DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Spolupráce s ostatními útvary úřadu a eGovernmentu

neboli **Vazby na navazující manažerské disciplíny a regulace.**

Všechny útvary OVS (včetně ICT samotného) jsou stávajícími nebo potenciálními klienty dodávky služeb ICT útvaru. Spolupráce s nimi, jako s klienty, je nejdůležitější formou vzájemných vztahů, ta je ale popsána průběžně ve všech ostatních kapitolách dokumentu, nikoli v této.

Tato kapitola se zabývá ostatními klíčovými vzájemnými vztahy útvaru ICT s odbornými a provozními útvary, ve kterých:

1. IT proces se dá úspěšně vykonat jenom ve spolupráci s těmito útvary (ekonomika, bezpečnost a ochrana soukromí, správa majetku, právní, personalistika apod.), nebo
2. odborníci ICT mají (nebo mají mít) důležitý podíl na výkonu procesů těchto útvarů (legislativa, strategie, transformace - digitální zmocněnec, bezpečnost apod.).

Všude tam, kde kterákoli dovednost řízení ICT má překryv s jinými disciplínami řízení úřadu, je nutné se vůči těmto disciplínám vymezit a stanovit jejich styčné plochy a kontaktní body s řízením ICT.

Stejně tak všude, kde je třeba průřezově přes celý úřad nebo korporaci zareagovat na nějakou novou regulaci nebo novou potřebu, sehraje informatika významnou roli, byť manažerská oblast nebo iniciativa nejsou primárně informatické.

Některé oblasti řízení a spolupráce již jsou takto upraveny v samostatných kapitolách (projektové řízení, řízení ekonomiky ICT, řízení kvality ICT, řízení personálních zdrojů ICT apod.). Jiné jsou uvedeny zde, a to stručným obecným obsahem, případně odkazem na samostatné materiály, shrnutím těchto materiálů nebo plným obsahem.

Primárně toto ve vztahu k ICT platí pro disciplíny:

- spolupráce na péči o klienty úřadu
- spolupráce na tvorbě strategií a legislativy
- spolupráce s digitálním zmocněncem OVS
- řízení ICT bezpečnosti, kde jde o spolupráci a kompetenční rozhraní zejména s:
  - Manažerem kybernetické bezpečnosti (dle ZoKB) a
  - Pověřencem pro ochranu osobních údajů (dle GDPR),
- správa byznys architektury, modelování a řízení interních procesů úřadu, tzn. aktivní spolupráce s útvarem úřadu, do jehož kompetence patří nejen řízení interních procesů úřadu, ale i např. sdílení dat,
- plánování a financování rozvoje ICT (nejen technologií = infrastruktury, ale i personálního zabezpečení a informačních procesů), tzn. spolupráce s:
  - finančním oddělením,
  - oddělením správy majetku a
  - personálním útvarem,
- realizaci veřejných zakázek, a to jak při pořizování technologií do majetku, tak při nákupu externích služeb[1)]. To kromě administrativních úkonů vyžaduje i dobrou znalost práva - zejména licenčního.

Do této kapitoly je zařazena i spolupráce útvaru ICT s odpovídajícími útvary a orgány veřejnoprávní korporace, pokud je její součástí, a s centrálními koordinačními orgány, tj. s Ministerstvem vnitra a Zmocněncem vlády pro IT a digitalizaci.

Podpora útvarů péče o klienty služeb úřadu

Informatika bude poskytovat stále rostoucí podporu procesům výkonu služeb veřejné správy pro její klienty, zejména v podobě rostoucího podílu digitálních služeb. Již nyní jsou to právě útvary ICT, které klientům digitálních služeb poskytují podporu.

V rámci digitální transformace úřadů by v nich ale měly vznikat nové útvary, které převezmou zodpovědnost za společnou problematiku obsluhy klientů a péče o ně, napříč agendami OVS a napříč obslužnými kanály, s rostoucím podílem univerzálních obslužných kanálů (CzechPOINT a PVS - Portál občana, případně celostátní call-centrum). Takové útvary se procesně nazývají anglickými výrazy Front-End nebo Front-Office.

Součástí jejich zodpovědnosti je jednotně definovat, evidovat, publikovat a propagovat služby úřadu, zejména ty digitální. Dále koordinovat dodávku těchto služeb odbornými útvary a jednotně zadávat a přejímat služby ICT podpory obsluhy klientů a vyhodnocovat jejich kvalitu.

Úkolem útvaru ICT je navázat spolupráci se vznikajícím útvarem Služeb (a péče) pro klienty a nalézt první hmatatelné společné body v jejich vztahu jako věcný a technický správce Front-Office řešení pro dodávku služeb úřadu. Jedněmi z prvních praktických společných úloh jsou:

- správa katalogu služeb ve všech kanálech obsluhy
- správa znalostí a poskytování podpory ve všech kanálech obsluhy apod.

Integrovaný externí ServiceDesk pro digitální služby

Příkladem praktické spolupráce s útvarem péče o klienty je společný, sdílený ServiceDesk pro digitální i tradiční obslužné kanály. Podstata spolupráce spočívá v tom, že klienti služeb úřadu, ve všech obslužných kanálech, obvykle potřebují podporu zejména ve dvou oblastech:

- obsahové - kde a jak hledat správné služby pro životní situace, co a jak vyplňovat do podání, jaké a jak dokládat přílohy apod.
- ICT - jak správně aplikace samoobslužných kanálů instalovat a užívat, jak se vyrovnat s chybami či neznalostmi.

Nejlepší praxe ukazuje, že úřad má mít přinejmenším pro své samoobslužné klienty jednotný ServiceDesk, zajišťující jak znalostní bázi, tak personálním obsazením podporu v obou výše uvedených okruzích problémů. To vyžaduje společné koordinované řízení z obou útvarů.

Specifické je, že útvar ICT zde vystupuje jak v roli technického správce sdíleného řešení, tak jako dodavatel znalostí a kapacit podpory uživatelů v technických aspektech služeb.

Přístup k legislativní podpoře informatizace VS

Další rozvoj informatizace VS ČR vyžaduje zejména tvorbu nových právních předpisů a změny předpisů stávajících tak, aby předpokládaly, umožňovaly a vynucovaly naplnění architektonických principů eGovernmentu, uvedených v IKČR, tj. byly tzv. digitálně přívětivé.

Vzhledem k tomu, že valná většina legislativních změn zahrnuje nebo vyvolává i změny IT podpory výkonu veřejné správy, měli by být IT analytici a architekti úřadů přizváni do procesu tvorby úprav agendové legislativy již na úrovni přípravy legislativního záměru. Změny legislativy musí ve svém znění i v doprovodných dokumentech zohledňovat logiku, algoritmizovatelnost a parametrizovatelnost zákonných regulací a proveditelnost jejich IT podpory, a to zejména formulováním přesného byznys zadání odpovídající IT podpory a dostatečné nebo postupně časované doby pro její realizaci - implementační lhůty.

Jedním z nezastupitelných úkolů architektury úřadu (veřejné správy) je být podkladem pro optimalizaci veřejné správy a pro optimalizaci legislativy. Architekti a analytici musejí být zapojeni do procesu přípravy tezí i konkrétní legislativy, a naopak do procesu realizace nové legislativy v úřadu. Více souvislostí k zapojení do tvorby legislativy ve fázi 2-Palánování a příprava etapy životního cyklu jednoho ISVS také v Řízení jednolitých ICT řešení.

Podstatné pro další rozvoj informatizace VS ČR bude také odblokování překážek vystavěných dosavadní legislativou v oblasti eGovernmentu, nákupu ICT a ve správě ICT zdrojů, zejména lidských, viz také vztah řízení lidských zdrojů a Státní služba.

Důležité pro implementaci IKČR je, aby všechny nové nebo významněji měněné právní předpisy byly adaptovány tak, že budou reálně naplňovat principy IKČR podle měřítek a kontrolních otázek Digitálně přívětivé legislativy[2)].

Digitálně přívětivá legislativa

IKČR se svými architektonickými principy a z nich plynoucími pravidly již je harmonicky sladěna se Zásadami pro tvorbu Digitálně přívětivé legislativy.

Z toho plyne, že důsledné uplatnění těchto Zásad při tvorbě legislativy, včetně její kontroly ověřovacími otázkami k naplnění zásad, podstatně napomůže k implementaci IKČR do praxe VS ČR.

Proto IKČR a MŘICT vede útvary informatiky, tj. Technické správce ISVS těch úřadů, které zodpovídají jak za přípravu nebo připomínkování legislativy, tak za následnou implementaci její ICT podpory, k tomu, aby:

- se účastnili přípravy věcného záměru zákona nebo jeho změny
- prosazovali architektonické a systémové myšlení jako logický základ proveditelných předpisů
- požadovali jako součást zadání pro budování IT podpory změny legislativy od svého příslušného Věcného správce již od prvotních záměrů odpovědi na kontrolní otázky dle DPL.

Jedním z konkrétních cílů (DC 4.2) IKČR je zavést nutnost naplnění DPL jako novou povinnost a nedílnou součást legislativního procesu.

IT bezpečnost a ochrana údajů v kontextu úřadu

Informatika jako systémová a celostní disciplína v úřadu je přirozeným partnerem podobných a příbuzných disciplín, jako je bezpečnost úřadu, ochrana údajů, dodržování pravidel, řízení kvality, výkonnosti a zodpovědnosti.

Je například v praxi ověřeno, že téměř všechny prvky architektury úřadu, jsou současně předmětem ochrany, ale současně také prostředkem ochrany a často i rizikovým faktorem (informace, technologie, zaměstnanci, budovy, činnosti apod.). To platí významnou měrou pro prvky architektury úřadu, které jsou ve správě útvaru ICT, tedy primární a podpůrná aktiva.

Proto informatika a pro její strategické plánování a řízení v MŘICT vyžadovaná metoda architektury úřadu mohou být výše uvedeným disciplínám v úřadu velmi užitečné. Architektura úřadu totiž postupně objevuje, pojmenovává a popisuje všechny podstatné součásti struktury a chování úřadu a tato znalost je klíčových východiskem práce ostatních disciplín. A obráceně, práce specializovaných disciplín ověřuje a doplňuje poznání architektury úřadu a je proto přinejmenším velmi užitečnou zpětnou vazbou.

Útvar ICT je povinen navázat s útvary zodpovědnými za výše uvedené disciplíny vzájemně výhodnou otevřenou spolupráci. Některé příklady spolupráce jsou uvedeny v následujících kapitolách, další věcná a odborná doplnění budou po projednání s odbornou veřejností obsažena v následujících vydáních MŘICT a ve Znalostní bázi.

Podíl IT na celkové bezpečnosti úřadu

Řízení kybernetických rizik a bezpečnosti jednotlivých IS a celé informatiky úřadu musí být vykonáváno v souladu s celkovým řízením rizik a bezpečnosti úřadu tak, aby identifikovaná rizika a přijímaná opatření byla součástí jednotných a celkových procesů a registrů rizik na úrovni celého úřadu a dle své závažnosti se i IT / kybernetická rizika stala součástí rozhodování a řízení celého úřadu.

Přijetím zákona o kybernetické bezpečnosti se vytvořilo ideální prostředí pro rozvoj procesů v ICT. Právě procesy řešené přes ICT deklarují měřitelnou úsporu, bezespornost, nezvratnost a mnoho dalších přirozených vlastností ze světa ICT.

Bohužel tyto procesy nejsou řešeny komplexně a každý úřad má procesy s kvalitní auditní stopou a procesy, které jsou beze stopy. Důraz na odpovědnost za jednotlivé oblasti působnosti v rámci stanovených rolí podle zákona má za následek kvalitní postupný rozvoj. Tento rozvoj však obvykle nemá svou finanční ani organizační změnu. Každý útvar ICT respektuje nová pravidla, ale zároveň se snaží postupně jednotlivé milníky oddálit, protože čeká na finanční úspory nebo personální navýšení pro realizaci změn. To má napravit i naplňování pravidel MŘICT, kde jsou již všechny tyto souvislosti vzaty v úvahu.

Podíl IT na ochraně údajů a GDPR

V oblasti řízení ochrany soukromí a osobních údajů musí všechny vrstvy architektury úřadu a IT dovednosti být uvedeny do souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 z 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, také jako „GDPR“) a stávajícím zákonem č. 110/2019 Sb., o zpracování osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, stanovujícími rozsah ochrany osobních údajů, který je nutné zohlednit při tvorbě informačních systémů a při návrhu systémů pro práci s dokumenty.

Přestože primární zodpovědnost za naplnění povinností z těchto předpisů leží na vedení úřadu, pověřenci (DPO) a věcných správcích, hraje útvar ICT významnou roli v analýze stavu a potřeb ochrany osobních údajů, v implementaci IT opatření, zajištění vstupních a výstupních bodů a v respektování jednotlivých rolí dle GDPR a jejich smluvních vztahů.

Z nařízení GDPR vyplývá, že zpracování osobních údajů musí být v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítě a informací, to jest schopnosti sítě nebo informačního systému odolávat na dané úrovni spolehlivosti, náhodným událostem nebo protiprávnímu či zlovolnému jednání ohrožujícímu dostupnost, pravost, správnost a důvěrnost uložených či předávaných osobních údajů a bezpečnost souvisejících služeb poskytovaných či přístupných prostřednictvím těchto sítí a systémů. Vlastní zodpovědností ICT je tedy plnění těchto daných požadavků.

Obdobně jako ve vztahu mezi zodpovědnostmi za dlouhodobé řízení ICT a zodpovědnostmi za kybernetickou bezpečnost i ve vztahu k GDPR a ochraně osobních údajů je nutné na sebe vzájemně mapovat klíčové role a sladit jejich povinnosti na jedné straně a klíčové potřebné schopnosti a dovednosti na druhé straně. Jde zejména o tyto role:

- správce, společní správci,
- zpracovatel,
- **pověřenec,**
- příjemce,
- třetí strana apod.

Těmto rolím musí IT poskytnout nebo od dodavatelů zprostředkovat nezbytné IT znalosti, současně prostřednictvím IT útvarem uzavíraných smluv přenést na své dodavatele odpovídající část povinností, spojených se zpřísněnou ochranou osobních údajů.

Úlohou IT útvaru jako technického správce je implementovat do všech dotčených informačních systémů opatření zajišťující tzv. mandatorní požadavky výše uvedených předpisů. Za formulaci konkrétních přesných požadavků/zadání implementace pro jednotlivé IS odpovídají jejich věcní správci ve spolupráci s odbornými rolemi GDPR.

Informační systémy, v rámci kterých uživatelé nakládají s osobními údaji fyzických osob, musí zajišťovat důslednou ochranu těchto dat před zneužitím. Za minimální bezpečnostní opatření lze považovat důsledné oddělení uživatelských účtů v systému, správu hesel, logování přístupů, možnost reagovat na personální změny v řadách uživatelů, nastavení přístupových práv apod. Opatření musí zahrnovat:

- Logování k přístupu k osobním údajům
- Šifrování osobních údajů
- Pseudonymizace osobních údajů
- Anonymizace osobních údajů
- Funkce pro realizaci práv subjektů práva
- Vyhledávání osobních údajů ve struktuře databází a hypertextem.

Požadavky vedoucí na tato opatření, převzatá primárně z evropské legislativy[3)], vyvolávají potřebu „nastartování“ nové etapy vývoje dotčených IS s fázemi 1, 2 a 3. Obdobně je tomu automaticky při výstavbě nového řešení, kde musí být tyto mandatorní požadavky zohledněny a příslušná opatření zahrnuta do rozsahu, návrhu a plánu řešení, viz také architektonický princip P7 Důvěryhodnost a bezpečnost a v něm zahrnuté zásady „Privacy by Default“ a „Privacy by Design“.

Role útvaru ICT je klíčovou ve všech fázích životního cyklu přípravy, výstavby, modifikaci a provozu nových či stávajících řešení. Osobní údaje jsou tak bezpečné, jak bezpečné je prostředí, ve kterých se osobní údaje zpracovávají. Proto je nezbytné z pohledu IT dostatečně zabezpečit následující oblasti, které mají primární vliv na prostředí, ve kterém se zpracovávají osobní údaje:

- Technické zabezpečení:
  - ICT technologie, kde dochází ke zpracování osobních údajů (Samotné řešení ve kterém dochází ke zpracování osobních údajů, včetně všech možnosti kde dochází vstupně výstupním operacím)
  - Podpůrné, globální či sdílené ICT, které jsou využívány pro zabezpečení provozu samotného řešení (Backend, Frontend)
  - Prostředky a techniky, kterými jsou osobní údaje přenášeny mimo primární ICT či mimo ICT zcela
  - Datové nosiče pro ukládání dat
- Smluvní zabezpečení
  - Smluvní vztahy se všemi poskytovateli produktů a služeb, kteří se dostávají do kontaktu s daným prostředím uvedeným v části Technické zabezpečení
- Procesy:
  - Vývoj
  - Změnová řízení
  - Provoz

Ideální způsob zabezpečení z pohledu GDPR je kombinace technicko-organizačních a smluvních opatření. Je nezbytné si uvědomit, že jeden druh ochrany není dostatečný.

Spolupráce s ostatními provozními útvary

Ačkoli je útvar informatiky svými schopnostmi a přínosy pro úřad v mnohém výjimečný, svou podstatou je to provozní servisní útvar, obdobný a příbuzný všem ostatním (personalistice, správě nemovitostí, ekonomice, správě znalostí, nákupu, případně dalším).

Při přechodu na řízení úřadu pomocí služeb je na útvaru ICT, aby porozuměl tomu, jaké služby těmto útvarům poskytuje a jaké od nich odebírá. Je důležité vyjasnit hranice spolupráce, na níž k této výměně vzájemných služeb dochází. Manažer a pracovníci útvaru informatiky si mají být dobře vědomi, jaké služby jsou oprávněni

v těchto provozních oblastech od „sesterských“ útvarů žádat.

Současně by si všechny provozní útvary měly uvědomit, že jejich společnými a jedinými klienty jsou všichni zaměstnanci úřadu. Proto by tyto útvary měly napřít síly, analyzovat, co již mají společného a jak se mohou dále sblížit a sjednotit, aby své služby zaměstnancům poskytovaly jednotným, přívětivým a efektivním způsobem, včetně zaměstnaneckých samoobsluh, viz Spolupráce s ostatními útvary úřadu a eGovernmentu o zapojení provozních útvarů do společného centra sdílených služeb pro zaměstnance.

Praktické příklady nejlepší praxe, návody, vzory a další akcelerátory pro oblasti spolupráce ICT s provozními útvary, zmíněné v následujících kapitolách, budou doplněny po projednání s odbornou veřejností a publikovány v následujících vydáních MŘICT a ve Znalostní bázi.

Spolupráce s ekonomickými útvary

Podstatou spolupráce CIO s útvary ekonomiky je, že manažer informatiky je sice zodpovědný za plánování rozpočtu, za platby smluvních závazků, za nákladový controlling projektů a jednotlivých řešení a za další ekonomické operace, ale není a ani nemá být expertem v této oblasti.

Část těchto úloh, zejména ve větších ICT útvarech, zajistí svým ekonomicky vzdělaným personálem v rolích ekonoma/-ky, kontroléra/-ky apod., přesto je oprávněn žádat adekvátní podporu službami ekonomických profesionálů z příslušných útvarů.

Příkladem obtíží ve spolupráci je proces financování rozvojových záměrů. Základním problémem tohoto procesu je čas, který proběhne mezi věcným záměrem a podpisem smlouvy. U nového zákona nebo jeho obsáhlé novely se jedná se o roky práce, které nemají dopad do rozpočtu, ale často se právě tyto finance v rozpočtu objeví. Naopak někdy RIA nemá finanční zatížení, protože se změna děje na jiném úřadě. Principem dobrého nastavení je disponibilita finančních prostředků, které jsou nutné pro řízení změn. ICT útvar by neměl řešit po kolaudaci svého ICT disponibilitu finančních prostředků na jeho provoz. Ekonomický útvar musí mít správné podklady od ICT útvaru, aby mohl disponibilitu řešit na úrovni celého rozpočtu, a útvar ICT musí pravidelně informovat o příslušných změnách.

Spolupráce s personálními útvary

Podstatou spolupráce CIO s personálními útvary je jeho potřeba získávat, udržovat a intenzivně vzdělávat svůj odborný personál.

Personální práce je přirozenou součástí práce každého manažera, ale ani ICT manažer na ni nemá být takovým odborníkem. Má plné právo žádat od personálních útvarů podporu při náboru nových zaměstnanců, přípravě zaměstnaneckých benefitů a pobídek, přípravě a realizaci vzdělávacích programů, při hodnocení zaměstnanců a plánování jejich dalšího růstu apod. Oprávněně očekává, že se mu dostane zejména služeb personálního a personálně-právního poradenství vzhledem ke služebnímu zákonu, zákoníku práce a dalším předpisům.

Spolupráce na veřejných zakázkách

Podstatou spolupráce CIO s útvarem právním a útvarem veřejných zakázek jsou jeho oprávněné potřeby bezpečně, tj. legálně zvládnout proces výběru dodavatele pod ZoZVZ bez rezignace na věcnou, odbornou podstatu zakázky.

Každá veřejná zakázka má nejméně dva hlavní aspekty. Prvním je potřeba toho, kdo nakupuje - musí tzv. „vědět, co chce“. Je úkolem útvaru ICT jako technického správce, obstarávajícího řešení pro věcného správce, aby do zakázky dodal správné a srozumitelné zadání, tj. architekturu řešení, jeho funkční a ne-funkční specifikaci, včetně SLA, část smluvních požadavků a další atributy spojené s jeho obvyklou rolí příkazce operace.

Oprávněně očekává službu od odborníků na právo a nákup, že do zakázky vloží bezchybnou procesní znalost a druhou část smluvních podmínek, které pro CIO následně zajistí smluvní vztah s dodavatelem, představující vyvážené partnerství[4)].

Běžným příkladem obtíží je nedostatek vzájemných znalostí a stále se měnící prostředí. Stejně jako garant aktiva potřebuje praxi pro svou roli, tak i odpovědné osoby za zakázky potřebují praxi a především dodržování protikorupčních pravidel. Únik informací před vypsáním veřejné zakázky lze významně omezit předběžnými tržními konzultacemi a samotný průběh zakázky lze často vyřešit jednacím řízením s uveřejněním, které umožňuje přístup všech dodavatelů a minimalizuje množství dodatečných informací.

Dalším obrovským dopadem výkladu ZoZVZ z let minulých jsou služby provozu na 4 roky, kde již minulý rok mnoho právních kanceláří vyzvalo ICT útvary k delším časům. Pokud zadavatel zachová vlastnictví zdrojových kódů u sebe a soutěží rozvoj, potom nic nebrání dlouhodobé údržbě. Možnost definovat delší časy v rámci veřejných zakázek tak, aby to odráželo standardní praxi, kdy například běžné doby na údržbu SW/HW (Maintenance) bývá nabízena na 3, 5, popřípadě 10 let by měla být diskutována při dalších revizích zákona.

Spolupráce se správou nemovitostí

Podstata spolupráce se správou a údržbou nemovitostí je dvojí:

1. Potřeba útvaru ICT využívat specifické prostory a s nimi spojené služby
2. Významná podobnost procesů poskytování služeb pro zaměstnance při péči o koncová ICT zařízení a při péči o ostatní pracovní vybavení, navíc často s potřebou časové synchronizace služeb, obojí mnohdy napojeno na personální služby (nástup, stěhování, odchod zaměstnance).

První bod spolupráce by měl vést k poskytování služeb správy nemovitostí s SLA obdobnými, jako jsou SLA, spojené s dodávkou služeb klientům útvaru ICT.

Druhý bod spolupráce by měl vést na společnou koordinaci poskytovaných služeb, sdílné metod, postupů, nástrojů i dispečerského personálu pro obě kategorie služeb, s možností rozšíření až do podoby centra sdílených provozních služeb, viz dále.

Společné zapojení v centru sdílených služeb pro zaměstnance

Společnými klienty provozních útvarů jsou zaměstnanci a manažeři úřadu, kteří všichni mají právě z těchto svých univerzálních rolí potřebu čerpat sady provozních služeb pro zaměstnance a někteří k tomu ještě sadu služeb pro manažery.

Jejich společnou potřebou je čerpat tyto služby snadno, jednotně, obslužným kanálem podle své volby, tj. osobně, v portálu úředníka nebo v call-centru dispečinku služeb.

Útvar ICT bude v takovém centru sdílených služeb hrát významnou roli, proto by měl ověřit takovou potřebu ve svém úřadu a potom napomoci procesní a digitální transformaci úřadu v provozní oblasti iniciováním a vybudováním takového centra sdílených služeb.

Dlouhodobým trendem je pro veřejnou správu ČR federativní uspořádání takových center s možností kombinace lokálních služeb se službami sdílenými na korporátní (resortní, krajské nebo obecní) úrovni a sdílenými provozními službami na celostátní úrovni (například eLearnig).

Centrální koordinace řízení ICT státu

Protože centralizace řízení VS ČR je stanovena zákonem[5)], musí být i eGovernment, který je vlastně VS

vykonávanou v digitálním (kybernetickém) prostředí, řízen centrálně. To pro ICT útvary úřadů znamená povinnost se nejen při provozu, ale již i při projektování rozvoje jimi pro výkon služeb VS zajišťovaných podpůrných ICT služeb (jak interní, tak externí) řídit a dodržovat centrálně vydávané dokumenty pro oblast ICT VS.

Že nutnost vybudování centrálních kompetencí vnímá i vláda ČR, dokládá i hlavní cíl č. 5 programu DČ, pilíře IKČR – Efektivní a centrálně koordinované ICT veřejné správy, konkrétně dílčí cíl č. 5.2 - Alokace adekvátních lidských a finančních zdrojů pro realizaci IK ČR.

V následujících kapitolách bude po projednání s odbornou veřejností v dalších vydáních MŘICT uvedena sada praktických doporučení pro manažery útvarů ICT, jak realizovat úspěšně spolupráci s centrálními koordinačními orgány.

Podrobnější informace, návody a další pomůcky budou průběžně aktualizovány ve Znalostní bázi.

Ekonomická koordinace

V situaci obtížné až faktické nevymahatelnosti i zákonných povinností, je jediným účinným nástrojem řízení centrální kontrola čerpání státního rozpočtu, a to již od fáze tvorby finančních plánů a odsouhlasování položek na kapitolu ICT jednak dle potřebnosti pro zajištění provozu a jednak dle souladu s IKČR a přínosů jednotlivých akcí / projektů pro naplňování státem prioritizovaných strategických cílů.

Programové financování

Více informací a potřebné akcelerátory k centrální koordinaci programového financování ICT bude po projednání s odbornou veřejností publikováno v následujících vydáních MŘICT, podrobnější informace, návody a další pomůcky bude obsahovat Znalostní báze.

Metodika logického rámce

Logický rámec (LR, LogFrame, logická rámcová matice – LRM) slouží jako pomůcka při stanovování základních parametrů projektu. Je součástí metodiky návrhu a řízení projektu označované jako „Logical Framwork Approach (LFA)“, která uceleně řeší přípravu, návrh, realizaci i vyhodnocení projektu.

Metodika logického rámce[6)], zpracovaná MPSV pro čerpání z Evropského sociálního fondu v rámci Operačního programu zaměstnanost, je osvědčeným nástrojem pro přípravu žádosti o registraci akce a získání příspěvku z EU a na základě zkušeností pozitivních zkušeností MPSV bude vhodné ji využívat pro všechny projekty v rámci eGovernmentu ve fázích 1 a 2 jejich životního cyklu.

V rámci logického rámce se identifikují cíle, přínosy a výstupy příslušného projektu, ale i vazby mezi nimi. Zároveň logický rámec obsahuje i objektivně ověřitelné ukazatele a zdroje k jejich ověření, která umožní stanovit míru dosažení cílů a přínosů projektu.

Více informací a potřebné akcelerátory k LRM bude obsahovat Znalostní báze.

Investiční záměr, CBA a Studie proveditelnosti

Klíčovým dokumentem pro čerpání státního rozpočtu je dle platných postupů Investiční záměr. Ten na základě schváleného rozpočtu a v kapitolním sešitě úřadu přidělených finančních prostředků, zpracovává a k registraci na Ministerstvu financí předkládá úřad.

Součástí požadavků na financování ICT projektů VS by vždy mělo být prokázání, že zvolena byla varianta:

- proveditelná,
- s nejlepším poměrem přínosů a nákladů, a to z pohledů:

- kybernetické bezpečnosti,
- uživatelské přívětivosti – jak pro občanskou veřejnost a komerční subjekty, tak pro úředníky VS,
- využitelnosti jak stávající ICT infrastruktury, tak znalostí a schopností interních pracovníků,
- dlouhodobé udržitelnosti.

Více informací a potřebné akcelerátory k Investičním záměrům, CBA a Studiím proveditelnosti bude obsahovat Znalostní báze.

Koordinace realizace změn a dosahování přínosů

Implementace změn probíhá formou projektů případně programů, pro jejichž řízení existuje celá řada vhodných metodik. Z hlediska projektů eGovernmentu se jeví jako zásadní jejich vzájemná koordinace, návaznost na strategii eGovernmentu a v neposlední řadě měření úspěchu implementace příslušné změny (projektu/ programu).

Pro tento účel je nejvhodnější metodika logického rámce popsaná výše, která jednak definuje cíle a přínosy implementovaných změn a zejména stanovení míry jejich dosažení. Logický rámec projektů by se měl stát povinnou součástí Centrálního katalogu záměrů a projektů zmíněného v následující kapitole a měl by se stát i součástí závěrečného hodnocení projektu nebo programu. Kromě míry dosažení cílů a přínosu projektu by součástí závěrečného hodnocení měla být i analýza pozitivních zkušeností, a zejména, pokud projekt nedosáhl stanovených cílů, analýza příčin neúspěchu.

Poznatky ze závěrečné analýzy by měly být k dispozici ostatním OVS, které je využijí pro optimalizaci svých projektů, ale zejména centrální kanceláři pro řízení projektů, programů a portfolia (P3O), která bude tyto poznatky využívat k dalšímu zkvalitnění procesů přípravy a řízení projektů, programů a portfolia.

Centrální řízení bude vhodné implementovat právě i v rámci řízení programů a portfolia, přičemž je zřejmé, že zejména v oblasti řízení programů a portfolia je nutná spolupráce různých subjektů VS, a to jak jejich IT organizací, tak i odborných složek. Pro koordinaci a řízení programů a portfolia projektů bude nutné implementovat centrální kancelář pro řízení projektů, programů a portfolia využívající metodiku P3O (Project, Programme, Portfolio Office vycházející z metodik PRINCE 2, MSP a MoP), pravděpodobně jako součást MVČR. Tato kancelář musí disponovat odborníky s příslušnými certifikáty, vybavenými dostatečnými pravomocemi pro jednání s různými subjekty VS a jejich organizačními jednotkami na všech úrovních řízení.

Centrální katalog záměrů a projektů

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

Řízení licencí a OSS/FS

Bude doplněno po projednání s odbornou veřejností a publikováno v následujících vydáních MŘICT a ve Znalostní bázi.

1)
V širším smyslu ICT služby, tzn. ne jen „pouhé“ podpory / maintenace (např.: update SW), ale i DaaS, cloudových služeb (zejm.: SaaS, IaaS, PaaS, DPaaS) apod.
2)

Z angl. Digital proper legislation (DPL), například na ria.vlada.cz
3)

GDPR
4)

Anglicky by se řeklo Win/win, tzn. přibližně, že obě strany jsou vítězi.
5)

Zákon č. 2/1969 Sb. - Zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky
6)

https:%%//%%www.esfcr.cz/documents/21802/782328/02_Metodika_logickeho_ramce.pdf/b840b4ad-5d37-44c4-ade4-70f663f8047f