DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Klíčové oblasti architektury eGovernmentu

Potřebnost a ekonomická výhodnost informačních systémů

Informační systémy by měly být vytvářeny k nějakému účelu a přinášet efekt za přiměřené peníze. Účelnost, efektivnost a hospodárnost (tzv. 3E) je vymezena v zákoně č. 320/2001 Sb., kontrolních standardech NKÚ či v manuálu Evropského účetního dvora. Úřady mají povinnost využívat majetek v souladu s 3E a sledovat a vyhodnocovat vynakládání výdajů v souladu s 3E dle zákona č. 219/2000 Sb. a 218/2000 Sb. Kromě Nejvyššího kontrolního úřadu provádí dohled nad 3E i útvar Hlavního architekta eGovernmentu (OHA), který posuzuje také potřebnost, realizovatelnost, přínosy a ekonomickou a personální náročnost projektů digitalizace veřejné správy. Je žádoucí, aby úřady při řízení jednotlivých ICT řešení postupovaly dle metod řízení ICT veřejné správy ČR.

Zvýšené riziko nedodržení účelnosti a hospodárnosti v případě realizace projektů digitalizace veřejné správy přitom vyplývá mj. i z neustálého velmi rychlého rozvoje digitálních technologií a tím i jejich extrémně rychlého morálního zastarávání a ekonomického znehodnocování coby praktického důsledku tzv. *Moorova zákona.* Právě to činí potenciálně neúčelným a nehospodárným např. pořízení jakýchkoliv informačních a komunikačních technologií, v jejichž případě nebude ani v horizontu nejbližších cca 18 měsíců přiměřeně využit jejich výpočetní výkon, přenosová kapacita, kapacita datových uložišť, vysoká dostupnost nebo nadstandardní úroveň jejich podpory.

Ať se jedná o projektové podklady, software nebo uspořádání dat, nakládání s nimi je omezené autorským právem, zejména zákonem č. 121/2000 Sb. Vedle vlastního vývoje formou zaměstnaneckého díla je většina software získávána platbou za licenci k užívání díla. Pokud kromě původce nebo jeho pověřeného zástupce dílo nesmí nikdo upravovat, poskytovat k němu další služby nebo je propojovat s jinými celky, měnit jeho uživatele a podobně, je tím zablokováno efektivní nakládání s dílem a objednatel je zcela závislý na libovůli původce. Takový stav nazýváme závislostí na konkrétním dodavateli a jeho řešení (tzv. vendor lock-in) a může vést k nehospodárnému vynakládání výdajů. Netýká se to jen software, ale také dodávek komplexních celků hardware omezující následnou volnost v údržbě a rozšiřování těchto zařízení, nákupů spotřebního materiálu a služeb, stejně jako vynucování servisních či "udržovacích" poplatků bez možnosti používat zařízení po vypršení takových podmínek. OHA sepsal příklady nevýhodných ujednání ve smlouvách a doporučuje taková ujednání v licenčních smlouvách co nejvíce omezit a nejlépe je nahradit ujednáními, která dávají uživateli nejširší možnou kontrolu nad ICT produktem. Existence vendor lock-in či riziko jeho vzniku může být příčinou nerealizovatelnosti příslušných projektů digitalizace veřejné správy a tím i jejich nehospodárné a neúčelné přípravy v důsledku porušení zásad transparentnosti, přiměřenosti, rovného zacházení a zákazu diskriminace stanovených zákonem č. 134/2016 Sb. a následného uložení zákazu plnění příslušné smlouvy ze strany Úřadu pro ochranu hospodářské soutěže.

Koncepce a strategie úřadů

Informační koncepce (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, má pouze stanovit směr, podle kterého se budou realizovat projekty. 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. Vedle jednotlivých IK existuje celostátní Informační koncepce ČR

(IKČR), která stanovuje principy a zásady, které jsou dále rozpracovány v jejích navazujících dokumentech, a určují směr digitalizace celé veřejné správy. 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 úřadu by měla navazovat také na strategii rozvoje služební úřadu, kterou mají úřady zpracovat dle metodického pokynu pro řízení kvality ve služebních úřadech do 30. 6. 2021.

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.

Informační koncepce, provozní dokumentace a další požadované dokumenty nejsou zbytečnou a zatěžující byrokracií či papírování. Tyto dokumenty by měly být brány jako základní součást každé organizace, která vlastní ICT. Provozní dokumentace je nedílnou součástí ICT, bez kterého je informační systém veřejné správy jen tzv. „blackbox“. Provozní dokumentace má tedy hlavně pomoci pochopit informační systém veřejné správy, jak se k němu chovat a jak jej spravovat.

Obslužné kanály veřejné správy

Obslužné kanály veřejné správy lze chápat jako způsoby či prostředky komunikace mezi klientem veřejné správy a veřejnou správou. Prostřednictvím obslužných kanálů lze provést digitální úkon a využít digitální službu. Právo činit digitální úkon a využívat digitální služby je zakotveno v zákoně č. 12/2020 Sb. 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.

Jedním z hlavních obslužných kanálů je Portál občana, který je webovým portálem české digitální veřejné správy a umožňuje centralizovaný přístup k 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 NIA či autentizační rozhraní Informačního systému datových schránek. Portál občana umožňuje různě pokročilé propojení (federace) portálů či systémů veřejné správy. Je tedy žádoucí, aby digitální služby a úkony poskytované úřady skrze jejich portály byly dostupné také na Portálu občana. Tím úřady podpoří mnoho architektonických principů, např. *P8: Jeden stát*, *P9: Sdílené služby veřejné správy* či *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. Asistovaným obslužným kanálem je např. Český Podací Ověřovací Informační Národní Terminál (Czech POINT). V oblasti centralizovaných webových portálů by měl v budoucnu vzniknout např. Portál podnikatele, který lze vedle Portálu Občana chápat jako rozšíření Portálu veřejné správy. Za zmínku stojí též jednotné obslužné kanály úředníků.

Vedle celostátních portálů existují i portály území, typicky pro kraj, obec, město či městskou část. Portál území může obsahovat kromě 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, 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.

Dále existují i 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 federovány do Portálu občana, avšak pouze za předpokladu, že SPUÚ je ohlášen v rejstříku a má povinnost elektronicky ověřovat totožnost klienta.

Elektronický oběh dokumentů

Výkon státní správy je doprovázen vytvářením dokumentů, jejich podepisováním, evidencí, odesíláním, příjmem, skartací atd. Tyto činnosti, souhrnně nazývané jako správa dokumentů, jsou vykonávány v rámci spisové služby. 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. Nepřehlédněte ani pravidla pro eSSL.

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 a digitálních pečetí. A právě využití elektronického podpisu, zaručeného elektronického podpisu a zejména kvalifikovaného elektronického podpisu, který je právně položen na úroveň ručního podpisu, umožňuje efektivní oběh dokumentů s jejich zaručením pravosti.

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, provozuje Ministerstvo vnitra ČR informační systém datových schránek (ISDS). Odesílání dokumentů přes ISDS pomáhá zajistit nejen nejpřísnější podmínky vyžadované v rámci kybernetické bezpečnosti, ale zároveň přispívá k posílení důvěry, zjednodušení komunikace a správnosti dokumentů mezi úřady. Takto odeslané a přijímané dokumenty prostřednictvím datových schránek mají pro právnické a fyzické osoby stejnou právní hodnotu jako kdyby byly odeslány v analogové podobě prostřednictvím podatelny. Činnosti v rámci ISDS jsou prováděny zdarma. Zpoplatněna je pouze konverze na žádost (30 Kč za stránku) a opakované vydání přístupových údajů (200 Kč). Úřadům doporučujeme využívat systém ISDS jako integrální součást jejich elektronické spisové služby.

Určení původci dokumentů (prakticky veškeré orgány veřejné moci) povinně provádí jejich uchovávání a výběr archiválií. Důležitým zdrojem pro výběr archiválií jsou dokumenty spravované v eSSL. Archivy provádějí dohled nad vedením eSSL a následně dokumenty vybírají ve skartačním řízení. Dalšími zdroji dokumentů pro výběr archiválií jsou samostatné evidence dokumentů, na něž se také vztahuje národní standard pro eSSL.

Orgány státní správy a samosprávy dle zákona č. 134/2016 Sb. nesmí odmítnout elektronickou fakturaci vystavenou dodavatelem za plnění veřejné zakázky. Národní standard elektronické fakturace umožňuje bezpapírovou výměnu strukturovaných elektronických faktur a dalších dokladů, jejich rychlé zpracování a přenositelnost mezi podniky, veřejnou správou i soukromými osobami. 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.

Identifikace v informačních systémech

Ke každému informačnímu systému (IS) přistupují uživatelé, a proto je nutné ověřit jejich totožnost, tzv. identitu, a nastavit jim práva k jednotlivým úkonům. V oblasti služeb státu je potřeba, aby toto ověření bylo spolehlivé a zaručené na VYSOKÉ úrovni v souladu s pravidly pro identifikaci klientů veřejné správy. Vždyť jde mnohdy o manipulaci s financemi (daňová přiznání), majetkem (katastr nemovitostí) nebo třeba i s citlivými údaji (zdravotní informace, sociální zabezpečení). K ověření totožnosti slouží elektronické identifikační prostředky, které je možno vnímat jako pomyslný klíč k otevření identifikační brány.

Jako identifikační prostředek lze v současné době využít občanský průkaz s aktivovaným kontaktním elektronickým čipem, NIA ID, mobilní klíč eGovermentu, moje ID, bankovní identitu (bank ID) či první certifikační autoritu. Informační systém datových schránek (ISDS) umožňoval využívat identitní prostor datových schránek k přihlašování do vlastních řešení - typicky portálů. Tento způsob identifikace a autentizace klienta veřejné správy byl umožněn pouze do července 2020, kdy vypršelo přechodné ustanovení zákona č. 250/2017 Sb., které zavedlo povinnost využívat systém Národní identitní autority (NIA). V případě vzdálené identifikace a autentizace prostřednictvím NIA je fyzická osoba jednoznačně identifikována bezvýznamovým směrovým identifikátorem (BSI), který je možné převést prostřednictvím informačního systému základních registrů (ISZR) na agendový identifikátor fyzické osoby (AIFO). Využitím elektronické identifikace úřady přispívají k naplnění *cílů 1.3, 1.6, 2.7 a 3.6 informační koncepce* ČR a dodržují architektonické principy *P8: Jeden stát* a *P11: eGovernment jako platforma*.

Díky nařízení eIDAS je elektronická identita osob uznávána v rámci EU, což podporuje architektonické principy *P5: Přeshraniční přístup jako standard* a *P6: Interoperabilita jako standard*. Prakticky to znamená, že každý občan členského státu EU má právo kdekoliv v rámci EU právoplatně prokazovat svoji elektronickou identitu s použitím notifikovaného identitního prostředku mateřského státu. Tedy například občan ČR se svým notifikovaným elektronickým prostředkem eObčanka (eOP) může prokázat v Dánsku a využívat služby skrze jejich portál. Informační systémy používané v rámci EU by tedy měly mít možnost ověření identity cizího státního příslušníka přes tzv. eIDAS node a dodržovat další pravidla pro NIA.

Státní zaměstnanci a ostatní pracovníci veřejné správy musí mít umožněno využívat pro svoji identifikaci do informačních systémů veřejné správy jednotný identitní prostor (JIP) a katalog autentizačních a autorizačních služeb (KAAS). Pokud informační systém využívají pouze interní zaměstnanci a pracovníci, nemusí se identifikovat pomocí JIP/KAAS, avšak úřad zodpovídá za to, že lokální identifikační systém je synchronizován s JIP/KAAS. Aby mohl IS využívat rozhraní JIP/KAAS, musí být připojen k centrálnímu místu služeb (CMS). V roce 2024 se připravuje spuštění generační náhrady za JIP/KAAS ve formě systému CAAIS (centrální autentizační a autorizační systém).

Strukturovaná data v ISVS, datové fondy a jejich sdílení

Každý informační systém (IS) 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 IS zajistit přístup ke všem datům, a to v otevřeném a strojově čitelném formátu, bez dodatečných nákladů a s možností libovolně s daty nakládat. Toto je podmínkou nejen pro efektivní výkon veřejné správy, ale také pro publikaci otevřených dat.

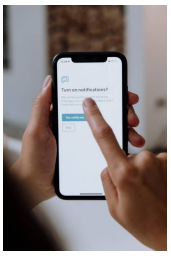
Nevíte, jak zajistit, aby byl váš IS připraven na publikaci otevřených dat? Přečtěte si whitepaper OHA. Aby se jednalo o otevřená data podle zákona č. 106/1999 Sb., musí je

úřad zaregistrovat do Národního katalogu otevřených dat (NKOD), kde si data mohou vyhledat občané, firmy i jiné úřady. Publikací nových datových sad či zkvalitněním stávajících publikací úřady přispívají k naplnění *cíle 1.5 a 5.10 informační koncepce ČR* a dodržují architektonické principy *P4: Otevřenost a transparentnost* a *P13: Otevřená data jako standard*. Více o otevřených datech se dozvíte na data.gov.cz a opendata.gov.cz.

V oblasti dat je samozřejmě nutné myslet i na ochranu osobních údajů. Doporučujeme dodržovat pravidla evidence subjektů a využívat tzv. Agendový identifikátor fyzické osoby (AIFO), který zajišťuje pseudonymizaci v rámci výkonu veřejné správy. Jako identifikátor by nemělo být používáno ani rodné číslo, jelikož zakládá možnost snadného zneužití údajů. Nepřehlédněte principy pseudonymizace.

Jedním z problémů v oblasti dat je jejich kvalita. V této oblasti doporučujeme zavedení kontrolních mechanismů na vstupu, popis struktury dat např. pomocí sémantických modelů a využití dostupných otevřených formálních norem (OFN), které přispívají ke standardizaci dat a interoperabilitě.

V souladu s principy eGovernmentu se plánuje zavedení veřejného datového fondu, který bude vedle otevřených dat a propojeného datového fondu jedním z nástrojů přístupu k datům. Díky tomuto nástroji si budou orgány veřejné moci vyměňovat veřejné údaje se zaručenou garancí, v první fázi např. číselníky.



Referenční rozhraní veřejné správy

Referenční rozhraní veřejné správy umožňuje více subjektům přistupovat k daným datům současně. V rámci tohoto rozhraní lze prostřednictvím Informačního systému základních registrů (ISZR) využívat data ze základních registrů, tj. Registru obyvatel (ROB), Registr osob (ROS), Registr územní identifikace, adres a nemovitostí (RÚIAN) a Registr práv a povinností (RPP). Ochrana osobních údajů je v základních registrech zajištěna převodníkem agendových identifikátorů fyzických osob (AIFO), díky němuž není možné při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v jiné agendě. Základní registry neslouží k přímému výkonu konkrétní agendy, nýbrž k dodávání garantovaných údajů subjektům, které mají právo údaje pro konkrétní agendy využívat. Jsou tedy nyní již nezbytným podpůrným nástrojem pro výkon většiny konkrétních agend ve veřejné správě v ČR.

Další komponentou referenčního rozhraní veřejné správy je eGovernment On-Line Service Bus / Informační systém sdílené služby (eGSB/ISSS). Skrze eGSB/ISSS si mohou úřady na základě oprávnění vyměňovat údaje vedené v agendových IS. Správce agendového IS, který data publikuje, vytvoří tzv. kontext, prostřednictvím kterého poskytne definované údaje. Doporučujeme, aby z každého IS byl publikován pouze jeden komplexní kontext, jehož dílčí části budou moci čerpat úřady dle svého oprávnění. eGSB je současně napojen přímo na ISZR, čímž zajišťuje komunikaci o osobách s vazbou na AIFO příslušné agendy. Použití eGSB pro využívání údajů mezi agendovými IS a současně pro poskytování výstupů subjektům práva úřad nejen zajišťuje naplnění legislativní povinnosti, ale přináší také jednoznačné zvýšení transparentnosti a díky komunikaci skrze Centrální místo služeb (CMS) také bezpečnost této výměny. Publikující subjekt jistě ocení i další výhody eGSB/ISSS, např. že 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 nebo dokonce do veřejné sítě Internet (existuje pouze jedno publikační rozhraní se zajištěnou kybernetickou ochranou v CMS). Současně dojde ke snížení nákladů na zajištění této činnosti.

ISZR a eGSB/ISSS tvoří společně Propojený datový fond, jehož rozvoj je *cílem 5.9 informační koncepce ČR* a podporuje řadu architektonických principů, např. *P2: Zásada „pouze jednou“*, *P6: Interoperabilita jako standard*, *P8: Jeden stát*, *P11: eGovernment jako platforma* či *P16: Konsolidace a propojování informačních systémů veřejné správy*. Nepřehlédněte ani globální architekturu PPDF. Je žádoucí, aby každý IS, který vede údaje o fyzických osobách nebo si takové údaje vyměňuje s jinými agendovými IS mimo resort, byl napojen na referenční rozhraní. Předpoklady napojení na referenční rozhraní jsou registrace IS v rejstříku ISVS, vedení aktuálních informací o agendě v RPP a zajištění konektivity do CMS.

Sdílené agendové informační systémy

Vedle centrálních služeb, za které ručí stát, existuje řada sdílených informačních systémů (IS), za které ručí příslušné úřady, přestože pokrývají celou veřejnou správu. V národním architektonickém plánu rozlišujeme sdílené agendové IS v přenesené působnosti (např. Živnostenský rejstřík, Evidence řidičů a Registr motorových vozidel) a sdílené agendové IS pro samostatnou působnost územních samospráv. Kromě toho existují i sdílené provozní IS, mezi které lze zařadit např. Integrovaný informační systém Státní pokladny (IISSP), Centrální registr administrativních budov (CRAB), Informační systém CEDR, MS2014+, registr smluv či Národní elektronický nástroj (NEN).

V těchto oblastech nejsou zatím stanovena specifická pravidla, nicméně Národní architektonický plán dává prostor pro jejich vytvoření. Je žádoucí, aby úřady, které mají v gesci sdílené agendové a provozní IS, vytvořily pravidla, které by měly ostatní úřady dodržovat. Jedná se například o uživatelská pravidla (tj. jak se mají uživatelé IS chovat), systémová pravidla (tj. jak je možné IS ostatních úřadů s daným IS propojit) a sémantická pravidla (tj. jaké údaje mají ostatní úřady do sdílených IS zadávat).

Komunikační infrastruktura veřejné správy

Komunikační infrastrukturu veřejné správy (KIVS)/Centrální místo služeb (CMS) můžeme nazvat privátní sítí pro výkon veřejné správy všech subjektů – tedy jak orgánů veřejné správy (OVS), tak i soukromoprávních uživatelů údajů (SPUÚ). 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 OVS naplňují architektonické principy *P8: Jeden stát* a *P11: eGovernment jako platforma*. Skrze CMS je také zajištěn přístup např. k propojenému datovému fondu. Přehled služeb CMS je pravidelně aktualizován.

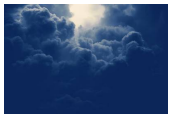
KIVS/CMS tedy nabízí pro jednotlivé OVS:

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

OVS a SPUÚ přistupují k propojenému datovému fondu výhradně přes CMS jedním ze čtyř možných způsobů:

1. Prostřednictvím Krajských sítí (aktuálně v krajích Vysočina, Plzeňském, Karlovarském, Zlínském a částečně Pardubickém + další budou-li vybudovány).
2. Prostřednictvím metropolitních sítí připojených např. na Integrovanou telekomunikační sít (ITS) 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.

Pokud chce úřad využít KIVS, tj. soutěž přes centrálního zadavatele Ministerstvo vnitra, je nutné definovat požadavky dle katalogových listů a následně zrealizovat nákup v dynamickém nákupním systému. Služby CMS lze čerpat také prostřednictvím Národních datových center.



Cloudové služby

Cloudové služby, či cloud computing nebo eGC, je v prostředí českého eGovernmentu upraven 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 předložili splnění všech podmínek a jsou tedy garancí určitých záruk pro orgány veřejné správy. Státní část je zatím v přípravě a měla by sloužit pro ty systémy, které jsou ohodnoceny jako kritické.

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).

Služby eGC zahrnují tři hlavní kategorie cloudových služeb: 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) a SaaS (Software as a Service – kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.).

Postup v oblasti Cloud computingu v rámci EU se v poslední době zabýval především nastavením pravidel a spolupráce s mimoevropskými poskytovateli. Prováděcí rozhodnutí Komise ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí bylo prohlášeno za neplatné rozsudkem Soudního dvora Evropské unie ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems (tzv. Schrems II) ze dne 16. července 2020. Náhradou za "štít soukromí" bylo 11.7.2023 vyhlášeno Evropskou komisí Adequacy Decision pro USA (na základě nového Data Privacy Framework, za jistých podmínek) viz https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 a https://uoou.gov.cz/novinky/vse/predavani-dat-evropska-komise-oznamila-dohodu-s-usa.