává jednoznačně identifikovaným fyzickým osobám prostředky pro vzdálenou autentizaci (prokázání totožnosti) a provádí veškeré činnosti spojené se správou těchto prostředků a prokazováním totožnosti fyzické osoby, tj. spravuje kvalifikovaný systém elektronické identifikace.
- ***Kvalifikovaný poskytovatel online služeb,*** který připojuje k Národnímu bodu online služby, ke kterým je vyžadováno přihlášení prostředky vydanými kvalifikovanými správci.
- **Základní registry**, které poskytují jednoznačnou identifikaci osoby a zajištění vazeb této osoby vůči referenčním údajům o osobě.
- ***Národní uzel eIDAS,*** který je samostatnou součástí Národního bodu a zajišťuje přijímání vzdáleného prokázání totožnosti z ohlášených systémů dle nařízení eIDAS a předávání vzdálené identifikace a autentizace z České republiky ostatním státům EU. Ostatní státy EU musí akceptovat české identity od 13. 9. 2020, kdy vypršela roční lhůta pro zavedení akceptace ohlášeného prostředku elektronického občanského průkazu.

►eID prostředky vydává tzv. kvalifikovaný správce – poskytovatel identifikačních prostředků, který získal akreditaci ministerstva vnitra a je napojen na Národní bod pro identifikaci a autentizaci (NIA). Identifikační prostředky vydané v souladu se zákonem č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů, jsou v současné době vydávány státem i soukromoprávními kvalifikovanými správci.

Co to vlastně eID prostředek je a co je nutné o něm vědět

Prostředky eID jsou určeny pro vzdálené prokazování totožnosti při využívání online služeb. Mohou nabývat různých fyzických forem, anebo vlastností či znalostí daného vlastníka eID prostředku (plastové karty s čipem, USB tokeny, „jméno a heslo“, scan rohovky oka, atd.). Podle toho, jak vysokou bezpečnostní úroveň záruky poskytují, jsou dle Nařízení eIDAS rozděleny na NÍZKÁ, ZNAČNÁ a VYSOKÁ. Hovoříme zde o úrovni jistoty, nakolik si může být poskytovatel služeb jistý, že jste to Vy, kdo používá Vaše eID k ověření služby, a ne někdo jiný, kdo se za Vás vydává.

- Nízká – u nízké úrovně nedošlo k zaručenému ověření totožnosti – uživatel volí uživatelské jméno a heslo a svoji identitu pouze deklaruje.
- Značná - (např. NIA ID) jde o tzv. dvoufaktorovou autentizaci – jméno, heslo a jednorázově zasílaný SMS kód. Totožnost byla ověřena před aktivací prostředku (na kontaktním místě veřejné správy Czech POINT, prostředkem stejné nebo vyšší úrovně důvěry nebo pomocí datové schránky). Tato úroveň je využitelná pro komunikaci s veřejnou správou.
- Vysoká - u vysoké úrovně jde o ztotožnění, kdy má fyzická osoba identifikační prostředek na bezpečném zařízení (např. na kontaktním čipu občanského průkazu, který má u sebe), při jeho vydání byla zaručeně ověřena totožnost a fyzická osoba zná přístupové údaje k jeho použití.

Úřad či obecně poskytovatel služby volí pro přístup k jednotlivým službám odpovídající úroveň důvěry. V některých případech stačí úroveň nízká, vyžadující pouze uživatelské jméno a heslo, bez dvou faktorové autentizace.

Kdo je to poskytovatel služeb (Service provider – dále SeP) a co je nutné o něm vědět?

SEP je poskytovatel služeb vůči kterému se klienti identifikují – přihlašují. Prakticky jde o provozovatele a poskytovatele různých služeb, ať už veřejné správy, anebo soukromoprávních. Typicky jde o portály státu, ministerstev, úřadů, krajů, měst a obcí, knihoven, nemocnic, zdravotních pojišťoven, škol apod. Seznam registrovaných SePů naleznete na https://info.identitaobcana.cz/sep/

Klientský kmen a klientský identifikátor

Úřad by si pro jednotnou a jedinou evidenci klientů, kterým poskytuje všechny své služby, měl zřídit a udržovat jejich evidenci tzv. klientský kmen. Tato evidence kmenových dat klientů s jejich osobními údaji prostřednictvím transparentního veřejného „Klientského identifikátoru" provazuje informace o tom, ve kterých systémech se o klientovi vedou transakční údaje o jednotlivých případech. Každý úřad má právo si takovouto evidenci vést a usnadnit si tak poskytování údajů o jedné osobě z více informačních systémů či evidencí.

Příkladem evidence, která může být zárodkem klientského kmene, je jmenný rejstřík z elektronického systému spisové služby. V něm se shromažďují údaje o fyzických a právnických osobách, kterých se týkají dokumenty uložené ve spisové službě. Protože však spisová služba nemusí obsahovat vše a ne každý klient se musí ve spisové službě objevit, je vhodné jej brát jen jako zdroj pro budování klientského kmene.

V klientském kmeni jsou všechny subjekty ztotožněny a přiděluje se jim klientský identifikátor, který je bezvýznamový, veřejný a slouží k identifikaci. Je to stejná situace, jako v soukromoprávním světě, kde je klientské číslo přidělováno např. pro potřebu platby faktur a sjednocení identifikace zákazníka mezi více divizemi společnosti.

Důležitou poznámkou je, že pro veřejnou správu se dlouhou dobu používá jako klientský identifikátor rodné číslo, které je pro některé agendy pouze přejmenováno např. na číslo plátce daně, číslo pojištěnce apod., ale jde stále o ten samý identifikátor. Rodné číslo a jeho význam pro identifikaci ve veřejné správě se má postupně utlumovat, protože nesplňuje parametry pro klientský identifikátor a jeho snadné zneužití a nemožnost revokace je přílišným rizikem.

6.2 Identifikace uživatelů interních systémů veřejné správy

Státní zaměstnanci a ostatní pracovníci veřejné správy by měli mít možnost pro přihlášení do systémů veřejné správy za účelem výkonu agendy využít prostředků elektronické identifikace dostupných v NIA. Protože však nemusí být vhodné ani žádoucí využívat identifikační prostředky, které jsou vydány fyzické osobě bez vazby na její roli či zaměstnání ve veřejné správy, pro výkon agendy, je k dispozici systém JIP/KAAS. JIP (jednotný identitní prostor) a KAAS (katalog autentizačních a autorizačních služeb) slouží jak pro identifikaci, autentizaci, tak i autorizaci a přidává tedy k ověřené identitě i její roli v rámci informačních systémů veřejné správy. Aby mohl informační systém veřejné správy využívat JIP/KAAS, musí být připojen k centrálnímu místu služeb (CMS).

JIP/KAAS jako autentizační systém

Orgán veřejné moci, který byl zaregistrován pro výkon agendy, nebo soukromoprávní uživatel údajů, který byl zaregistrován pro výkon agendy, může provést autentizaci fyzické osoby, která je nositelem role. Orgán veřejné moci, který byl zaregistrován pro výkon agendy, nebo soukromoprávní uživatel údajů, který byl zaregistrován pro výkon agendy, využívá k autentizaci fyzické osoby, která je nositelem role, informační systém sloužící k autentizaci fyzických osob, které jsou

nositeli rolí, (dále jen „autentizační informační systém“) nebo informační systém, jehož je správcem.

► 56a odst. 1 zákona č. 111/2009 Sb., o základních registrech

Kvalifikované systémy elektronické identifikace jsou dostupné a poskytované skrze Národní bod pro identifikaci a autentizace (známý také jako NIA)

Z pohledu uživatele přihlašujícího se k informačnímu systému veřejné správy, ve kterém chce vykonávat agendu, by měla být vždy dostupná možnost využít systém JIP/KAAS. Následně je na daném uživateli zda využije identifikační prostředky NIA (čímž se naplní povinnost § 2 zákona č. 250/2017 Sb.) nebo dedikované prostředky JIP/KAAS.

6.3 Popis optimálního stavu, základní principy a pravidla

S nastupujícími novými technologiemi, zejména pak v oblasti aplikací pro chytré telefony, se tlačí do popředí Mobilní klíč eGovernmentu (MEG). Jde o aplikaci pro Android nebo iOS, která umožňuje na základě biometriky a snímání QR kódu jednoduché přihlášení k Národnímu bodu identifikace a autorizace. Tím se pro uživatele výrazně zjednodušuje a tím i usnadňuje proces přihlášení a ověření vlastní identity.

Ke konci roku 2021 provozovalo svoje elektronické služby přes 200 kvalifikovaných poskytovatelů, SePů. Po skončení výjimky v platnosti zákona o elektronické identifikaci (30. 6. 2020) registruje ČR rychlejší přírůstek jednotlivých portálů a poskytovatelů služeb, které ruší svůj lokální identifikační kmen a přechází na identifikaci přes Národní bod identifikace a autorizace. Stálicemi v oblasti četnosti elektronické identifikace k jednotlivým poskytovatelům jsou portály veřejné správy. Zde se jasně ukazuje, že naše úsilí ve vytvoření kvalitních služeb státu je oceňováno občany ČR, kteří stále více používají tyto služby k online vyřízení svých úkonů vůči státu.

Co se týká vlastních úřadů, jde téměř výhradně o tzv. portály občanů, popřípadě klientů různých úřadů. Tedy o situace, kdy se daný občan přihlašuje k portálu a prokazuje svoji identitu, aby mohl následně nahlížet na data a činit úkony vůči danému úřadu. Dříve se občan musel nejprve zaregistrovat a úřad zavedl identitu klienta ve svém systému. Úřady by měly tento způsob identifikace zrušit a nahradit mechanismem volání NIA pro ověření identity.

6.4 Klíčové otázky

1)	**Je pro všechny klienty veřejné správy při potřebě identifikace využit Národní bod pro identifikaci a autentizaci?** *Je potřeba si vyžádat dokumentaci popisující možnosti přístupu klientů ke službám úřadu a posoudit nakolik je využit doporučovaný způsob přihlašování přes NIA. Pokud není zaveden vyžádat si plán zavedení.*
2)	Je pro **úředníky přistupující k informačním systémům veřejné správy vykonávající agendu dostupný systém JIP/KAAS?** *Je potřeba si vyžádat seznam osob s autorizací přistupujících k JIP/KAAS. Pokud úřad přístup nevyužívá, vyžádat si odůvodnění. Je potřeba zjistit která osoba v úřadu je v roli lokálního administrátora JIP/KAAS a zdali tuto činnost vykonává.*
3)	**Vedete si všechny klienty v jednotné evidenci? Využíváte pro provázání (identifikaci) klientů mezi systémy a evidencemi klientský identifikátor?** *Je potřeba si vyžádat prohlášení o způsobu vedení klientských identifikátorů, a pokud je jím rodné číslo, vyžádat si záměr přechodu na bezvýznamový identifikátor.*

4)	**Je úřad připraven fungovat v agendách bez rodného čísla jako identifikátoru fyzické osoby?** *Je potřeba si vyžádat prohlášení o způsobu vedení klientských identifikátorů, a prohlášení o způsobilosti úřadu vést agendu bez rodného čísla.*

6.5 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Úřad kromě standardních postupů spočívající ve fyzické přítomnosti klienta nebo listinném zaslání podání poskytuje také možnost vyřízení služeb na portálu úřadu. Pro zajištění jednoznačné ověřené totožnosti je úřad registrován jako kvalifikovaný poskytovatel služeb v NIA a poskytuje možnost přihlášení klientovi pouze těmito prostředky. Po přihlášení má úřad státem garantovanou jistotu, že jde o osobu, za kterou se vydává a může jí poskytovat stejný rozsah služeb, jako pro klienta na fyzické přepážce.

Úřadu odpadá značné množství klientů, kteří si služby vyřídí samoobslužně, čímž šetří čas a prostředky nejen své, ale i svých klientů.

▸ Příklad špatné praxe

Úřad kromě standardních postupů spočívající ve fyzické přítomnosti klienta nebo listinném zaslání podání poskytuje také možnost vyřízení služeb na portálu úřadu. Pro zajištění přihlášení vydává každému, kdo o to fyzicky na přepážce úřadu požádá, přihlašovací údaje.
Jelikož klienta vždy fyzicky ztotožnil a tím ověřil jeho identitu, má toto řešení úřad za nejlepší možné. Bohužel s postupem času a narůstajícím počtem klientů úřad zjistit, že správa vydaných přihlašovacích údajů si vyžaduje práci a čas více lidí a prostředků. Nejedná se totiž jen o samotné vydání, ale i blokace např. z důvodu prozrazení hesla, nutnost poskytovat klientům součinnost, pokud zapomenou heslo atd.

Úřad tedy neefektivně nakládá se svými prostředky, protože veškerou zodpovědnost za identifikaci a autentizaci mohl přenést na stát. Nehledě na klienty, kteří si kvůli tomuto úřadu musí pamatovat další přihlašovací údaje, ačkoliv většina z nich disponuje alespoň jedním z prostředků Národního bodu pro identifikaci a autentizaci.

7 Elektronický oběh dokumentů

Výkon státní správy a samosprávy je doprovázen vytvářením dokumentů, jejich podepisováním, evidencí, odesíláním, příjmem, skartací atd. Tyto činnosti, souhrnně nazývané jako správa dokumentů, jsou vykonávány především v rámci spisové služby, ale dalších evidencí. Řada subjektů má dle zákona č. 499/2004 Sb. povinnost vykonávat spisovou službu v elektronické podobě, tj. prostřednictvím systémů elektronické spisové služby (eSSL). Podrobné technické požadavky na aplikační a byznysové funkce eSSL stanovuje národní standard pro eSSL a své požadavky stanovuje také Národní architektonický plán v části pravidla pro eSSL.

Zaručení pravosti dokumentů v digitální podobě

Aby mohl být oběh dokumentů realizován elektronicky, musí povinné subjekty zajistit připojení autentizačních a autorizačních prvků na vytvářené dokumenty v digitální podobě a ověření autenticity doručených dokumentů. Nařízení eIDAS poskytuje konzistentní právní rámec pro používání a uznávání elektronických podpisů, pečetí a časových razítek. A právě využití elektronického podpisu, zaručeného elektronického podpisu a zejména kvalifikovaného elektronického podpisu, který je právně položen na úroveň vlastnoručního podpisu, umožňuje efektivní oběh dokumentů s jejich zaručením pravosti.

Věrohodnost původu dokumentu

Pro dokumenty v digitální podobě, kde se jejich uchováváním rozumí rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, a konečně i tvorba a správa metadat náležejících k těmto dokumentům (musí být v souladu s tímto zákonem, připojené údaje prokazují existenci dokumentu v čase). Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.

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

Zasílání dokumentů elektronicky a právní účinky elektronické komunikace

Pro zajištění důvěryhodné, bezpečné a průkazné elektronické komunikace mezi orgány veřejné moci na straně jedné a fyzickými či právnickými na straně druhé, jakož i mezi orgány veřejné moci navzájem, slouží informační systém datových schránek (ISDS). ISDS pomáhá zajistit nejen nejpřísnější podmínky vyžadované v rámci kybernetické bezpečnosti, ale zároveň přispívá k posílení důvěry, zjednodušení komunikace a správnosti dokumentů mezi úřady. **Datové zprávy odeslané a přijímané mezi orgány veřejné moci prostřednictvím datových schránek mají stejné právní účinky,** jako kdyby byly odeslány v analogové podobě prostřednictvím podatelny. Datové zprávy mezi úřady a mezi úřady a klienty jsou bez poplatku.

Datové formáty dokumentů a možná konverze

Zákon o archivnictví a spisové službě zavádí pojem „výstupní datové formáty dokumentů“, tj. formáty, které musí veřejnoprávní původci přijímat. Definice těchto formátů je uvedena v § 23 vyhlášky č. 259/2012 Sb. Zákon o archivnictví a spisové službě též stanoví specifické podmínky pro práci s dokumenty v digitální podobě jako je například převod mezi analogovou a digitální podobou nebo změna datového formátu.

Automatizovaný oběh dokumentů

K zajištění efektivního oběhu digitálních dokumentů v úřadu je nezbytné integrovat spisovou službu a příslušný agendový informační systém. Plná integrace těchto systémů umožní automatizované zpracování dokumentů a sníží prostor pro duplicity a chyby. Někdy však tento způsob samozřejmě není možný, například u dokumentů s utajovanými informacemi.

Elektronická fakturace

Elektronická fakturace umožňuje bezpapírovou výměnu strukturovaných elektronických faktur a dalších dokladů, jejich rychlé zpracování a přenositelnost mezi podniky, veřejnou správou i soukromými osobami. Informace o národním standardu elektronické fakturace jsou zveřejňovány na stánkách MV ČR.

Povinnost elektronické fakturace

Povinnost akceptovat elektrickou fakturu se týká všech zadavatelů, kteří přijímají platbu plnění veřejné zakázky. Tato povinnost platí od 1. 1. 2019 pro ústřední orgány moci a od 1. 4. 2020 pro uzemní samosprávu. Všechny povinné orgány veřejné moci musí kromě procesních změn zajistit i příjem a vydávání elektronických faktur dle evropských a českých pravidel.

► v §221 zákona č. 134/2016, o zadávání veřejných zakázek

► Usnesení vlády č. 347/2017, k realizaci úplného elektronického podání a povinném přijímání elektronických faktur ústředními orgány státní správy

Užívání elektronické fakturace je jednou z klíčových priorit, které významně přispívá k dosažení klimatické neutrality EU, závazků ČR do obnovitelných zdrojů a cirkulárního hospodaření, jež vyplývají ze strategických dokumentů vlády ČR. [15]

Řešení digitální kontinuity – zajištění dlouhodobé důvěryhodnosti informací a dokumentů

Zjednodušeně lze říci, že opatření mají charakter nového elektronického podepsání, nového zapečetění či nového opatření kvalifikovaným elektronickým časovým razítkem. Všechny tyto tři možnosti totiž znamenají, že se na autentizaci původního dokumentu použijí aktuálně dostatečně silné kryptografické postupy a tím je zajištěna dostupnost, důvěra a integrita dokumentů.

Elektronizace procesů nad všemi dokumenty kolujícími v rámci úřadu respektuje architektonické principy *P1: Standardně digitalizované* a *P12: Vnitřně pouze digitální* a určuje kvalitu a efektivitu práce státní správy a územní samosprávy.

IK ČR stanovuje v oblasti elektronického oběh dokumentů dosažení následujících cílů:

- 3.02 Digitalizace dosud nedigitalizovaného obsahu důležitého pro podporu konkurenceschopnosti a rozvoj eGovernment služeb pro veřejnost.

[15] Programové prohlášení vlády České republiky, viz. programove-prohlaseni-vlady-Petra-Fialy.pdf (vlada.cz)

- 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu.
- 5.08 Podpora budování agendových systémů v samosprávné působnosti, spisové služby a oběhu dokumentů a provozních systémů (Mail, ERP, HR).
- 6.02 Digitalizace vnitřních činností a dokumentů úřadů.
- 6.04 Modernizace podpůrných a provozních informačních systémů úřadu.

7.1 Popis optimálního stavu, základní principy a pravidla

Úřad využívá systém ISDS jako integrální součást jejich elektronické spisové služby. Elektronická spisová služba zároveň umožňuje přijímání faktur ve formátu ISDOC (Information System Document).

Shrneme-li základní požadavky, pak povinné subjekty musí:

1. Vykonávat spisovou službu tak, aby evidovala dokumenty v elektronickém systému spisové služby, nebo v samostatné evidenci dokumentů.
2. Zajistit soulad eSSL a všech samostatných evidencí dokumentů vedených v elektronické podobě s požadavky Národního standardu pro elektronické systémy spisové služby.
3. Zajistit integraci ostatních informačních systémů na eSSL či samostatnou evidenci dokumentů dle požadavků Národního standardu.
4. Přiřazovat bezvýznamové identifikátory osobám vedených ve jmenném rejstříku a vytvářet a spravovat vazby všech dokumentů obsahujících osobní údaje na osoby v tomto rejstříku.
5. Řádně uchovávat a spravovat digitální dokumenty a jejich komponenty v eSSL nebo samostatné evidenci dokumentů.
6. Provádět evidenci metadat o spisech, dokumentech a dalších entitách a zajistit evidenci všech transakcí a definovaných operací v eSSL či v samostatné evidenci v souladu s požadavky Národního standardu
7. Zajistit příjem, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování dokumentů ve skartačním řízení v souladu s archivním zákonem, spisovou vyhláškou a Národním standardem
8. Zajistit řádné ověření autenticity a integrity doručených dokumentů v digitální podobě v souladu s nařízením eIDAS a zákonem č. 297/2016 Sb. a zajistit v souladu s uvedenými předpisy řádné připojení autentizačních a autorizačních prvků na dokumenty v digitální podobě vyhotovené původcem.
9. Uchovávat dokumenty a umožnit výběr archiválií, vybrané archiválie v analogové podobě předávat příslušnému státnímu archivu a archiválie v digitální podobě příslušnému digitálnímu archivu.

7.2 Klíčové otázky

1)	**Jak často probíhá kontrola spisové služby?** *Je potřeba si vyžádat záznamy o provedených kontrolách.*
2)	**Umožňuje úřad přijímat elektronickou fakturaci a automatizovaně ji přepisovat do spisové služby?** *Je potřeba si vyžádat prohlášení o způsobu a formátu zpracování elektronické faktury dle povinnosti stanovené §221 zákona č. 134/2016 Sb. a způsobu přepisu elektronické fakturace do spisové služby. Pokud není automatizovaná vyžádat si prohlášení o záměru realizace.*
3)	**Obíhají dokumenty v úřadu ve výlučně elektronické podobě. (Respektive je plně dodržen architektonický princip: Vnitřně pouze digitální).** *Je potřeba si vyžádat seznam digitalizovaných a nedigitalizovaných agend úřadu a posoudit plnění digitalizace úřadu deklarované v informační koncepci úřadu.*
4)	**Kolik má úřad digitalizovaných agend z celkové počtu ohlášených agend? Kolik z nich má procesy integrovány s elektronickým systémem spisové služby?** *Je potřeba si vyžádat seznam digitalizovaných a nedigitalizovaných agend úřadu a porovnat je se seznamem ohlášených agend viz https://rpp-ais.egon.gov.cz/gen/agendy-detail/.* *Je potřeba si vyžádat prohlášení o integraci procesů ohlášených agend se spisovou službou.*
5)	**Je spisová služba organizace v souladu s národním standardem pro elektronické systémy spisové služby?** *Je potřeba si vyžádat deklaraci dodavatele spisové služby o souladu s národním standardem.*

7.3 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Úřad prošel procesem digitalizace vybraných agend, které představovaly největší zátěž úředníků s cílem zrychlit vyřizování žádostí a tím zefektivnit chod úřadu. V procesu přípravy digitalizace agendy byl vidět zřetelný a jasný dopad na zaběhnutý způsob používání spisové služby, kde jsou vyřizované žádosti evidovány.
Úřad zadal realizaci digitalizace agendového informačního systému včetně analýzy vykonávaných činností a rolí. Součástí dodávky byla i integrace spisové služby, kde bylo přesně vydefinováno rozhraní mezi agendovým IS a systémem spisové služby.

Úřad zadal výběrové řízení tak, aby dodavatel respektoval všechny relevantní zákonné normy a vyhlášky povinné vůči úřadu v oblasti spisové služby. Úřad rovněž věnoval úsilí k vyškolení úředníků tak, aby měli dostatečný prostor přejít na nový způsob práce.

▸ Příklad špatné praxe

Úřad funguje v režimu papírového oběhu dokumentů. Úředníci většinu dokumentů tisknou a předkládají k podpisu oprávněné osobě, dokumenty jsou průběžně archivovány dle zákona o archivnictví a spisové službě. Dokumenty jsou tedy fyzicky přenášeny z kanceláře do kanceláře. V lepším případě jsou evidovány ve spisové službě, kde se vede evidence aktuálního stavu přidělení dokumentu k vyřízení.
Úřad již v minulosti vydal pokyn k vyřizování dokumentů v elektronické podobě ve spisové službě. Pokyn však nemohl být dodržován, protože nebyly provedeny úpravy agendových informačních systémů ani jejich integrace se systémem spisové služby.

Stav přetrvává a teprve vnější tlaky vyplývající například ze zákona o právu na digitální službu, nutí úřad digitalizovat agendy a tak potažmo zefektivnit chod úřadu.

8 Komunikační infrastruktura veřejné správy

V této kapitole jsou popsány nástroje veřejné správy, které umožňují přistupovat úředníkům ke službám eGovernmentu a službám od jiných úřadů. Příručka se omezuje na základní informace a odkazuje na zdroje Ministerstva vnitra a organizací spravující toto prostředí. Na úvod je potřeba vysvětlit důležité pojmy:

Centrální místo služeb (CMS)

Soubor technického a programového vybavení, jehož prostřednictvím jsou poskytovány služby informačních systémů veřejné správy a jehož prostřednictvím jsou využívány a propojovány sítě elektronických komunikací. CMS je základním komunikačním uzlem eGovernmentu.

Klíčovým důvodem vzniku CMS je skutečnost, že je určeno ***pouze pro veřejnou správu,*** jedná se o vyhrazené a zabezpečené prostředí izolované od veřejného prostoru, např. internetu a může tak poskytovat svoje služby bez ohledu na chování a vliv externích uživatelů. CMS je budováno v rozsahu daném platnou legislativou, včetně zákona o kybernetické bezpečnosti.

Povinnost využívat CMS

Orgány veřejné správy zajistí, aby jimi spravované informační systémy veřejné správy s výjimkou provozních informačních systémů uskutečňovaly vazbu mezi informačními systémy veřejné správy na informační systémy veřejné správy spravované jinými orgány veřejné správy nebo na informační systémy soukromoprávních uživatelů údajů prostřednictvím centrálního místa služeb.

► § 6h odst. 4 zákona č. 365/2000 Sb. o informačních systémech veřejné správy

Úřady se k CMS musí připojit, aby mohly konzumovat služby od jiných úřadů. Přístup ke službám eGovernmentu pro úřady přes veřejný internet je nezákonný.

Komunikační infrastruktura veřejné správy (KIVS)

Komunikační infrastrukturu veřejné správy je nedílnou součástí systému CMS a proto se často uvádí jako jeden společný pojem. Pokud chce úřad využít KIVS, musí realizovat soutěž přes centrálního zadavatele Ministerstvo vnitra. Bude definovat požadavky na připojení na KIVS dle katalogových listů a následně zrealizovat nákup v dynamickém nákupním systému.

Vláda České republiky na svém zasedání dne 30. května 2012 přijatým usnesením č. 385 o Koncepci nákupu datových a hlasových služeb Komunikační infrastruktury veřejné správy v období po 27. březnu 2013 (dále jen "Usnesení") schválila záměr nákupu datových a hlasových služeb Komunikační infrastruktury veřejné správy (dále jen "služby KIVS") v období po 27. březnu 2013, který pro všechny orgány státní správy znamená povinnou účast na centralizovaném nákupu datových přípojek Komunikační infrastruktury veřejné správy do Centrálního místa služeb (dále jen "CMS").

Komunikační infrastrukturu veřejné správy (KIVS)/Centrální místo služeb (CMS) můžeme nazvat privátní sítí pro výkon veřejné správy všech úřadů. Tato síť poskytuje především bezpečné propojení informačních systémů veřejné správy (ISVS), případně soukromoprávních systémů pro využívání údajů (SSVÚ), působící v agendách veřejné správy s jinými ISVS, ale i například bezpečný přístup do

veřejného Internetu. Díky KIVS/CMS je přístup ke službám eGovernmentu zajištěn s definovanou bezpečností a SLA parametry. V souladu s dílčím *cílem 3.5 Informační koncepce ČR* je KIVS/CMS koncepčně rozvíjen. OVS mají povinnost poskytovat služby ISVS dle zákona č. 365/2000 Sb. prostřednictvím KIVS/CMS, s tím souvisí také pravidla pro KIVS/CMS.

Využitím KIVS/CMS se naplňují architektonické principy *P8: Jeden stát* a *P11: eGovernment jako platforma*. CMS také zajišťuje přístup např. k propojenému datovému fondu. Přehled služeb CMS je pravidelně aktualizován.

KIVS/CMS nabízí:

- 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 veřejné správy ze sítě internet.

Úřady přistupují k propojenému datovému fondu výhradně přes CMS jedním ze čtyř možných způsobů:

1. Prostřednictvím krajských sítí (například v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím metropolitních sítí připojených např. na Integrovanou telekomunikační síť MVČR.
3. Prostřednictvím Komunikační infrastruktury veřejné správy (KIVS) s využitím komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra.
4. Prostřednictvím veřejného internetu, a to přes zabezpečený tunel VPN SSL nebo VPN IPSec.

IK ČR stanovuje v oblasti komunikační infrastruktura veřejné správy dosažení následujících cílů:

- 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.
- 6.05 Modernizace a posílení digitální infrastruktury úřadu.

8.1 Popis optimálního stavu, základní principy a pravidla

Vazby mezi informačními systémy veřejné správy jednotlivých úřadů musí být uskutečňovány výlučně s využitím CMS. Tato povinnost se však nevztahuje na provozní informační systémy.

Prosté splnění zákonné povinnosti však není jediným důvodem, proč by správci informačních systémů veřejné správy měli uskutečňovat vazby na jiné systémy s využitím CMS. Infrastruktura KIVS/CMS je privátní síťová infrastruktura veřejné správy, která zajišťuje adekvátní bezpečnost a tím zabezpečený přenos mnohdy citlivých údajů mezi jednotlivými informačními systémy veřejné správy. Takové údaje nelze sdílet prostředím veřejného internetu. Dalším faktorem je pak samozřejmě spolehlivost. Informační systémy jsou a v budoucnu stále více budou pro výkon veřejné správy velice důležité, a proto je nutné minimalizovat riziko jejich výpadku resp. výpadku jejich komunikace mezi sebou. Právě propojení informačních systémů s využitím infrastruktury KIVS/CMS toto riziko snižuje na minimum.

8.2 Klíčové otázky

1)	**Komunikují vaše agendové informační systémy (AIS) a informační systémy (ISVS) s AIS a ISVS jiného orgánu veřejné správy nebo orgánu veřejné moci prostřednictvím CMS/KIVS?** *Je potřeba vyžádat prohlášení o připojení úřadu na CMS/KIVS. Pokud není připojen vyžádat zdůvodnění.*
2)	**Využíváte vlastního přístupu do veřejného internetu? Proč nevyužíváte bezpečného internetu jako služby CMS?** *Je potřeba vyžádat zdůvodnění proč nepoužívá úřad služby CMS a případně předložit schválení výjimky Hlavního architekta MV/OHA, který schvaluje realizační projekty informačních systémů veřejné správy.*

8.3 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Úřad se rozhodl respektovat zákonnou povinnost a aktivně ochránit citlivá data a nahradil komunikaci s ostatními úřady otevřeným internetem. Jeho agendové informační systémy (AIS), ale i jeho informační systémy veřejné správy (které vyžadují komunikaci s jinými úřady) komunikují s AIS a ISVS jiného OVS/OVM výhradně prostřednictvím CMS/KIVS. Infrastruktura CMS/KIVS nabízí spolehlivé zajištění komunikace mezi jednotlivými informačními systémy veřejné správy a snížení rizika odcizení citlivých dat.

Jedním z příkladů dobré praxe je napojení na Základní registry. Pokud AIS/ISVS komunikuje se ZR, musí pro tuto komunikaci výhradně využít KIVS a k ZR být připojen prostřednictvím CMS.

Výhodou je uzavřená komunikace v KIVS, probíhající mimo veřejný internet.

▸ Příklad špatné praxe

Agendové Informační Systémy (AIS) a Informační systémy veřejné správy (ISVS) daného OVS/OVM komunikují s AIS a ISVS jiného OVS/OVM prostřednictvím internetu mimo CMS/KIVS. Nezajištění komunikace jednotlivých informačních systémů veřejné správy prostřednictvím CMS/KIVS, a jejich komunikace s využitím veřejného internetu může vést k odcizení mnohdy velmi citlivých dat.

Úřad historicky komunikuje se Základními registry v otevřeném internetu. Kromě porušení zákona je připojení negarantované. Existuje riziko nedostupnosti např. z důvodu DDoS útoku na IP adresu základních registrech, vystavenou do internetu, riziko kompromitace citlivých údajů a jejich zneužití nepovolanou osobou.

9 Cloudové služby

Cloudové služby, či cloud computing nebo eGovernment Cloud (eGC), jsou v prostředí českého eGovernmentu upraveny zákonem č. 365/2000 Sb. Zákon předpokládá existenci tzv. komerční části cloud computingu a státní části cloud computingu. Komerční část obsahuje nabídky jednotlivých soukromých poskytovatelů, kteří splnili všechny podmínky a jsou tedy garancí určitých záruk pro jejich uživatele / úřady. Státní část je zatím v přípravě a měla by sloužit pro ty systémy, které jsou klasifikovány jako kritické informační systémy.

Cloud computing

je způsob zajištění provozu informačního systému veřejné správy nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému veřejné správy

►§2 odst. 1 písm. x zákona č. 365/2000 Sb., o informačních systémech veřejné správy

Postupy a pravidla využití cloud computingu ve veřejné správě jsou detailně popsány v dokumentu **„Návod na využívání cloud computingu ve veřejné správě“**, který je dostupný na webu MV (https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09Mw%3d%3d). V této kapitole uvádíme pouze základní informace určené pro výchozí orientaci pracovníků úřadu s problematikou cloud computingu ve veřejné správě.

Hlavními cíli využití cloudových služeb pro provoz informačních systémů veřejné správy jsou:

- Zvýšit rozsah sdílení aplikačních služeb VS a tím snížit náklady na IT ve veřejné správě.
- Zrychlit a zefektivnit nákup standardních (komoditních) ICT služeb.
- Snížit náklady na služby veřejné správy přepočtené na jednu ICT službu a jednoho uživatele.
- Zajistit potřebnou bezpečnost a spolehlivost provozu informačních systémů VS.

Informační koncepce ČR zohledňuje základní cíle a koncepty eGC, stanovené usnesením Vlády ČR ve Strategickém rámci Národního cloud computingu (UV 1050/2016) a rozpracovávané v rámci projektu Příprava vybudování eGovernment cloudu, jehož výstupy byly schváleny v listopadu 2018 vládou ČR (UV 749/2018).

Průběžné informace k eGovernment cloudu jsou aktualizovány na stránkách MV (https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09Mw%3d%3d).

Povinnost využívat cloud computing

Úřady nejsou povinny využívat cloud computing (neexistuje princip „cloud first“). Jsou však povinny tvořit pro své informační systémy veřejné správy tzv. hodnocení ekonomické výhodnosti způsobu provozu. Na základě tohoto hodnocení musí úřad dojít k rozhodnutí, zda je hospodárně, účelné a efektivní provozovat svůj informační systém na současné infrastruktuře nebo přejít na cloud computing.

► § 5 odst. 2 písm. j) zákona č. 365/2000 Sb. o informačních systémech veřejné správy

►§ 5 odst. 2 písm. k) zákona č. 365/2000 Sb. o informačních systémech veřejné správy

Katalog cloud computingu

Katalog cloud computingu je seznam, ve kterém se vedou údaje o poptávkách cloud computingu, poskytovatelích cloud computingu, nabídkách cloud computingu a o cloud computingu využívaném úřady. V současné podobě je zveřejněn na stránkách MVČR[16], v budoucnu by měl být součástí informačního systému cloud computingu.

Katalog je podstatný pro úřady především z důvodu povinností, které se k němu váží:

- Úřady nesmí využívat cloud computing, který není zapsán v katalogu.
- Pokud úřad využívá cloud computing, musí jej do katalogu zapsat.

Katalog cloud computingu

Úřad může využívat pouze cloud computing, který poskytovaný

a) poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu na základě nabídky cloud computingu tohoto poskytovatele zapsané v okamžiku jejího přijetí orgánem veřejné správy v katalogu cloud computingu,

b) v rámci vertikální nebo horizontální spolupráce podle právního předpisu upravujícího zadávání veřejných zakázek nebo

c) v rámci obecné výjimky z povinnosti zadat veřejnou zakázku v zadávacím řízení podle právního předpisu upravujícího zadávání veřejných zakázek.

► § 6l odst. 1 zákona č. 365/2000 Sb. o informačních systémech veřejné

IK ČR stanovuje v oblasti cloudových služeb dosažení následujících cílů:

- 5.04 Realizace optimálního modelu koordinace činnosti státních organizací a podniků, specializovaných na poskytování ICT služeb.
- 5.05 Vytvoření eGovernment cloudu.
- 5.06 Vydání a aktualizace národních funkčních a servisních standardů.
- 6.05 Modernizace a posílení digitální infrastruktury úřadu.

9.1 Popis minimálního doporučeného stavu, principy a pravidla

Prvními dvěma oblastmi při řešení oblasti cloud computingu je zajištění požadované bezpečnosti (jak fyzické, tak bezpečnostní v kybernetickém pojetí slova) informačního systému úřadu a dále posouzení ekonomické výhodnosti cloud computingu pro zajištění provozu tohoto IS.

[16] https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d

► a. Zajistit naplnění zákona č. 365/2000 Sb., o informačních systémech veřejné správy, HLAVA VI § 6i – 6z

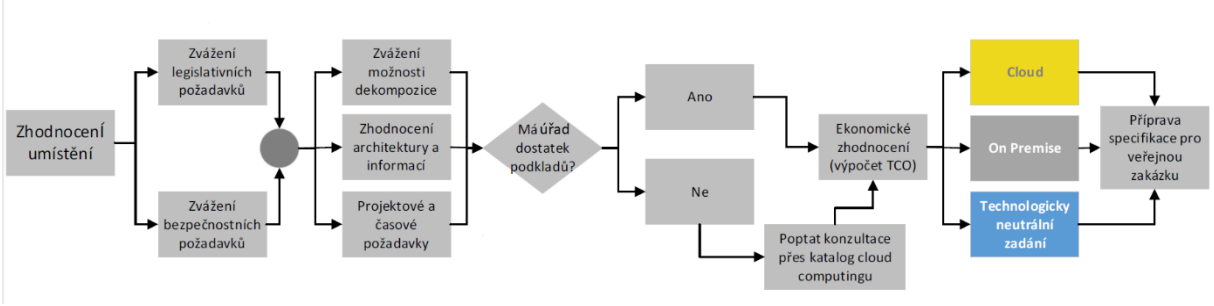
Volba cloudového řešení

Základním pravidlem pro využití služeb eGC nebo KeGC je zajištění požadované úrovně bezpečnosti služeb eGC (zde je hodnocení dopadů a klasifikace bezpečnostních úrovní) v závislosti na bezpečnostní úrovni informačního systému veřejné správy, pro který jsou cloudové služby využívány. Bezpečnostní úroveň se odvozuje od dopadů při výpadku služeb daného informačního systému (z jakéhokoli důvodu).

- Státní eGC zajistí nejvyšší úroveň bezpečnosti a je určen pro provoz služeb eGC nejvyšší bezpečnostní úrovně (kritická).
- Komerční eGC je určen pro provoz služeb eGC ostatních bezpečnostních úrovní (nízká, střední, vysoká) a v maximální míře umožňuje využití tržních mechanismů pro zajištění tržních (předpoklad konkurence a optimálnosti) cen. Povinnosti komerčních poskytovatelů služeb eGC stanoví zákon o informačních systémech veřejné správy a na základě tohoto zákona pak vydané vyhlášky ministerstva a NÚKIB. Řídící orgán eGovernment Cloudu pak na základě zákona a vyhlášek připravuje a vydává metodické pokyny. Již nyní však platí pravidla pro nutnost připojení přes infrastrukturu CMS/KIVS a tím i respektování katalogového listu služby připojení přes IPSec.

Druhým rozhodujícím kritériem pro využití služeb eGC je kalkulace ekonomické výhodnosti (příklad pomocné kalkulace naleznete zde) za porovnání nákladů vlastnictví (TCO) jednotlivých IS v modelu provozu on-premise (na vlastní infrastruktuře) a s využitím služeb eGC. Při ověřování vhodnosti cloud computingu při řízení záměru pořízení a obnovy ICT řešení je možno využít doporučeného postupu, standardizovaného procesu (Obrázek 1).

Obrázek 1 – Proces při ověření vhodnosti cloud computingu při řízení záměru pořízení a obnovy ICT řešení



Zdroj: Cloud in public IT projects – report, upraveno

Diagram znázorňuje rozhodovací mechanismu, kde je třeba věnovat pozornost bodu „zvážení možnosti dekompozice“ (systému), kde správce rozhoduje o dekompozici informačních systémů a správné vymezení systémů určených pro cloud. Měl by vyhovovat legislativním požadavkům a potřebám klienta veřejné správy. V praktickém důsledku to znamená, že například výpočetní výkon, platforma ale i aplikace tedy i samotné úrovně systému cloud computingu se mohou dělit i horizontálně, tedy čerpat cloud hybridně, viz příklad dobré praxe. Tedy neplatí mýtus, že buď je v cloudu vše, nebo nic.

Pravidla tvorby architektury ISVS pro jeho správce

Každý správce informačního systému veřejné správy musí kontinuálně dbát na to, aby při tvorbě či rozvoji i udržování těchto systémů činil takové kroky, které podporují nebo zajišťují oddělení vrstvy platformy a technologií od vrstvy komunikační a ty zas byly striktně odděleny od vrstvy aplikační. Takto navržená architektura je připravena pro realizaci optimalizované cloudové řešení.

Dalším pravidlo vymezuje zákonem stanový seznam zapsaných poskytovatelů cloud computingu podle § 6q zákona č. 365/2000 Sb. Tito poskytovatelé jsou uvedeni v katalogu cloud computingu, který obsahuje dělení služeb dle horizontál:

- IaaS (Infrastructure as a Service – služby na úrovni datových center, sítí a HW).
- PaaS (Platform as a Service – služby na úrovni standardních SW platforem, jako jsou databáze, webové servery).
- SaaS (Software as a Service – kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.).

Publikování webového portálu úřadu a soukromoprávních uživatelů údajů

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. Portál musí též 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. Klientovi musí poskytnout též tzv. profil neboli personifikovanou část, kde si portál drží základní údaje o klientovi, které zná úřad nebo které klient sdělit sám ze své vůle.

Popis Portálů veřejné správy a soukromoprávních uživatelů údajů je uveden v rámci Národní architektury veřejné správy ČR. Zde jsou rozlišeny typy portálů, povinnosti jejich správců a pravidla využívání.

9.2 Postup úřadu při využití služeb cloud computingu

Tato podkapitola stručně shrnuje postup úřadu při využití cloud computingu pro provoz informačního systému úřadu. Detailně je postup popsán v dokumentu **„Návod na využívání cloud computingu ve veřejné správě“.**

1. Informační systém veřejné správy (ISVS) úřad dekomponuje na jednotlivé architektonické a provozní komponenty - viz metodika dekompozice ISVS.
2. Každé komponentě přiřadí bezpečnostní úroveň (nízká, střední, vysoká nebo kritická) – viz dokument „Průvodce *zařazením poptávaného cloud computingu do bezpečnostní úrovně“* publikovaný na stránkách NÚKIBu.
3. Pro jednotlivé komponenty ISVS úřad v katalogu cloud computingu vyhledá certifikované služby cloud computingu, které mohou být pro realizaci komponent ISVS použity, a současně vyhledá poskytovatele těchto služeb. Katalog cloud computingu, který obsahuje certifikované služby pro jednotlivé bezpečnostní úrovně je dostupný na webu eGC.
4. Na základě informací o cenách služeb cloud computingu uvedených v katalogu cloud computingu úřad zkalkuluje celkové náklady tohoto řešení ISVS za pět let – viz metodika TCO. Tyto náklady se porovnají s náklady on-premise varianty provozu ISVS. V případě, že celkové náklady cloudové varianty jsou nižší, úřad zvolí pro řešení ISVS cloudovou variantu.
5. Úřad realizuje výběrové řízení na dodavatele potřebných služeb cloud computingu. Ve výběrovém řízení oslovuje jen ty poskytovatele, jejichž služby jsou zapsány v katalogu cloud computingu.

9.3 Klíčové otázky

1)	**Zvážil váš úřad využití cloud computingu pro zajištění vyšší efektivity a bezpečnosti informačních systémů?** *Je potřeba vyžádat provedenou kalkulaci ekonomické výhodnosti dle § 5 odst. 2 písm. j) zákona č. 365/2000 Sb. o informačních systémech veřejné správy a závěrečné doporučení. Je potřeba zjistit nakolik se úřad zavázal k využití cloud computingu v informační koncepci.*
2)	**Provedl váš úřad hodnocení ekonomické výhodnosti způsobu provozu pro všechny informační systém veřejné správy? Řídí se výsledky tohoto hodnocení?** *Je potřeba vyžádat provedenou kalkulaci ekonomické výhodnosti dle otázky č. 1 a závěrečné doporučení.*
3)	**Využívá úřad pouze takové služby cloud computingu, které jsou vedené v katalogu cloud computingu jako nabídky?** *Pokud úřad využívá služby cloud computingu je potřeba zjistit jestli využívá jiné poskytovatele, než je uvedeno v katalogu cloud computingu.*
4)	**Má úřad přehled o tom, zda jsou data v případě využívání služeb cloud computingu uložena v perimetru EU, nebo jen ČR a proč?** *Je třeba si vyžádat specifikaci používaných služeb cloud computingu.*

9.4 Příklady dobré a špatné praxe

▸ Příklad dobré praxe

Provozní zlepšení provozu na základě kontinuálního zlepšování

Úřad v rámci ročního vyhodnocování své Informační koncepce a architektury systémů učinil několik závěrů:

- Architektura informačních systémů VS úřadu je do značné míry dekomponovaná na služby na úrovni datových center, sítí a HW; služby na úrovni standardních SW platforem, jako jsou databáze, webové servery); služby SW jako služby - funkcionalita standardních nebo standardizovatelných aplikací, např. e-mail, ekonomický systém, spisová služba apod.).
- Úřad identifikoval náklady na provoz jednotlivých vrstev architektury a také rozpočítal náklady alokované na klíčové aplikace (ISVS).
- Úřad identifikoval systémy vhodné pro migraci do cloudu.
- Úřad ověřil, zda je legálně možné migrovat tyto systémy do eGovernment cloudu z hlediska ochrany citlivých dat, bezpečnosti.

Úřad se rozhodl provést ekonomickou analýzu výhodnosti využití cloud služeb uvedených v katalogu cloudových služeb pro vybrané systémy.

▸ Příklad špatné praxe

Nový webový portál úřadu

Úřad, větší obec, se po změně zastupitelstva rozhodla dotvořit webový portál a vypsala veřejnou zakázku, kde s byl striktně vyžadováno cloud řešení na základě názoru a přesvědčení vedení úřadu, že on-premise řešení je dnes již překonané a neefektivní. Do otevřeného řízení se přihlásilo více dodavatelů a byla vybrána nejvýhodnější nabídka.
Úřad však pochybila již tím, že o takovéto změně neinformovala před vypsání zakázky útvar Hlavního architekta eGovernmentu.
Vysoutěženo bylo řešení, nasazené mimo perimetr úřadu v prostředí cloud computingu komerčního subjektu, kdy hosting serverů a na nich uložených dat byl situován mimo území EU. Pro komunikaci mezi portálem a soustavy aplikací úřadu bylo využito komunikace pomocí přiřazení pevných IP adres a portů přes vydaný systémový certifikát.
Propojení služeb Národního bodu bylo implementováno, ale komunikace o ztotožněném uživateli přes překlad BSI od základních registrů však nebylo ošetřeno, neboť provozovatel cloudu nedisponuje přípojkou KIVS a přestože úřad přípojku do KIVS má, tak toto pře-routování nebylo v plánech a úřad tak musel dodatečně zaplatit změny na propojení těchto služeb dále přes perimetr úřadu.

Kontrolou bylo zjištěno, že k řadě problémů by se předešlo, kdyby se postupovalo dle pravidel využívání cloud řešení ve veřejné správě a bylo zkontrolováno, zda nabízený produkt je schválen v katalogu cloud computingu. Toto pochybení by bylo eliminováno kontrolou na OHA.

Ministerstvo financí ČR

Sekce 04 – Finanční řízení a audit
Odbor 47 – Centrální harmonizační jednotka