Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ministerstvo vnitra
Česká republika

Informační a komunikační technologie

skripta ke zvláštní části úřednické zkoušky oboru státní služby 28

Autor: Martin Rod
a kolektiv autorů

Verze: 0.1.1
Rok vydání: 2023

Materiál vychází ze zpracovaných skript kolektivu autorů Ministerstva vnitra, Správy základních registrů a Národní agentury pro komunikační a informační technologie, s. p. a byl zpracován v rámci projektu „Podpora profesionalizace a kvality státní služby a státní správy“ s registračním číslem CZ.03.4.74/0.0/0.0/15_019/0006173.

Vydalo Ministerstva vnitra

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

Seznam obsahuje pouze použité zkratky za povinnou, první, část kapitol. Zkratky v doplňujících částech jsou typicky obdobné.

3E	Účelnost, účinnost (efektivnost), hospodárnost
AIFO	Agendový identifikátor fyzické osoby
AIS	Agendový informační systém
BTS	Základnová stanice ("vysílač telefonního signálu")
CAAIS	Označení druhé verze systému JIP/KAAS, viz JIP/KAAS, JIP/KAAS 2.0 či JIP /KAAS NG
CERT	Computer emergency response team (akční tým odpovědi na kybernetické nebezpečí)
CIO	Hlavní informatik
CMS	Centrální místo služeb
CMS/KIVS	Ekosystém CMS a KIVS, viz jednotlivá hesla
COBIT	Kontrolní cíle zájmu pro informační a příbuzné technologie
Czech POINT	Český Podací Ověřovací Informační Národní Terminál
ČR	Česká republika
ČR	Česká republika
D	Důvěrné (stupeň utajení)

DESI	Digital Economy and Society Index
DoS	Odepření služby (Denial of Service)
DPO	Pověřenec pro ochranu osobních údajů
DS	Datová schránka
eIDAS	nařízení (Evropské unie) o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
EU	Evropská Unie
GDPR	obecné nařízení (Evropské unie) o ochraně osobních údajů
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICT	Informační a komunikační technologie, řídce též jako IKT
IEC	Mezinárodní elektronická komise, téže jako označení standardu v případě přidání řady/čísla normy
IKČR	Informační koncepce České republiky
IKOVS	Informační koncepce orgánu veřejné správy
IKT	Informační a komunikační technologie, běžně jako ICT
IoT	Internet věcí
IPSec	Internet Protocol Security
IS	Informační systém
ISDS	Informační systém datových schránek
ISO	Mezinárodní organizace pro normalizaci, téže jako označení standardu v případě přidání řady/čísla normy
ISSSPUÚ	Informační systém soukromoprávních uživatelů údajů
ISVS	Informační systém veřejné správy
ISZR	Informační systém základních registrů
ITIL	Information Technology Infrastructure Library
JIP/KAAS	Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb
JIP/KAAS 2.0	Označení druhé verze systému JIP/KAAS, viz JIP/KAAS, JIP /KAAS NG či CAAIS
JIP/KAAS NG	Označení druhé verze systému JIP/KAAS, viz JIP/KAAS, JIP/KAAS 2.0 či CAAIS
KB	Kybernetická bezpečnost
KBI	Kybernetický bezpečnostní incident
KBU	Kybernetická bezpečností událost
KII	Kritická informační infrastruktura
KIVS	Komunikační infrastruktura veřejné správy
KMVS	Kontaktní místo veřejné správy
LDAP	Lightwight Directory Acces Protocol ("databáze uživatelů pro definici jejich přístupu)"
MŘICT	Metody řízení ICT (veřejné správy České republiky)
MV	Ministerstvo vnitra (České republiky)
NAKIT	Národní agentura pro informační a komunikační technologie, s. p.
NAR	Národní architektonický rámec
NIA	Národní identitní autorita
NKÚ	Nejvyšší kontrolní úřad
OHA	Odbor Hlavního architekta eGovernmentu
OVM	Orgán veřejné moci
OVS	Orgán veřejné správy
PDZ	Poštovní datová zpráva
POb	Portál občana
PPDF	Propojený datový fond

PT	Přísně tajné (stupeň utajení)
PVS	Portál veřejné správy
RACI matice	Matice zodpovědností
ROB	Registr obyvatel
ROS	Registr osob
RPP	Registr práv a povinností
RÚIAN	Registr územní identifikace, adres a nemovitostí
RVIS	Rada vlády pro informační společnost
SDG	Jednotná digitální brána
SLA	Smluvní parametr (úroveň kvality služby)
SMS	Krátká textová zpráva (zasílaná typicky prostřednictvím mobilních telefonů)
SPUÚ	Soukromoprávní uživatel údajů
SSL	Secure Sockets Layer
SSO	Single Sing-On
SW	Software
SZR	Správa základních registrů
T	Tajné (stupeň utajení)
TCO	Celkové náklady vlastnictví
TCO5	Celkové náklady vlastnictví pro pět let provozu (včetně všech investičních nákladů)
TLS	Transport Layer Security
TOGAF	Architektonický rámec spravovaný společností Open Group
V	Vyhrazené (stupeň utajení)
VIS	Významný informační systém
VPN	Virtuální privátní síť
VS	Veřejná správa
WAF	Webový aplikační firewall
XML	Extensible Markup Language ("značkovací jazyk pro zápis dat")
ZFO	Zazipovaná (komprimovaná XML data)
ZoKB	Zákon o kybernetické bezpečnosti
ZR	Základní registr

Úvod

Informační a komunikační technologie (ICT) zasahují do všech aspektů našich životů. Mobilní telefony, počítače, ale i domácí spotřebiče jako jsou pračky, či lednice obsahují integrované obvody, tedy čipy založené na poznatcích a úspěších matematiky a dalších disciplín. Váš oblíbený e-shop, ale i kamenná prodejna bude typicky podporovaná informačním systémem pro správu zásob, účetnictví, či jiné.

Nejinak je tomu i v případě veřejné správy (VS). Moderní elektronický občanský průkaz není pouze „plastovou kartičkou" ale umožňuje jako plnohodnotný prostředek vstup do českého digitálního governmentu (eGovernmentu), např. do Portálu občana. Pro zaručené odeslání a doručení je zbudován informační systém datových schránek. Správu těchto dokumentů a jejich cirkulaci zas podporuje elektronický systém spisové služby.

Důležité je, že informační systém je schopen naplnit konkrétní potřeby, tedy poskytovat služby externím klientům veřejné správy, jako jsou občané nebo firmy, či obsloužit klienty interní, např. úředníci. Nikdo by neměl tedy stavět systém jen tak, ale vždy s rozmyslem jeho účelu. Informační a komunikační technologie jsou vhodným prostředkem, nikoliv samotným cílem. Právě až konzumací služeb informačního systému dostává tento informační systém přidanou hodnotu.

Smysl těchto skript je dvojí:

- Představit a předat znalosti na základě uceleného materiálu skript pro oblast informačních a komunikačních technologií v prostředí veřejné správy.
- Připravit uchazeče na úspěšné složení speciální části úřednické zkoušky v oboru informační a komunikační technologie.

Hlavní část skript tvoří její číslované kapitoly. Každá kapitola odpovídá jedné otázce z úřednické zkoušky. První část každé kapitoly v rozsahu dvou stran je částí povinnou a nutnou pro přípravu na úspěšné složení zkoušky. Druhá část kapitoly je doplňujícího charakteru, kdy rozvíjí myšlenky první části. Pokud se chcete dozvědět více, či se s danou problematikou setkáváte na denní bázi, tak právě tato doplňující část může sloužit k získání dalších detailnějších informací či je naopak uvést do širšího kontextu.

V případě nalezení chyb, jak věcných, tak jazykových, nám prosím dejte vědět, a to nejlépe pomocí e-mailu zaslaného na adresu (oha@mvcr.cz). Přílohou skript jsou errata, která tyto opravy reflektují. V dalších verzích skript budou Vaše podněty zohledněny a zapracovány.

Ať se Vám při zkoušce daří!

Martin Rod
a kolektiv autorů

martin@rod.icu
oha@mvcr.cz

1 Informační a komunikační technologie – základní pojmy, etika

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména nařízení EU č. 910/2014, zákon č. 365/2000 Sb., zákon č. 111/2009 Sb., zákon č. 12/2020 Sb.

1.1 Základní pojmy

Informační a komunikační technologie (ICT z anglického Information and Communication Technologies, česky též IKT) jsou jak vědním oborem, tak i souborem řešícího / spravujícího využívání technických prostředků pro komunikaci a práci s informacemi. Typicky se jedná o:

- **zařízení** (hardware – HW) jako je mobil, počítač, server,
- **aplikace** (software – SW) jako je operační systém Windows, tabulkový kalkulátor Excel,
- **data** (respektive informace) jako je obrázek, databáze, video, audio,
- **služby** jako je možnost učinit elektronické podání, koupit dálniční známku (vinětu) online,
- **lidský element** jako je programátor nebo uživatel a jeho interakce se systémem,

ale může se jednat i o samotnou metodologii vědy (jako je pojetí umělé inteligence), a další.

Informační systém (IS) je obecně celek složený z počítačového hardwaru a souvisejícího softwaru, k němuž patří také lidé, kteří tento hardware a software využívají, a procesy (činnosti), které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení. **Komunikačním systémem** lze pak nazvat takový systém, který primárně zajišťuje přenos informací mezi koncovými účastníky. Informační systém veřejné správy (ISVS) je definován v § 2 písm. b) zákona č. 365/2000 Sb. Jeho definice je uvedena i v doplňující části textu.

ICT služba je podtyp služby, která je dodána pomocí, nebo se týká ICT. Službou se myslí definovaná aktivita, která naplňuje potřeby klienta (interního nebo externího.) ICT službou je například výše zmiňované elektronické podání, ale může být třeba i služba údržby tiskáren. Pro moderní digitální government jsou důležité **digitální služby**, ty jsou definovány zákonem č. 12/2020 Sb.

Pro ICT jsou důležité pojmy **data** – symboly (např. x, Brok, 2, 37), **informace** – symboly s významem (Brok je jméno mého psa, 2 je počet mých dětí), **znalosti** – informace v kontextu mezi sebou (pokud 37 zároveň značí vzdálenost bydliště od centra Prahy v kilometrech a Brok je německý ovčák, tak se dá vydedukovat, že pravděpodobně bydlím v domě se zahradou).

Architektura úřadu je manažerskou metodou, která představuje celostní poznání organizace, jejích cílů, chování a vnitřní struktury (vedení, klienti, aplikace, produkty, služby, technologie) pro její efektivní řízení.

Užití aplikace (softwaru) je typicky zatíženo **licencí**, ta představuje právo užití od držitele autorských práv dané aplikace. Příkladem může být licencování operačního systému např. Windows, úplatnou licencí, nebo operačního systému typu Linux, který je typicky bezúplatný.

1.2 Etika (v digitální společnosti)

Etika vždy souvisí s morálkou. Co je v určité době a v určitém regionu považováno za morální, určuje myšlení většinové populace. ICT však intenzivně využívá pouze část lidí a to poměrně nezávisle na

geografické poloze – **svět ICT nezná hranic**. Tato oblast tedy přináší nové možnosti a situace, které dříve nebyly myslitelné (například možnost kopírovat neomezeně autorská díla bez ztráty kvality), proto v této oblasti vzniká nová morálka, která není ustálená a která se pod vlivem nových technologií stále vyvíjí.

Díky rozvoji ICT vznikají zcela nové formy podnikání, zejm. poskytování i standardních – ne ICT služeb (např. sdílené služby dopravy – Uber, ubytování – Airbnb, dodávání informačního obsahu – Google), pro které se konstantně hledají, utváří a mění zákonné hranice, které by etické principy a zásady běžného světa prosadily i ve světě digitálním.

Tato novodobá etická pravidla uceluje tzv. desatero přikázání počítačové etiky:

1. Nepoužiješ počítače ke škodě jiného.
2. Nebudeš ničivě zasahovat do práce druhých lidí.
3. Nebudeš slídit v souborech jiných lidí.
4. Nepoužiješ počítače ke krádeži.
5. Nepoužiješ počítače pro křivé svědectví.
6. Nepoužiješ nebo nepořídíš kopii softwaru, který jsi nezaplatil/a.
7. Nepoužiješ neoprávněně počítačového zdroje jiných lidí.
8. Nepřivlastníš si intelektuální dílo jiného.
9. Budeš přemýšlet o společenských následcích programu, který jsi stvořil/a.
10. Budeš používat počítače ohleduplně a s úctou.

Otázky k procvičení:

1. Zkuste si vybavit, s jakými ICT prostředky přicházíte během vaší práce do styku. Zařaďte je do kategorie: zařízení, aplikace, data, služba, lidský element.

S velkou pravděpodobností z hlediska zařízení přicházíte do styku s mobilním telefonem, počítačem, notebookem, ale třeba i chladničkou či mikrovlnou troubou – i ty dnes typicky obsahují čipy, stejnak jako současné automobily. Nepřímo pak typicky různé wifi routery/rozbočovače, či pro telefonní signál stožárové vysílače (tzv. BTS). Jako aplikace – poštovní klient, operační systém, spisová služba, velice oblíbené jsou i webové stránky s jídelním lístkem na intranetu. Zmíněný lístek je vlastně datový soubor, to samé budou jednotlivé spisy ve spisovce. Službou bude přihlášení se do systému, možnost v něm vykonávat akce – např. přiřazení spisu, zobrazení atd. Lidským elementem je schopnost tato data na obrazovce vnímat

2. Jaká data, informace a znalosti bude nejspíše obsahovat systém spisové služby?

Částečně zmíněno výše – v systému budou typicky informace pro spis – dokumenty, data přijmu a odeslání zpracovatel aj. Spisová služba není znalostním systémem, ale některá pravidla by se dala zjistit, například předpověď zatížení pracovníků na podatelně vzhledem k svátkům.

3. Pro usnadnění splnění služebního úkolu jste na nalezl/a na internetu počítačový program, který by řadu činností automatizoval. Porušíte etiku, pokud program svévolně nainstalujete? Co vše lze spatřovat v tomto konání jako riziko?

Bez zmocnění byste neměli do aplikačního vybavení zasahovat. Vystavujete riziko ohrožení počítače virem. I kdybyste práva měli, tak byste měli zjistit, zda je legální program používat – licence

4. Váš kolega/kolegyně odchází na oběd, vy si všimnete, že pracovní počítač je odemknutý. Jak se zachováte?

Např. počítač byste mu měli zamknout (klávesa Windows + klávesa L), tento tip mu pak prozradíte.

1.3 Doplňující část

1.3.1 Informační a komunikační technologie

V praxi je užíván i pojem informační technologie (IT) přidání slova komunikace je zdůvodňováno zdůraznění potřeby propojenosti a přenosu dat a informací v dnešní moderní znalostní společnosti. Obecně se však jedná o synonyma.

Primárním důvodem nasazování prostředků ICT byla a dodnes je snaha o zvyšování efektivnosti zejména opakovaných činností – automatizace. ICT není cílem, představuje pouze prostředek/nástroj k zefektivnění činnosti. Kritériem pro hodnocení rozvoje ICT není výsledný počet nebo výkon počítačů, ale dosažená změna efektivnosti klíčových procesů organizace díky např. vyšší dostupností nezávisející na konkrétním místě (geografické poloze) a lepším výběrem informací potřebných pro rozhodování.

1.3.2 Informační systém

Základní třídění (klasifikace) informačních systémů je:

- TPS – technickoprovozní = transakční,
- MIS – manažerské,
- DSS – podpora rozhodování,
- EIS – exekutivní.

Každý informační systém zahrnuje / využívá:

- určitá data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a
- nástroje umožňující výkon informačních činností.

V prostředí veřejné správy, se rozumí: informačním systémem veřejné správy funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále technické a programové prostředky, případně jiné nástroje umožňující výkon informačních činností – viz zákon č. 365/2000 Sb. § 2 písm. b).

1.3.3 Komunikační systém

Přestože každý informační systém dnes komunikuje, tak by nebylo zcela správného ho nazvat komunikačním systémem. Komunikační systém, oproti informačnímu systému, je tvořen primárně pro účel komunikace – např. systém PEGAS. Oproti tomu např. informační systém evidence obyvatel je evidencí o obyvatelích, a přestože tyto data dále komunikuje (předává dál), tak by nebylo zcela vhodné ho za komunikační systém nazývat. Komunikace mezi systémy je typicky šifrovaná – tedy, aby nikdo třetí nemohl komunikaci odposlouchávat (např. hovor, či odeslaná datová zpráva přes datové schránky).

Doplnění k heslu digitální služba: Digitální služby definuje zákon č. 12/2020 Sb. jako: úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy a vedený v katalogu služeb jako úkon v elektronické podobě; za digitální službu se považuje i úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agendy.

1.3.4 Licence a autorské právo

Dle platné legislativy jsou veškeré počítačové programy autorským dílem. SW licence tak představuje právo poskytnuté držitelem autorských práv uživateli daný program užívat, distribuovat, upravovat atd.

Měnit toto právo – licenci, je oprávněn pouze autor. V případě kolektivního díla je nutný souhlas všech autorů. Rozsah a různorodost licencí i velmi rozšířených programů jsou obvykle velmi komplikované, kdy jejich tvorbě se věnují specializovaní právníci. Pro veřejnou správu je užívání SW legislativně upraveno, a to konkrétně usnesením vlády ČR č. 624 ze dne 20. června 2001 o Pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů. Dle tohoto usnesení musí jednotlivé OVM vést evidenci všech na ICT zařízeních v majetku úřadu (tzn. i na mobilních zařízeních včetně např. služebních chytrých mobilních telefonech) instalovaných SW licencí a opakovaně kontrolovat, zda jsou licence užívány legálně, tzv. v souladu s příslušným licenčním ujednáním.

Kromě komerčních licencí, které je třeba buď koupit (do majetku) nebo platit za jejich užívání (včetně pořízení formou SaaS – de-facto se jedná o pronájem licence, právo daný SW vyžívat – obvykle vzdáleně, tzn. bez nutnosti jeho instalace na vlastním zařízení, které je obvykle smluvně přiznáno na určitou dobu), existuje i řada licenčních forem, jejichž legální užívání SW je bezplatné, ale vztahují se na ně jiná omezení, např.:

- volné licence, jejichž autoři je poskytují – obvykle ale pouze pro nekomerční využití, zdarma, tzv. freeware,
- GNU GPL – obecně jde o veřejnou licenci, kterou lze volně užívat, ale šířit pouze za splnění licenčních podmínek,
- opensource licence – zde má uživatel právo upravovat nebo rozšiřovat zdrojové kódy software, protože je máte k dispozici,
- trial / demo a shareware – což jsou nejčastěji zkušební / testovací verze softwaru, který je jinak komerční, přičemž obvykle je jeho funkcionalita omezena časově nebo jsou dostupné pouze některé funkcionality,
- public domain – jsou licence, u kterých se autoři programů vzdali svých autorských práv, lze je jakkoliv upravovat i volně šířit.

1.3.5 Slovník eGovernmentu

Vzhledem k nutnosti so porozumět, tedy dostát jednotného výkladu pojmů je Ministerstvem vnitra zpracován Slovník eGovernmentu. Tento slovník je průběžně doplňován a je veřejně dostupný.

Aktuálně Slovník obsahuje stovky pojmů včetně originálního znění a výkladu. U řady pojmů obsahuje i odkaz na původní zdroj a u původně českých pojmů i oficiální znění překladu výkladu do angličtiny.

1.3.6 Odkazy

- Slovník eGovernmentu na stránkách Národní architektury eGovenrnmentu:

https://archi.gov.cz/slovnik_egov

2 Rozhodující trendy v současném ICT

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména nařízení EU č. 910/2014, zákon č. 365/2000 Sb., zákon č. 111/2009 Sb., zákon č. 12/2020 Sb.

2.1 Technologické trendy

Hlavními převládajícími trendy, udávající podobu současné digitální společnosti, jsou:

- **existence levných zařízení** pro komunikaci a vznik samostatné třídy přenosných univerzálních digitálních zařízení – mobily, tablety, laptopy.
- **dostupnost všudypřítomný veřejných telekomunikačních sítí** pro přenos dat, určených pro poskytování přístupu k síti internet, včetně bezdrátových, jejich rostoucí územní pokrytí a přenosový výkon.

Cloud, téže jako cloud computing, nebo cloudová služba, je označení režimu poskytování služeb přes síť ze vzdáleného serveru. V doslovném překladu cloud znamená mrak, což odpovídá premise, že mrak můžeme pocítit například díky dešti, ale jen těžko si na něj sáhneme. Výhodou ze strany zákazníka cloudu je to, že neřeší technickou infrastrukturu – budování serverů, jejich údržba), ze strany poskytovatele pak úspora plyne díky premise, že ne všechny služby jsou užívány zároveň, tedy může infrastrukturní zdroje efektivně sdílet a rozkládat mezi více zákazníků dle potřeby.

Ohledně efektivní práce se zdroji serverů je vyvinut a dnes běžné užíváno a kombinováno:

- **virtualizace** – např. 2 fyzické servery tvoří 1 virtuální, či právě naopak. V tomto konceptu hovoříme o vertikální virtualizaci
- **kontejnerizace** – stav, kdy chceme jednu aplikace používat ve více instancích, například pošta pro Ministerstvo vnitra (MV), Policii a úřad vlády. Namísto virtualizace přes celé prostředí, lze multiplikovat pouze aplikaci samotnou, tedy není potřeba virtualizovat vícekrát např. operační systém. V tomto konceptu se jedná o horizontální virtualizaci.

Díky těmto technologickým principům je tak možno řešení efektivně a dynamicky **škálovat**, tedy v případě potřeby vysokého výkonu je možné aplikaci i samostatně rozdělit do vícero-modulů, byť se stejnou funkcionalitou, ale díky tomu obsloužit vysoké množství klientů.

Dalším trendem je přidání elektroniky schopné komunikovat přes síť internet do téměř všech zařízeních (např. chytrá pračka nebo osvětlení, kterou obsluhujete mobilní aplikací v chytrém mobilu, ale i např. různé multifunkční měřiče vlhkosti, srážek atp.). Hovoříme o tzv. **internetu věcí** (Internet of things, IoT). Díky IoT je možné získávat spoustu dat – měřiče i data jsou pak levná, nicméně uložení a zpracování vysokých objemů těchto dat je komplikovanější, a tedy celkově oproti senzorům dražší – tento problém se snaží podchytit **big data**. Komplementárně se užívají **datové sklady** pro práci s historickými, strukturovanými daty společnosti. Důležité je, že datový sklad a big data koncept si navzájem nekonkurují, tedy nedá se říci, že by jeden převzal roli druhého.

Dále jsou data i prostředkem pro řešení řady úkolů, např. např. pokud máme videozáznam např. bezpečnostní kamery a dokážeme identifikovat, co je chtěné chování – otevření vrat, když přijíždíme autem domů a nežádoucí chování – případný lupič přelézající zeď. Právě tyto problémy

jsou dnes řešeny pomocí **strojového učení**, v běžné řeči známějšího jako **umělá inteligence**. Ve své podstatě se jedná o pokročilé algoritmy (jasně definované kroky činností), které na základě dat dokáží rozhodnout o výsledku (např. je na obrázku želva? – Ano, s pravděpodobností 99 %) nebo výsledek případně predikovat (S jakou pravděpodobností žadatel bude bezproblémově splácet úvěr? – S pravděpodobností 79 % se splácením nebude mít žadatel problém). Dalším uplatněním v praxi je strojově vidění/rozpoznání obrazu, či tvorba vizuálních děl na základě textového vstupu.

Posledním zmíněným technologickým trendem je **blockchain** (což je nezfalšovatelný seznam transakcí) a jeho užití v podobě **kryptoměn** jako je například Bitcoin či jiné. Evropská unie (EU) pracuje na tzv. digitální identitní peněžence (European Digital Identity Wallet), která by mohla být poháněna právě technologií blokchain.

2.2 Netechnologické trendy

Práce z domova (tzv. home office) i díky pandemii covid-19 zažívá znovuobrození a v komerční sféře je jedním z nejoceňovanějších benefitů. Veřejná správa se s tímto fenoménem bude muset dříve či později vypořádat.

Sociální sítě jako je Facebook, Twitter, Instagram, TikTok dnes protkávají jak prostředí osobní, tak komerční i eGovernmentu. Jsou prostorem pro sdílení informací, ale i reklamu, či případně fake-news (falešné, typicky poplašné zprávy).

Vliv je možný spatřovat i v stále pokračující **specializaci ICT** již několik desetiletí není jedna role, ale skrývá se v ní řada specializací – vývojář programovacího jazyka Python neumí, respektive nepotřebuje umět nakonfigurovat wifi router, natožpak vyměnit toner v tiskárně.

Cyklicky dochází k myšlenkové (logické) nebo faktické (fyzické) **centralizaci** a **decentralizaci** systémů, služeb aj. Stejnak je tomu v případě **outsourcingu** (přesunutí výkonu agendy na třetí stranu), kde dnes se řeší problematiku jak tyto agendy a zejména znalosti opětovně dostat zpět, tzv. **re-insourcing**.

Je potřeba téže zmínit vznik a existenci firem jako **hegemonů a technologických gigantů**, kdy například čipy pro počítače vyrábí zejména tři firmy (Intel, AMD, Apple), cloudové poskytovatele zas zejména Microsoft, Amazon, Google.

Otázky k procvičení:

1. Používá vaše organizace cloud? Kde má váš úřad datová centra pro běh informačního systému (areál postačuje).

Ministerstvo vnitra rozhodně služby cloudu využívá (např. část Portálu veřejné správy / Portálu občana). V rámci umístění do datových center se dá zmínit areál Olšanská, nebo Zeleneč.

2. Je vaše organizace aktivních na sociálních sítích?

Například MV uvádí na svých stránkách odkazy na Twitter, Facebook a Toutube.

3. Jaké technologické trendy by se užili, při vylepšení kamerového systému města?

Pravděpodobně rozpoznání obrazu (člověk a i případně tvář a konkrétní identifikace), převod obrazu na text – například poznávací značky automobilů. V rámci IoT čidel i třeba detekce plynulosti dopravy, dále pak znečištění ovzduší aj.

2.3 Doplňující část

Obecná dostupnost sítě a užívání přenosných zařízení má za důsledek rozsáhlé změny v užívání služeb. Vznikly služby ukládání dat a později mediálních souborů, nejčastěji fotografií, přímo z jednotlivého zařízení a jejich přenášení na další zařízení v majetku uživatele, třeba počítač nebo tiskárnu. Později přibyly možnosti jejich sdílení dalším uživatelům a spolupráce v reálném čase. K psaným textovým diskuzím přibyly nejdříve telefonní a později videokonferenční hovory.

Se zvyšováním výkonu a schopností hardware i software se objevily aplikace provozovatelné přímo v internetovém prohlížeči bez instalace. Tyto programy vystačí s nižším výkonem a kapacitou, což umožňuje jejich využití v přenosných zařízeních. Z toho profitují zejména systémy pro sběr, zpracování a sdílení dat (jako je Seznam, či Google), týmové hraní her, ale třeba i pro práci s dokumenty (kancelářské balíky Office – Microsoft, Google).

V síti jsou nabízeny také infrastrukturní služby, jako poskytování prostoru pro ukládání souborů a dat (Storage as a Service, Cloud Disk, Data as a Service) - Základní registr by se daly považovat za Data as a Service providera.

Doplňujíc část cloud:

Poskytovatelé služeb nabízejí díky virtualizaci své sdílené výpočetní prostředky (procesor, paměť) a úložiště (diskový prostor) pomocí samoobsluhy nebo technickým rozhraním (API). Získat různě výkonné „počítače“ lze během několika minut. Kapacity vhodně navrženého IS lze průběžně škálovat podle aktuálních potřeb a docílit celkově nižší provozní náklady ve srovnání se statickými IS. Služba může být účtována za rezervované kapacity (jistota), za skutečné využití (úspora), nebo dokonce v okamžité nepotřebné kapacitě dodavatele zdarma (vývoj, testy). Nákupem služeb správy lze dále ušetřit za expertní zaměstnance. Pronájem licencí užívaných programů zlevní a zjednoduší licencování.

Pronajmout lze jak holý virtuální stroj (IaaS, Infrastructure as a Service), stroj s předinstalovaným operačním systémem a provozním vybavením (PaaS, Platform as a Service), tak i stroj s předinstalovanou softwarovou aplikací (SaaS, Software as a Service). Okraj nabídky tvoří vzdálený fyzický hardware (MaaS, Machine as a Service). Na druhé straně dodavatelé a tvůrci mohou své informační systémy a aplikace poskytovat k přímému použití včetně údržby (AaaS, Application as a Service).

Vedle virtuálních počítačů jsou nabízeny další užitečné funkce, například load balancer pro vyvažování příchozí zátěže na více spuštěných strojů, oddělená síť pro komunikaci mezi zákazníkovými stroji, VPN mezi lokalitami a do zákazníkova datacentra nebo průběžné zálohování dat.

Moderní informační systémy se dnes tvoří především cloudovým způsobem). Uživatelé okamžitě vidí přijaté změny, přistupují současně z více zařízení a spolupracují odkudkoliv. Správci a programátoři testují a zavádějí nové verze bez místní instalace, dosahují tak lepších výsledků levněji.

Cloud je počítač cizího provozovatele. Vlastnictví dat a bezpečnost a slučitelnost práva zpracovatele jsou důležitou součástí hodnocení rizik a nastavení vztahů. Jak organizačních – smlouvy, záruky, certifikace, pojištění, tak technických – pseudonymizace, anonymizace, šifrování při přenosu a v úložišti, rozdělené zpracování. Soubory citlivých údajů také mohou zůstat ve vlastním, privátním cloudu a veřejný cloud lze využít pro nízko klasifikované komponenty IS. Takový hybridní provozní model sníží náklady a dodrží bezpečnostní úrovně údajů a celých databází.

Vedle komerčních poskytovatelů podporují stávající technologie také budování privátních a komunitních cloudových služeb. Takový privátní cloud vzniká i pro potřeby eGovernmentu.

2.3.1 Doplnění pro škálování, virtualizace, ochestraci

Virtualizace, kontejnerizace, škálování a orchestrace jsou technické trendy, umožněné zvyšováním výkonu a kapacit hardware, pro lepší využití zdrojů sdružováním (konsolidací) zdrojů a poskytovaných služeb (zátěže) pod společnou správu.

Virtualizace je způsob užívání počítačů a odpovídajícího návrhu informačních systémů, který podporuje sdružování výpočetní zátěže a zdrojů (konsolidaci). Pro více současných funkcí, uživatelů a procesů je využíván (sdílen) společný hardware běžné komoditní kvality (a tedy levný).

Virtualizace vyžaduje změny v přístupu k vytváření informačních systémů, nákupu hardware a jeho správě, které zlevňuje a zjednodušuje. Za to snižuje počet počítačů až o polovinu. Přináší vyšší míru využití, vyšší dostupnost a přizpůsobitelnost výkonu informačních systémů.

Základem virtualizace je izolace jednotlivých „hostů“ od sebe navzájem. Nejstarší metodou je řízení přístupu uvnitř aplikace a operačního systému (Unix, Plan 9, Linux, OS/2, Windows NT a novější). Virtualizace pracovní plochy na jednom společném serveru (Remote Desktop, RDP) dnes stále zpřístupňuje koncepčně zastaralé centrální informační systémy odkudkoliv.

Pokročilejším přístupem k izolaci a sdílení prostředků je vytvoření kontejnerů, obsahujících prostředí pro jeden nebo více běžících programů. Hostem může být mikroslužba nebo obraz operačního systému. Známé kontejnerizační platformy jsou Docker a LXD.

Za virtuální počítač označujeme prostředí, ve kterém je simulován hardware počítače. Hostem je libovolný a úplný operační systém. K dosažení maximálního výkonu spoléháme na podporu hardware hostitelského počítače (VTx/VTd, AMD-x, vPro), dnes běžnou v serverech i desktopech. Užívané virtualizační platformy jsou např. vSphere (VMware), KVM/QEMU (Linux), HyperV (Microsoft).

Virtuální počítač nebo kontejner zřídíme a nasadíme snadno a rychle. Můžeme jej i za chodu přesouvat mezi hostiteli. Také hostitele můžeme přidávat a odebírat bez ovlivnění běžících hostů. Šířku a výšku informačního systému postaveného z komponent proto můžeme snadno přizpůsobovat potřebám – škálovat, a to bez přerušení poskytování služeb. Jak kvantitativně měnit počet virtuálních serverů (scale-out), tak kvalitativně – aktualizovat komponenty a přidávat funkce (scale-up).

Schopnost škálování je důležitá zejména pro ekonomickou výhodnost systémů s výrazně proměnlivou nebo setrvale rostoucí zátěží a dále tam, kde je požadován nepřetržitý provoz.

Ke zjednodušení administrace hostitelské infrastruktury a životního cyklu hostů, automatizaci škálování podle zátěže komponent spolu s reakcí na havárii některého z hostů vznikly.

Známé orchestrační platformy jsou Kubernetes (RedHat Linux), OpenNebula (Linux) a vSphere (VMware). Otevřené platformy dovedou orchestrovat nejen virtualizační, ale i cloudové služby.

Vedle virtualizace počítačů hovoříme o virtualizaci sítí – více izolovaných okruhů nad jednou kabeláží (VLAN), softwarově definovaných sítích (SDN), nebo o virtualizaci úložišť – více logických disků nad jedním diskovým polem (SAN) a softwarově simulovaných úložištích bez speciálního hardware (vSAN).

2.3.2 Internet věcí

Internet věcí (anglicky Internet of Things = IoT) je označení pro síť fyzických zařízení (senzory, aktuátory) a jejich celků – vozidel a dopravního zařízení, domů (technická zařízení budov, bezpečnost), komunálních zařízení (semafory, veřejné osvětlení, popelnice, produktovody, kanalizace, monitory prostředí), domácích spotřebičů, osobních zařízení (tlakoměr, glukoměr, detektor pádu a bezvědomí) a dalších zařízení, vybavených elektronikou a síťovou konektivitou (od nízkoenergetického přenosu až po internet), která umožňuje těmto zařízením se propojit a vyměňovat data.

Internet věcí má usnadnit člověku pokrýt širokou škálu potřeb, na druhou stranu může vést až k přílišné závislosti na tom, že chytré systémy budou za nás leccos dělat, rozhodovat a potažmo i za nás myslet. Reálná je zejména hrozba zneužití (kyberútoků) na nedostatečně zabezpečená zařízení a sítě, což může zásadně ovlivnit chování „chytrých zařízení“. Problémy Internetu věcí jsou zejména:

- Bezpečnost – zařízení s nízkou spotřebou a dlouhou dobou života jsou zranitelná, s malým výkonem je těžké až nemožné použít tradiční firewall, antimalware a bezpečnostní aktualizace
- Fragmentace – aktuálně velký počet výrobců a technologií, nesjednocené standardy.
- Soukromí – existuje značný potenciál k ohrožení soukromí, sledování a sociální manipulaci.
- Design a udržitelnost – rychlejší zastarávání, zkracování životního cyklu a rychlejší obměna vede k vyšším nákladům koncových spotřebitelů a zvýšení produkce elektroodpadu.

2.3.3 Umělá inteligence a strojové učení

Umělá inteligence je věda o vytváření strojů nebo systémů, které budou při řešení určitého úkolu užívat takového postupu, který, kdyby jej vykonával člověk, bychom považovali za projev jeho inteligence.

Technické systémy rozhodování jsou neunavitelné opakovanou činností, objektivní, rychlejší a přesnější. Umělá inteligence dnes nestaví na analýze a programování, ale na statistice a strojovém učení. Při asistovaném strojovém učení umíme bez programování „natrénovat“ vyhodnocování vstupních dat podle „učitele.“ Při trénování ale může reakce navázat na nesprávné vstupní podněty, což není snadné odhalit, stejně jako převzetí nevědomého neobjektivního postoje „učitele.“

Umělá inteligence složená z algoritmů a asistovaného učení by mohla ve veřejné správě podpořit procesní součásti, vyhodnocovat podklady a navrhovat rozhodnutí jednodušších řízení, což se dnes děje například při odhalování překračování rychlosti na komunikacích. Také při jednání Poslanecké sněmovny běží automatický přepis řeči do záznamu.

2.3.4 Velká data, datová analytika, datové sklady, datová jezera

Provozní data, vznikající při poskytování služeb, jsou ukládána jako záznamy o těchto transakcích. Objem dat plynule roste a jednou zapsané údaje se již nemění. Z nich se odvozují různé skutečnosti – fakta. Fakta mohou být agregovatelnými metrikami, nebo hodnotami, které je kategorizují, tzv. dimenzemi.

Business Intelligence (BI) se zabývá zpracováním, analýzou a historickým srovnáním metrik zaznamenaných transakcí podle různých dimenzí za účelem vyhodnocování kvality služeb a vytváření předpovědí dalšího vývoje pro plánování budoucích potřeb. Výstupy publikuje koncovým uživatelům, manažerům, ve formě analytických nebo manažerských reportů, dashboardů a manažerských kokpitů.

Big data, velká data, jsou podle jedné z definic soubory dat tak velké a složité, že tradiční software je pro jejich zpracování nedostatečný a nedokáže je zpracovávat v rozumném čase.

Velké objemy dat jsou ukládány předzpracované ve strukturované podobě, v předem daných cyklech a následně analyzovány již připravenými algoritmy v datových skladech.

Datový sklad (anglicky Data Warehouse, DWH) jsou nástroje pro práci s velkými daty z více zdrojů s cílem uložit data v datových strukturách vhodných pro rychlý, předem definovaný reporting.

Analýza předem nezpracovaných dat může nalézt nové vazby a pohledy též např. v boji proti zločinu.

Datové jezero (anglicky Data Lake, DL) jsou nástroje pro práci s velkými daty s cílem uložit všechna primární data, aby z nich bylo možné vytěžit znalosti pro budoucí předem neznámé potřeby reportingu.

Velká data se uplatňují ve vědeckých oborech, obchodních a reklamních firmách a vládních institucích, které se pravidelně potýkají s velkými datovými sadami v oblastech, jako je vyhledávání na internetu, meteorologie, genomika, demografie, biologie, environmentální výzkum, městská informatika.

Dále navazují netechnologické trendy, do této skupiny řadíme trendy, jejichž „netechnologické základy“ převažují ty „technologické.“

2.3.5 Specializace, centralizace poskytování služeb, outsourcing

Rozvoj ICT vyžaduje stále více pracovníků, mezi kterými díky kratší době přípravy nutně dochází ke specializaci. Celou šíři ICT na profesionální úrovni v celé šíři oboru dnes těžko zvládne jeden univerzální „ajťák.“ Běžná údržba, doplňování tonerů v tiskárnách nebo zakládání uživatelů navíc nevyžaduje vysokou odbornost. Vedle původních profesí správců, síťařů, techniků hardware jsou

dnes specialisté pro konkrétní databázi, programátoři pro konkrétní programovací jazyk a další. Zcela noví jsou třeba specialisté kybernetické bezpečnosti, IT architekti, projektoví manažeři se specializací na ICT.

Specializované firmy dnes nabízejí své služby od pronájmu technologií, přes opravy, každodenní správu a zakázkový vývoj, až po zabezpečení proti kybernetickým rizikům a konzultace při specifikaci zadání pro výběrová řízení prostřednictvím efektivních týmů specialistů. A tak si organizace, které ICT využívají pro podporu své hlavní činnosti (finanční sektor, dopravní sektor, obchod, výroba atd.), ponechávají pouze pracovníky na základní údržbu a kvalifikovanější činnosti si najímají. I veřejná správa projevuje tuto závislost na cizích službách. Vzhledem k tomu, že jednak využívá a spravuje data občanů a zajišťuje fungování a bezpečnost státu, je tento přechod pomalejší, ale jeví se podobně nevyhnutelný.

Dalšímu prostředky je rozbití jednotlivých služeb to základních stavebních kostek (mikroslužby). Či multitenantní řešení – správcovství a řízení zejm virtualizovaných prostředí a ekosystémů. Dalšími aspekty je práce odkudkoli – práce z domova, přístup se sdílenými dokumenty aj.

2.3.6 Sociální sítě

Pojem sociální síť označuje skupinu lidí, která spolu udržuje komunikaci různými prostředky. V oblasti ICT zahrnuje komunikační služby poskytované v digitálním prostředí internetu. Registrovaní členové vytvářejí osobní či firemní profily, diskutují s ostatními členy o zájmových tématech, sdílejí informace, fotografie, hudbu a videa veřejně nebo ve vymezených skupinách pomocí vzkazů (post) ve sdíleném prostředí skupiny (nástěnka, zeď), nebo privátně pomocí zpráv mezi dvěma a více účastníky.

Světově asi nejrozšířenější jsou Facebook, Twitter a Instagram, ale seznam rychle roste i díky regionálním sítím (DACH, Asie, Afrika). Na významu nabírá například profesní sociální síť LinkedIn.

Sociální sítě využívá řada OVS (města, muzea, nemocnice) nejen pro publikování sdělení, ale i pro příjem reakcí od občanů. Jejich používání, stejně jako u elektronické pošty, není v ČR upraveno bližšími zákonnými pravidly. Komunikace na sociálních sítích nenahrazuje používání oficiálních informačních kanálů, webů a elektronických úředních desek, jsou však vhodným doplněním.

2.3.7 Kryptoměny a blockchain

Blockchain (řetězec bloků) je způsob distribuovaného a veřejného (peer-to-peer) vedení a stvrzování pravosti transakčních záznamů, vícenásobně chráněný před podvody. Je využitelný k vedení a prokazování skutečností, například v dodavatelsko-odběratelských vztazích. Pro VS je díky své ochraně proti chybám a neoprávněné manipulaci vhodný třeba pro vedení trvalých záznamů v registrech.

Bitcoin poprvé použila osoba či skupina osob pod pseudonymem „Satoshi Nakamoto, jakožto anonymní autor, dne 3. ledna 2009 jako technologický koncept a důkaz užitečnosti blockchainu. Symbolicky měl sloužit pro odměňování uživatelů za využitý výpočetní výkon na počítání náročných kryptografických ochranných (kontrolních) součtů (hash).

Za určený objem výpočtů provozovatel (crypto miner, „kryptotěžař“) získá („vydoluje“) jednu „bitovou minci“ – „Bitcoin.“ O tom jsou dále vedeny transakční záznamy svázané s jeho „peněženkou.“ Omezená celková emise a zpomalování výdeje (čím později, tím více výpočtů), nemožnost podvádět (žádný „inflační dotisk“), nezávislost na vládách a bankách, spolu s potenciální anonymitou vytvořily z Bitcoinu zajímavou alternativu státních peněz a z jeho uživatelů nepřítele centrálních bank a autoritářských vlád.

Kolem měny Bitcoin vznikly krypto burzy a díky krypto směnárníkům pronikl do reálného světa. Stal se platidlem lidí, kteří chtějí chránit své soukromí a vyhýbat se dohledu autorit, ale také kriminálních živlů. Je také vzorem pro další kryptoměny.

2.3.8 Chytré telefony – mobilní superpočítače

Zejména „chytré“ mobilní telefony a jejich větší bratři, tablety, nezastírají, že jsou přenosnými počítači multimediální výbavou. Jejich operační systémy stahují z katalogu aplikací programy ovládané dotykem displeje nebo hlasem. Bezdrátově přistupují k internetu přes mobilní data nebo WiFi. Přes Bluetooth obsluhují sluchátka, chytré hodinky, fitness náramky, nositelnou elektronikou a ostatní počítače.

Aplikace jsou buď zcela zdarma, nebo placené zobrazováním reklamy a provizí z nákupů, platbami za používání nebo odemčení některých funkcí (mikroplatby) nebo s tradičně placenou instalací. Některé placené programy pro stolní počítač nebo cloudovou službu zahrnují i licenci pro na mobilní zařízení.

Přenosné počítače (laptop, notebook) a mobilní internetová zařízení (chytrý telefon, tablet), dovolují na cestách nejen zábavu, ale rovněž práci kdekoliv, i v terénu, a práci z domova, a to nejen komerčním firmám, například stavebním, lesním správcům, ale i veřejné správě.

Zejména „chytré“ mobilní telefony a jejich větší bratři, tablety, nezastírají, že jsou přenosnými počítači multimediální výbavou. Jejich operační systémy stahují z katalogu aplikací programy ovládané dotykem displeje nebo hlasem. Bezdrátově přistupují k internetu přes mobilní data nebo WiFi. Přes Bluetooth obsluhují sluchátka, chytré hodinky, fitness náramky, nositelnou elektronikou a ostatní počítače.

Aplikace jsou buď zcela zdarma, nebo placené zobrazováním reklamy a provizí z nákupů, platbami za používání nebo odemčení některých funkcí (mikroplatby) nebo s tradičně placenou instalací. Některé placené programy pro stolní počítač nebo cloudovou službu zahrnují i licenci pro na mobilní zařízení.

Přenosné počítače (laptop, notebook) a mobilní internetová zařízení (chytrý telefon, tablet), dovolují na cestách nejen zábavu, ale rovněž práci kdekoliv, i v terénu, a práci z domova, a to nejen komerčním firmám, například stavebním, lesním správcům, ale i veřejné správě.

2.3.9 Odkazy

- Národní architektonický plán na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/nap_dokument:celkovy_dokument

3 ICT veřejné správy – smysl očekávání, rizika, prostředky

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména nařízení EU č. 910/2014, zákon č. 365/2000 Sb., zákon č. 111/2009 Sb., zákon č. 12/2020 Sb.

3.1 Smysl a očekávání

ICT jsou **typicky prostředkem/podporou činnosti**, kterou mají **zefektivnit** či **umožnit** např. automatizace odesílání, přijímání a zpracování pošty v digitálním světě. Smyslem není postavit systém, ale doručit klientovi službu, kdy právě tato služba je přidanou hodnotou. Veřejné správy musí být v souladu s tzv. **principy 3E** – účelnost (dělat správné věci), účinnost (dělat věci správně), hospodárnost (minimalizovat zdroje vůči chtěné kvalitě), více k 3E viz kapitola 5.

Pro každého občana je však smysl a zejména očekávání ohledně veřejné správy různorodé. Někteří volají po minimalizaci státního aparátu, jiní např. zase preferuji sociální jistoty. Finální obraz těchto přesvědčení je reflektován politicky – viz např. volební program stran a hnutí. ICT veřejné správy je utvářeno programem **Digitální Česko** (usnesením vlády č. 629 z 3. října 2018), kdy materializovaným podkladem příslušné strategické dokumenty (poslední aktualizace usnesením vlády č. 931 ze dne 9. listopadu 2022):

- **Česko v digitální Evropě** – vztah digitálního světa České republiky (ČR) a EU, tři hlavní cíle.
- **Informační koncepce České republiky** – rozvoj eGovernmentu ČR, šest hlavních cílů:
  - Uživatelsky přívětivé a efektivní on-line služby pro občany a firmy,
  - Digitálně přívětivá legislativa,
  - Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu,
  - Zvýšení kapacit a kompetencí zaměstnanců ve veřejné správě,
  - Efektivní a centrálně koordinované ICT veřejné správy,
  - Efektivní a pružný digitální úřad.
- **Digitální ekonomika a společnost** – výzkum, jeho aplikace a provázání, osm hlavních cílů.

Hlavní cíle zbylých dvou dokumentů jsou v doplňující části. Informační koncepce České republiky (IKČR) dále obsahuje čtyři **navazující dokumenty**, které zpracovává a průběžně aktualizuje Odbor Hlavního architekta eGovernmentu (OHA) Ministerstva vnitra (tabulka 1). Právě IKČR je stěžejním dokumentem pro samotný eGovernment. Dle zákona č. 365/2000 Sb. má každý **orgán veřejné správy** (OVS) svoji **informační koncepci** (IKOVS), která obsahuje jednotlivé cíle a způsob jejich naplnění, kdy tato koncepce OVS musí být s v souladu s Informační koncepcí České republiky.

Tabulka 1 – Navazující dokumenty Informační koncepce České republiky

Název dokumentu	Stručná charakteristika
Metody řízení ICT veřejné správy ČR (MŘICT VS ČR)	Pravidla upravující centrálně koordinované řízení ICT.
Slovník pojmů eGovernmentu	Vytvoření slovníku pro sjednocení chápaní a vyjadřování myšlenek všech jednotlivých aktérů v prostředí ICT veřejné správy.
Národní architektonický rámec (NAR)	Myšlenkový a metodický rámec pro popis Národní architektury veřejné správy ČR na všech jejích úrovních.
Národní architektonický plán (NAP)	Jedná se o popis současného stavu jednotlivých úřadů, ale zejména i promítnutí jejích plánovaných stavů budoucích.

3.2 Rizika

Budování digitálního governmentu a jeho kontinuálního zlepšování, jakožto jakákoliv **změna** se však pojí s **riziky**. Veřejná správa na rozdíl od soukromého sektoru činí pouze to, k čemu má zmocnění (např. plynoucí ze zákona). Samotné **ocenění efektivity v soukromém sektoru** oproti komerčním je značně komplikováno – např. běžné metriky jako zisk, či maximalizace hodnoty firmy nelze na hodnocení veřejného sektoru takto použít.

Dalším rizikem je i způsob dosažení výsledku, předesláno bylo hodnocení 3E, nad kterým bdí i Nejvyšší kontrolní úřad (NKÚ). Digitalizace procesu má měnit a uzpůsobit fungování úřadu, avšak typickým rizikem je, že místo **digitalizace** dojde pouze k **elektronizaci** – převodu z analogového světa bez invence, či optimalizace. Tyto elektronické kopie služeb a procesů jsou pak již od základu odsouzeny k záhubě.

Digitální svět se též liší svým dosahem a způsobem fungování, vždy musí být zohledněno **bezpečnostní riziko** (jak fyzické, tak kybernetické), tak aby služba byla bezpečná, např. aktuální tématem jsou služby cloudu. Další informace lze nalézt v kapitolách 10, 11, 19 a 20).

3.3 Prostředky

Mezi hlavní prostředky ICR veřejné správy patří **informační systém veřejné správy** (zmiňovaný v kapitole 1). Jiným pohledem nad informačními systémy je klasifikace dle zákona č. 111/2009 Sb., který definuje tzv. Agendový informační systém (AIS) – veřejný sektor a dále pracuje s pojmem Informační systém soukromoprávních uživatelů údajů (ISSPUÚ) – soukromý sektor.

Tedy hlavním stavebním blokem jsou informační systémy – služby, aplikace, servery, ale i lidi, a to jak klienti, tak např. administrátoři. Role služeb je i díky zákonu č. 12/2020 Sb. dále posilována.

Otázky k procvičení:

1. Jaký smysl spatřujete ve vaší činnosti? Jaké očekávání máte od českého eGovernmentu?

Zkuste najít jak agendové, tak průřezové zákony, podle kterých vykonáváte státní službu (např. pro ministerstvo dopravy: zákon č. 361/2000 Sb. (o provozu na pozemních komunikacích) a č. 250/2017 Sb. (o elektronické identifikaci) a další. Odpovídá to očekáváním? Lze něco zlepšit?

2. Jak je strategicky utvářeno a řízeno ICT veřejné správy?

Hlavním oporou je program Digitální Česko a jeho tři strategické dokumenty: IKČR…

3. Jaké cíle, či např. projekty řeší informační koncepce vašeho úřadu?

Pohledem do informační koncepce MV jsou nyní řešeny projekty jako je digitální sbírka (digitalizace právní agendy, cíl digitálně přívětivé legislativy), či eMatrika (digitalizace matriční činnosti, cíl uživatelsky přívětivé a efektivní on-line služby pro občany a firmy).

3.4 Doplňující část

ICT způsobily změny takového rozsahu (jak geograficky, kde již obsáhly celý svět, tak ovlivněním prakticky všech sfér života). Masové rozšíření a užití ICT je dnes označováno jako digitální revoluce (3. průmyslová revoluce). Tímto však tento trend nekončí, nyní jsme v období tzv. čtvrté průmyslové revoluce (taktéž známé jako Industry 4.0), která se vyznačuje další automatizací, spoluprací a komunikací strojů a IoT.

Důsledkem je, že termíny jako jsou bezpapírová kancelář, digitální a mobilní pracoviště se z propagačních hesel staly realitou. Jedná se o jednoznačné, obecně platné trendy, v rámci, kterých se díky novým technologickým možnostem kvalitativně mění pracovní procesy nejen v komerční oblasti, ale i ve veřejné správě. Využívání ICT prostředků dnes prakticky v žádné oblasti lidské činnosti není volbou, ale nutností. Zatímco v komerční sféře představuje ICT jeden z rozhodujících nástrojů dosahování zisku, ve veřejné sféře je nástrojem ke zvyšování kvality a hospodárnosti výkonu veřejné správy, tzn. efektivnosti poskytování služeb veřejné správy.

3.4.1 Strategické cíle informatizace VS ČR – Digitální Česko

Strategické cíle informatizace VS ČR koncepčně vychází z programu Digitální Česko, který byl zakotven usnesením vlády č. 629 z 3. října 2018. Tento program se skládá ze třech pilířů (dílčích koncepcí / strategií): Česko v digitální Evropě, Informační koncepce České republiky, Digitální ekonomika a společnost. Významný posun představoval zákon č. 12/2020 Sb., o právu na digitální služby. Druhý zmíněný dokument, Infomační koncepce České republiky (IK ČR), představuje koncepci budování eGovernmentu v ČR 2018+ a jeho IT podpory podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Tabulka 2 – Digitální Česko, struktura programu a hlavní cíle

Hlav. cíl	Česko v digitální Evropě	Informační koncepce České republiky	Digitální ekonomika a společnost
1.	Institucionální zajištění koordinace a financování implementace koncepce	Uživatelsky přívětivé a efektivní on-line služby pro občany a firmy	Efektivnější systém přímé i nepřímé podpory výzkumu, vývoje a inovací
2.	Zajištění účinné komunikace o aktuálních tématech a příležitostech v digitální agendě EU	Digitálně přívětivá legislativa	Zralost a připravenost sektorů ekonomiky na digitální transformaci
3.	Prosazování národní pozice ČR u prioritních témat v digitální agendě EU	Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu	Připravenost občanů na změny trhu práce, vzdělávání a rozvoj digitálních dovedností
4.		Zvýšení kapacit a kompetencí zaměstnanců ve veřejné správě	Podpora konektivity a infrastruktury digitální ekonomiky a společnosti
5.		Efektivní a centrálně koordinované ICT veřejné správy	Zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti
6.		Efektivní a pružný digitální úřad	Legislativa podporující všechny aspekty digitální ekonomiky a společnosti

7.	Optimální systém financování digitální ekonomiky a společnosti
8.	Institucionální zajištění centrální koordinace politik na podporu digitální ekonomiky a společnosti

Každý z těchto pilířů obsahuje své hlavní cíle. Pro pilíř IK ČR je v současné době definováno šest hlavních cílů, které se zaměřují na právě ICT veřejné správy, a to jak na pro-klientský orientované služby, tak i způsoby jak jich dosáhnout od legislativního základu po efektivní spolupráci jednotlivých orgánů veřejné správy, tyto cíle jsou dále rozepsány do detailnějších cílů dílčích, se základním popisem způsobem jejich naplnění, které jsou dále realizované implementačním plánem. Součástí IK ČR jsou i čtyři navazující dokumenty, viz níže.

Tabulka 3 – Navazující dokumenty k IKČR

Název dokumentu	Stručná charakteristika
Metody řízení ICT veřejné správy ČR	Soubor pravidel upravující centrálně koordinované řízení ICT
Slovník pojmů eGovernmentu	Vytvoření slovníku pro sjednocení chápaní a vyjadřování myšlenek všech jednotlivých aktérů v prostředí ICT veřejné správy pro snížení bariér komunikace
Národní architektonický rámec	Myšlenkový a metodický rámec pro popis Národní architektury VS ČR na všech jejích úrovních
Národní architektonický plán	Jedná se o popis současného stavu jednotlivých úřadů, ale zejména i promítnutí jejích plánovaných stavů budoucích.

3.4.2 Smysl a očekávání ICT veřejné správy

eGovernment – z elektronizace k digitalizaci Prostý překlad slova eGovernment odpovídá spojení elektronické vládnutí. Nicméně obecným principem eGovernmentu v současné době není pouze podpora agendy v jeho elektronické podobě, ale samotná změně paradigmatu, kde nové, ale současné služby jsou vytvářeny v kontextu dostupných technologií, propojování dat a přístupu eDemokracie, tedy participace samotných občanů a dalších zainteresovaných osob. Tomuto způsobu uvažování se téže říká „Digitální Government“, což je termín ražený i předními útvary v rámci Evropské unie.

Hlavní myšlenkou výkonu eGovernmentu (Digitálního Governmentu) v praxi je správa věcí veřejných za využití moderních digitálních nástrojů, díky kterým je veřejná správa k občanům přátelštější, dostupnější, rychlejší a také levnější.

Posláním útvarů informatiky a IT komunity ve veřejné správě ČR je podporovat programy a oddělení úřadů při poskytování veřejných služeb a informací pomocí cenově výhodných, inovativních, sdílených, spolehlivých a bezpečných technologií.

Z hlediska hospodárnosti čerpání veřejných rozpočtů není obecně žádoucí ani přípustné, aby v rámci veřejné správy docházelo k tvorbě systémů nebo jejich částí, které by duplikovaly funkce / služby poskytované již jako sdílené služby eGovernmentu.

Stejně tak je nehospodárné vytvářet a spravovat lokálně data shodná s referenčními daty spravovanými některým ze základních registrů. Všechny útvary veřejné správy tak aktuálně musí

v souladu se svými aktuálními zmocněními, využívali maximálně již existující referenční a garantovaná data.

Ověření možných duplicit je povinným krokem již v rámci zpracovávání projektového záměru na budování nové, nebo na změnu již existující ICT služby, a jako takové musí být, spolu s uvedením, které existující služby eGovernmentu předkladatel již využívá a které hodlá využívat, dokládáno v žádosti o stanovisko Hlavního architekta eGovernmentu.

I když cílem veřejné správy není tvorba zisku a o tom, co je správné, nerozhodují úředníci, ale v demokratických státech volení zástupci, i pro veřejnou správu a ji řídící pracovníky platí povinnost chovat se při plnění výkonu veřejné správy jako dobrý hospodář, tzn. dodržovat princip 3E: hospodárnosti, efektivity a účelnosti, a to v rámci celého životního cyklu informačního systému, tzn. od zahájení úvodních analýz potřeb a rizik, přes formulaci kritérií, výběr konceptu řešení, specifikaci zadání, řízení realizace výstavby a produkčního provozu systému, až po likvidaci.

Plnění této povinnost je ve VS navíc sledováno řadou kontrolních úřadů a za její nedodržování hrozí usvědčeným právní postih.

Plnit princip 3E jinak řečeno znamená realizovat potřebné služby (funkce IS) s potřebnými vlastnostmi (parametry), které odpovídají tvrzení: „dělat správné věci, dělat je správně a dělat je za přiměřené náklady“.

Agendy, procesy, činnosti a funkce musí odpovídat zákonným a dalším požadavkům. Při návrhu zadání ICT služby (funkcionalit informačního nebo komunikačního systému) je tedy třeba zohlednit a zapracovat nejen věcnou legislativu popisující kdo, co, proč, pro koho, za jakých předpokladů atd. vykonává (např. správní řád), ale i všechny další „obecné“ IT legislativní požadavky (spisové služby, elektronický podpis, otevřená data apod.) a světově akceptované zkušenosti a doporučení, např. ITIL.

Příklady změn praxe výkonu veřejné správy způsobené ICT:

- Distribuce dokumentů a informací – dříve se dokumenty musely přepravovat na velké vzdálenosti k příslušným úředníkům, dnes mají úředníci všechny dokumenty k dispozici ihned.
- Vyhledávání – dříve se dokument nebo informace musely vyhledávat v archivech a kartotékách mezi tisíci jinými, dnes je možné vyhledávat fulltextově nebo pomocí metadat i dokumenty uložené na druhém konci světa.
- Spolupráce – dříve byly procesy lineární, dokud jeden úředník dokument nezpracoval, nemohl na něm začít pracovat následující, dnes je možné pracovat s elektronickým obrazem dokumentu a rozhodnutí vytvářet i kolaborativně (více osob tvoří současně jeden dokument).

Právě rozdílnost kompetencí – tedy práv a povinností – způsobuje různé úhly pohledů účastníků a téže jejích zájmů.

3.4.3 Hodnota dat

Data a zejména z nich vytvářené informace jsou základním aktivem každé organizace. Je to dáno jejich významem pro existenci a pro úspěšnost fungování (u komerčních organizací pro prosperitu, u veřejné správy pro efektivnost) organizace.

Hodnotu mají data a informace nejen v komerčním světě, kde jsou dnes běžně součástí nehmotného majetku, a tedy hodnoty firmy, ale i ve veřejné správě.

Hledisko nákladové (historické hledisko). Hodnota dat a informací je dána nejen náklady na jejich pořízení (např. nákup databáze). Celkově je určována vynaloženými prostředky zejména na jejich:

- sběr – často již neopakovatelný nebo jen velice pracně,
- vytvoření – zejména ruční vložení (navstupování pomocí klávesnice) do IS,
- aktualizaci – v rámci průběžného vedení agendy VS (např. matrik),
- ukládání – z hlediska bezpečnosti obvykle replikovaně na více místech.
- současné hledisko
- Současné hledisko, dnešní pojetí ICT oceňuje data a informace i z pohledu dopadů, které by mohlo způsobit např. jejich:
- poškození, tj. ztráta komplexnosti, neaktuálnost a nesprávnost, chybějící nebo nesprávně modifikované vzájemné vazby atd.,
- nedostupnost (ať už z důvodu poruchy IS, ztráty dat nebo nefunkčnosti připojení od uživatele k němu),
- únik – zpřístupnění neoprávněným osobám a využití těchto dat k nezákonným aktivitám, přičemž nejde pouze o náklady na obnovu či penalizaci, ale i o náklady způsobené výpadkem nebo chybným výkonem agend na těchto datech založených a o ztrátu prestiže, v případě veřejné správy i o ztrátu důvěry občanů.

3.4.4 Smluvní úroveň služeb (SLA)

Chápeme-li ICT službu jako prostředek k dosažení cíle, je jasné, že nestačí pouze definovat jeho náplň / předmět cíle (např. přenést elektronickou zprávu od odesilatele k adresátovi), ale že je nutné stanovit / sjednat mezi uživatelem a poskytovatelem její klíčové parametry a pro každý z dohodnutých parametrů stanovit jeho přijatelné hodnoty a metodiku měření splnění těchto hodnot.

Sjednané parametry a přijatelné hodnoty služby se souhrnně označují jako SLA (zkratka anglického pojmu Service Level Agreement).

Poznámka: V oblasti komunikací se pro rezervaci a řízení datových toků v telekomunikačních a počítačových sítích často používá i termín QoS (Quality of Service), např. v rámci dělení dostupné přenosové kapacity, aby nedocházelo zahlcením sítě ke snížení kvality síťových služeb.
Příklady:

- klíčový parametr - např.: velikost zprávy, počet adresátů, „pracovní“ dobu poskytovatele rychlost reakce obsluhy v případě výpadku, max. % nedoručených zpráv / ztracených paketů atd.,
- (ne)přijatelná hodnota - např.: max. velikost zprávy 3 GB, min. propustnost 2 Tb/sec., rychlost dokončení přenosu po odeslání zprávy do 10 s…),
- metodika měření splnění těchto hodnot = oboustranně odsouhlasená metodika měření (monitoringu), jejíž výsledky budou oběma stranami akceptovány i jako podklad sankcionalizace pro případy neplnění SLA ze strany dodavatelů.

Z hlediska ekonomického je třeba rozlišovat 4 základní režimy služeb:

- služby placené paušálně – typickým příkladem jsou služby platformové a služby, u kterých je nezbytné, aby jejich poskytovatel držel jejich výkonové parametry včetně dostupnosti, a to i když právě využívány nejsou, např. provoz webového portálu, provozování služby HelpDesk a bezpečnostní monitoring provozu, správa virtuálního prostředí datového centra,
- služby výkonové, tj. služby placené (ne nutně koncovým uživatelem = klientem, ale často inzerenty, v případě veřejné správy orgánem veřejné správy odpovědným za danou agendu) dle skutečně odebraného výkonu na základě měřitelných údajů (např. množství přenesených dat, průměrná velikost obsazeného datového prostoru, počet potištěných stran, počet reinstalovaných PC atd.),
- služby placené metodou Time & Material (výkazy práce specialistů za dohodnutou / smluvní cenu [Kč/člověkoden] plus prokazatelné náklady na materiál),
- kombinace výše uvedených.

3.4.5 Celkové náklady na vlastnictví (TCO)

Aby principy 3E opravdu platily, a to za celou dobu životního cyklu ICT služby, musí být i ICT služby provozované interně posuzovány komplexně, tzn. zohledňovat jak náklady, tak přínosy, a to co možná komplexně a objektivně.

Standardní metodou pro objektivní výpočet nákladů je metoda celkových nákladů na vlastnictví (Total Cost of Ownership = TCO), která zahrnuje jak:

- pořizovací náklady (analýzy, konzultace, nákup technologií, implementace, školení uživatelů atd.), tak i
- provozní výdaje (veškeré smluvní závazky spojené s provozem systému, např. podpora výrobce antiviru, výdaje za spotřební materiál, náhradní díly, energie, interní správu/obsluhu atd.) po celou plánovanou dobu životnosti, a započteny by v nich správně měly být i
- náklady na likvidaci.

3.4.6 Rizika ICT veřejné správy

Jak dokládají např.:

- Usnesení vlády ČR č. 241 o metodické podpoře v oblasti kybernetické bezpečnosti pro rok 2018 ze dne 18. dubna 2018, kterým vláda ukládá členům vlády a vedoucímu Úřadu vlády, aby informační a komunikační technologie využívané jimi řízenými ústředními správními úřady zabezpečili podle požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), alespoň na stejné úrovni, která je touto vyhláškou stanovena pro významné informační systémy.
- Usnesení vlády ČR č. 18 k hrozbě v oblasti kybernetické bezpečnosti ze dne 7. ledna 2019, kterým vláda správcům kritické informační infrastruktury a významných informačních systémů ukládá provést analýzu rizik se zohledněním varování Národního úřadu pro kybernetickou a informační bezpečnost, ze 17. prosince 2018.

Zajistit bezpečnost dat spravovaných orgány veřejné moci představuje naprosto základní požadavek.

Proto je tato problematika podrobněji rozebrána v samostatných kapitolách:

- odpovědnost v Kap. 10 – Životní cyklus služby a klíčové role veřejné správy,
- bezpečnostní kategorizace v Kap. 19 - Kategorizace dat a dokumentů (veřejné správy) z pohledu potřeby zajištění jejich ochrany,
- jak data chránit v Kap. 20 - Způsoby a prostředky ochrany informací / dat v současných informačních a komunikačních technologiích (ICT).

Pro využití Cloud Computingu orgány veřejné správy jsou určujícími hledisky zejména:

- soulad s legislativními pravidly,
- úroveň bezpečnosti zpracovávaných dat a poskytovaných digitálních (ICT) služeb.

3.4.7 Prostředky ICT veřejné správy

Informační systém veřejné správy je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností (definice ze zákona č. 365/2000 Sb.).

Informační systém veřejné správy (ISVS) slouží pro účely výkonu agend veřejné správy, tedy neslouží pro podporu interních procesů jednotlivých úřadů. Systémy řešící právě tyto úlohy se nazývají provozními informačními systémy.

Zákon dále specifikuje, na které ISVS se tento zákon dále nevztahuje (typicky informační systémy bezpečnostních složek) a naopak, na které provozní systémy je hleděno jako na ISVS dle tohoto zákona (například elektronický systém spisové služby, systém elektronické spisové služby, či informační systémy pro odměňování zaměstnanců).

Agendový informační systém je informační systém veřejné správy, který slouží k výkonu agendy, využívání elektronických formulářů nebo elektronické identifikaci (definice ze zákona č. 111/2009 Sb).

Agendový informační systém (AIS) umožňuje oprávněnému orgánu veřejné moci či soukromoprávnímu uživateli údajů přistupovat prostřednictvím Informačního systému základních registrů (ISZR), který provozuje Správa základních registrů (SZR) k údajům základních registrů či údajům jiných agend (jiných AIS). Orgány, které neprovozují vlastní AIS, mohou využívat CzechPOINT@office.

AISy se podle režimu užívání mohou rozdělit do dvou skupin:

- Centrální AIS – jeho správcem je ústřední správní úřad a mohou jej celoplošně využívat orgány veřejné moci k výkonu určité agendy, např. AIS evidence obyvatel, AIS cizinců, AIS zbraně a střelivo, AIS působnostní registru práv a povinností, aj.
- Uživatelský AIS – jeho správcem je OVM, který jej sám, či spolu s dalšími OVM, využívá k výkonu určité agendy, např. integrované krajské informační systémy.

Podmínkou napojení AIS na ISZR je:

- Registrace ISVS do registru práv a působností (RPP), včetně definice agendy vykonávané tímto AIS a potřebných napojení na základní registry (ZR),
- splnění podmínek stanovených SZR a souhlas s dodržováním těchto pravidel SZR.

3.4.8 Odkazy

- Digitální Česko:

https://www.digitalnicesko.cz/

- Informační koncepce České republiky na stránkách Národní architektury eGovernmentu

https://archi.gov.cz/ikcr

4 Právní normy, standardy a doporučení v oblasti ICT veřejné správy

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména nařízení EU č. 910/2014, zákon č. 365/2000 Sb., zákon č. 111/2009 Sb., zákon č. 12/2020 Sb.

4.1 Právní předpisy Evropské unie

Mezi hlavní právní akty Evropské unie (EU) přímo ovlivňující ICT veřejné správy patří závazné **nařízení 910/2014** electronic IDentification, Authentication and trust Services (**eIDAS**, česky o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu), ta přináší možnost interoperabilního užití digitální identity pro služby digitálního govenrmentu napříč Evropskou unií (např. se pomocí české eObčanky jako prostředku identity přihlásit do portálu finského eGovernmentu). Další závaznou a všeobecně známou legislativní úpravou je nařízení General Data Protection Regulation (GDPR, česky obecné nařízení o ochraně osobních údajů), které definuje klíčové principy zpracování, přístupu, opravy, výmazu a přenositelnosti osobních dat, což musí splňovat i každý informační systém

Dále je vhodno zmínit **směrnici 2016/1148** o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, která řeší důvěryhodný a členským státům dostupný přenos dat.

4.2 Právní předpisy České republiky

Krom hlavních zákonů upravující ICT veřejné správy (tabulka 4) je vhodné alespoň zmínit zákon o svobodném přístupu k informacím, zákon o zpracování osobních údajů, či zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. Taktéž pokud je podpora agendy řešena informačním systémem, tak jeho zakotvení by obsahoval i každý takový **agendový zákon**.

Tabulka 4 – Vybrané hlavní právní předpisy pro oblast ICT veřejné správy

Právní předpis	Řešení oblast ve vztahu k ICT veřejné správy
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy	ISVS, Provozní informační systémy, IKČR, IKOVS, povinnost schvalování investičních záměrů a technického zhodnocení určených informačních systémů.
Zákon č. 111/2009 Sb., o základních registrech	Základní registry (ZR), referenční rozhraní, oblast propojeného datového fondu (PPDF).
Zákon č. 12/2020 Sb., o právu na digitální služby	Právo na digitální službu, právo činit digitální úkon všemi určenými obslužnými kanály, katalog (digitálních) služeb.
Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů	Datové schránky, informační systém datových schránek, konverze dokumentů z listinné na papírové a vice versa.
Zákon č. 499/2004 Sb., o archivnictví a spisové službě	Archivy, elektronický systém spisové služby.
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce	Kvalifikovaný a uznávaný elektronický podpis, razítko, pečeť.
Zákon č. 250/2017 Sb., o elektronické identifikaci	Kvalifikovaný systém (Národní Identitní Autorita – NIA), kvalifikovaný správce, prostředek pro elektronickou identifikaci (eObčanka…).

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti	Bezpečnostní požadavky na informační systémy (v důsledku i ISVS), kritická informační infrastruktura (KII), významný informační systém (VIS), národní a vládní CERT (Computer Emergency Response Team, obdoba integrovaného záchranného systému, ale pro informační systémy).
Zákon č. 127/2005 Sb., o elektronických komunikacích	Regulace zajišťování elektronických komunikací (např. sítě internet) a poskytování služeb těchto komunikací. Radiová pásma a kmitočty. Souvislosti s rozhlasovým a televizním vysíláním.
Zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů	Veřejné rejstříky (např. Obchodní rejstřík, Rejstřík společenství vlastníků jednotek) a procesní postup – zápis, práce s údaji. Evidence svěřenských fondů
Zákon č. 340/2015 Sb., o registru smluv	Speciální účinnost smluv podléhající zveřejnění. Informační systém registru smluv.
Zákon č. 134/2016 Sb., o zadávání veřejných zakázek	Druhy a podmínku pro soutěžení ve veřejné správě.
Zákon č. 480/2004 Sb. Zákon o některých službách informační společnosti	Služby informační společnosti, typicky obchodní sdělení.
Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací	Přístupnost pro znevýhodněné skupiny občanů (např. nevidomí). Připravenost stránek na zobrazení jak na monitoru počítače, tak v mobilním telefonu (responzivní design)
Národní architektonická plán vydaný Ministerstvem vnitra (na úrovni usnesení vlády)	Národní architektura veřejné správy, znalostní báze, více viz kapitola 9.

4.3 Standardy a doporučení

Vybrané mezinárodní standardy (ISO, Mezinárodní organizace pro normalizaci, zde přeneseně jako označení standardu vydané touto organizací; IEC, Mezinárodní elektronická komise, pro standard, zde přeneseně jako označení standardu vydané touto organizací):

- Řada ČSN **ISO/IEC 20000** Management ICT služeb („formalizovaný ITIL“).
- Řada ČSN **ISO/IEC 27000** Bezpečnostní techniky – Systémy řízení bezpečnosti informací.
- Řada **ISO 9000** – Kvalita, a **ISO 14 000** ochrana životního prostředí.

Vybrané standardy, doporučení / dobrá praxe:

- **ITIL** – Information Technology Infrastructure Library (česky: soubor praxí prověřených konceptů a postupů) management ICT služeb na základě dobré praxe.
- **TOGAF** – The Open Group Architecture Framework je v současné době nejrozšířenějším rámcem a standardem podnikové architektury, zaveden do českého digitálního governmentu v rámci IKČR a její příloh.
- **COBIT** – Control Objectives for Information and Related Technologies (česky: kontrolní cíle zájmu pro informační a příbuzné technologie) je soubor praktik, umožňující dosažení strategických cílů organizace díky efektivnímu využití zdrojů a minimalizaci ICT rizik.

Otázky k procvičení:

1. Dle jakého zákona se bude soutěžit nový informační systém?

Jednoznačně dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

2. Dohledejte zakotvení informačního systému, se kterým pracujete.

Např. spisová služba bude zakotvena přímo v zákoně, viz § 63 zákona č. 499/2004 Sb.

4.4 Doplňující část

Poskytování a zveřejňování informací a dat je zakotveno především zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ale některá dílčí data, informace a dokumenty jsou zveřejňovány podle specifických zákonů (např. výroční zpráva dle zákona č. 110/2019 Sb., o zpracování osobních údajů nebo ARES dle zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob).

4.4.1 Povinnosti v digitálním světě

Digitální prostředí (kybernetický prostor), které je dnes díky internetu prakticky celosvětové, přináší nejen řadu nových možnosti, které lze využívat nejen pozitivně.

Primární nutností a zároveň problémem dneška je nalezení rovnováhy mezi osobní svobodou danou zejména anonymitou uživatelů v celosvětovém digitálním prostoru a osobní, vymahatelnou odpovědností za nepřekročení platných pravidel – společenských / etických, i zákonných.

Např. autoři uměleckého obsahu chtějí mít zabezpečeno dodržování svých = autorských práv (přičemž za tento obsah nesou odpovědnost) obecně, tzn. stejně v reálném i v digitálním světě.

Ani svoboda daná anonymitou ale nesmí překračovat hranice dané právy na bezpečnost a ochranou soukromí ostatních uživatelů. V reálném i v digitálním světě musí platit shodná pravidla, i když forma jejich kontroly a vynucování je jiná. Podstata je stále táž: neomezovat práva a bezpečnost soukromí jiných osob, nešířit poplašné zprávy a dezinformace.

Zajištění dohledatelnosti autorství všech veřejně publikovaných a šířených zpráv, sdělení, prohlášení i multimediálního obsahu v digitálním / kybernetickém prostoru, je tak nutným předpokladem pro zabránění a postihování např. šíření poplašných zpráv (hoaxů), šíření nepravdivých zpráv nebo závadného obsahu, a zejména pak vydávání se za někoho jiného / konání pod cizí (falešnou) identitou.

Cílem současného zpřísňování dohledu nad chováním ve veřejném digitálním prostoru je dosažení bezpečnosti, což vyžaduje:

- ponechat v digitálním světě nadále anonymní pouze takové činnosti, které nemění existující ani nevytváří nový obsah, nebo nemění existující ani nevytváří nové služby,
- všechny ostatní činnosti podmínit individuální autentizací (jak osoby, tak SW aplikace, která by danou činnost měla provádět), která zajistí jak její přiřazení odpovídajícím přístupovým právům, tak v případě potřeby i její prokazatelnou dohledatelnost.

Samozřejmostí je, že úroveň autentizace (podrobněji viz Kap. 19.) musí být úměrná hodnotě a významnosti bezpečnosti předmětných informací a kontinuity předmětných ICT služeb.

Autentizace je ale pouze jedním z předpokladů. Druhým je správná autorizace – blíže viz kapitola 19.

4.4.2 Povinnosti VS plynoucí ze zákona č. 12/2020 Sb., o právu na digitální služby.

Zákon o právu na digitální služby posiluje rovnocennost digitálních a tradičních obslužných kanálů veřejné správy. Stanovuje, že služby zapsané jako digitální v registru práv a povinností (RPP) je

každý oprávněn čerpat digitálně a že prostředky identifikace osob a autentizace dokumentů musejí být přijímány a uznávány, pokud přišly důvěryhodným kanálem od autentikovaného uživatele službami vytvářejícími elektronickou důvěru nebo jsou podepsány kvalifikovaným podpisem osoby. To zahrnuje jak datovou schránkou přijatý dokument bez podpisu, tak elektronickou poštu s kvalifikovaně podepsaným dokumentem.

Dalším významným požadavkem je, že skutečnosti a úřední listiny není třeba dokládat úřadu, stačí pouze uvést odkaz na příslušný dokument, o skutečnost v agendě, nebo doklad o právním stavu, zapsaný v registru práv a povinností. V neposlední řadě zákon č. 12/2020 Sb., zákon o právu na digitální služby, dovoluje občanovi do registru zapsat své mobilní telefonní číslo a adresu elektronické pošty, na kterých si přeje dostávat notifikační SMS a e-mailové zprávy. Předpokládá se jejich využití agendami pro jednotné notifikace o změnách vztahů, vypršení dokladů, termínech povinností.

4.4.3 Druhy právních předpisů EU

Obecně je třeba rozlišovat:

- Nařízení Evropského parlamentu a Rady (EU) – je právně závazné a přímo použitelné. Platí v celém svém rozsahu v celé EU.
- Směrnice – právní akt stanovující cíl, který musejí všechny země EU splnit. Je však na jednotlivých zemích, jak formulují příslušné vnitrostátní zákony a jak těchto cílů dosáhnou. Pro jednotlivé státy se stává závazným až po své transpozici do národní legislativy daného státu.

Jedním z příkladů je směrnice EU o právech spotřebitelů, která posiluje práva spotřebitelů v celé EU, například tím, že eliminuje skryté poplatky a náklady při nakupování na internetu, a prodlužuje lhůtu, ve které mohou spotřebitelé odstoupit o kupní smlouvy.

- Rozhodnutí je závazné pro všechny, kterým je určeno (např. pro členský stát EU nebo určitou obchodní společnost), a je přímo použitelné.
- Komise například vydala rozhodnutí o účasti EU v různých protiteroristických organizacích. Rozhodnutí se vztahuje pouze na tyto organizace.
- Doporučení není závazné.

Když Komise vydala doporučení, aby soudní orgány zemí EU více využívaly videokonferencí, aby usnadnily přeshraniční spolupráci v soudních záležitostech, nemělo žádné právní důsledky. Prostřednictvím doporučení mohou orgány EU dát najevo svůj názor a navrhnout určité kroky, aniž by z nich vyvozovaly zákonnou povinnost pro toho, komu je určeno.

- Stanovisko. Pomocí „stanoviska“ se orgán EU může vyjádřit k určité otázce nezávazným způsobem, tzn., aniž by tak zakládal zákonnou povinnost pro toho, komu je stanovisko určeno. Stanovisko může vydat hlavní orgán EU (Komise, Rada a Evropský parlament), Výbor regionů a Evropský hospodářský a sociální výbor. Tyto dva výbory vydávají během legislativního procesu stanoviska k návrhům z pohledu regionů nebo hospodářství a sociální oblasti.

Výbor regionů například vydal stanovisko k balíčku Čisté ovzduší pro Evropu.

4.4.4 Nařízení Evropského parlamentu a Rady (EU)

GDPR (zkratka anglického názvu „General Data Protection Regulation“, česky: Obecné nařízení o ochraně osobních údajů) označuje zkráceně nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

Klíčové principy práce s osobními a citlivými údaji dle GDPR – práva vlastníka osobních údajů a povinnosti jejich zpracovatelů (pro zpracovatele povinné ze zákona, tj. OVM a bezpečnostní složky, jsou některé povinnosti omezeny):

- Zabezpečení zpracování – dle článku 32 má správce a zpracovatel s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, zajistit vhodná technická a organizační opatření k zajištění zabezpečení odpovídající danému riziku, včetně šifrování, pseudonymizace, integrity, důvěrnosti, testování a hodnocení.
- Právo na přístup – dle článku 15 má subjekt údajů právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.
- Právo na opravu – dle článku 16 má subjekt údajů právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají.
- Právo na výmaz – dle článku 17 má subjekt údajů právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat.
- Právo na přenositelnost – dle článku 20 má subjekt údajů právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.

Nařízení Evropského parlamentu a Rady EU č. 2014/910 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Hlavním důvodem pro přijetí nařízení eIDAS byla snaha unijních orgánů dobudovat jednotný vnitřní digitální trh, tedy snaha o odstranění existujících bariér, které brání přeshraničnímu využívání elektronických služeb. Bylo identifikováno několik příčin tohoto nežádoucího stavu, mezi které např. patří nedostatečná interoperabilita, nedostatek právní jistoty a v neposlední řadě i nárůst kybernetické kriminality.

4.4.5 Směrnice EU

Směrnice evropského parlamentu a rady o autorském právu na jednotném digitálním trhu 2016/0280 (COD), nazývaná také Směrnice EU o autorském právu, je směrnice Evropské unie, která má zajistit „dobře fungující trh pro využívání děl a jiných předmětů s přihlédnutím zejména k digitálnímu a přeshraničnímu využití chráněného obsahu. Rovněž rozšiřuje stávající právní předpisy Evropské unie o autorských právech a je součástí projektu jednotného digitálního trhu EU.

Směrnice dne 26. 3. 2019 úspěšně prošla schvalovacím procesem. Členské státy EU jsou povinny přijmout zákony implementující tuto směrnici. ČR má 2 roky na implementaci směrnice do českého právního řádu.

Směrnice vytváří podmínky k tomu, aby vydavatelé mohli chránit jimi vytvořený obsah na digitálním trhu a jednat s těmi, kdo jej dále komerčně využívají o podmínkách poskytnutí finančních kompenzací za toto používání. Tím se otevírá cesta k tomu, aby vydavatelé stejně jako další tvůrci obsahu získávali z komerčního využívání svého obsahu třetími stranami další finanční prostředky využitelné pro financování tvorby kvalitního obsahu. To má nesmírný význam pro další budoucnost nezávislého, kvalitního a profesně vytvářeného obsahu.

4.4.6 Důležité právní normy dotýkající se informatiky a eGovernmentu ČR

České právní předpisy:

Předpisy stanovující závazná pravidla chování v kybernetickém prostoru

- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), který upravuje zejména problematiku práv autora k jeho dílu vzhledem ke změnám, které neustále probíhají. Nově také obsahuje právní ochranu pořizovatele databáze k jím pořízené databázi, která dosud nebyla naším právem upravena. Autorský zákon odděluje osobnostní a majetková práva autorů. Na základě autorského práva, může např. kvůli patentu či pro zákazníka nevýhodně uzavřené smlouvy dojít k tzv. vendor lock-inu, tedy uzamčení zákazníka (blíže viz Kap. 8), což je situace, kdy je zákazník zcela závislý na produktech a službách konkrétního dodavatele a nemůže jej změnit.
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, který upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány. Mezi subjekty mající povinnost poskytnout informace patří státní orgány, orgány územní samosprávy, orgány veřejné správy a subjekty, jimž zákon svěřil rozhodování v oblasti veřejné správy. Tento zákon stanovuje, jaké informace jsou subjekty povinny poskytnout a jakým způsobem, jaká omezení se vztahují na poskytování informací (obchodní tajemství, ochrana osobnosti a utajovaných informací) a stanovuje průběh podávání a vyřizování žádostí o poskytnutí informace. Zákon č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon). Tento zákon upravuje systém knihoven poskytujících veřejné knihovnické a informační služby a podmínky jejich provozování. Nevztahuje se na knihovny provozované na základě živnostenského oprávnění. Mimo základní pojmy vymezuje systém knihoven v ČR, druhy knihoven a poskytování služeb uživatelům.
- Zákon č. 110/2019 Sb., o zpracování osobních údajů, navazuje na obecné nařízení EU o ochraně osobních údajů fyzických osob (GDPR). Upravuje tedy ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů, a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států.
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, uveřejněn ve Sbírce zákonů dne 19. září 2016. Jeho cílem je adaptace právního řádu České republiky na přijetí nařízení eIDAS pro oblast služeb vytvářejících důvěru. V zákoně je upraveno pouze to, co

nařízení výslovně nechává na úpravu vnitrostátním právním řádem. Zákon rovněž stanovuje Ministerstvo vnitra jako orgán dohledu nad poskytovateli služeb vytvářejících důvěru. V zákoně není upravena elektronická identifikace, která je řešena samostatně.

- Zákon č. 250/2017 Sb., o elektronické identifikaci, stanovuje pravidla prokazování totožnosti v elektronickém prostředí, toto prokázání zajišťuje Národní identitní autorita – blíže o ní viz Kap. 20.
- Zákon č. 328/1999 Sb., o občanských průkazech, upravuje využití e-občanky v elektronické komunikaci.
- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, upravuje problematiku veřejných zakázek. Stanovuje i pravidlo, že při každé veřejné zakázce je nutné dbát o to, aby stanovila takové podmínky, aby i budoucí zakázky mohly být v souladu se zákonem volně soutěženy.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, a usnesení vlády č. 86 ze dne 27. ledna 2020, stanovuje povinnost, že každý záměr povinných subjektů vynakládat prostředky týkajícího se tzv. určeného informačního systému musí být schválen OHA MV.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti stanovuje bezpečnostní opatření pro kritickou informační infrastrukturu a významné informační systémy.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, stanovuje povinné dokumentace k ISVS (bezpečnostní dokumentaci a informační koncepci), ustanovuje PVS, Centrální místo služeb (CMS) a Czech POINT.
- Zákon č. 111/2009 Sb., o základních registrech, stanovuje podmínky využívání sdíleného datového fondu.
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, stanovuje povinnosti v souvislosti s datovými schránkami a konverzí dokumentů.
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, stanovuje povinnosti v souvislosti s poskytováním informací a podmínky publikování otevřených dat.
- Zákon č. 110/2019 Sb., o zpracování osobních údajů, stanovuje podmínky ochrany soukromí a upravuje práva a povinnosti při zpracování osobních údajů.
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě, stanovuje povinnost vést elektronickou spisovou službu a podrobnosti archivace dokumentů.
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (Nařízení eIDAS) stanovuje podmínky a způsoby elektronické autentizace osob.
- Zákon č. 297/2016 Sb., o službách vytvářející důvěru pro elektronické transakce.
- Zákon č. 197/2009 Sb., o certifikaci veřejných dokladů s biometrickými údaji.
- Nařízení Rady (ES) č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních dokladech vydávaných členskými státy.

Obecné právní předpisy, jež se týkají ICT

- Zákon č. 89/2012 Sb., občanský zákoník - stanovuje základy majetkových práv a tak vytváří prostředí pro obchodní vztahy.
- Zákon č. 40/2009 Sb., trestní zákoník - ustanovuje základy trestního práva a základy trestných činů v kyberprostoru, především § 230 až 232.

4.4.7 Legislativní úprava práva na informace

Povinnými subjekty, které mají povinnost poskytovat informace vztahující se k jejich působnosti, jsou:

- státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce,
- subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.

Povinné subjekty jsou povinny zveřejnit:

- základní údaje (identifikace, adresy ad.),
- výroční zprávu za kalendářní rok o činnosti v oblasti poskytování informací,
- do 15 dnů informace poskytnuté na žádost (v některých případech jen vyjádřit obsah poskytnutých informací) na internetu,
- výhradní licence, sazebníky apod.

Povinný subjekt může proaktivně zveřejnit jakékoli informace, pokud jsou v souladu se zákonem o svobodném přístupu k informacím a zveřejnění nebrání žádný zvláštní právní předpis.

Způsoby poskytnutí informací jsou:

- Prostřednictvím Portálu občana - blíže viz Kap. 15, na základě osobní identifikace – viz kap. 7.
- Poskytnutí na základě žádosti
    - žádost může podat fyzická i právnická osoba (i jiné povinné osoby) a to ústně nebo písemně (vč. elektronických způsobů),
    - žádost musí obsahovat (jinak je žadatel vyzván do 7 dnů k doplnění):
    - jasné určení, komu je adresována,
    - že se jedná o žádost podle zák. č. 106/1999 Sb., o svobodném přístupu k informacím,
    - kdo ji podává (jméno, datum narození a adresa pro fyzické osoby (FO) nebo název, IČ a adresu pro právnické osoby (PO)),
    - elektronická žádost musí směřovat na podatelnu povinného subjektu,
    - do 7 dnů může být žadatel požádán o doplnění žádosti, pokud je nesrozumitelná, příliš obecná nebo nejasná,
    - odpověď na žádost se musí poskytnout do 15 dnů od jejího přijetí, ojediněle lze prodloužit o dalších 10 dní,
    - informace jsou poskytnuty ve formátu a jazyce, který byl uvedený v žádosti, pokud jej má povinný subjekt k dispozici (formát ani jazyk nemusí být měněny jen kvůli žádosti),
    - pokud by poskytnutí informací mělo představovat nepřiměřenou zátěž, může být poskytnutí zpoplatněno.
- Poskytování zveřejněním
    - povinně zveřejňované informace musí být v souladu s Vyhláškou č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup,
    - zveřejněním se poskytují i otevřená data – blíže viz kapitola 19,

- musí být v otevřeném formátu (nezávislý na konkrétním SW vybavení, tedy raději CSV než Excel),
- pokud je to možné být ve strojově čitelném formátu (tedy raději Word než naskenované PDF),
- měla by být připojena i příslušná metadata a otevřená licence,
- zveřejnění ve všech formátech a jazycích, ve kterých vznikla.

4.4.8 Omezení práva na informace

Poskytnout se nesmí informace:

- označené jako utajované,
- zasahující do osobnostních práv vymezených zákonem č. 110/2019 Sb., o zpracování osobních údajů, přičemž je třeba brát zřetel na judikaturu vymezující informace, kde veřejný zájem na jejich zveřejnění převyšuje zájem na ochranu osobnosti (např. platy některých zaměstnanců),
- chráněné obchodním tajemstvím,
- o majetkových poměrech třetích osob (např. získané dle zákona o daních),
- vzniklé bez použití veřejných prostředků osobou, jíž to zákon neukládá,
- podléhající ochraně práv třetích osob k předmětu práva autorského,
- která se týká stability finančního systému,
- na které se vztahuje mlčenlivost (např. know-how zjištěné během kontrolní činnosti),
- o probíhajícím trestním řízení, rozhodovací činnosti soudů s výjimkou rozsudků, plnění úkolů zpravodajských služeb atd.,
- o údajích vedených v evidenci incidentů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila nebo jejichž poskytnutí by ohrozilo účinnost reaktivního nebo ochranného opatření podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

OVM nemusí poskytnout informace:

- které již jsou zveřejněny, pokud byla žádost podána elektronicky, tehdy stačí odpovědět jen informací s odkazem na místo zveřejnění,
- určené výlučně k vnitřním pokynům a personálním předpisům,
- nové, které vznikly při přípravě odpovědi,
- poskytnuté NATO nebo EU, které není žádoucí zveřejnit.

4.4.9 Osvědčené postupy, mezinárodní doporučení pro oblast ICT

Dobrá praxe v řízení ICT vzniká každý den a státní správa by se ji měla snažit kopírovat a adaptovat do praxe a prostředí, ve kterém má vykonávat svoji činnost. Příklady dobré praxe řízení ICT jsou adaptovatelné a přenositelné do dalších oblastí mimo ICT, i ve státní správě. Nejúspěšněji společnosti v soukromém sektoru právě metody řízení, politiky a pomocné nástroje, které vznikly prvně pro ICT, aplikují i v jiných oblastech činnosti, například ve službách a výrobě. Dobrým zdrojem inspirace jsou začínající „Start Up“ společnosti z oblasti San Franciska („Silicon Valley“).

Takovýmito případy jsou například:

- Využívání cloudových služeb – existují moderní společnosti, které uplatňují zásadu „cloud only“, kdy **veškeré činnosti jsou vedeny v cloudu.** Dále je nutno zmiňovat, že tyto organizace jsou plně digitální, bez používání „papírů“, což je jedním z principů IKČR, konkrétně zásada P12 „Vnitřně pouze digitální (Inside only digital)“
- Znalostní báze – původně nástroj pro udržování znalostí o rozsáhlém kódu aplikován na udržování znalostí v celé organizaci, aby informace byly vždy dostupné a aktuální.
- Využívání nástrojů pro řízení práce „workflow“- nástroje, jež byly používány pro vývojové účely a úkoly, jdou použít pro zpřehlednění práce v organizaci.

4.4.10 Aktuální standardy

České a mezinárodní normy:

- Řada ČSN ISO/IEC 20000 Informační technologie - Management služeb – tato řada norem více formalizuje ITIL, ze které vychází.
- Řada ČSN ISO/IEC 27000 – Tato norma podchycuje Management bezpečnosti, jako jedna z mála ISO norem je certifikovatelná (dále ISO 9000 – Kvalita, ISO 14 000 ochrana životního prostředí).
- ČSN ISO/IEC 25000 (369006) Systémové a softwarové inženýrství - Požadavky a hodnocení kvality systémů a softwaru (SQuaRE) - Pokyn ke SQuaRE – Norma pro řízení kvality kódu a zdrojového kódu.
- ISO IEC - ISO/IEC 38500:2015 Information technology - Governance of IT for the organization - řízení organizace IT.

Mezinárodně uznávané metodiky zaměřené na ICT: Pro řízení služeb v ICT se využívají metodiky, jež jsou produkovány respektovanými organizacemi, v mnohých případech jsou tyto skupiny otevřené dalším členům. Tyto metodiky se používají pro tvorbu, správu ICT služeb a produktů. Jejich přínosy jsou:

- úspory finančních prostředků,
- úspory lidských zdrojů,
- určení odpovědností,
- společný jazyk s ICT světem,
- kvalitnější produkty a služby,
- zkrácení institucionálního učení.

ITIL – **Information Technology Infrastructure Library** (česky: soubor praxí prověřených konceptů a postupů) umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií (IT), a to jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků.

TOGAF – The Open Group Architecture Framework je v současné době nejrozšířenějším "standardem" určujícím, co by mělo být součástí popisu organizace a jak by se tento popis měl provádět. TOGAF tvoří standart architektury pro český eGovernment, a jeho zakotvení v ČR pro veřejnou správu upravuje Usnesení vlády č. 629 ze dne 3. 10. 2018 „Digitální Česko“.

COBIT – **Control Objectives for Information and Related Technologies** (česky: kontrolní cíle zájmu pro informační a příbuzné technologie) je soubor praktik, které by měly umožnit dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik.

4.4.11 Technické standardy ICT VS ČR

Lze zmínit usnesení vlády č. 982 ze dne 18. 12. 2013 stanoví pro státní správu povinnosti:

- vyžadovat podporu technologie DNSSEC při nákupu všech relevantních služeb,
- zpřístupnit prostřednictvím internetového protokolu verze 6 (**IPv6**) elektronické podatelny,
- zabezpečit všechny domény prostřednictvím technologie DNSSEC,
- zahrnout požadavek na podporu IPv6 do všech relevantních výběrových řízení, a to jak na dodávky služeb, tak zboží (hardware), i jako nedílnou součást požadavků na všechny nově podpořené projekty a jejich součásti financované ze strukturálních fondů v tomto i nadcházejícím finančním období.

4.4.12 Odkazy

- Portál EUR-Lex - Přístup k právu evropské unie

https://eur-lex.europa.eu/homepage.html?locale=cs

- Sbírka zákonů a Sbírka mezinárodních smluv

https://aplikace.mvcr.cz/sbirka-zakonu/

5 Ekonomická výhodnost ICT veřejné správy

Související právní předpisy: zejména zákon č. 134/2016 Sb., průřezově zákon č. 340/2015 Sb., zákon č. 181/2014 Sb., zákon č. 365/2000 Sb.

5.1 Princip 3E

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 ve smyslu zákona č. 12/2020 Sb., tak souběžně také cestou snižování provozních nákladů na tyto služby na straně občanů i veřejné správy.

Výhodnost a výkonnost veřejné správy **z pohledu občanů** je poměřována **poměrem** celkových **přínosů** k celkové hodnotě **veřejných prostředků** (tj. veřejných financí, věcí, majetkových práv a jiných majetkových hodnot) na ni vynakládaných nebo k digitalizaci VS využívaných.

Výhodnost ale vždy musí být posuzována též **v kontextu bezpečnosti**. Zejména úřady VS, které využívají osobní údaje občanů, mají velkou zodpovědnost. Kdy musí služby poskytovat občanům a komerčním subjektům **co nejdostupněji a co nejsnadněji**, ale zároveň zajistit **maximální ochranu soukromí**, tj. zajistit důvěrnost jí svěřených údajů.

Pro určení ekonomické výhodnosti se standardně ve veřejné správě, dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě užívá kritérium 3E:

- **Účelnost** (anglicky Effectiveness) – takové použití veřejných prostředků, které zajistí optimální míru dosažení cílů veřejné správy, tj. **dělat správné věci**.
- **Účinnost** (v zákoně užito slovo **Efektivnost**, anglicky Efficiency) – 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, tj. **dělat věci správně**.
- **Hospodárnost** (anglicky Economy) – takové využití veřejných prostředků, jež zajistí s jejich co nejnižším využitím dosažení stanovených cílů veřejné správy v odpovídající kvalitě, tj. **minimalizovat zdroje vůči chtěné kvalitě**.

Předpokladem je dodržení souladu s právním prostředím – **legalita**.

5.2 Ekonomická výhodnost pořizování a podpory ICT

Při zadávání veřejných zakázek je za účelem zajištění ekonomické výhodnosti pořizování a podpory ICT při digitalizaci VS formou dodávek ICT produktů a služeb od externích dodavatelů nezbytné dodržovat zejména základní zásady zadávání veřejných zakázek dle zákona č. 134/2016 Sb.:

- **Zásada transparentnosti a přiměřenosti**.
- **Zásada rovného zacházení a zákazu diskriminace**.

Tedy např. zadáváním veřejných zakázek na dodávku produktů a služeb využívajících technologie nebo specifické konfigurace oprávněně (což je nutné doložit) vázané na konkrétního

producenta a/nebo jeho obchodní partnery **odděleně** od zadávání veřejných zakázek na dodávku produktů a služeb nabízených na trhu výrazně širším okruhem potenciálních dodavatelů.

Za účelem zajišťování ekonomické výhodnosti pořizování a podpory ICT je přitom veřejná správa povinna zohlednit a promítnout do zadávací dokumentace veřejných zakázek také dostupnost svých interních lidských zdrojů a prioritu jejich dlouhodobě účelného, hospodárného a efektivního využití k zajišťování a rozvoji interních kompetencí a znalostí za účelem minimalizace závislosti na dodavateli příslušných ICT produktů a služeb.

Zejména v případě externích dodávek počítačového software a/nebo projektových podkladů je totiž veřejná správa povinna dodržovat také příslušná autorská práva, což je stanoveno zejména zákonem č. 121/2000 Sb., autorský zákon.

S výjimkou vlastního vývoje formou zaměstnaneckého díla je totiž většina software získávána platbou za licenci k užívání díla. Pokud kromě jeho původce nebo pověřeného zástupce nesmí předmětné dílo 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 je označován jako **závislost na konkrétním dodavateli a jím dodaném řešení** (tzv. vendor lock-in), která může vést k nehospodárnému vynakládání výdajů. Což se netýká jen software, nýbrž také dodávek komplexních celků hardware omezujících následnou volnost v jejich údržbě a rozšiřování, nákupů spotřebního materiálu a služeb nebo vynucování servisních či "udržovacích" poplatků bez možnosti používat zařízení po vypršení smluvních záruk. Konkrétní příklady negativních ekonomických důsledků protiprávního zadávání veřejných zakázek a zároveň dlouhodobé závislosti na konkrétním dodavateli jsou podrobněji popsány např. v relevantních kontrolních závěrech NKÚ.

5.3 Celkové náklady vlastnictví

Celkové náklady vlastnictví (anglicky Total Cost of Ownership – TCO) jsou ukazatelem celkové přímé i nepřímé finanční náročnosti. V českém digitálním governmentu se pro poměřování užívá normované **TCO5** – tedy celkové náklady vlastnictví pro pět let provozu ICT řešení (investiční náklady jsou započteny vždy). Příslušné orgány VS jsou povinny provést při přípravě vytváření nového ISVS nebo při významné inovaci již užívaného ISVS kalkulaci TCO, a to i z pohledu provozu na on-premises (vlastní infrastruktura), či cloudu (sdílená infrastruktura).

Otázky k procvičení:

1. Pro projekt nového ICT systému chcete soutěžit vývoj aplikace a tu umístit do datového centra úřadu, které ale bude muset rozšířit (potřeba nových serverů). Jak bude zakázka vypadat?

Bude se jednat minimálně o dvě zakázky, předmět první bude vývoj aplikace. Druhá bude nákup hardwaru do zmíněného datového centra. Aby zakázky byly smysluplné, tak zakázka na aplikaci bude muset splňovat technologické a provozní standardy datového centra. Naopak díky odhad složitosti aplikace lze určit potřebný výkon serverů a tedy objem prostředků druhé zakázky.

2. Systém bude provozován právě 5 let. Mátě dvě varianty systému s TCO5. Jaký variantu zvolíte?

Při stejné kvalitě, zvolíme tu s nižším TCO5. Provoz systému pouze na 5 let je však podezřelý...

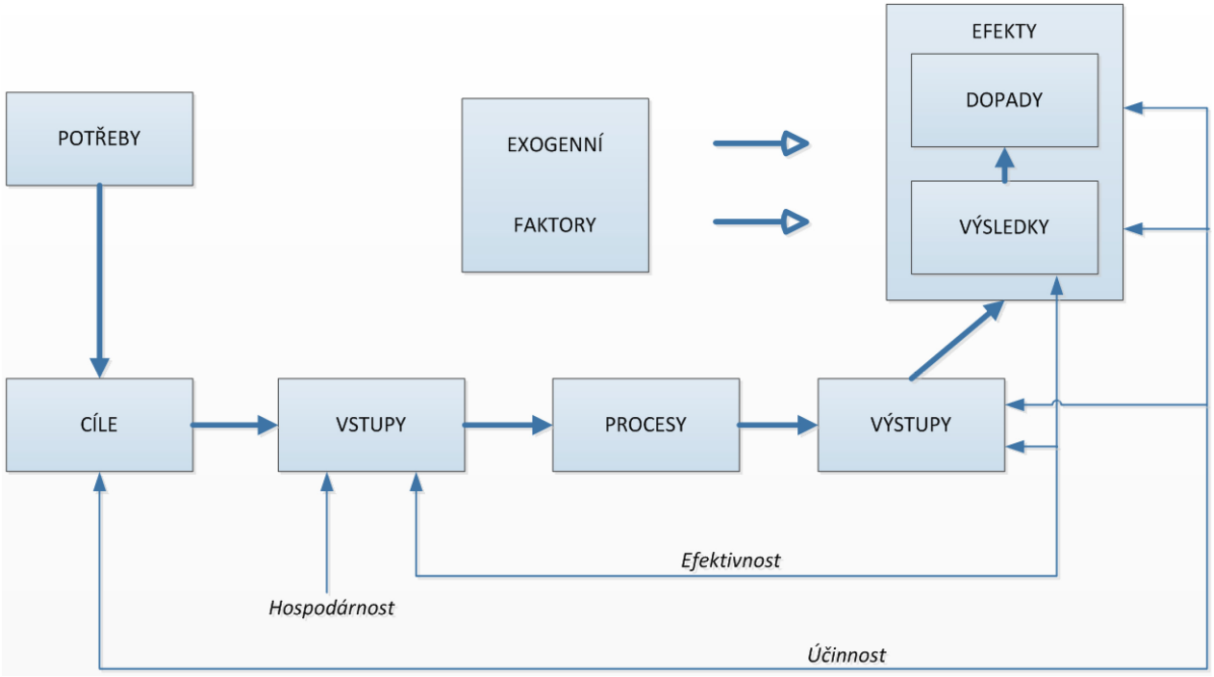
5.4 **Doplňující část**

5.4.1 Dílčí povinnosti ekonomické výhodnosti

Dílčí povinnosti, lze vyhledat dále v příslušných ustanoveních dalších zákonů ČR aj. právních předpisech zakotveny nejen např. v § 39 odst. 3 zákona č. 218/2000 Sb., o rozpočtových pravidlech, nebo také hned v několika odstavcích § 14 aj. zákona č. 219/2000 Sb., o majetku ČR, nýbrž dále také v čl. 4, odst. c) Přílohy usnesení vlády ČR č. 86/2020, o uložení povinností informovat vládu v souvislosti s výdaji v oblasti informačních a komunikačních technologií, kterou jsou stanoveny Základní zásady postupu při posuzování záměrů výdajů v oblasti informačních a komunikačních technologií.

Právě pro stanovování cílů jednotlivých projektů digitalizace VS ČR a objektivně ověřitelných ukazatelů jejich dosažení je přitom mimořádně důležité ustanovení § 4 odst. 2 zákona č. 320/2001 Sb., které zakládá povinnost individuálního stanovení konkrétních dílčích kritérií tak, že pokud nejsou takováto kritéria *„…stanovena právními předpisy, technickými nebo jinými normami, **musí být předem stanovena vedoucím orgánu veřejné správy, a to na základě objektivně zjištěných skutečností**.“*

Obrázek 1 – Logický model hodnocení ekonomické výhodnosti digitalizace VS podle principu 3E



Zdroj: (Evropský účetní dvůr, 2017)

5.4.2 Rizika nedodržení kritérií ekonomické výhodnosti digitalizace VS

Zvýšená rizika nedodržení kritérií ekonomické výhodnosti digitalizace VS jsou důsledkem neustálého velmi rychlého rozvoje digitálních technologií a tím i jejich extrémně rychlého morálního zastarávání a ekonomického znehodnocování coby praktického důsledku tzv. Moorova zákona, kdy se v jeho důsledku ICT zařízení stále zlepšují

Právě to činí potenciálně neúčelným a nehospodárným vynaložením veřejných prostředků s důsledkem porušení rozpočtové kázně např. pořízení jakýchkoliv informačních a komunikačních technologií, v jejichž případě lze předpokládat, že ani v horizontu nejbližších cca 18 měsíců nebude přiměřeně využit jejich výpočetní výkon, přenosová kapacita, kapacita datových uložišť, nepřiměřeně vysoká dostupnost a schopnost obnovy po havárii nebo nepřiměřeně nadstandardní úroveň jejich podpory.

Při naplňování kritérií ekonomické výhodnosti digitalizace VS je tedy nutné být v souladu s 3E také při stanovování přiměřených konkrétních úrovní zajištění kybernetické bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB) a jeho prováděcí vyhlášky č. 82/2018 Sb. (VoKB), které definují kybernetickou bezpečnost jako zajištění informací a dat z hlediska jejich:

- Důvěrnosti.
- Integrity.
- Dostupnosti.

Úrovně zajištění integrity a dostupnosti informací a dat a s nimi spjatá organizační a technická opatření proto musí být stanovovány na přiměřené úrovni s přiměřeně definovanými parametry jejich zajištění tak, aby náklady na jejich zajištění nepřevyšovaly identifikovaná rizika.

Např. minimální celková úroveň požadované dostupnosti primárních i podpůrných aktiv i dílčí úrovně dostupnosti jejich jednotlivých technických prvků ovlivňujících celkovou dostupnost, které jsou specifikovány např. parametry tzv. vysoké dostupnosti (anglicky High Availability – HA) a/nebo parametry schopnosti tzv. obnovy po havárii (nebo též zotavení po katastrofě, anglicky Disaster recovery, dále také DR), by tak měly být stanoveny účelně, a to na základě průkazných kalkulací přiměřených parametrů HA a/nebo DR.

5.4.3 Ekonomická výhodnost pořizování a podpory ICT při digitalizaci VS

Z hlediska ekonomické výhodnosti digitalizace VS nezbytné také při zadávání veřejných zakázek na dodávky ICT-produktů a služeb pro potřeby veřejné správy zajišťované externími dodavateli. Problematiku zadávání veřejných zakázek a povinnosti jejich zadavatelů přitom upravuje zejména zákon č. 134/2016 Sb., o zadávání veřejných zakázek. Ten napomáhá veřejné správě ČR *držet ÚHEL* prostřednictvím ochrany hospodářské soutěže, na kterou dohlíží Úřad pro ochranu hospodářské soutěže, který je ústředním orgánem státní správy ČR s velmi rozsáhlými pravomocemi v oblasti ochrany hospodářské soutěže, dohledu nad zadáváním veřejných zakázek, monitoringu a koordinace veřejné podpory.

Typické příklady nevýhodných ujednání ve smlouvách a doporučení, jak taková ujednání v licenčních smlouvách co nejvíce omezit a co možná nejlépe je nahradit ujednáními, která dávají uživateli nejširší možnou kontrolu nad ICT produktem, publikuje Odbor Hlavního architekta eGovernmentu MV ČR formou dokumentu nazvaného *Nevýhodná ujednání ve smlouvách na dodávku ICT produktů.*

5.4.4 Odkazy

- Celkové náklady vlastnictví na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/znalostni_baze:tco

- Metodika určení TCO pro pořízení a provoz ICT služeb v rámci Government Cloudu:

https://www.mvcr.cz/soubor/priloha-c-3-metodika-kalkulace-tco.aspx

6 eGovernment – principy, směry rozvoje, klíčové dokumenty

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména nařízení EU č. 910/2014, zákon č. 365/2000 Sb., zákon č. 111/2009 Sb., zákon č. 12/2020 Sb.

6.1 Principy eGovernmentu

V České republice veřejná správa může konat pouze to, co jí umožňují legislativní předpisy (např. zákony, dále viz kapitola 4) tzv. **zásada enumerativnosti veřejnoprávních pretenzí**. To samé logicky platí i pro český eGovernment.

eGovernment (elektronické vládnutí, v současnosti více užívaným pojmem **digitální government**, tedy digitální vládnutí) je výkon veřejné správy – jak státní správy, tak samosprávy, s vhodným využitím digitálních prostředků (informační systémy, chytré telefony, internet věcí aj.) tak, aby poskytované služby byly smysluplné a kvalitní – viz princip 3E kapitola 5.

Český eGovernment obsahuje celkem **dvacet principů** (pro principy se užívá také označení architektonické principy dle přístupu podnikové architektury (viz kapitola 9). Prvních sedm klíčových principů (tabulka 5), které jsou zároveň v souladu s přístupu evropské unie. Principy jsou obsaženy v Informační koncepci České republiky, viz kapitola 3. Architektonické principy jsou kontrolovány během schvalování ICT projektů veřejné správy odborem Hlavního architekta eGovernmentu (OHA), kdy je po odůvodnění potenciálně možné získat časově omezenou **výjimku**.

Tabulka 5 – Klíčové principy eGovernmentu

ID	Název principu	Popis principu
P1	Standardně digitalizované (Digital by default)	Orgány veřejné správy mají poskytovat služby primárně digitálně a samoobslužně, zároveň musí udržovat otevřené i další kanály pro ty, kteří nemohou buď z vlastního rozhodnutí, lidských nebo technických důvodů využívat digitální služby. Kromě toho veřejné služby mají být poskytovány i asistovaně, prostřednictvím jednotného kontaktního místa a prostřednictvím různých obslužných kanálů. Klient veřejné správy musí však mít právo zvolit si pro komunikaci s veřejnou správou i tradiční obslužné přepážky jednotlivých orgánů veřejné moci (OVM), tzv. (opt – out princip).
P2	Pouze jednou (Once only)	Orgány veřejné správy (OVS) musí zaručit, že občané a podniky poskytují stejné informace celé veřejné správě pouze jednou. OVS využívají při výkonu působnosti tyto sdílené údaje opakovaně, přičemž musí dodržovat pravidla ochrany údajů.
P3	Podpora začlenění a přístupnost (Inclusiveness and Accessibility)	Orgány veřejné správy musí digitální veřejné služby koncipovat tak, aby standardně podporovaly začlenění a vyhovovaly z pohledu funkcí, UX/UI designu a způsobem ovládání specifickým potřebám nejrůznějších skupin klientů z pohledu jejich věku, schopností nebo lidem s různými formami zdravotního postižení.
P4	Otevřenost a transparentnost (Openness and Transparency)	Orgány veřejné správy mezi sebou mají sdílet informace a data a musí občanům a podnikům umožnit přístup ke kontrole vlastních údajů a možné opravě. Musí uživatelům umožnit sledování správních procesů, které se jich týkají a musí do koncipování a poskytování služeb zapojit zúčastněné strany jak z komerční, akademické i občanské sféry a spolupracovat s nimi.
P5	Přeshraniční přístup jako standard (Cross border interoperability)	Orgány veřejné správy mají relevantní digitální služby zpřístupnit napříč hranicemi a mají zabránit dalšímu růstu jejich fragmentace, a tím usnadnit mobilitu na jednotném trhu.

P6	Interoperabilita jako standard (Interoperability by design)	Veřejné služby mají být koncipovány tak, aby hladce fungovaly v rámci celého jednotného trhu a napříč různými organizačními jednotkami, a opíraly se o volný pohyb údajů a digitálních služeb v Evropské unii. Současně je nezbytné zajistit interoperabilitu veřejných služeb uvnitř veřejné správy ČR jako předpoklad odstranění místní příslušnosti a snížení omezujícího vlivu věcné příslušnosti služeb VS na jejich klienty.
P7	Důvěryhodnost a bezpečnost (Security & Privacy by design)	Všechny iniciativy mají přesahovat pouhé dodržování právního rámce pro ochranu osobních údajů, soukromí a bezpečnost informačních technologií a mají tyto prvky zahrnout již do fáze přípravy architektury výkonu služeb veřejné správy. Sloučení principů záměrné a standardní ochrany osobních údajů (Privacy by design a Privacy by default) a záměrné a standardní řízení bezpečnosti (Security by design). Omezení zpracování osobních údajů jeho účelem a minimalizace zpracovávaných osobních údajů je zásadní, stejně jako proaktivní a kontinuální řízení bezpečnosti na všech architektonických vrstvách.

6.2 Směry rozvoje

Jednotlivé směry lze situovat dle hlavních cílů Informační koncepce České republiky, tedy pro:

- **Uživatelsky přívětivé a efektivní on-line služby pro občany a firmy** – např. národní katalog (digitálních) služeb. Bezpečná komunikační infrastruktura pomocí systému Centrálního místa služeb (viz kapitola 17). Jednotné UX/UI – vizuální přívětivost, jednoduchost a služeb
- **Digitálně přívětivá legislativa** – např. metodika pro veřejné zakázky v oblasti ICT, tak tvorba návrhů nové legislativy eGovernmenty, tak dokončení projektu eSbírky a eLegislativy.
- **Rozvoj prostředí podporujícího digitální technologie v oblasti eGovernmentu** – čerpání mimorozpočtových zdrojů, podpora a rozvoj základních registrů, další digitalizace služeb apod.
- **Zvýšení kapacit a kompetencí zaměstnanců ve veřejné správě** – systemizace expertních profesí, spolupráce s vysokými školami a jejich absolventů, využití kompetenčních center aj.
- **Efektivní a centrálně koordinované ICT veřejné správy** – např. řízení pomocí architektury veřejné správy, koordinace státního ICT, vytvoření eGovernment cloudu.
- **Efektivní a pružný digitální úřad** – zejm. vnitřní digitalizace úřadu, modernizace provozních informačních systémů, ICT podpora práce úředníků, či nové metody řízení úřadu.

6.3 Klíčové dokumenty

Mezi klíčové dokumenty patří materiály programu Digitální Česko, zejm. **IKČR**, její navazující dokumenty, dále jednotlivé informační koncepce úřadů, ale i dokumenty týkající se hodnocení, například **Benchmark veřejné správy** či tzv. **DESI** (Digital Economy and Society Index) států EU.

Otázky k procvičení:

1. Vaše organizace chce po vzoru rybářských lístků vydávat lístky na chytání paryb, zákon legalizující tento proces věcně již máte schválen. Samotné lístky plánujete vydávat osobně a pouze na hlavní pobočce úřadu. Je takovýto postup v pořádku?

Hlavní nelogičnosti, krom tedy samotné myšlenky chytání paryb budou zejm.: V rámci prvního principu neumožňujete čerpání služby digitálně – v případě kdy si do zákona organizace vynutí pouze jeden kanál je pak v rozporu s myšlenkou zákona č. 12/2020 Sb.

2. Vyhledejte, jestli vaše systémy/projekty splňují principy, či mají získanou výjimku od OHA.

Např. systém ISPOP – Ministerstvo životního prostředí, má výjimky kvůli technologickému dluhu.

6.4 Doplňující část

6.4.1 Další strategické dokumenty.

Strategické cíle informatizace VS ČR (viz výše), vycházející z platných strategických cílů veřejné správy ČR a představují východiska dále uvedených pravidel pro řízení rozvoje informatizace VS ČR, jsou, viz tabulka níže.

Tabulka 6 – Strategické cíle informatizace

Oblast	Cíl
Služba	vnímavě, přístupně a mobilně sloužit vnitřním i vnějším klientům úřadů veřejné správy.
Inovace	vést a inspirovat své úřady ke spolupráci a zlepšování služeb VS díky využití rozvíjejících se ICT technologií.
Bezpečnost	zajistit bezpečnost a spolehlivost informačních technologií i uchovávaných údajů.
Optimalizace	přidávat hodnotu pro klienty, resp. zvyšovat efektivitu pro úřady.
Pružnost	flexibilně a kompetentně reagovat na měnící se potřeby úřadů, díky architektuře a schopnostem.

Strategie rozvoje ICT služeb veřejné správy a její opatření na zefektivnění ICT služeb Materiál MV se zaměřuje na realizaci strategického cíle „Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu."

Největší význam dokumentu spočívá v jasném zakotvení kompetencí útvaru Hlavního architekta eGovernmentu a stanovení postupu při čerpání finančních prostředků na IT útvary veřejné správy.

Strategie rozvoje infrastruktury pro prostorové informace v České republice do roku 2020 Materiál MV rozpracovává základní principy rozvoje veřejné správy a eGovernmentu v oblasti prostorových informací a navrhuje zajištění kvalitních garantovaných prostorových informací a služeb nad prostorovými daty nejen pro efektivní výkon veřejné správy, ale i pro potřeby celé společnosti.

Strategický rámec rozvoje veřejné správy ČR 2014-2020 Materiál MV zřizuje odborný poradní orgán vlády pro oblast veřejné správy „Rada vlády pro veřejnou správu." Pro rozvoj eGovernmentu je důležitý strategický cíl 3 „Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu." Zejména je plánováno dobudování eGovernmentu ve 4 vrstvách, zajištění architektonické konzistence ICT projektů veřejné správy, Otevřená data a další.

Informační koncepce orgánu veřejné správy – Informační koncepce ČR je dokumentem závazným pro všechny úřady VS. Ty musely do dvou let od jejího vydání, tzn. do 03. 10. 2020 uvést do souladu s ní své informační koncepce, jejichž zpracování jim ukládá zákon č. 365/2000 Sb., o informačních systémech VS a jeho prováděcí vyhlášky, zejména vyhláška č. 529/2006 Sb., která stanovuje podrobnosti IK jednotlivých OVS ve třech oblastech:

- Informační koncepce jako dokument pro dlouhodobé řízení informačních systémů.
- Provozní dokumentace jednotlivých informačních systémů veřejné správy.
- Řízení a požadavky na kvalitu a bezpečnost ISVS.

Informační koncepce OVS je koncepčním dokumentem OVM pro dlouhodobé řízení ISVS a ICT v oblasti řízení kvality a bezpečnosti spravovaných informačních systémů a obecných principů jejich pořizování, vytváření a provozování. Vyhláška stanoví obsah, strukturu a postupy OVS při vytváření, vydávání a vyhodnocování dodržování IK a požadavky na řízení bezpečnosti a kvality ISVS.

Informační koncepce OVS obsahuje především:

- Charakteristiku každého ISVS, stručnou charakteristiku jeho současného stavu a předpokládané změny v tomto systému.
- Záměry na pořízení nebo vytvoření nových ISVS.
- Dlouhodobé cíle v oblasti řízení kvality ISVS, požadavky na kvalitu a plán řízení kvality.
- Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS, požadavky na bezpečnost a plán řízení bezpečnosti.
- Soubor základních pravidel pro:
    - pořizování a vytváření ISVS,
    - provozování ISVS včetně jejich změn a rozvoje.

Informační koncepci jsou správci povinni nejen tvořit, ale i atestovat. Atest mohou vydávat jen subjekty akreditované Ministerstvem vnitra. Platnost **atestu** smí být nejvýše 5 let, nicméně informační koncepce musí být minimálně **jednou za 24 měsíců vyhodnocována**.

6.4.2 Další směry rozvoje

Mobilita a práce odkudkoliv (Work anywhere) – Spolu se zřizováním přípojek a propojováním systémů státní správy a samosprávy prostřednictvím a se sítí internet, případně KIVS, dovolují stále dostupnější mobilní zařízení umenšovat závislost na kanceláři jako pevném místě výkonu činností. To dovoluje poskytovat služby VS mimo prostory úřadu (CzechPOINT, Datové schránky), manažerům řídit činnosti a správcům kontrolovat, nastavovat a opravovat systémy vzdáleně. I přes nesporné výhody zatím nelze zcela zrušit tradiční kontaktní místa styku s klienty, zejména tam, kde je to procesně nezbytné, například u Policie ČR.

Velmi důležitá je též připravenost informačního systému na podporu vzdálené práce. Dříve byla dosahována pomocí vzdálené pracovní plochy (Remote Desktop), dnes je součástí moderních IS s uživatelským rozhraním ve webovém klientu (prohlížeči) nebo tenké mobilní aplikaci (Android, IOS).

Při využívání vyhrazených mobilních internetových zařízení (MID) pro práci mimo kancelář hraje důležitou roli ochrana dat uložených v mobilním zařízení při jeho používání (obvykle šifrováním) a potenciální ztrátě (vzdáleným vymazáním) spolu s bezpečnou komunikací (šifrovaný přenos – HTTPS, VPN). Samozřejmým požadavkem je silná autentizace uživatele, nejlépe s využitím více faktorů

Práce z domova (Work From Home / HomeOffice) – Tyto termíny popisují plnohodnotnou práci z domova nebo místa pobytu. Jsou umožněny stejným rozvojem komunikačních a pracovních technologií jako předchozí trend práce odkudkoliv a rozšiřují jej z příležitostného na pravidelný režim.

Od března roku 2020 došlo i u nás k posunu ve vnímání tohoto přístupu zaměstnavateli z kategorie „benefitu“ mezi běžné metody organizace práce. Je vhodná zejména pro výkon znalostních profesí s hodnocením úkolů, které lze zadávat i kontrolovat dálkově. Vhodně může doplnit snižování počtu přímých kontaktních míst a přinést úsporu času zaměstnanců při dojíždění a nákladů zaměstnavatelů na velikost a provoz kanceláří. Náklady však zcela nezaniknou – některé náklady na vybavení a provoz jsou skrytě přenesené na zaměstnance a objevují se požadavky na zvážení jejich kompenzace.

Díky vynucenému rychlému přechodu je práce z domova často prováděna prostřednictvím vlastních zařízení zaměstnanců. Ta nejsou spravována ICT oddělením a bezpečnostními parametry často nevyhovují. Kvůli tomu je nezbytné zavádět další ochranná opatření, která při zcela nepřipraveném informačním systému nebo extrémně vysokých nárocích na ochranu dat vytvoří efektivní překážku v práci. Tu lze překonat poskytnutím pracovního nástroje, počítače, pod plnou správou zaměstnavatele. Další možností je rozvinutí mobilního zabezpečeného pracoviště s přiměřenou infrastrukturou.

Chytrá města (Smart Cities) – Pod pojmem chytré město je myšleno využívání ICT technologií k efektivnějšímu řízení a plánování rozvoje komunitních (městských i obecních) aktiv a zdrojů, ale i podpory rozhodování. Jedná se o sběr, přenos a vyhodnocování dat z různých zdrojů, zejména

- různých typů senzorů (snímačů), např. četnosti průjezdu vozidel na ulici, v křižovatce nebo vjezdu na parkoviště, sledování naplněnosti veřejného odpadkového koše, sledování slunečního svitu, srážkové činnosti, vlhkosti půdy, kvality ovzduší, množství osob na veřejných místech, čekajících na zastávkách hromadné dopravy
- netradičních zdrojů, např. satelitních a leteckých snímků veřejné zeleně
- propojeného datového fondu, např. geografická data
- data z jiných „chytrých systémů,“ například kooperace vozidel (C-Roads, C-ITS)
- jiné údaje od občanů a osob.

Zpracovaná data mohou sloužit pro optimalizaci svozu odpadu, správu dopravních a přepravních systémů, elektráren, vodovodů, odpadového hospodářství, vymáhání práva, městských informačních systémů, škol, knihoven, nemocnic a dalších komunit. Je to jedna z „nejmladších“ oblastí, kde uplatnění ICT slibuje spolu s úsporami přinést dosud nepředstavitelné změny kvality služeb veřejné správy.

Provozování IS s využitím cloudových technologií – Jedním z velmi obtížných úkolů při definování a nákupu technologické vrstvy IS je volba výpočetního výkonu, objemu paměti a úložišť a rychlosti sítě – **sizing**. Ten musí být přiměřený očekávaným požadavkům a nákladům na pořízení a provoz. Zpočátku tak bývá IS předimenzovaný a později nedostatečný. Vedle pořízení ICT do majetku (kapitálové náklady, CAPEX) existuje i možnost pronájmu ICT zdrojů, které jsou nákladem provozním (OPEX). Těmito úvahami je přímo ovlivňována ekonomická výhodnost ICT, popsaná v kapitole **Chyba! Nenalezen zdroj odkazů.**. Tím je založen požadavek na snižování množství t echniky pro poskytování rostoucího počtu služeb, **konsolidaci hardware** a umožnění růstu kapacit podle potřeb.

Ke konsolidaci docházelo historicky v místě používání systému (on-premise). Významné inovace posledních dvou dekád, zejména virtualizace počítačů), cloudové služby) a přechod na užívání služeb v síti), umožnily vznik celého odvětví cloudových služeb, zaměřené na provozování informačních systémů na vzdálených počítačích bez konkrétní fyzické formy, přístup k těmto systémům přes síť, automatizovanou správu, monitoring a řízení provozu pomocí rozsáhlé samoobsluhy. Prostřednictvím aplikačních rozhraní (API) cloudové služby může informační systém ovládat přizpůsobení svých jednotlivých součástí aktuální zátěži.

Poskytovatelé dnes nabízejí různé modely plateb za cloud computing. Od stálé (paušální) platby za poskytnutou kapacitu zdrojů až po model zaplať, co spotřebuješ. Vhodným kombinováním takových nabídek s vlastním technickým vybavením vznikne tzv. hybridní cloud, který, je-li navíc podpořen vhodnou architekturou řešení informačního systému, dovolí současně dosáhnout úspor nákladů a je připravený na vykrytí špiček zájmu o služby, např. při podávání žádostí o dotace či daňových přiznání.

Cloudy poskytují služby na třech definovatelných úrovních. Od holé infrastruktury, virtuálního počítače připojeného do sítě (IaaS), přes platformní služby od operačního systému po generické servery pro databáze, elektronické pošty nebo webové platformy (PaaS) až po kompletní standardizované aplikace pro zpracování dokumentů a dat s vestavěnou správou uživatelů, sdílenými kalendáři, poštou a kolaborací (SaaS). Nabízené služby mohou dále obsahovat i pronájem licencí k příslušnému softwaru a usnadňují tak správné licencování.
Autoři specializovaného software mohou nabízet vlastní aplikace s využitím cloudových služeb jiných poskytovatelů, například spisovou službu, jako komplexní využití principu SaaS (AaaS)

Za cloudové služby nejsou považovány služby datacenter typu Housing a Hosting, které mohou být chápány jako nižší součásti IaaS, ale nejsou škálovatelné. Virtuální hosting webových prezentací zpravidla nesplňuje podmínku izolace, a též nemůže být považován za cloud computing. Lze jej vhodně zapojit jako komponentu IS pro statický, neindividuální a neklasifikovaný obsah.

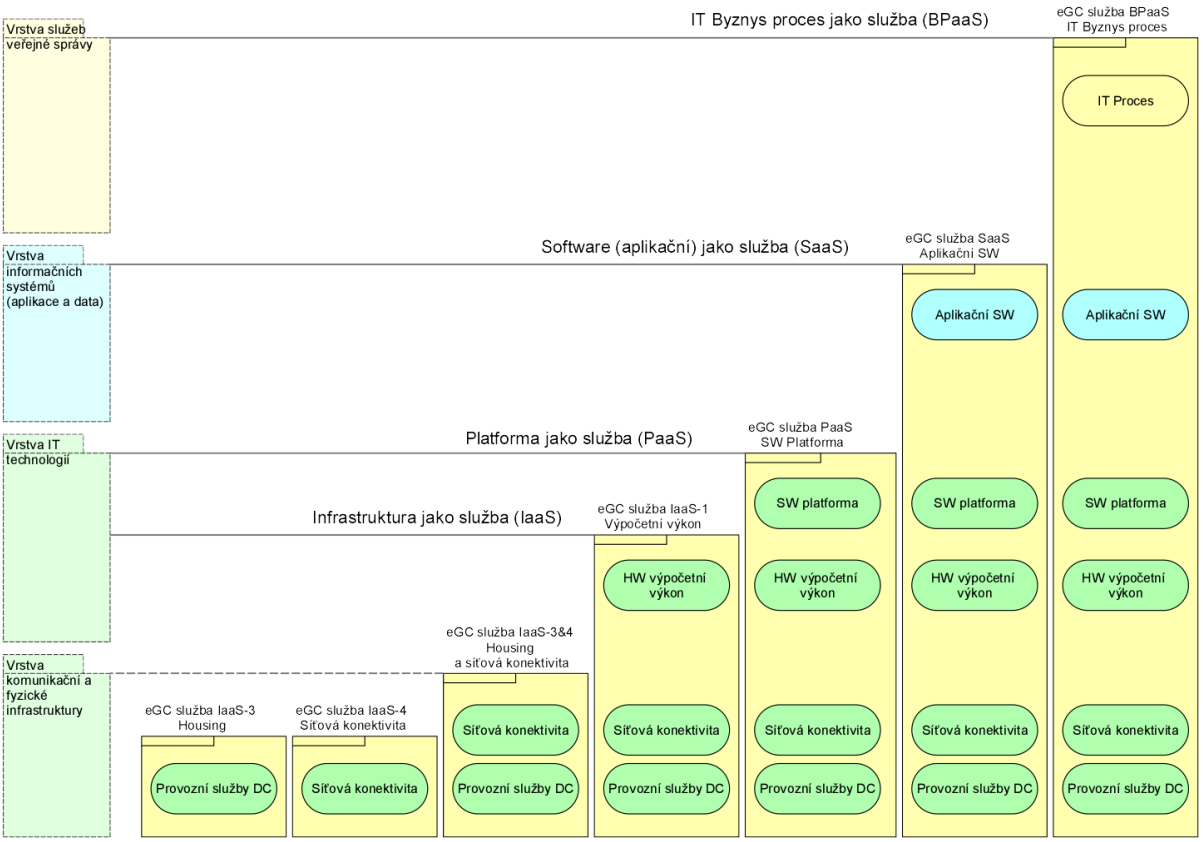
eGovernment Cloud – Ministerstvo vnitra na základě usnesení vlády č. 749/2018 Sb., o souhrnné analytické zprávě, výstupu Fáze I. projektu Příprava vybudování eGovernment cloudu (dále jen „eGC“), má v gesci též činnost Řídícího orgánu eGC (dále jen „ŘOeGC“). Projekt eGC je koordinován se strategií „Digitální Česko“, zejména s pilířem „Informační koncepce České republiky.“ Projekt přímo naplňuje dílčí cíl 5.5 „Vytvoření eGovernment cloudu“ IK ČR a podporuje řadu dalších dílčích cílů.

Základním cílem projektu eGC je prosazení přístupu 3E při současném zvýšení kvality a bezpečnosti při pořizování a provozu ISVS využíváním sdílených cloudových služeb eGC. Dalším cílem projektu je v maximální míře usnadnit jednotlivým správcům ISVS architektonické, bezpečnostní, nákupní a projektové procesy využíváním služeb eGC. Z celkového a dlouhodobého pohledu je souvisejícím cílem eGC také konsolidace datových center a ICT platforem veřejné správy.

Cloudové služby eGC zahrnují všechny tři hlavní kategorie cloudových služeb, **IaaS**, **PaaS** a **SaaS** a jsou rozděleny do dvou částí:

- **komerční eGC** (KeGC – služby provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury),
- **státní eGC** (SeGC – služby provozované v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem).

Obrázek 2 – Schematické znázornění vrstev služeb eGC v architektonickém členění.



Rozhodujícím **kritériem pro využití služeb eGC je kalkulace** a porovnání nákladů vlastnictví (**TCO**) jednotlivých ISVS v modelu provozu on-premise (na vlastní infrastruktuře) a s využitím služeb eGC.

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

Rozhodovacím kritériem pro využití služeb státní nebo komerční části eGC je úroveň bezpečnostních dopadů daného ISVS. **SeGC zajistí maximální úroveň bezpečnosti** a je určen pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická). **KeGC umožňuje využití tržních mechanismů pro zajištění optimálních cen** a je určen pro provoz služeb eGC bezpečnostních úrovní 1-3 (Nízká, Střední, Vysoká).

6.4.3 Hodnocení úrovně rozvoje eGovernmentu

Benchmark veřejné správy – Provádění ICT benchmarku veřejné správy vychází z Metodiky programu Digitální Česko, který schválila Vláda ČR svým usnesením č. 629 ze dne 3. října 2018. Cílem benchmarku je zjištění aktuálního stavu řízení úřadu, stavu připravenosti úřadu na realizaci

změn a oblast řízení ICT, které vedou k implementaci „plného" eGovernmentu. Zaměření a struktura benchmarku je úzce provázána s principy a zásadami obsaženými v Informační koncepci ČR a poslouží tak také jako komplement při tvorbě informačních koncepcí jednotlivých orgánů veřejné správy. Součástí výstupů benchmarku je identifikace příkladů dobré praxe a zajištění jejich následného sdílení.

DESI, Index digitální ekonomiky a společnosti (Digital Economy and Society Index - „**DESI**" zavedla Evropská komise, aby mohla hodnotit pokrok při budování digitálních ekonomik a digitální společnosti v členských státech EU.

Jde o **soubor ukazatelů** sdružených do 6 oblastí: pokrytí území komunikační sítí (**konektivita**), dovednosti v používání internetu a elektronických médií (**lidský kapitál**), jak lidé využívají internet ve volném čase, pro zábavu, ke komerčním účelům a k vlastním aktivitám komunikace, on-line transakce (**používání internetu**), digitalizace podniků, elektronické obchodování (**integrace digitálních technologií**), existence a využívání elektronických služeb VS (**eGovernment**, digitální veřejné služby), ICT projekty (**výzkum a inovace**).

Data pro stanovení indexu DESI čerpá Komise z šetření v rámci Digitální Agendy pro Evropu: EUROSTAT, výkazy, měření úplnosti on-line postupů (On-line Service Completion), hodnocení otevřených dat (Open Data - European Data Portal).

eGovernment Benchmark – eGovernment Benchmark je srovnání vyspělosti veřejné správy. Zpracovává ho společnost Capgemini ve spolupráci s Evropskou komisí. Data čerpají z uživatelských dotazníků a metody „mystery shopping".

- Z pohledu uživatelů se zkoumají **čtyři životní události** (life event): PODNIKÁNÍ – pravidelné obchodní operace, odvod daní, lidské zdroje, STĚHOVÁNÍ – informace místních úřadů, např. ohledně školních, sportovních a zdravotních zařízení, VLASTNICTVÍ A ŘÍZENÍ AUTA, SPRAVEDLNOST – reklamační řízení, stížnosti.
- U jednotlivých situací životní události se **hodnotí**: **zaměření na uživatele** – rozsah služeb, které jsou poskytovány on-line a jak uživatelé vnímají jejich kvalitu v ukazatelích on-line dostupnost, využitelnost a rychlost využití, **transparentnost** – transparentnost vládních opatření, procesů doručovacích služeb a přístupnost k osobním datům uživatelů, **přeshraniční pohyb** – přeshraniční on-line dostupnost a využitelnost, **klíčoví činitelé** – technologie klíčových činitelů pro zlepšení on-line veřejné služby. Jedná se o e-registry, autentizační zdroje, e-dokumenty, e-podpis a e-identifikaci.

U všech oblastí se **zjišťuje**, zda se jedná o: **automatickou službu**, **službu on-line**, ale ne přes portál, **informace on-line**, ale ne přes portál, **službu on-line** a přes portál, **informace on-line** a přes portál, **službu offline**.

Zároveň se u všech sledovaných služeb **hodnotí transparentnost služby**, tedy **on-line dostupnost** následujících informací: **oznámení** o doručení, **sledování** průběhu vyřizování, **ukládání** žádosti, očekávaná **doba** vyřizování, **termín** vyřízení, **max. doba** vyřízení, **informace o průběhu** vyřizování.

Dalšími často používanými **indikátory**, nejen ve veřejné správě jsou: **Mobilní přívětivost** – hodnocení jednoduchosti nalezení a přístupu k hledaným informacím na libovolných přístrojích, zejména mobilních, schopnost poskytování služeb v mobilním přívětivém prostředí, **Penetrace**, **Spokojenost**, **Digitalizace**, **Harmonizace**.

6.4.4 Odkazy

- Portál strategických dokumentů České republiky

https://www.databaze-strategie.cz/

- Strategické a akční plány v oblasti kybernetické bezpečnosti

https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

7 Identifikace / autentizace uživatelů digitálních služeb

Související právní předpisy: nařízení EU č. 910/2014, zákon č. 250/2017 Sb., zákon č. 297/2016 Sb., zákon č. 111/2009 Sb., průřezově zákon č. 181/2014 Sb., zákon č. 365/2000 Sb.

7.1 Identifikace, autentizace a autorizace

Mezi základní pojmy pro přístup ke službám patří:

- **Identifikace** je proces určení identity subjektu/objektu, tedy klient (uživatel) služby. Identitu udává subjekt/objekt.
- **Autentizace** (také jako autentikace, nebo autentifikace) je proces ověření identity uživatele, pomocí informací, které jsou s identitou spojeny – viz faktory níže.
- **Autorizace** je proces navazující na autentizaci. Autorizace je potvrzení souhlasu, schválení, umožnění přístupu či provedení konkrétní operace daným subjektem.

Pro bezpečnou elektronickou identitu a její užití (autentizace) se využívají následující tři faktory:

- **Faktor znalosti** – něco, co uživatel ví/zná (optimálně pouze on) a je dohodnuto mezi autentizujícím a autentizovaným. Typicky se jedná o heslo k danému účtu (identitě).
- **Faktor vlastnictví** – kdy autentizující ověřuje autentizovaného na základě přístupu/vlastnictví k něčemu, co nejde lehce okopírovat a kdy toto vlastnictví se dá na dálku ověřit. Příkladem je přístupová čipová karta, USB token s certifikátem, chytrý telefon se speciální aplikací, či telefonní číslo, kam je zasláno časově omezené heslo pomocí SMS (krátké textové zprávy). Poslední zmiňovaný způsob, časově omezené heslo pomocí SMS, je však na ústupu, neboť útoky je možno vést vícero způsoby (různé vektory útoky) a jsou relativně lehce realizovatelné.
- **Faktor charakteristiky** – je unikátní vlastnosti uživatele, jejíž sdílení mezi dalšími uživateli (a tedy i zcizení) je nemožné, či velice nepravděpodobné. Běžně se jedná o obraz krevního řečištěm, otisk prstu, duhovka oka, hlas či podpis.

Kombinací více faktorů mluvíme o tzv. **vícefaktorové autentizaci**. Pohledem na řádky výše je zřejmé, že bezpečnost více faktorové autentizace je mnohem vyšší, než při užití např. samotného hesla – faktoru znalosti zejm. pokud heslo je jednoduché (malý počet znaků, žádné speciální znaky).

7.2 Přístup občanů k digitálním službám

Ekosystém jednotného přihlašování v ČR (a napřímo pomocí bran eIDAS i EU) sdružuje **Národní bod pro identifikaci a autentizaci**, téže známý jako Národní identitní autorita (**NIA**). NIA je ukotvena zákonem č. 250/2017 Sb., kdy poskytuje uživatelům služby elektronické identifikace na nejvyšší úrovni důvěry definované evropským nařízením eIDAS. Správcem systému NIA je Správa základních registrů (SZR).

Občané se k digitálním službám dostávají pomocí prostředků **elektronické identity**. NIA následně tento prostředek propojí s uživatelskou digitální identitou – ta je pouze jedna a je zachycena v registru obyvatel. Posléze NIA vydá poskytovateli služby, ke které se občan hlásí požadované údaje vyžádané (identifikační) údaje, za předpokladu souhlasu občana. Tyto souhlasy jsou transparentní, a občan může zpracovat jednotlivé souhlasy přes portál NIA v souladu s GDPR.

Prostředky elektronické identifikace lze rozdělit na **státní** a **komerční**. Mezi státní patří: Mobilní klíč eGovernmentu, eObčanka, NIA ID, IIG – mezinárodní brána uzlu eIDAS. Komerčními prostředky pak je: Bankovní identita (Air Bank, Česká spořitelna, ČSOB, FIO banka, Komerční banka, MONETA Money Bank, Raiffeisenbank), MojeID, I.CA identita s kartou Starcos. Každý prostředek má svoji **úroveň důvěry** dle eiDAS – **nízká** (v podstatě se nepoužívá), **značná/střední** (většina prostředků), **vysoká** (eObčanka, MojeID).

Dále je vhodné zmínit, že v současné době je možné se přihlásit i pomocí identifkátoru datové schránky a jejích přihlašovacích údajů. Nicméně do budoucna je plánováno, že datové schránku nebudou mít své proprietární heslo, ale bude užívat pouze přihlášení přes elektronický prostředek (což je dnes již umožněno).

Řádky výše popisovaly digitální přístup k digitálním službám veřejné správy. Samozřejmě je však možné k těmto službám přistupovat v jejich asistované podobě při fyzické návštěvě úřadu, či klientského místa veřejné správy (Czech POINT, viz kapitola 13). Pro prokázání identity se pak užívá zejm. osobních dokladů jako je občanský průkaz, či cestovní pas. Vůle a možnost konat (autentizace a autorizace) lze dovodit samotným dostavením a činěním těchto úkonů.

7.3 Přístup úředníků pro výkon agendy

Pro řízení přístupu úředníků k výkonu agendy slouží centrální systém **Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb** (**JIP/KAAS**, v rámci rozvoje systému, kdy dochází k funkčnímu oddělení JIP/KAAS od systému Czech POINT se užívají pro odlišení zkratky JIP/KAAS 2.0, JIP/KAAS NG nebo CAAIS). JIP/KAAS je ukotven zákonem č. 111/2009 Sb. Správcem systému je Ministerstvo vnitra.

JIP/KAAS je založen na definování uživatelských účtů a jejich rolí dle ohlášené agendy. V praxi se jedná o úzké propojení mezi JIP/KAAS, registrem práv a povinností (RPP) a předmětným agendovým informačním systémem do kterého se přihlašuje úředník. V JIP/KAAS prostřednictvím RPP je typicky definován pouze zevrubný přístup k systému. Detailní role jsou řešeny interní uživatelskou databází včetně skupin a rolí konkrétního systému (zejména založené na technologii LDAP – Lightweight Directory Access Protocol).

V rámci **federace NIA do JIP/KAAS** se může úředník k přihlášení užít své občanské digitální identity, užitím příslušného prostředku. Zaměstnavatel však tento přístup nemůže plošně vynutit.

Otázky k procvičení:

1. K mobilu se přihlašujete pomocí gesta (propojování symbolů na obrazovce) o jaký faktor autentizace se jedná? Má nějaké nevýhody?

Jednoznačně se jedná o faktor znalosti. Nevýhodou je, že lze snadněji odkoukat, než třeba heslo.

2. Může mít občan více digitálních identit v českém eGovernmentu? Co elektronické prostředky?

Občan má v českém eGovernmentu pouze jednu digitální identitu. Prostředků může mít samozřejmě vícero.

7.4 Doplňující část

7.4.1 Ověřené výpisy ISVS

Samotné vydávání ověřených výstupů z informačních systémů veřejné správy se řídí § 9 a násl. zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Správce informačního systému veřejné správy je povinen předat výstup z informačního systému, opatřený datem a časem s uvedením hodiny, minuty a sekundy:

- kdy byl výstup vytvořen,
- okamžiku, ke kterému správce odpovídá za soulad výstupu se stavem zápisu v informačním systému, tzv. "okamžik platnosti údajů".

Správce výstup předává zabezpečený způsobem zajišťujícím integritu a původ dat. Zároveň, pokud je výstup předáván z neveřejné evidence, rejstříku nebo registru, pak je správce povinen předat výstup tak, aby tento výstup byl odpovídajícím způsobem skryt před třetími osobami.

Ověřeným výstupem se rozumí listina, která vznikla úplným převodem výstupu z informačního systému z elektronické do listinné podoby. Ověřený výstup obsahuje ověřovací doložkou, která obsahuje:

- údaj o ověření toho, že ověřený výstup odpovídá výstupu z informačního systému veřejné správy,
- údaj o tom, z kolika listů se skládá ověřený výstup,
- údaj o tom, že ověřený výstup obsahuje částečný výpis z informačního systému veřejné správy, pokud neobsahuje výstup úplný,
- místo a datum vyhotovení doložky o ověření,
- pořadové číslo, pod kterým je ověření vedeno v evidenci ověření výstupu z informačního systému veřejné správy,
- otisk úředního razítka a podpis ověřujícího.

Ověřující před vydáním ověřené výstupu je povinen provést veškeré úkony potřebné k tomu, aby ověřil tu skutečnost, že výstup z informačního systému je zabezpečen způsobem zajišťujícím integritu, případně původ dat. Ověřující je povinen vést evidenci vydaných ověřených výstupů. Výpis v listinné podobě, výstup z informačního systému veřejné správy a ověřený výstup jsou veřejnými listinami.

7.4.2 Odkazy

- Portál Identity občana:

https://info.identitaobcana.cz/ups/

- Portál Jednotného identitního prostoru / Katalogu autentizačních a autorizačních služeb:

https://www.czechpoint.cz/public/vyvojari/jip-kaas/

8 Řízení eGovernmentu – úrovně řízení a kompetenční útvary

Související právní předpisy: zejména zákon č. 365/2000 Sb., Národní architektonický plán vydaný Ministerstvem vnitra.

8.1 Úrovně řízení a zodpovědností

Podle významu a také podle základních zodpovědností a funkcí, které jednotlivé subjekty v dané úrovni zodpovědnosti vykonávají, rozlišujeme dvě hierarchie (pyramidy) zodpovědností:

- **hierarchie z hlediska řízení služby a informačního systému**, která se týká konkrétní služby veřejné správy a s ní souvisejících informačních systémů,
- **hierarchie z hlediska řízení a ekonomiky ICT** týkající se samotného řízení informatiky v kontextu s vnitřním řízením veřejné správy v rámci úřadu.

Protože obě hierarchie musí respektovat rozdílnosti kompetencí způsobů financování OVS a OVM, lze jejich úrovně popsat jen rámcově, z pohledu přímého ovlivňování kvality ICT ve veřejné správě je státní správa jednoznačně podřízena řízení na vrcholové úrovni, zatímco samospráva pouze částečně. Naopak, vzhledem k potřebám podpory se samospráva mnohdy stává klíčovým klientem státní správy, a to i co se týče ISVS a sdílených služeb a ICT prostředků.

Tabulka 7 – Význam jednotlivých úrovní řízení z pohledu řízení služby a informačního systému

Úroveň řízení	Typický úřad	Popis významu
Vrcholová	Vláda, Rada vlády pro informační společnost (RVIS), MV/OHA či další.	Stanovuje, CO a JAK se bude dělat a pro jednotlivé služby stanovuje motivační a základní byznysové prvky, také schvaluje právní předpisy.
Gesční	Gestor za danou agendu či oblast.	Připravuje právní předpisy k agendě/oblasti, řídí výkon agendy a stanovuje působnost a podmínky výkonu, v některých případech poskytuje a spravuje centralizovaný AIS.
Institucionální	OVM a korporát VS,	Úroveň jednotlivého úřadu či korporátu (krajský korporát, obecní korporát, resortní korporát), vykonává agendu/ činnosti a k tomu využívá lidské a technické zdroje, spravuje a provozuje svoje ISVS.
Služby	Jednotlivý ISVS či služba.	Reprezentuje každý ISVS jako logický celek komponent sloužící pro podporu výkonu nějaké služby a také danou službu veřejné správy.

Tabulka 8 – Význam úrovní řízení ICT z ekonomického pohledu

Úroveň	Kdo/co	Popis významu
Vláda	Vláda a MV ČR a MF ČR.	Vrcholová úroveň jak pro eskalaci, tak především pro stanovování ekonomických a rozpočtových mantinelů.
Kapitola	Správce rozpočtové kapitoly.	Orgán určující podobu rozpočtové kapitoly a strukturu rozpočtových a personálních prostředků.
Korporace	Úřad či jeho korporace.	Resort i s jeho podřízenými organizacemi, nebo krajská či veřejnoprávní korporace určující a vykonávající služby a činnosti s přidělenými prostředky.
Organizace	Každá konkrétní organizace.	Na základě prostředků řídí svoje ICT a řídí a realizuje služby, včetně služeb veřejné správy.

Útvar	Jednotlivé útvary v organizaci zodpovědné za schopnost či službu.	Jednotlivé útvary, jež jsou věcně zodpovědné za konkrétní schopnost, agendu či službu v úřadu, jsou byznysovými vlastníky dané služby a zajišťují její realizaci, ale také spoluřídí a určují její ICT prostředky.
Systém	Konkrétní IS či komponenty.	ICT útvar řídí a rozvíjí ICT prostředky (včetně informačních systémů) ve spolupráci s věcnými gestory.

8.2 Kompetenční útvary

Kompetenční útvary lze rozdělit na útvary pro řízení, metodiku nebo podpory. Jako **útvary řízení** lze zmínit **vládu ČR**, dále pak jejím usnesením, tedy usnesením vlády ze dne 24. listopadu 2014 č. 961 o zřízení Rady vlády pro informační společnost, byla zřízena **Rady vlády pro informační společnost** (RVIS) jako odborný poradní (ale i v některých oblastech výkonný) orgán pro oblast informační společnosti. V rámci programu Digitální Česko byla definována role **digitálního zmocněnce** na všech ministerstvech/centrálních úřadech.

Mezi klíčové **metodické útvary** patří **Odbor Hlavního architekta eGovernmentu** (OHA), jehož kompetence jsou postupem času stále zvyšovány, a plynou zejm. zákonem č. 365/2000 Sb. (a jejich přiřazení dle vnitřního řádu MV), usnesením vlády ze dne 2. listopadu 2015 č. 889, usnesení vlády č. 86 z 27. ledna 2020. OHA zpracovává národní architektonický plán (NAP) a další navazující dokumenty IKČR (viz kapitola 3), dále centrálně schvaluje projekty zabývající se ICT veřejné správy, ale i koná školení a předává know-how.

Jako **útvar podpory**, lze zmínit tzv. **kompetenční centrum** zařazené do Národní agentury pro informační a komunikační technologie, s. p. (NAKIT) zřizovaný MV. To pomáhá např. s informačními koncepcemi jednotlivých ministerstev či úřadů.

8.3 Dlouhodobé řízení informačního systému veřejné správy

Základní vymezení dlouhodobého řízení ISVS na straně orgánů veřejné správy je zakotveno v zákoně č. 365/2000 Sb. Dlouhodobé řízení ISVS realizuje úřad prostřednictvím informační koncepce orgánu veřejné správy. Požadavky na tento dokument jsou detailně rozpracovány ve vyhlášce č. 529/2006 Sb., vyhláška o dlouhodobém řízení ISVS. Mezi základní **hlavní procesy** patří: **tvorba a aktualizace informační koncepce**, **tvorba a aktualizace provozní dokumentace**, **vyhodnocování informační koncepce**, **řízení kvality ISVS**, **řízení bezpečnosti ISVS**.

Otázky k procvičení:

1. Jaké úrovně řízení rozlišujeme z pohledu řízení služby a informačního systému?

Dle materiálu se jedná o vrcholovou, gesční, institucionální a služby.

2. Jaké dva hlavní dokumenty souvisí s dlouhodobým řízením ISVS?

Jedná se o informační koncepci orgánu veřejné správy a provozní dokumentaci.

3. Účastnili jste se školení pořádané OHA – architektura veřejné správy, či problematika otevřených dat či jiných kompetenčních úřadů? Pokud ano, tak jaké máte pocity/zkušenosti?

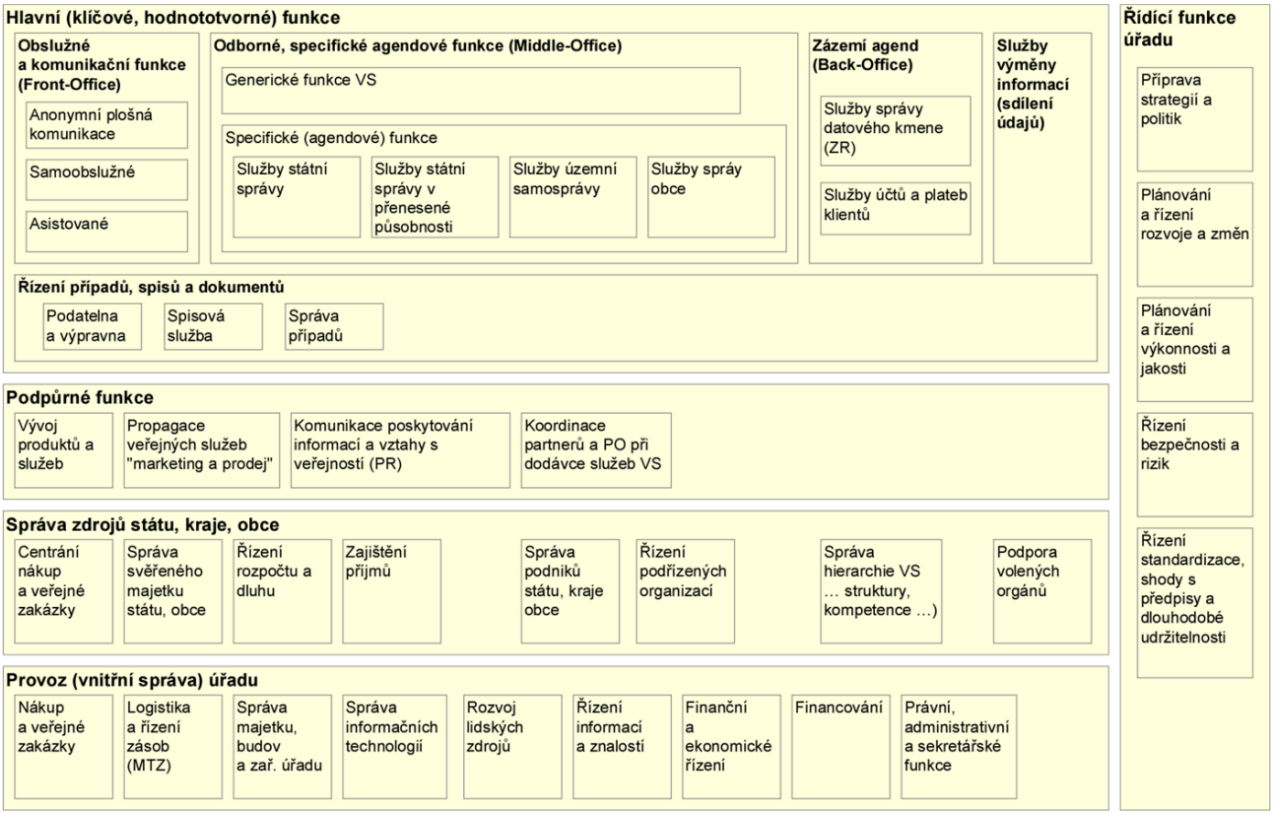
Krom zmíněných OHA, lze zmínit třeba odbor eGovenrmentu a jeho procesní modelování agend. Oba odbory lze zkontaktovat v případě zájmu přes příslušné emailové schránky oha@mvcr.cz, oeg@mvcr.cz.

8.4 Doplňující část

8.4.1 Referenční byznys model VS

Vše, co OVS činí / koná, je možné z hlediska ICT podpory rozdělit (dekomponovat) do pěti hrubých procesních kategorií a každou z nich ještě jemněji členit. Grafické znázornění tohoto členění zachycuje obrázek níže.

Obrázek 3 – Referenční model byznys vrstvy



Veřejná správa funguje na odlišném principu než soukromoprávní subjekty. Výkon veřejné správy se řídí zásadou, dle které veřejná moc může konat jen tehdy, stanoví-li to zákon (má-li k danému konání konkrétní úřad platné zákonné zmocnění), a jen způsobem stanoveným zákonem. Jinými slovy, co není zákonem nařízeno, je zakázáno.

Rozvoj ICT veřejné správy, tzn. ne pouze digitálních služeb, ale i technologických prostředků a personálního zabezpečení vychází primárně z výše uvedených dokumentů, přičemž jako takový je ale primárně určován výší finančních prostředků.

8.4.2 Kompetenční matice eGovernmentu

Kompetenční matice obecně přiřazuje vybraným rolím (tj. útvarům nebo osobám, které je zastávají) konkrétní kompetence (tj. práva: co od koho žádat, resp. komu co uložit, a povinnosti: co za jakých podmínek, s jakými parametry, na základě, jakého podnětu a od koho udělat) k vybraným agendám / činnostem / úkonům.

Kompetenční matice řízení a rozvoje eGovernmentu ČR se odvíjí od povinností stanovených v § 3 a § 4 zákona č. 365/2000 Sb., o ISVS. V § 3 zákona č. 365/2000 Sb., je konstatováno, že vláda schvaluje Informační koncepci České republiky, a rozhoduje o programech a investičních záměrech akcí obsahujících pořízení nebo technické zhodnocení informačních systémů veřejné správy vypracovaných podle zvláštního právního předpisu. Při svém rozhodování se vláda opírá o svůj poradní orgán – RVIS.

Ministerstvo vnitra v souladu s § 4 zákona č. 365/2000 Sb., o informačních systémech veřejné správy, koordinuje eGovernment v podobě zpracovávání návrhů strategických dokumentů v oblasti informačních systémů veřejné správy a předkládá tyto dokumenty vládě, sleduje a analyzuje informační potřeby veřejné správy a stav informačních systémů veřejné správy, dále se pak vyjadřuje k záměrům pořízení nebo technickému zhodnocení informačních systémů veřejné správy. Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele dokumentace programu a k potřebám zajištění řádného výkonu veřejné správy, a zajišťuje tvorbu metodických pokynů pro výkon odborných činností spojených s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy.

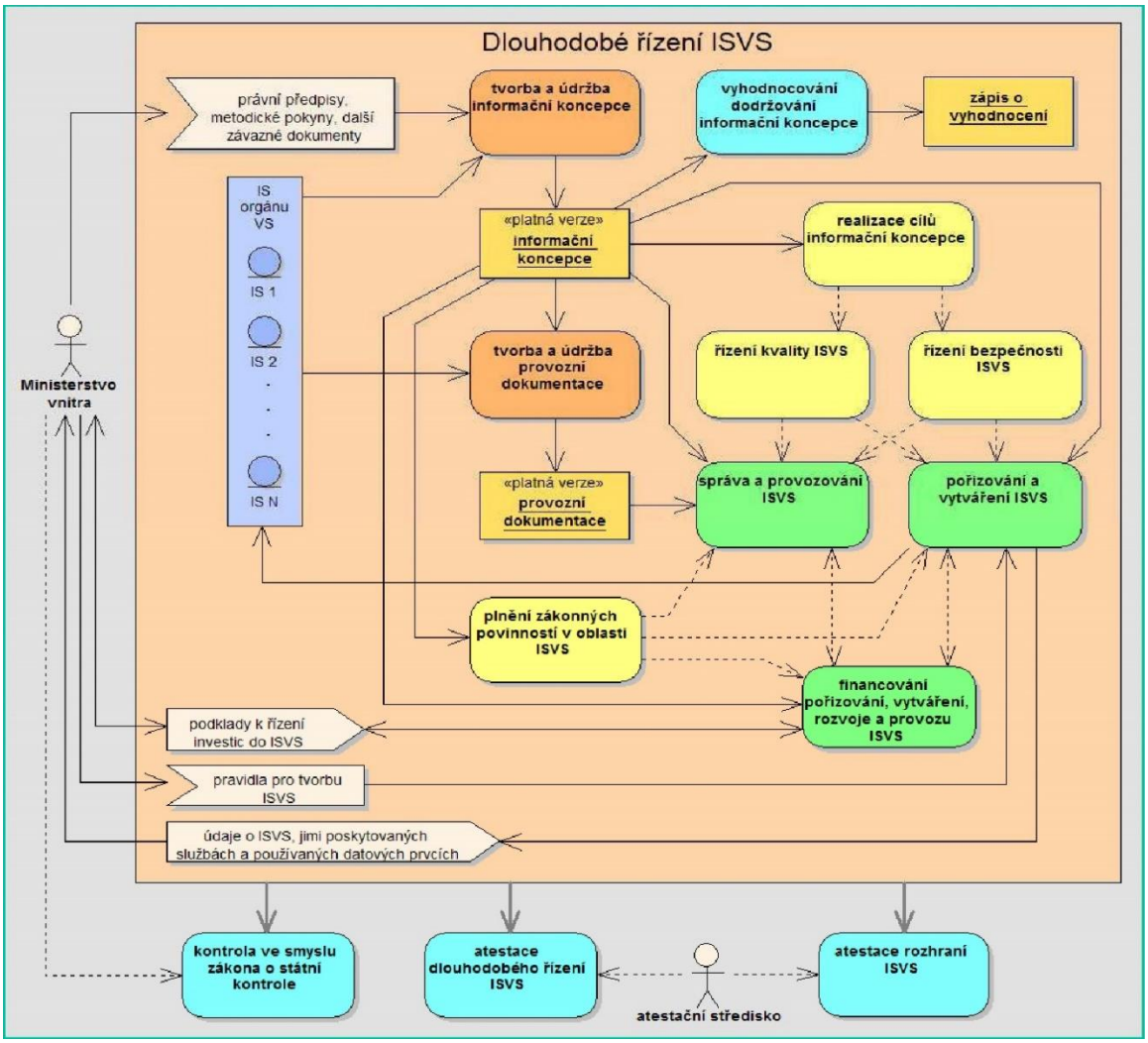
Na úrovni jednotlivých resortů jsou řízení a rozvoj eGovernmentu vymezeny v organizačních řádech upravujících strukturu kompetencí jednotlivých útvarů. Každý resort je povinen dodržovat pravidla a povinnosti vyplývající ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy, zejména pak § 5, 5a, 5b. Ve své informační koncepci si resort stanoví proces řízení změn v oblasti informačních systémů veřejné správy a služeb eGovernmentu resortu. Resort je také povinen svou informační koncepci aktualizovat poté, co je schválena Informační koncepce ČR, tak aby byly reflektovány trendy a cíle eGovernmentu stanovené vládou.

Resort ve své informační koncepci definuje řízení a rozvoj na úrovni jednotlivých informačních systémů resortu. V souladu s usnesením vlády ze dne 2. listopadu 2015 č. 889 by měl resort určit u každého ISVS konkrétního věcného správce, technického správce a provozovatele daného systému. Zároveň se u jednotlivých rolí musí určit odpovědnosti vyskytující se v jednotlivých etapách životního cyklu systému / služby.

8.4.3 Dlouhodobé řízení ISVS

Přehled procesů dlouhodobého řízení ISVS v grafické podobě ilustruje obrázek níže.

Obrázek 4 – Přehled procesů dlouhodobého řízení ISVS



8.4.4 Odkazy

- Webová prezentace Vlády České republiky:

https://www.vlada.cz/

- Odbor Hlavního architekta eGovernmentu Ministerstva vnitra České republiky

https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu-agenda-odboru-hlavniho-architekta-egovernmentu.aspx

9 Význam ICT architektury veřejné správy

Související právní předpisy: zejména zákon č. 365/2000 Sb., Národní architektonický plán vydaný Ministerstvem vnitra.

9.1 Význam ICT architektury

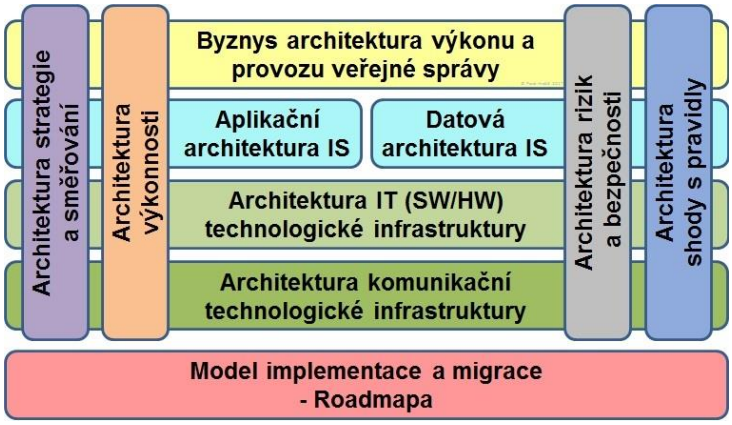
Příčinou vzniku architektury ICT jako podstatné součásti ICT byla nutnost uspořádání a sjednocení historicky vzniklých pravidel, procesních i technických standardů atd. včetně vztahu ICT s okolím (ostatními oblastmi lidské činnosti), aby **ICT řešení** byla navzájem **kompatibilní**, byly dosahovány **synergické efekty** a optimalizováno **využívání zdrojů** – jak informačních, tak technických, lidských, finančních i časových.

Přestože se dodnes užívají pojmy jako ICT architektura, ICT architekt, tak v rozšířeném smyslu je ICT architektura chápána včetně všech doprovodných rolí, tedy z hlediska návrhu informačních systémů se neřeší pouze ICT pozadí, ale holisticky (celostně) všechny části podniku – byznysové procesy (v prostředí VS procesy vykonávané agendou), zúčastněné osoby – klienti externí (např. občané), tak interní (např. úředníci), tak i dalších zainteresovaných osob, které mají své zájmy (např. ředitelé úřadů). V tomto kontextu se užívají pojmy (synonyma) jako **architektura úřadu** (v prostředí VS), **podniková architektura** či původní anglický výraz Enterprise Architecture.

9.2 ICT architektura veřejné správy

Architektura úřadu definována **Národním architektonickým rámcem** (NAR) a práce s ní zakládá na agendovém přístupu výkonu VS. Výkon správy je rozdělen na agendy a danou agendu typicky podporuje ICT řešení – ISVS/AIS, obecně informační systém. Každý IS obsahuje prvky ze všech čtyř vrstev architektury úřadu. K tomu jsou průřezové řešeny aspekty, tedy vlastnosti, které protínají všechny architektonické vrstvy jako je například architektura strategie a směřování (obrázek 5).

Obrázek 5 – Domény Národního architektonického rámce VS ČR



Poznámka: Vrstvy architektury jsou na obrázku vyjádřeny vodorovně, aspekty svisle. Model implementace a migrace – Roadmapa je speciální konstrukt definující dynamiku, změnu stavu architektury mezi dvěma a více časovými okamžiky, tedy přestože je vodorovně, tak není za vrstvu považován.

Na každé **vrstvě architektury** obsahuje IS více různých prvků (aktivních, pasivních a chování), které je třeba identifikovat, klasifikovat a řídit. IS nikdy není izolován, vždy je součástí architektury větších celků v pořadí: úřadu; jednotlivé organizace/korporace/resortu nebo územního celku (kraje a obce); veřejné správy ČR; veřejné správy EU. Detailnější rozpad konkrétní pro domény architektury úřadu zachycuje tabulka níže.

Tabulka 9 – Domény architektury úřadu – základní charakteristika

Doména	Řešená oblast
Byznys architektura výkonu a provozu veřejné správy.	Jaké funkce a služby VS dělá, komu je poskytuje / od koho je čerpá a kdo jsou jejich uživatelé (druh, počet, charakter...).
Aplikační architektura IS, Datová architektura IS.	Jaké (vlastní nebo sdílené) digitální služby na podporu svých činností úřad využívá / jaké informační systémy mu v tom pomáhají (např. systém spisové služby, datové schránky a vlastní portál).
Architektura IT (SW/HW) technologické infrastruktury.	Na jakém HW a SW či platformách (např. vícero datových center v clusteru pro zaručení vysoké dostupnosti).
Architektura komunikační technologické infrastruktury.	Na jaké komunikační infrastruktuře VS a v jakých datových centrech, s kým, kudy a za jakých podmínek (forma, protokoly...) úřad komunikuje uvnitř i ven (např. interní síť, dále napojená do komunikační infrastruktury veřejné správy – viz kapitola 17).
Architektura strategie a směřování.	Kam chce úřad jít (např. všechny služby jsou i digitální, úředník bude mít pouze notebook a dojde k odbourání stolních počítačů).
Architektura výkonnosti.	Jak dobrý chce úřad ve své činnosti být (např. pouze minutový výpadek).
Architektura rizik a bezpečnosti.	Jaké zranitelnosti a jaké hrozby úřad identifikoval, jaké a jak významné jsou jejich možné dopady. Jaká je přijatelná hranice zjištěných kybernetických rizik. Co a v jakém pořadí / termínech proti tomu úřad hodlá dělat (např. četnější bezpečnostní školení).
Architektura shody s pravidly.	Jakými pravidly je ICT úřadu svázáno (např. architektonické principy)
Model implementace a migrace – Roadmapa.	Jak se úřad hodlá / plánuje dostat k cíli a jaké zdroje k tomu hodlá využít. (např. postupná migrace, big bang, zavedení nové služby)

Prostředkem pro řízení je tedy **strukturovaný model architektury** (užívá se modelovací jazyk **ArchiMate**). Aby byl pro jednotlivé zúčastněné osoby čitelný, tak typicky bývá upraven do více pohledů, které danou osobu zajímavý a použitelný (viz doplňková část hlediska a pohledy)

Mezi **vybrané klíčové tematické okruhy architektury** patří (dále viz doplňková část): **obslužné kanály** (např. Czech POINT), **meta-informační systémy** (např. registr práv a povinností), **sdílení údajů** (např. propojený datový fond a veřejný datový fond), **elektronická výměna dokumentů** (např. datové schránky), **sdílené platformy** (např. cloud) aj.

Otázky k procvičení:

1. Jak byste definovali pojem podniková architektura / architektura úřadu?

Ve veřejné správě se jedná o synonyma, architektura úřadu svým názvem zdůrazňuje zaměření veřejný sektor. Podniková architektura / architektura úřadu je manažerská holistická disciplína pokorného a systematického pochopení organizace a řízení jejího směřování.

2. Využívá váš úřad přístup architektury úřadu? Pokud ano, tak v jakých oblastech?

Ministerstvo vnitra přístup architektury úřadu užívá. Užití zejména pro doménu ICT projektů, včetně schvalování žádostí o stanovisko OHA.

9.3 Doplňující část

9.3.1 Hlediska a pohledy

Národní architektonický rámec představuje řadu hledisek (stanovení komu má daný model sloužit a jak by tedy obecně měl vypadat) ovlivňující podobu výsledných pohledů modelu. Architektonický čtyřvrstvý model je základním prostředkem pro řízení a rozhodování o celé architektuře systémů, jedná se o architekturu, či přehledovou architekturu právě celého funkčního celku informačního systému, viz tabulka níže.

Tabulka 10 – Čtyřvrstvý architektonický model jako podpora pro rozhodování

Byznysová vrstva – Podporované agendy / služby veřejné správy (CO?)	
Okruh otázek	Realizace / aplikace
▪ Centrální vs. lokální procesy. ▪ Vlastní nebo sdílené služby. ▪ Speciální nebo univerzální obslužné kanály. ▪ Asistované vs. on-line služby. ▪ Sdílené údaje: Propojený datový fond (PPDF) a Veřejný datový fond (VDF).	▪ Registr práv a povinností. ▪ Procesní modelování agend veřejné správy. ▪ Zavádění úplného elektronického podání.
Příklady:	▪ *Výplata* sociálních *dávek* ▪ *Vydávání řidičského průkaz* ▪ *Výměna občanského průkazu*
Aplikační a datová vrstva (JAK?)	
Okruh otázek	Realizace / aplikace
Aplikace / služby ▪ Logicky centralizované / distribuované. ▪ Vyvinuté na zakázku / balíčkové produkty (Off the Shelf). ▪ On Premise / Cloud. **Data** ▪ Referenční ze ZR, agendové a vlastní údaje.	▪ Základní registry (ZR). ▪ Datové schránky (ISDS). ▪ CzechPOINTy. ▪ Portál veřejné správy (PVS). ▪ Systémy pro propojení datového fondu, pro publikace open dat, pro vzájemné uznávání evropských ID, pro publikaci formulářů, propojení rozhraní na životní situace.
Příklady:	▪ *Elektronická identita.* ▪ *Výdej referenčních údajů.* ▪ *Zaručené doručení, zaručené podání, zaručená publikace údajů.* ▪ *Akceptace změn.*
Vrstva technologické platformy (KDE?)	
Okruh otázek	Realizace / aplikace
▪ Platformy (Databáze, Aplikační servery, interní sítě - LAN apod.). ▪ Výpočetní výkon a datové úložiště.	▪ Národní i regionální datová centra propojená vzájemně i do EU se společným dohledem zejména na úrovni průřezových služeb informační společnosti. ▪ Definované služby standardní, kritické a krizové. ▪ Definované standardy SLA, provozní a bezpečnostní standardy. Intranet OVM (LAN).
Příklady:	▪ *Hostingové služby datového národního centra.* ▪ *Platforma jako služba.* ▪ Provozní *dohled jako služba.*
Vrstva komunikační infrastruktury (KUDY?)	

Okruh otázek	Realizace / aplikace
▪ Datové centrum (NDC, komerční DC). ▪ Komunikační sítě (externí – WAN = centrálně řízený KIVS a Internet).	▪ Na úrovni komunikační infrastruktury se jedná o externí (WAN) vzájemné propojení OVM (včetně rozhraní Intranetu a Internetu), tj. techn. prostředky komunikačních sítí ve správě OVM. ▪ Definované služby standardní, kritické a krizové infrastruktury. ▪ Definované standardy SLA, provozní a bezpečnostní standardy.
Příklady:	▪ *Univerzální klientská přípojka z fixní lokace.* ▪ *Klientská přípojka z mobilní lokace.* ▪ Propojení *do EU / mezi datovými centry.*

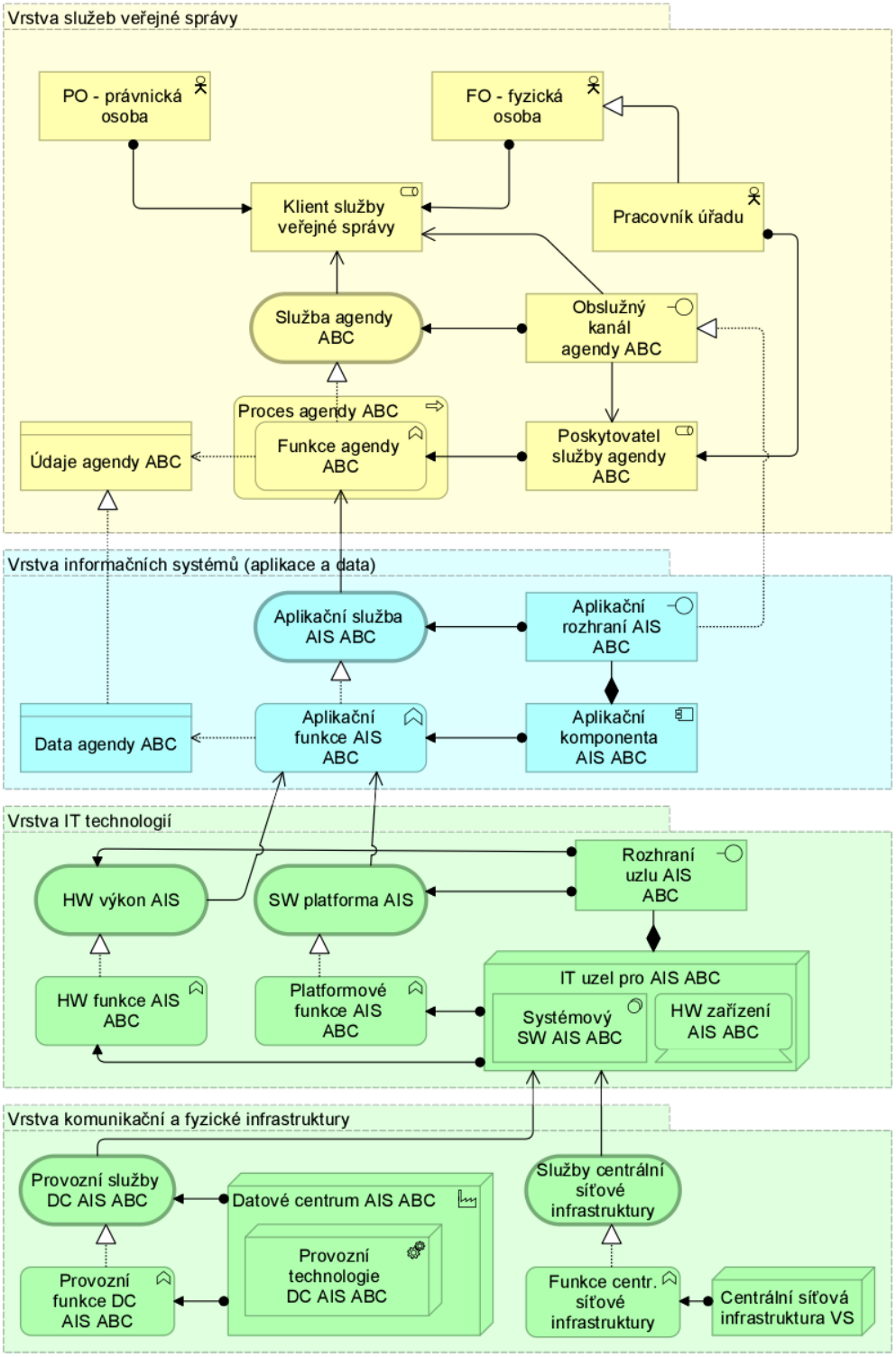
9.3.2 Klíčové tematické okruhy Národní architektury veřejné správy

Na základě schválené Informační koncepce České republiky (IKČR) je schválen, užíván a kontinuálně udržován a upravován Národní architektonický plán (NAP). Ten přináší nejen popis a smysl současných existujících centrálních sdílených služeb eGovernmentu ale i budoucí plán architektury s výhledem budoucích změn, dále obsahuje i pravidla jejich správného využití v architekturách jednotlivých aktérů VS, a to zejména v těchto oblastech:

- Meta-informační systémy eGovernmentu
  - RPP jako základní registr pro řízení eGovernmentu,
  - Úložiště architektonických modelů a katalogů. (v realizaci)
- Kontaktní místa, obslužné kanály pro klienty VS
  - PO v PVS a mobilní aplikace – samoobslužné
  - CzechPOINT – jako asistované služby
- Jednotné identitní prostory (JIP) a systémy elektronické identifikace pro klienty a pro úředníky
  - Elektronická identifikace, autentizace pro fyzické osoby (zejm. občany ČR) (NIA)
  - Identifikace, autentizace a autorizace pro úředníky veřejné správy ČR (JIP/KAAS)
- Propojený datový fond (PPDF)
  - Základní registry
  - Informační systém sdílené služby (I3S/ ISSS, či znám téže jako eGSB)
- Veřejný datový fond (VDF)
  - Otevřená data,
  - Veřejné rejstříky
- Elektronická výměna dokumentů (EVD) a elektronické úřadování
  - Datové schránky
  - Elektronické pečetě a časová razítka
- Sdílené agendové IS (AIS)
  - Sdílené agendové IS v přenesené působnosti,
  - Sdílené agendové IS pro samostatnou působnost územních samospráv
- Sdílené provozní informační systémy
- Jednotné obslužné kanály a uživatelská rozhraní úředníků
  - Portál úředníka
  - CzechPOINT@Office.
- Sdílené platformy a ICT infrastruktura VS ČR
  - Národní datová centra
  - eGovernment Cloud.
  - Sdílená síťová a komunikační infrastruktura

V rámci hlavní části bylo zmíněno modelování, v prostředí veřejné správy se užívá jazyk ArchiMate, kdy metamodel architektury služeb VS zachycuje grafika níže.

Obrázek 6 – Generický model architektury služeb VS



9.3.3 Odkazy

- Architektura úřadu na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/nap_dokument:pravidla_tvorby_a_udrzby_vlastni_ctyrvrstve_architektury_jednotlivych_uradu

10 Životní cyklus digitální služby

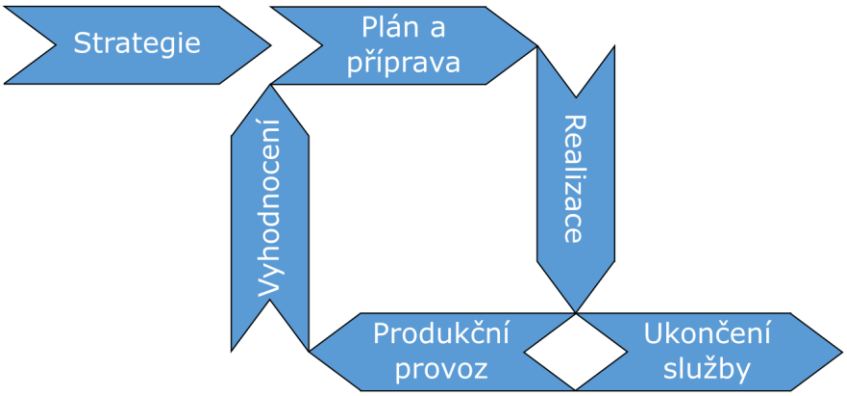
Související právní předpisy: zejména zákon č. 12/2020 Sb., zákon č. 365/2000 Sb., Národní architektonický plán vydaný Ministerstvem vnitra.

10.1 Životní cyklus digitální služby

Složitost a charakter digitální (ICT) **služby** poskytované jednotlivými informačními systémy **se typicky různí**, navíc i jeden informační systém může mít jak služby jednoduché, tak extrémně komplikované podporované řetězcem procesů. Avšak samotný **životní cyklus služby** (a ostatně informačního systému) **je typicky stejný** bez rozdílu agendy veřejné správy, ke které slouží.

V souladu s ITIL a TOGAF (viz kapitola 4) Národní architektura veřejné správy rozlišuje pro ICT služby a informační systém šest etap: **Strategie**, **Plán a příprava**, **Realizace**, **Produkční provoz**, **Vyhodnocení**, **Ukončení služby**. Je možné si povšimnout vyobrazené cykličnosti, kdy úsek od etapy Plánu a přípravy až do etapy Vyhodnocení se může vícečetně opakovat. Etapa Plán a příprava je vždy ovlivněna současnou strategií, např. na úrovni úřadu jeho informační koncepcí (obrázek 7).

Obrázek 7 – Etapy životního cyklu ICT služby / systému veřejné správy



Hlavní činnosti spárované s životním cyklem digitální služby, s konkrétními povinnostmi a právy jsou klíčové role (viz kapitola 11) rozpracovány v matici zodpovědností (RACI matice). Matice je zpracovávána jako příloha k dokumentu Metody řízení ICT VS ČR.

10.2 Popis etap

Každá etapa se skládá z fází. V některých standardech se používá druhé členění, kdy je fáze nadřazená etapě. Národní architektura veřejné správy, používají první zmíněné členění.

Strategie je výchozí etapou, která definuje předpokladu služby / systému. Je ovlivněna strategickými dokumenty jako je IKČR, Informační koncepcí úřadu. Fáze:

1. vize,
2. identifikace nové povinnost / potřeby změny povinností,
3. strategické cíle,
4. podniková architektura (architektura úřadu),
5. rámcový plán (roadmapa).

Plán a příprava obsahuje detailnější rozpad cíle, způsob jeho naplnění (požadavky), správná formulace požadavků (náklady na změnu ze špatně zadaného požadavku v rámci postupem projektu dramaticky rostou. Fáze:

1. záměr,
2. analýza kritérii a možných variant řešení,
3. stanovaní hlavního cíle a cílů dílčích projektu (klíčových požadavků),
4. předběžný design,
5. prioritizace uspokojování požadavků
6. finanční zabezpečení projektu / rozpočtová opatření.

Realizace je etapou, kdy dochází k samotnému vytvoření služby / systému. Fáze:

1. poskytnutí kompletních podkladů včetně zmocnění externích osob,
2. business architektura,
3. návrh změn enterprise architektury (podnikové architektury),
4. detailní návrh (architektura řešení),
5. implementace,
6. školení uživatelů a zpracování provozní dokumentace,
7. nastavení – uživatelské, patch managementu, zálohování aj.,
8. testování,
9. finalizace dokumentace,
10. akceptace aj.

Produkční provoz – v této etapě je služba / systém schopen plnit svůj účel. Fáze:

1. převzetí smluvního plnění do produkčního provozu vč. zavedení do majetku,
2. poskytování služeb / funkcionalit v rámci smluvních parametrů (SLA),
3. patch management (Update SW), aktualizace (Upgrade SW),
4. změny: nastavení oprávnění, parametrů, funkcionalit (reportů), integrace, včetně aktualizace dokumentace,
5. zálohování, archivace,
6. provozní monitoring plnění smluvních parametrů (SLA),
7. profylaxe, operativní údržba, audit aj.

Vyhodnocení obsahuje porovnání chtěného a skutečného stavu, obsahuje i poučení se z projektu, samotné vyhodnocení může spustit další cyklus rozvoje, či naopak ukončení. Fáze:

1. vyhodnocení projektu = (ne)dosažení cílů projektu,
2. analýza provozních dat / plnění znalostní databáze (Best Practice),
3. formulace doporučení od změn nastavení po další rozvoj / ukončení provozu,
4. rozhodnutí o ukončení poskytování služby / provozu systému.

Ukončení služby (či systému) obsahuje řízené kroky ovlivněného prostředí. Fáze:

1. ověření využitelnosti komponent (přemístění, prodej, likvidace)
2. administrativní opatření,
3. technická opatření.

Otázky k procvičení:

1. Jaká etapa zahajuje/identifikuje potřebu nové služby? Kdy (etapa) je služba dostupná klientovi?

Zahajuje se etapou Strategie. Služba je dostupná v etapě Produkční provoz.

2. V jaké etapě jsou jednotlivé digitální služby, které váš úřad poskytuje?

Například služba odesílání datové zprávy pomocí informačního systému datových schránek je v produkčním provozu. Ale je možné, že kolegové z MV mají připravený návrh nové verzi této služby, tato nové verze by pak pravděpodobně byla v etapě Plánu a přípravy.

10.3 Doplňující část

Doplňující část k růstu cen opravy chyby/změny požadavku v rámci etap: Primární význam má v 2. etapě správné, komplexní popsání (specifikace) požadavku věcným gestorem (garantem primárních aktiv). Tuto skutečnost dokumentují typické ekonomické dopady špatných požadavků (obrázek 8). Oprava chyb je mnohem levnější v raných fázích projektu, tedy ve fázi strategie, plánu a přípravy. V relativní škále, pakliže oprava chyby ve fázi formalizace požadavků stála 1.000 Kč, při tvorbě designu oprava stojí již 1.000 Kč a dále 2.000 Kč až 3.000 Kč na opravu již odvedené práce. Pakliže by si chyby všiml až uživatel, oprava chyby by stála 100.000 Kč.

Obrázek 8 – Znázornění rozdílnosti nákladů na opravu v závislosti na etapu změnového požadavku

10.3.1 Odkazy

- Řízení jednotlivých ICT řešení na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/metody_dokument:rizeni_jednotlivych_ict_reseni

11 Klíčové role ICT veřejné správy

Související právní předpisy: zejména zákon č. 365/2000 Sb., zákon č. 181/2014, Národní architektonický plán vydaný Ministerstvem vnitra.

11.1 Klíčové role

Předmětem / cílem práce úředníka veřejné správy je výkon agendy veřejné správy. Pro podstatnou část služeb veřejné správy je typické, že se jedná o služby individuální. Jeden konkrétní úředník řeší potřebu jednomu konkrétnímu klientovi (externímu nebo internímu). Principiálně služba úředníka přináší klientovi hodnotu, za kterou je ochoten zaplatit, buď přímo, nebo skrze placení daní, kdy tato služba se řídí předem danými formálními pravidly.

Správce systému je klíčovou rolí, její vnímání se však dle kontextu zákona rozlišuje na:

- **Správce informačního systému** (zákon č. 365/2000 Sb.) je orgán nebo osoba, která určuje účel zpracování informací a podmínky provozování informačního systému, a poskytuje služby informačního systému veřejné správy a za informační systém veřejné správy odpovídá.
- **Správce komunikačního systému** (zákon č. 181/2014 Sb.) je orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování.

Metody řízení ICT VS ČR dále rozlišují tyto role:

- **Věcný správce** (též gestor nebo garant primárních aktiv, dále viz níže a kapitola 18) je orgán nebo osoba, který rozhoduje o obsahu a pravidlech fungování služby. Věcný správce je zodpovědný za data, definici procesu, který služba automatizuje, za určení a kategorizaci službou využívaných a zpracovávaných dat, za shodu funkcionalit aplikace s legislativou a za definici objemových a kvalitativních parametrů ICT služby (počet uživatelů, doba provozu služby, dostupnost služby, doba odezvy atd.).
- **Technický správce** (též garant podpůrných aktiv, dále viz níže a kapitola 18) je orgán nebo osoba, který rozhoduje o technickém zajištění služby (jakým softwarem a hardwarem), kým, (určuje interní provozovatele a uzavírá smlouvy s externími), z jakého místa, (kterou cestou, bude služba realizována). Stanovuje podmínky realizace podpůrných ICT služeb tak, aby předmětná služba byla dodávána v souladu s požadavky jeho věcného správce.

Ohlašovatel agendy je orgán veřejné moci, který ohlašuje agendu pro potřeby jejího výkonu, ohlášením se myslí její zaregistrování a schválení v Registru práv a povinností (RPP). Platí pro ministerstva a ústřední správní úřady, a dále pro Nejvyšší kontrolní úřad a Českou národní banku. Ohlášení obsahuje informace zejm. o aktérech, službách a úkonech, údajích a oprávněními.

Správce dle zákona č. 365/2000 Sb. Je povinen zaevidovat tento systém do rejstříku ISVS (součást RPP) a tento zápis aktualizovat. Zpracovat a aktualizovat provozní dokumentaci daného ISVS. Být v souladu s Informační koncepcí úřadu a lze dovodit, že svými znalostmi systému se na ní podílet.

Garant aktiv, role prováděcí vyhlášky č. 82/2018 Sb. zákona č. 181/2014 Sb., se dále člení:

- **Garant primárního aktiva**, což je fyzická osoba pověřená věcným správcem systému ke stanovení základních cílů a podmínek systémem poskytovaných ICT služeb, tj. k zajištění, rozvoje, použití a bezpečnosti primárních aktiv systému.

- **Garant podpůrných aktiv** je fyzická osoba pověřená (v souladu s věcným správcem) provozovatelem systému k tomu, aby úroveň poskytovaných služeb dlouhodobě splňovala parametry kvality (stanovená SLA).

Role provozovatele, poskytovatele a dodavatele:

- **Provozovatel** informačního nebo komunikačního systému je orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém. Provozováním informačního systému veřejné správy může správce pověřit jiné osoby nebo jejich součásti, pokud to jiný zákon nevylučuje.
- **Poskytovatel** je organizace, útvar nebo osoba, která službu dle zadání technického správce provozuje a dodává.
- **Dodavatel** je právnickou nebo fyzickou osobou, která dodává zboží nebo poskytuje služby. Správce ve smlouvě stanoví podmínky (úroveň kvality služby – SLA), za jakých bude dodavatel dodávku plnit a sjednané služby poskytovat.

Klient (běžně užíváno i slovo uživatel) služby může být **interní** (interní pracovník, co se systémem pracuje – např. úředník) nebo **externí** (právnická, fyzická osoba – např. tedy občan), jiným členěním může být klient rozdělen na klienta **anonymního** nebo **autorizovaného** (např. přihlášení do Portálu občana svojí digitální identitou).

Dále je uveden prostý výčet vybraných dalších významných rolí: vrcholný představitel úřadu (ministr, hejtman aj.), hlavní architekt úřadu, správce / koordinátor interních procesů úřadu, hlavní projektový/programový manažer, hlavní informatik (CIO) / digitální zmocněnec, bezpečnostní ředitel / manažer kybernetické bezpečnosti úřadu / pověřenec pro ochranu osobních údajů (DPO), průřezově i personální ředitel (sekce statní služby), ekonomický ředitel (účetnictví, správa majetku), hlavní manažer výkonnosti, kvality a zodpovědnosti, hlavní nákupčí.

Otázky k procvičení:

1. Restrukturalizací úřadu byl vytvořen útvar interního ICT, který má sloužit k ucelené ICT podpoře úřadu. Útvar zabývající se účetnictvím mezd používá účetní systém, který je běžným komerčním řešením a byl zakoupen přímo od vývojářské firmy SuperMzdy s. r. o. Systém běží v a na infrastruktuře úřadu (tedy nikoliv v cloudu). Jaké role diskutované v této kapitole byste jednotlivým aktérům (útvar majetku, útvar interního ICT, firma SuperMzdy s. r. o.) přiřadili?

Jedním z logických členění by mohlo být následující rozdělení:

Útvar majetku – správce informačního systému, věcný správce, ohlašovatel agendy, garant primárního aktiva, interní klient, autorizovaný klient

Útvar interního ICT – technický správce, garant podpůrných aktiv, provozovatel, poskytovatel

Firma SuperMajetek s. r. o. – dodavatel

2. Kdo ve vaší organizaci zastává roli digitálního zmocněnce, pověřence pro ochranu osobních údajů, ekonomického ředitele?

Pokud naleznete, tak s velkou pravděpodobností, pokud nejste z menší samosprávy, tak role budou vykonávány odlišnými osobami, neboť jejich zaměření je značně rozdílné.

11.2 Doplňující část

11.2.1 Garant aktiv

Je definována ještě role **Garant technických aktiv**, což je fyzická osoba pověřená technickým správcem, případně provozovatelem systému k zajištění provozu konkrétního technického aktiva, zodpovědná za zajištění plné funkcionality technického aktiva tak, aby tato byla v souladu se SLA, stanovenými pro poskytování služeb daným systémem při současném dodržení platných předpisů (požadavky výrobce, obecná legislativa, interní akty řízení atd.).

11.2.2 Odkazy

- Klíčové role na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/metody_dokument:celkovy_dokument#klicove_role_v_ict_a_egovernmentu

12 Registr práv a povinností – metainformační systém státu pro výkon veřejné správy

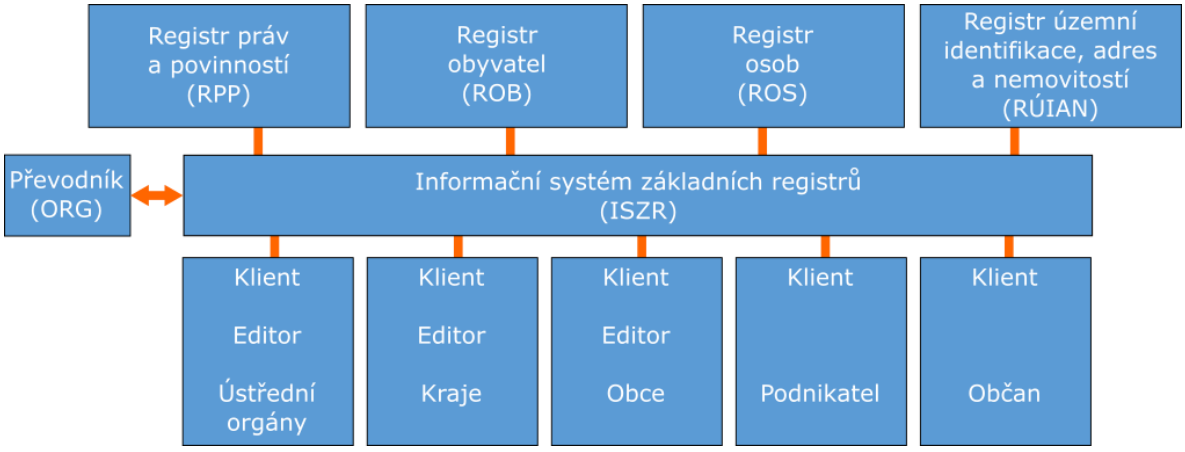
Související právní předpisy: zejména zákon č. 111/2009 Sb., průřezově zákon č. 365/2000 Sb., zákon číslo 181/2014 Sb.

12.1 Základní registry

Základní registry jsou ukotveny zákonem č. 111/2009 Sb. V České republice existují čtyři základní registry: **Registr práv a povinností** (RPP), **Registr obyvatel** (ROB), **Registr osob** (ROS), **Registr územní identifikace adres a nemovitostí** (RÚIAN) (obrázek 9). Základní registr (ZR) si lze představit jako databázi údajů, o kterých se nepochybuje, tedy úředník je může užít a má v nich právní jistotu (jedná se **referenční údaj**, dále viz doplňující část). V případě nalezení chyby lze takový údaj reklamovat. Pro zvýšení bezpečnosti informací je pro komunikaci užíváno bezvýznamových identifikátorů, zejména důležitým je **agendový identifikátor fyzické osoby** (AIFO). Více informací o celém ekosystému je v doplňující části.

Vzhledem k tomu, že registry obsahují opakovaně potřebné údaje, například jméno, příjmení a datum narození klienta, tak nedává smysl vést takovýto údaj ve všech systémech zvlášť, ale efektivně ho sdílet právě pomocí základního registru. Ve zmíněném případě by to byl registr obyvatel. Kdyby byly všechny státní evidence propojeny a automatizovány, tak pak v případě změny jména by nemuselo být například nutné tuto změnu aktivně hlásit pro získání nového občanského průkazu, ale takovýto průkaz by byl automaticky vyhotoven a předán klientovi.

Obrázek 9 – Ekosystém Informační systému základních registrů



12.2 Registr práv a povinností

Registr práv a povinností, dle zákona přesný název: Základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností (RPP) je **nejdůležitějším základním registrem**, neboť vede zejména oprávnění na přístupy k údajům vedených ve zbývajících základních registrech a agendových informačních systémech. Obsahuje tedy sdružená metadata (data o datech) všech ZR, tak i dalších AIS. Správcem systému RPP je Ministerstvo vnitra.

RPP vede údaje:

- služeb veřejné správy včetně jejich popisů,
- agend a oprávnění k jejich údajům,
- agend a jejich činností,
- orgánů veřejné moci (OVM) a soukromoprávních uživatelů údajů (SPUÚ),
- o agendových informačních systémech a soukromoprávních systémech využívání údajů,
- veřejnoprávních smluv (o výkonu agend v území),
- o právech a povinnostech fyzických a právnických osob.

RPP obsahuje katalogy:

- katalog agend,
- katalog výkonu agend,
- katalog orgánů veřejné moci a soukromoprávních uživatelů údajů,
- katalog informačních systémů veřejné správy a soukromoprávních systémů pro využívání údajů,
- katalog datových typů údajů agendy,
- rejstřík převodu agend,
- katalog služeb veřejné správy, včetně služeb podle jednotné digitální brány (SDG) EU.

RPP poskytuje klíčové funkcionality:

- výdej dat ze ZR podle zákonných předpisů – matice oprávnění,
- evidenci údajů pro výkon veřejné správy,
- evidenci vazeb údajů RPP na právní předpisy, které je vymezují,
- podporu sdílení dat v rámci propojeného datového fondu a veřejného datového fondu,
- komplexní mapu vazeb výkonu veřejné správy, zejména: OVM/SPUÚ, systémy, agendy, činnosti a služby veřejné správy, tzn. jaký úřad, kde a co vykonává, jaké služby poskytuje, na základě, jakých kompetencí, případně veřejnoprávní smlouvy),
- rozhraní pro veřejný přístup k údajům RPP (tj. bez nutnosti přihlášení či registrace).

Otázky k procvičení:

1. V následujícím textu odhalte chyby: „V České republice existují čtyři základní registry: Registr práv a povinností (RPP), Registr osob (ROB), Registr územní identifikace, nemovitostí a adres (RÚIAN).“

Chyby jsou dvě – text hovoří o čtyřech registrech (správně), ale uvádí pouze tři – chybí Registr obyvatel (ROB). Registr osob má zkratku ROS v textu je použita nesprávně zkratka ROB.

2. Jaký je smysl RPP? Co je jeho hlavním obsahem?

Jedná se o metainformační systém – spojuje, vysvětluje a garantuje data tak, aby byla použitelná, srozumitelná, dostupná jak pro klienta, tak dílčí jednotlivé agendové informační systémy. Hlavními částmi jsou údaje, katalogy a zprostředkované funkcionality, viz výše.

12.3 Doplňující část

12.3.1 Ekosystém základních registrů

Nejdůležitějším posláním základních registrů je vedení referenčních údajů s jednoznačně definovanou odpovědností orgánu veřejné moci za jejich správnost (věcnou i časovou). Systém základních registrů tvoří:

- **registr obyvatel** (ROB) spravovaný Ministerstvem vnitra. Obsahuje základní údaje o občanech a cizincích s povolením k pobytu,
- registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci zkráceně též: **registr osob** (ROS) spravovaný Českým statistickým úřadem. Obsahuje zejména údaje o právnických osobách, podnikajících fyzických osobách a nekomerčních subjektech,
- **registr územní identifikace, adres a nemovitostí** (RÚIAN) spravovaný Českým úřadem zeměměřičským a katastrálním. Obsahuje údaje o základních územních a správních prvcích,
- registr agend orgánů veřejné moci a některých práv a povinností zkráceně též: **registr práv a povinností** (RPP) spravovaným Ministerstvem vnitra. Obsahuje referenční údaje o orgánech veřejné moci, soukromoprávních uživatelích údajů, agendách, právech a povinnostech osob a další údaje, které stanoví zákonem č. 111/2009 Sb.

Dalšími částmi systému základních registrů jsou:

- informační systém základních registrů (dále jen „ISZR“) spravovaný Správou základních registrů ISZR je jediným přístupovým rozhraním k základním registrům a zajišťuje publikaci služeb základních registrů (eGON služby), ověřuje oprávnění pro přístup do základních registrů, zaznamenává a ukládá všechny logy do základních registrů,
- informační systém ORG (dále jen „ORG“) spravovaný Úřadem pro ochranu osobních údajů. Zajišťuje zejména ochranu osobních údajů v systému základních registrů, a to prostřednictvím náhrady rodného čísla systémem bezvýznamových identifikátorů. Tyto identifikátory jsou pro jednotlivé agendy specifické a neumožní tak při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v agendě jiné.ORG přiděluje zdrojové identifikátory fyzických osob (ZIFO), generuje agendové identifikátory fyzických osoby (AIFO) pro cílové agendy, zajišťuje převody AIFO jedné agendy na AIFO druhé agendy, komunikuje výhradně a pouze s ISZR.

12.3.2 Správa základních registrů

Správa základních registrů je zřízena podle zákona o základních registrech a zajišťuje zejména:

- provoz a bezpečnost ISZR, Informačního systému sdílené služby (dále jen „ISSS“), ROB, ROS a RPP,
- realizaci vazeb mezi jednotlivými základními registry (dále jen „ZR“), jednotlivými agendovými informačními systémy (dále jen „AIS“), jednotlivými ZR a AIS,
- zpřístupnění referenčních údajů obsažených v ZR a údajů vedených v AIS,
- vedení záznamů o událostech souvisejících s provozováním ISZR.

12.3.3 Klíčové pojmy

- **referenční údaj** – státem garantovaný údaj vedený v některém ze základních registrů, který je označen jako referenční údaj, jehož správnost se při výkonu působnosti orgánu veřejné moci neověřuje,
- **provozní údaj** – jedná se o údaje k referenčním údajům zapisované prostřednictvím informačního systému základních registrů, např. důvod a účel přístupu OVM k údaji vedenému v některém základním registru. Tyto údaje jsou držitelům datových schránek zasílány v pravidelných ročních výpisech o využití automaticky, případně je lze kdykoliv vyžádat na kontaktním místě CzechPOINT či elektronicky přes CzechPOINT@home,
- **matice rolí a oprávnění** – součást RPP. Matice rolí a oprávnění obsahuje role jednotlivých OVM a jejich oprávnění ke konkrétním údajům v základních registrech. Cílem je umožnit oprávněné osobě přístup k údajům a osobě neoprávněné v přístupu zabránit,
- **zdrojový identifikátor fyzické osoby** (ZIFO) - neveřejný identifikátor fyzické osoby, ze kterého nelze dovodit osobní ani jiné údaje o fyzické osobě, jíž byl přiřazen,
- **agendový identifikátor fyzické osoby** (AIFO) - neveřejný identifikátor, který je jednoznačně přiřazen záznamu o fyzické osobě v příslušném agendovém informačním systému nebo základním registru. Je odvozen ze zdrojového identifikátoru fyzické osoby a kódu agendy a je užíván výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen. Z agendového identifikátoru fyzické osoby nelze odvodit zdrojový identifikátor fyzické osoby a nelze z něj ani dovodit osobní nebo jiné údaje o fyzické osobě, jíž byl přiřazen.

12.3.4 Registr práv a povinností

Od zahájení provozu 1. července 2012 prošel ve srovnání s ostatními základními registry nejrozsáhlejším rozvojem.

2012 – 1. července 2012 zahájení provozu. RPP slouží jako rejstřík přístupových práv k datům základních registrů. Vede informace o agendách (zákonech) a činnostech jednotlivých OVM, strukturu údajů v ROB, ROS, RUIAN a oprávnění na tyto údaje, o působnostech OVM v agendě a rozhodnutích o změně referenčních údajů.

2017 – implementace změn podle zákona č. 192/2016 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech. Rozšíření datové domény o rejstřík orgánů veřejné moci a evidenci údajů vedených v agendě. Byla provedena změna procesu registrace agendy, tzn. stanoviska správců údajů, jsou vyžadována před registrací agendy.

2019 – implementace změn podle zákona č. 251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci. Přibývá rejstřík informačních systémů veřejné správy, který nahrazuje původní Informační systém o informačních systémech veřejné správy. Zavádí se evidence adres úřadoven OVM, evidence úkonů na žádost, evidence přenosu výkonu agendy prostřednictvím veřejnoprávních smluv, evidence technické struktury údajů, data RPP je možné čerpat jako Open Data.

2020 – zejména implementace změn podle zákona č. 12/2020 Sb., o právu na digitální službu. Přibývá Katalog služeb a otevřené API (rozhraní pro programování aplikací) katalogu služeb a služeb podle nařízení (EU) č. 2018/1724 o jednotné digitální bráně (SDG).

2021 a 2022 – současná podoba, viz první část této kapitoly.

12.3.5 Odkazy

- Portál ISZR:

https://www.szrcr.cz/cs/

- Veřejné dostupný seznam agend Registru práv a povinností:

https://rpp-ais.egon.gov.cz/gen/agendy-detail/

C:\Users\scharnaglr\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\KK7T13RX\www.szrcr.cz\

13 IS Czech POINT a kontaktní místa veřejné správy

Související právní předpisy: zejména zákon č. 365/2000 Sb., zákon č. 300/2008 Sb., zákon č. 111/2009. Sb., průřezově zákon 12/2020 Sb.

13.1 Czech POINT

Czech Point, první slovo vzniklé přeložením z češtiny, druhé je slovní hrou na anglické slovo bod (i jako kontaktní místo) z názvu **Český Podací Ověřovací Informační Národní Terminál** je jedním ze základních pilířů českého eGovernmentu. Hlavním důvodem vzniku Czech POINTu byla snaha zredukovat přílišnou **byrokracii** ve vztahu občana a veřejné správy, tedy zjednodušit a zlepšit **komunikaci občana se státem** a přiblížit výkon veřejné správy blíže občanovi. Czech POINT je univerzální asistované místo, kde každý občan může získat ověřené výpisy z centrálních registrů a jednotně přistupovat k vybraným službám státu. Splňuje tak dané motto: ***obíhat mají data a ne občan***.

Czech POINT a jeho síť kontaktních míst veřejné správy jsou dnes téměř v každé obci. Díky nim mohou občané na jednom místě získat řadu dokumentů a využít služby, kvůli kterým do té doby museli osobně navštívit několik různých úřadů. Na přítomnost kontaktního místo, na obecním úřadě, či třeba pobočce České pošty, upozorňuje příslušné logo (obrázek 10.)

Obrázek 10 – Logo Czech POINTu

Czech POINT je definován zákonem č. 365/2000 Sb. Dalšími důležitými zákony, bez nichž by Czech POINT nemohl existovat, je zákon č. 300/2008 Sb., a zákon č. 111/20019 Sb. Jednotlivé poskytované služby jsou pak definovány ve speciálních zákonech.

Informační systém **Czech POINT neobsahuje** své žádné **agendové údaje**, proto se o něm hovoří také jako o rozhraní. Smyslem je přenést údaje z ostatních systému ke klientovi, či naopak od klienta údaje dodat do cílových systémů. Systém CzechPOINT tak loguje pouze uskutečněnou událost, kdo a kdy ji provedl a o jaký typ výpisu se jednalo.

Informační systém Czech POINT poskytuje dvě uživatelská rozhraní:

- rozhraní pro **kontaktní místa veřejné správy** (KMVS),
- rozhraní pro úředníky orgánů veřejné moci, tzv. **CzechPOINT@office**

Kontaktní místa veřejné správy jsou zákonem určené orgány veřejné moci (zejm. notáři, krajské úřady, matriční úřady, držitelé poštovní licence (Česká pošta a Hospodářská komora), na žádost obecní úřady, úřady městské části nebo městského obvodu, dále pak vybrané zastupitelské úřadu definované Ministerstvem zahraničních věcí, na žádosti banky, zdravotní pojišťovny, pojišťovny a poskytovatelé univerzálních služeb).

Smyslem tohoto kontaktního místa je poskytnutí občanům a podnikatelům fyzicky (osobně) **asistované služby** (obsluha, např. zaměstnanec na přepážce úřadu klientského místa asistuje u této služby a činí úkony přes technické prostředky klientského centra) jako je žádost o výpisy z veřejných i neveřejných rejstříků a registrů a činí vybraná podání vůči veřejné správě. Tyto služby jsou obecně zpoplatněny dle zákona č. 634/2004 Sb. o správních poplatcích.

Služby poskytované kontaktním místem veřejné správy pro veřejnost lze obecně rozdělit do těchto kategorií:

- **výpisy z informačních systémů veřejné správy** – např. výpis z Rejstříku trestů nebo Katastru nemovitostí, výpis Bodového hodnocení z registru řidičů, výpis z veřejného rejstříku atp.,
- **podání vůči státní správě** – např. ohlášení živnosti do registru živnostenského podnikání,
- **agenda základních registrů** – např. výpisy ze základních registrů, nebo podání žádosti o změnu údajů,
- **agenda datových schránek** – např. žádost o zřízení datové schránky, žádost o zneplatnění přístupových údajů a vydání nových atd.,
- **autorizovaná konverze na žádost a související služby** – tj. převedení listinného dokumentu do elektronické podoby a naopak. Součástí je i služba Úschovny a Centrálního úložiště ověřovacích doložek,
- **agenda zprostředkovaná identifikace osoby** – agenda slouží pro identifikaci účastníků obchodu vůči povinným osobám (jedná se například o registraci hráčů k hazardním hrám, založení podnikatelského účtu, uzavření smlouvy o koupi nemovitosti apod.).

Rozsah poskytovaných služeb na kontaktních místech veřejné správy se odvíjí od aktuálního stavu legislativy. Výpisy v listinné podobě, dále výstupy z informačního systému veřejné správy vydané na KMVS jsou veřejnými listinami.

CzechPOINT@office je neveřejným prostředím pro úředníky orgánů veřejné moci, pro vnitřní potřebu úřadu. Prostřednictvím CzechPOINT@office lze jednak získávat výpisy a opisy z rejstříků a registrů z moci úřední, či provádět autorizovanou konverzi dokumentů z moci úřední. CzechPOINT@office je ale také editačním nástrojem, prostřednictvím kterého lze editovat cílové rejstříky a evidence, např. aktualizace údajů v rámci agendy evidence obyvatel (včetně matričních a soudních úkonů) a agendy evidence přestupků. Každému orgánu veřejné moci jsou zpřístupněny jen takové služby/agendy, ve kterých vykonává působnost. K ostatním poskytovaným službám nemá přístup.

Otázky k procvičení:

1. Jaké je rozdíl mezi KMVS a CzechPoint@office?

Obojí jsou rozhraními systému Czech POINT, avšak zatímco kontaktní místo veřejné správy zprostředkovává asistované služby pro občany a podnikatele, tak CzechPoint@office je interním rozhraním pro úřady a jejich pracovníky.

2. Je možné na KMVS vyžít službu autorizované konverze?

Ano, služba je na všech KMVS k dispozici – služba je zpoplatněna, viz kapitola 16.

13.2 Doplňující část

13.2.1 Odkazy

- Portál Czech POINT:

https://www.czechpoint.cz/public/

14 Informační systém datových schránek

Související právní předpisy: zejména zákon č. 300/2008 Sb., průřezově zákon č. 365/2000 Sb., zákon číslo 181/2014 Sb.

14.1 Informační systém datových schránek

Informační systém datových schránek (ISDS) je ISVS, který nabízí elektronickou alternativu k doručování v listinné podobě. Správcem tohoto informačního systému je Ministerstvo vnitra a provozovatelem je držitel poštovní licence, tj. Česká pošta, s. p.

Datová schránka (DS) je elektronické úložiště, které je určeno k doručování orgány veřejné moci, k provádění úkonů vůči orgánům veřejné moci a k dodávání dokumentů fyzických, podnikajících fyzických osob a právnických osob. Datové schránky vznikly a jsou vedeny na základě zákona č. 300/2008 Sb.

Datovou zprávu lze podle zákona č. 300/2008 Sb. zjednodušeně charakterizovat jako obálku, obsahující předepsané elementy (metadata) a přílohy, které do ní vkládá odesílatel. Obálka je v okamžiku podání opatřena eleketronickou značkou Ministerstva vnitra a kvalifikovaným časovým razítkem. Technicky je datová zpráva ISDS ve formátu ZFO, což jsou komprimovaná (zazipovaná) data značkovacího jazyka XML (Extensible Markup Langauge). Fikce podpisu (pravidlo, že datová zpráva se považuje za podepsanou odesílatelem) se vztahuje k celé datové zprávě včetně metadat. K prokazování je tedy nutné vždy dokládat celý soubor ZFO, tedy datovou zprávu včetně tzv. košilky.

Obrázek 11 – Logo datových schránek

Hlavní typy datových schránek jsou:

- datová schránka fyzické osoby,
- datová schránka podnikající fyzické osoby,
- datová schránka právnické osoby,
- datová schránka orgánu veřejné moci.

Datová schránka je **ze zákona** založena všem orgánům veřejné moci, právnickým osobám, které jsou zapsány v obchodním rejstříku a podnikajícím fyzickým osobám typu: advokát, daňový poradce, insolvenční správce a statutární auditor, znalec, soudní tlumočník a soudnímu překladatel.

Datovou schránku na žádost si mohou zřídit fyzické osoby, podnikající fyzické osoby, právnické osoby, které nejsou zapsány v obchodním rejstříku a další datovou schránku si pro své odůvodněné účely mohou zřídit orgány veřejné moci.

K roku 2023 je plánována změna, kdy se rozšiřuje seznam o založení schránek dle zákona na všechny právnické osoby a podnikající fyzické osoby v registru osob (ROS). Téže byla plánována změna, kdy bude založena datová schránka fyzické osobě, pokud se přihlásí k službám

eGovernmentu pomocí prostředku pro elektronickou identifikaci s úrovní záruky značná nebo vysoká, tento bod byl však ke konci roku odložen.

Je běžné a správné, že občan může mít několik datových schránek, a to, pokud se vyskytuje v dalších rolích, kdy je datová schránka umožněna – například DS pro fyzickou osobu, ale občan je zároveň i podnikatelem a advokátem. Optimálně by datové zprávy měly být odesílány z a přijímány do DS odpovídají roli vystupování daného uživatele. Tedy podnikatelské záležitosti do DS právnické osoby, osobní záležitosti směrem k eGovermentu do DS fyzické osoby) Dle současné judikatury je v nestandardních případech je možné doručení do DS jiné role, zde se však ale neuplatní 10denní fikce doručení, lhůta začíná běžet teprve až po přihlášení se do dané datové schránky.

Zřízení datové schránky ze zákona se provádí bezodkladně po získání informace o vzniku nového subjektu**.** Naopak **zřízení na žádost** lze provést:

- **osobně** na Kontaktním místě veřejné správy (Czech POINT),
- **podáním** v listinné podobě s úředně ověřeným podpisem žadatele,
- **online** v prostředí klientského portálu ISDS, nebo v Portálu občana, pokud je užito identifikačního prostředku se zárukou značná nebo vysoká (např. eObčanka, prostředky bankovní identity, mobilní klič eGovernmentu).

Hlavními **přínosy datových schránek** je:

- **Věrohodnost** – odeslaná datová zpráva má stejné právní účinky jako podepsaný dokument v listinné podobě. Okamžik doručení je pro adresáta OVM okamžiku dodání do DS adresáta. Pro adresáta fyzická osoba okamžikem, kdy se do DS přihlásí osoba, která má příslušné oprávnění s touto DS a jejím obsahem nakládat. Naopak v absenci přihlášení se po deseti dnech zpráva považuje za doručenou.
- **Náklady** – zejm. na straně občané, kdy s veřejnou správou komunikují bezplatně. Autorizovaná konverze (viz kapitola 16) je však zpoplatněna.
- **Možnost komunikovat odkudkoli** – postačuje připojení k internetu. OVM mají povinnost doručovat do DS, s výjimkou, kdy osoba výslovně požádá o změnu způsobu doručování, pokud zaslání do DS není technicky možné, či právní předpis deklaruje jiný způsob doručení.
- **Rychlost** – mnohanásobně rychlejší oproti listinné korespondenci.
- **Autentizace** – Vlastnictvím DS lze čerpat vyšší úroveň služeb, kdy výstupem je dokument.
- **Možnost komunikace se soukromoprávními subjekty** – Možnost přijímat poštovní datové zprávy (PDZ) soukromoprávních subjektů (např. banky, pojišťovny, energetické společnosti).

Otázky k procvičení:

1. Je komunikace mezi fyzickou osobu a veřejnou správou pomocí datové schránky zpoplatněna?

Není, za komunikaci fyzická osoba žádnou částku nemusí uhrazovat.

2. Máte zřízenou datovou schránku? Proč ano, proč případně ne? Jaký přínos vidíte v jejím užívání, či naopak v absenci jejího užívání?

Necháno na kritickém zamyšlení čtenáře. Jako osnovu lze vzít přínosy, které lze kriticky zhodnotit.

14.2 Doplňující část

14.2.1 Odkazy

- Portál informačního systému datových schránek:

https://info.mojedatovaschranka.cz/info/cs/

15 Portál veřejné správy a portál občana

Související právní předpisy: zejména zákon č. 365/2000 Sb., zákon č. 12/2020 Sb., průřezově zákon číslo 181/2014 Sb.

15.1 Portál veřejné správy

Portál veřejné správy (PVS) je informační systém veřejné správy ukotvený zákona č. 365/2000 Sb. Portál je provozován se záměrem usnadnit široké veřejnosti, státní správě a samosprávě, státním i soukromým organizacím, včetně podnikatelů, živnostníků a cizinců vzdálený přístup k informacím a službám celé veřejné správy. Správcem PVS je Ministerstvo vnitra. PVS zajišťuje komunikaci s veřejnými orgány prostřednictvím datových schránek, prostřednictvím přístupu se zaručenou identitou do informačních systémů veřejné správy nebo elektronických aplikací spravovaných těmito veřejnými orgány a prostřednictvím kontaktních míst veřejné správy.

PVS poskytuje přístup do jednotlivých sekcí:

- **Přístup do Portálu občana** – transakční části PVS, více viz níže.
- **Služby veřejné správy** – Cílem katalogu je informovat klienta o dostupných službách veřejné správy, jejich benefitech či způsobech vyřízení. Řada položek je také v anglickém znění.
- **Životní události** – Průvodce životními událostmi jsou jednoduché návody, které uživatelům pomohou lépe se orientovat ve službách veřejné správy, např. co vše zařídit pro svatbu/manželství. Díky nim se klient dozví o povinnostech a budete vědět, na co má právo.
- **O životě v ČR** – Sekce poskytuje strukturované a srozumitelné informace v českém i anglickém jazyce o životě a podnikání v ČR. Je určena pro občany, podnikatele a cizince.
- **Časté dotazy** – Obsahuje odpovědi na nejčastější dotazy k možnostem využívání on-line služeb, Portálu občana, PVS, ale také datovým schránkám nebo elektronické identitě obecně.
- **Kam dál** je rozcestníkem pro dalšími podsekcí Portálu veřejné správy, zahrnuje např.:
    - Věstníky – což jsou publikační sbírky předpisů a metodických pokynů vydávané ústředními správními úřady a dalšími institucemi dle zákona č. 365/2000 Sb. V rámci Portálu veřejné správy probíhá jejich zveřejňování, přičemž každý věstník obsahuje informaci o tom, která instituce jej zveřejnila a od kterého data je předpis nebo metodický pokyn účinný,
    - Povinně zveřejňované informace – obsahují veřejné informace, které jsou publikovány jednotlivými orgány veřejné správy na základě různých legislativních předpisů.
    - Nepotřebný nemovitý majetek – zahrnuje aktuální nabídku nepotřebného nemovitého majetku státu.
    - Formuláře pro registr smluv – prostřednictvím kterých lze snadno připravit a odeslat informace ke zveřejnění v registru smluv. Odeslání probíhá přes datové schránky subjektu.
    - Formuláře pro úřady – Úřady a jiné zákonné subjekty mohou využít nabídku elektronických formulářů pro výkon svých agend a naplnění legislativních povinností. Odeslání probíhá přes datové schránky subjektu.

- Formuláře pro občany a podnikatele – Občané a podnikatelé, kteří jsou vlastníky příslušného typu datové schránky, mohou na Portálu veřejné správy zažádat o elektronické výpisy z nabídky registrů státní správy.
- Rejstřík orgánů veřejné moci – ve formě přehledného seznam s možností filtrování.
- Seznam držitelů datových schránek – obsahuje aktuální údaje o držitelích datových schránek a identifikační údaje pro všechny aktuálně zpřístupněné datové schránky s výjimkou těch fyzických osob, které požádaly o vymazání z tohoto seznamu.
- Digitální úřad – Nabízí snadný přístup k informacím o webech a projektech eGovernmentu.

15.2 Portál občana

Portál občana (POb) je branou k elektronickým službám státu, samoobslužným místem pro bezpečnou a důvěrnou komunikaci mezi občanem a státem. Na rozdíl od PVS, který funguje jako hlavní informační rozcestník, POb je transakční částí, zajišťující osobní přístup prostřednictvím přihlášení uživatele.

Portál občana byl nasazen do ověřovacího provozu během roku 2018. Na základě digitalizace služeb veřejné správy je Portál občana **centrálním bodem** přístupu občana k **digitálním službám** eGovernmentu. To však neznamená, že všechny služby musí být přímo na Portálu občana vystaveny. Portál občana má být přehledný a obsahovat přímou pouze základní a esenciální služby veřejné správy. Méně užívané, služby by pak měly být odkazovány do příslušeného agendově specifického portálu. Pro zvýšení komfortu uživatele se v rámci federace portálů veřejné správy nemusí opětovně přihlašovat – princip Single Sign-On (SSO).

Přihlašování probíhá standardně pomocí identifikačního **prostředku elektronické identity**, (např. eObčanka, prostředky bankovní identity, mobilní klič eGovernmentu). Vybrané služby, které Portál občana po přihlášení obsahujem, jsou například:

- výpis bodového hodnocení řidiče,
- založení datové schránky,
- archivace datových zpráv,
- výpis z rejstříku trestů,
- výpis z živnostenského rejstříku,
- informace z katastru nemovitostí,
- notifikace platnosti dokladů,
- výpis z registru obyvatel,
- přístup k podání daňového přiznání na portálu MOJE daně,
- přístup k eReceptu,
- přístup do ePortálu ČSSZ pro přehled o důchodovém pojištění,
- přístup k portálům krajů, měst a obcí,

Otázky k procvičení:

1. Jaké je rozdíl mezi Portálem veřejné správy a Portálem občana?

Zatímco Portál veřejné správy poskytuje zejména obecné nepersonalizované informace, tak Portál občana je vystaven jako samobslužný portál obsahující transakční služby přihlášených uživatelů.

2. Jakým způsobem se můžete přihlásit do Portálu občana a čerpat jeho služby?

Pomocí identity občana, resp. prostředku elektronické identity jako je eObčanka, či mobilní klíč eGovernmentu.

15.3 Doplňující část

15.3.1 Odkazy

- Portál veřejné správy:

https://www.portal.gov.cz/

- Portál občana:

https://obcan.portal.gov.cz/

16 Elektronická komunikace VS

Související právní předpisy: zejména zákon č. 300/2008 Sb., zákon č. 499/2005 Sb., zákon č. 297/2016 Sb., nařízení EU č. 910/2014, průřezově zákon č. 365/2000 Sb.

16.1 Autorizovaná konverze dokumentů

Nejdůležitějším předmětem komunikace je adresné předávání informací, v rámci veřejné správy nejčastěji formou evidovaných (číslem jednacím odesílatele) dokumentů. Dokumenty – jak v **listinné**, tak **elektronické** formě mají **shodnou platnost**.

K vzájemnému převodu z jedné formy do druhé slouží proces konverze. Proces splňující státem definované parametry se nazývá **autorizovaná konverze** (zákon č. 300/2008 Sb.), v tomto případě mají i po převodu dle zákona stejnou platnost, konverzí se však nepotvrzuje správnost a pravdivost dokumentu a jeho údajů. Autorizována konverze může být z **moci úřední** (provádí OVM pro výkon své působnosti) nebo **na žádost** jako služba pro veřejnost (zde se hradí správní poplatek) prováděna KMVS či advokátem.

16.2 Elektronická spisová služba

Předepsaným prostředkem pro komunikaci mezi orgány veřejné moci (výkon spisové služby), v souladu se zákonem č. 499/2004 Sb. je **elektronická spisová služba**. Výkon spisové služby spočívá v zajištění odborné správy dokumentů vzniklých z činnosti původce. Metodickou pomoc ke spisové službě poskytuje Národní archiv a Státní oblastní archivy.

Základní povinností veřejnoprávních původců je vykonávat spisovou službu v souladu se zákonem a jeho prováděcími předpisy (vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby a Národní standard pro elektronické systémy spisové služby), zejména:

- **vydat spisový řád**, kterým upraví svůj výkon spisové služby, jako je označovat a ukládat dokumenty podle spisového a skartačního plánu,
- **vyřazovat dokumenty** způsobem stanoveným zákonem prostřednictvím příslušného archivu,
- **vykonávat spisovou službu**, pokud vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, musí mít být tento systém v souladu s **národním standardem pro elektronické systémy spisové služby.**

Práce s dokumenty je tak standardizována, což zvyšuje důvěru a efektivitu práce s dokumenty. Mezi klíčové principy patří zejm. schopnost práce jak s listinnými, tak digitálními dokumenty, automatizace příjmu a odesíláním dokumentů přes ISDS převádět dokumenty do PDF/A formátu či dalších předepsaných formátů zaručující integritu dat (více viz doplňková část).

16.3 Elektronický podpis, certifikáty aj. a jejich souvislosti

Základní přehled termínů certifikát, elektronický podpis, elektronická pečeť, elektronické časové razítko a jejich definice je obsažen v tabulce níže.

Tabulka 11 – Elektronický podpis, certifikáty a souvislosti

Termín	Definice
Certifikát	Je potvrzení, které spojuje data pro ověřování platnosti elektronických podpisů s určitou fyzickou osobou (potvrzuje alespoň její jméno nebo pseudonym) a data pro ověřování platnosti elektronických pečetí s určitou právnickou osobou (potvrzuje její název). Certifikát vydá po ověření totožnosti žadatele tzv. certifikační autorita, které se důvěřuje.
Elektronický podpis	Jsou data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující fyzická osoba používá k podepsání. Elektronický podpis je elektronickou alternativou vlastnoručního podpisu. Je jednoznačně spojen s podepisující osobou a umožňuje její identifikaci. Zároveň zajišťuje nepopíratelnost, tedy podepisující osoba nemůže popřít, že dokument podepsala. Podpis je k datům připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.
Elektronická pečeť	Jsou data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu. Hlavním rozdílem oproti elektronickému podpisu je to, že certifikát pro elektronickou pečeť se vydává výhradně právnickým osobám (nemůže být vydán fyzické osobě). Typicky se používá u dokumentů, které jsou výsledkem automatizovaného zpracování (např. výpisy z informačních systémů). Elektronická pečeť by měla sloužit jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytovat jistotu o původu a integritě dokumentu.
Elektronické časové razítko	Jsou data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku. Pomocí časového razítka lze zajistit a udržovat digitální kontinuitu elektronicky podepsaného či opečetěného dokumentu. Platnost elektronického podpisu a pečeti (resp. certifikátu) je časově omezena (zpravidla na jeden rok). Před vypršením platnosti certifikátu elektronického podpisu nebo pečeti lze připojit k dokumentu elektronické časové razítko, které zaručí prodloužení platnosti o dobu, na jakou bylo časové razítko vydáno (obvykle na tři nebo pět let). V případě nutnosti opětovného prodloužení digitální kontinuity se použije další časové razítko.

16.4 Služby vytvářející důvěru

Kvalifikované služby vytvářející důvěru jsou oprávněny poskytovat jak organizace, tak i fyzické osoby. Aby poskytovatel mohl poskytovat kvalifikované služby vytvářející důvěru, musí splnit podmínky stanovené nařízením eIDAS a zákonem č. 297/2016 Sb. Poskytovatelé služeb vytvářejících důvěru mají odpovědnost za škodu při provozování služeb vytvářejících důvěru.

16.5 Online spolupráce

Dnešní týmová spolupráce stále více možností sdílené on-line komunikace. Význam této on-line komunikace v posledních letech ovlivnil covid-19 a následná práce z domova (tzv. home office). Mezi hlavní nástroje patří: Microsoft Teams, CISCO Webex, Google Meet, WhatsApp, Zoom či Skype.

Otázky k procvičení:

1. Může fyzická osoba získat a pracovat s elektronickou pečetí?

Nikoliv, elektronická pečeť slouží právnickým osobám. V praxi samozřejmě s možností pečetit pracuje typicky zprostředkovaně fyzická osoba, neboť právnická osoba „nemá ruce a nožičky“.

2. Jakou platnost má elektronický dokument vzniklý autorizovanou konverzí z listinného dokumentu? Jak by tomu bylo při autorizované konverzi v opačném směru?

V obou případech stejnou. Tedy v rámci práva České republiky si jsou rovnocenné.

16.6 Doplňující část

16.6.1 Klíčové principy práce s dokumenty

- Výkon spisové služby je podporován programovými prostředky, kterými je elektronický systém spisové služby, případně samostatné evidence dokumentů v elektronické podobě. Tyto nástroje zastřešují správu dokumentů v analogové (zpravidla listinné) podobě i dokumentů v digitální podobě (elektronické).
- Tyto prostředky musí zajistit mimo jiné automatizovaný příjem dokumentů ze systému ISDS, doručovaných na elektronickou adresu podatelny (e-mailová adresa podatelny) a případně z dalších systémů. Dalším zdrojem elektronických dokumentů jsou centrální a další informační systémy (např. systém MS2014+, eKLEP, ISRB Technologické agentury ČR a další), kde tato automatizovaná vazba obvykle neexistuje, ale jejich výstupy podléhají evidenci dokumentů, jsou součástí spisové služby původce.
- Nakládání s e-maily z běžné komunikace má řešit spisový řád organizace. Pokud mají e-maily úřední charakter (ve smyslu činnosti původce), musí být označeny a zaevidovány. E-maily doručené na elektronickou adresu podatelny je potřeba vždy pokládat za "úřední."
- Všechny dokumenty je nutné převádět do formátu PDF/A či dalších předepsaných formátů (podrobněji viz dále). Převod dokumentu je možné provádět automatizovaně, bez porovnání každého vstupu a výstupu převodu fyzickou osobou. Záznamy a dokumenty je nutné převádět při jejich vyřízení (uzavření spisu), nejpozději před uložením do spisovny. Vždy musí obsahovat podpis a časové razítko, ovšem vzhledem k tomu, že hash dokumentu je zaznamenán v transakčním protokolu, jehož denní dávka je opatřena elektronickou značkou a časovým razítkem, lze povinnost opatření doložkou, elektronickým podpisem a časovým razítkem realizovat prostřednictvím transakčního protokolu – pokud bude zaručeno trvalé spojení dokumentu s doložkou i v případě exportu mimo elektronický systém spisové služby. Tato možnost ale neplatí pro odesílané dokumenty.
- V případě doručování dokumentů obsahujících úkony orgánů veřejné moci vůči adresátům veřejné moci se pro náležitosti těchto úkonů uplatní procesní předpisy (občanský soudní řád, správní řád). Ty požadují vesměs opatřit úkony orgánů veřejné moci podpisem. Zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce pak stanovuje obecná pravidla stran výběru konkrétního typu elektronického podpisu. Dokumenty (právní jednání) od orgánů veřejné moci, u kterých je stanoven požadavek podpisu, mají být podepsány kvalifikovaným elektronickým podpisem a opatřeny kvalifikovaným elektronickým časovým razítkem.. Tyto normy se uplatní přednostně před obecným pravidlem v zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (úkon učiněný osobou oprávněnou k přístupu do datové schránky či pověřenou osobou má stejné účinky jako úkon učiněný písemně a podepsaný). Opatření úkonů orgánů veřejné moci adresovaných adresátům veřejné moci kvalifikovaným elektronickým podpisem je nezbytné i z toho důvodu, že adresáti si nemohou dokument, který není opatřený elektronickým podpisem, nechat autorizovaně zkonvertovat. V případě výkonu spisové služby v elektronické podobě v elektronickém systému

spisové služby musí tedy fyzická osoba určeného původce vždy disponovat kvalifikovaným elektronickým podpisem.

- Neexistuje povinnost digitalizovat např. všechny doručené analogové dokumenty, nicméně vyhláška uvádí, že: „…zpravidla převede doručený dokument v analogové podobě…".
- Výstup z autorizované konverze nebo převodu dokumentu podle § 69a archivního zákona není originálem. V případě převodu podle § 69a zákona č. 499/2004 Sb., o archivnictví a spisové službě, má výstup právní účinky ověřené kopie. V případě autorizované konverze má výstup z konverze stejné právní účinky jako předložení originálu.
- Jestliže veřejnoprávní původce poškodí nebo zničí archiválii, nebo dokument, nevykonává spisovou službu podle § 63 zákona č. 499/2004 Sb., o archivnictví a spisové službě, nevydá spisový řád a spisový a skartační plán, neoznačuje dokumenty spisovými znaky, skartačními znaky a skartačními lhůtami, nedodržuje stavebně technické podmínky pro ukládání dokumentů a neukládá dokumenty podle spisového a skartačního plánu, dopouští se správního deliktu, za který mu může být ve správním řízení uložena pokuta do výše 200 tisíc Kč.

Elektronická spisová služba musí v souladu s vyhláškou č. 259/2012 Sb., o podrobnostech výkonu spisové služby a v souladu s Národním standardem pro elektronický systém spisové služby splňovat, mimo jiné, zejména parametry: Přijímání příchozích dokumentů, Napojení na ISDS, Kontrola připojených certifikátů, časových razítek, pečetí a podpisů, Stanovení skartačního znaku a skartační lhůty, Sdružování dokumentů do spisů, Procesy nad dokumenty: vznik, schválení, distribuce (oběh), odeslání dokumentu, podepsání dokumentu, Ukládání dokumentů a spisů do spisovny, Šablony dokumentů, Auditní logování operací, tvorba a ukládání transakčních protokolů, Historizace změn, a Evidence uživatelů a stanovení rolí a oprávnění.

16.6.2 Právní rámec elektronické spisové služby

Ministerstvo vnitra ve Věstníku MV, částka 57/2017, zveřejnilo nový národní standard pro elektronické systémy spisové služby (dále jen „NESSS"). Nové znění NESSS bylo upraveno na základě praktických zkušeností původců i dodavatelů elektronických systémů spisové služby. Zároveň byla provedena celková revize původního národního standardu, která spočívala v posouzení textu a v odstranění tzv. doporučených (nepovinných) požadavků a duplicitních ustanovení.

V rámci této novelizace bylo provedeno začlenění popisu rozhraní na propojení systémů spravujících dokumenty (nového schématu XML) a došlo také ke zpřesnění schémata XML pro předávání metadat dokumentů (analogových i digitálních) k trvalému uložení do archivu jako součásti datového balíčku SIP. Nový NSESSS již také obsahuje upravené postupy pro elektronické podepisování tak, aby vše bylo v souladu s nařízením EP a Rady (EU) č. 910/2014 ze dne 23. července 2014 (eIDAS) a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

Napojení na ISDS: pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby (dále jen "eSSL"), je příjem datových zpráv součástí eSSL nebo na něj má automatizovanou vazbu. eSSL umožňuje přijímat a odesílat datové

zprávy (dokumenty) prostřednictvím ISDS. Toto je ustanoveno § 17 odst. 1 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, a je to požadavek vyplývající z kapitoly 6.6.1 NSESSS.

Odesílání dokumentů v elektronické podobě: V souladu s § 23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, odesílaný dokument v digitální podobě musí být ve výstupním datovém formátu, pokud je pro daný druh komponenty takový formát stanoven:

- pro statické textové dokumenty a statické kombinované textové a obrazové dokumenty - PDF/A, ISO 19005 (reálně jde o ISO 19005, ISO 19005-1 a ISO 19005-3, tj. PDF/A-1 až PDF/A-3.),
- pro statické obrazové dokumenty - PNG, ISO/IEC 15948; TIF/TIFF, revize 6 – nekomprimovaný; JPEG/JFIF, ISO/IEC 10918,
- pro dynamické obrazové dokumenty - MPEG-2, ISO/IEC 13818; MPEG-1, ISO/IEC 11172); GIF,
- pro zvukové dokumenty - MPEG-1 Audio Layer II nebo MPEG-2 Audio Layer II (MP2); MPEG-1 Audio Layer III nebo MPEG-2 Audio Layer III (MP3); WAV s PCM modulací,
- pro databáze - XML, kde součástí předávaného dokumentu v datovém formátu XML je popis jeho struktury pomocí schématu XML nebo DTD, o kterém veřejnoprávní původce vede dokumentaci.

Pro ostatní druhy komponent není datový formát stanoven. Předepsané formáty musí být použity také pro všechny dokumenty ukládané do spisovny v digitální podobě.

16.6.3 Elektronické podpisy, časová razítka a další detailněji

Při komunikaci v rámci orgánů veřejné moci se požívají elektronické podpisy a časová razítka. Spisový řád každého orgánu musí obsahovat podmínky podepisování včetně podmínek používání kvalifikovaného elektronického podpisu, kvalifikované elektronické pečetě a kvalifikovaného elektronického časového razítka a podmínky používání úředních razítek. Systém eSSL musí umět připojit k dokumentu elektronický podpis nebo elektronickou pečeť a kvalifikované elektronické časové razítko.

Elektronický podpis – V případě, že dokument má být odeslán, musí být opatřen elektronickým podpisem nebo elektronickou pečetí a kvalifikovaným elektronickým časovým razítkem dle příslušné specifikace ETSI – v případě PDF standard PAdES, v případě XML XAdES. Takto definované požadavky stanovuje v § 65 odst. 4, § 65 odst. 7, § 65 odst. 8 zákona č. 499/2004 Sb., o archivnictví a spisové službě v § 17 odst. 1 vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, NSESSS v kapitole 10.7.9 a § 5 až 11 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (zákon o službách vytvářejících důvěru).

Elektronické podpisy a další „autentizační prvky“ definuje od 1. 7. 2016 nařízení EP 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 (nařízení eIDAS). Před účinností nařízení eIDAS definoval elektronické podpisy a další „autentizační prvky“ zákon č. 227/2000 Sb., o elektronickém podpisu.

Zákon o elektronickém podpisu byl k 19. září 2016 zrušen zákonem č. 297/2016 Sb., o službách vytvářejících důvěru. Jedná se o adaptační právní předpis, kterým se adaptuje český právní řád na

nařízení eIDAS a to konkrétně na oblast služeb vytvářejících důvěru. Zákon o službách vytvářejících důvěru upravuje zejména pravidla používání elektronického podpisu, pečeti, časového razítka v České republice (tj. např. pro jaký typ právního jednání by se měl použít jaký typ elektronického podpisu). V souvislosti s tímto zákonem byl rovněž přijat zákon č. 298/2016 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru.

Definice dle eIDAS:

- **Elektronický podpis**: data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena, a která podepisující osoba používá k podepsání.
- **Zaručený elektronický podpis**: elektronický podpis, který je jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby, je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou a je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.
- **Kvalifikovaný elektronický podpis**: zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.
- **Elektronická pečeť**: data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.
- **Zaručená elektronická pečeť**: elektronická pečeť, která je jednoznačně spojena s pečetící (právnickou) osobou, umožňuje identifikaci pečetící (právnické) osoby, je vytvořena pomocí dat pro vytváření elektronických pečetí, kterou může pečetící osoba s vysokou úrovní důvěry použít k vytváření elektronické pečeti pod svou kontrolou a je k datům, ke kterým se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.
- **Kvalifikovaná elektronická pečeť**: zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.

Podle zákona o službách vytvářejících důvěru se **uznávaným elektronickým podpisem** rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis. Samotný elektronický dokument podepsaný kvalifikovaným elektronickým podpisem je možné doručit libovolným způsobem a je zcela rovnocenný listině s vlastnoručním podpisem (viz článek 25.2 nařízení eIDAS).

K projevu vůle fyzické osoby má podle nařízení eIDAS sloužit elektronický podpis viz definice, kdy elektronickým podpisem se rozumí data v elektronické podobě, […] která podepisující osoba používá k podepsání. Elektronický podpis je určen pro fyzické osoby (plyne z definice podepisující osoby). Pokud je dokument podepsán zaručeným elektronickým podpisem či kvalifikovaným elektronickým podpisem, je možné následně detektovat změnu podepsaných dat (pokud někdo např. záměrně upraví podepsaný elektronický dokument).

Certifikáty – elektronické podpisy, které se uznávají při komunikaci s veřejnou správou, musejí být založeny na kvalifikovaných certifikátech pro elektronické podpisy (pro tyto podpisy se používá

zkratka uznávané elektronické podpisy). Technologie elektronických podpisů založených na certifikátech využívá principů asymetrické kryptografie, kdy existují dva páry klíčů – soukromý klíč a veřejný klíč. Soukromý klíč si musí podepisující osoba chránit, neboť pomocí soukromého klíče se vytváří elektronický podpis. Naopak veřejný klíč musí mít k dispozici osoba, která chce následně elektronický podpis ověřit. Veřejný klíč je součástí certifikátu, který rovněž obsahuje údaje o podepisující osobě (umožňuje tak ověřit její identitu, alespoň jméno) a dále také např. o autoritě, která certifikát vydala. V rámci elektronického podepisování a ověřování se používají také tzv. hash algoritmy, což jsou jednocestné funkce, pomocí kterých lze vypočítat otisk dat. Tento otisk dat se následně zašifruje soukromým klíčem a tak vlastně vznikne elektronický podpis.

Elektronická pečeť má sloužit jako důkaz toho, že elektronický dokument vydala určitá právnická osoba, a poskytovat jistotu o původu a integritě dokumentu. Pečetící osobou může být pouze právnická osoba (plyne z definice pečetící osoby). Podobně, pokud je dokument opečetěn zaručenou či kvalifikovanou elektronickou pečetí, je možné následně detektovat změnu opečetěných dat (pokud někdo např. záměrně upraví elektronický dokument opatřený elektronickou pečetí). Elektronické pečetě se zpravidla používají jako potvrzení zprávy vytvořené podatelnou. Využívá se stejných principů, jako u technologie elektronických podpisů založených na certifikátech. Pro dokument opatřený kvalifikovanou elektronickou pečetí platí domněnka integrity dat a správnosti původu dokumentu, se kterým je kvalifikovaná elektronická pečeť spojena.

Elektronické časové razítko – Kvalifikované elektronické časové razítko je definováno od 1. 7. 2016 nařízením eIDAS. Před účinností eIDAS definoval časová razítka zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Nyní je tento zákon nově nahrazen zákonem o službách vytvářejících důvěru.

Definice Kvalifikovaného elektronického časového razítka:

- Nařízení eIDAS: Data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku. Zároveň musí spojovat datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat, musí být založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem a musí být podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.
- Kvalifikované elektronické časové razítko poskytuje důkaz o existenci dat, se kterými je spojeno, v čase (např. o existenci elektronického dokumentu ke konkrétnímu časovému okamžiku). Používá se zejména v souvislosti s elektronickým podepisováním, resp. pečetěním.

Dle nařízení eIDAS:

- Pro elektronický dokument opatřený kvalifikovaným elektronickým časovým razítkem platí domněnka správnosti data a času, které udává, a integrity elektronického dokumentu.
- Elektronickému časovému razítku nesmějí být upírány právní účinky a nesmí být odmítáno jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické časové razítko.
- Kvalifikované elektronické časové razítko vydané v jednom členském státě se uznává jako kvalifikované elektronické časové razítko ve všech členských státech EU.

Nařízení eIDAS rozlišuje „obyčejné“ elektronické časové razítko a kvalifikované elektronické časové razítko. Na kvalifikovaná elektronická časová razítka nařízení eIDAS klade samozřejmě větší požadavky. Použitím elektronických časových razítek lze zajistit digitální kontinuitu podepsaných/označených dokumentů. Podle zákona o službách vytvářejících důvěru, se elektronicky podepsané či opečetěné dokumenty veřejné správy musejí vždy opatřit kvalifikovaným elektronickým časovým razítkem.

16.6.4 Služby vytvářející důvěru

Kvalifikované služby vytvářející důvěru jsou oprávněny poskytovat jak organizace, tak i fyzické osoby. Aby poskytovatel mohl poskytovat kvalifikované služby vytvářející důvěru, musí splnit podmínky stanovené nařízením eIDAS a zákonem o službách vytvářejících důvěru. MV ČR jakožto orgán dohledu udělí na žádost poskytovateli a jeho službám kvalifikovaný status, v rámci kontroly, zda poskytovatel splňuje podmínky nařízení eIDAS a zákona o službách vytvářejících důvěru, musí poskytovatel předložit zprávu o posouzení shody zpracovanou subjektem posuzování shody, který je akreditován. Poskytovatelé služeb vytvářejících důvěru mají odpovědnost za škodu při provozování služeb vytvářejících důvěru.

16.6.5 Odkazy

- Autorizovaná konverze na portálu Czech POINT:

https://www.czechpoint.cz/public/verejnost/autorizovana-konverze/

- Národní standard pro elektronické systémy spisové služby:

https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx

17 Centrální místo služeb, komunikační infrastruktura veřejné správy a radiokomunikační systém PEGAS

Související právní předpisy: zejména zákon č. 365/2000 Sb., směrnice EU č. 2016/1148, průřezově zákon č. 181/2014 Sb.

17.1 Centrální místo služeb

Centrální místo služeb je systém, pro systematické propojení informačních systémů veřejné správy a sdílení dat a služeb těchto systémů jak mezi sebou, tak i v definovaných případech se soukromým sektorem, zejm. pak soukromoprávní uživatelé údajů (SPUÚ).

Zákon č. 365/2000 Sb. zavedl povinnost publikovat služby ISVS jednotlivým klientům prostřednictvím **Centrálního místa služeb** (CMS)**,** které je součástí **Komunikační infrastruktury veřejné správy** (KIVS). CMS v kombinaci s KIVS zavádí pro jednotlivé orgány veřejné správy bezpečnou, od internetu oddělenou, komunikační infrastrukturu poskytující:

- 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 službám ISVS určeným pro koncové klienty VS ze sítě internet.

Centrální místo služeb / Komunikační infrastrukturu veřejné správy můžeme tak nazvat **privátní sítí pro výkon veřejné správy všech subjektů** – tedy jak orgánů veřejné správy (OVS), tak i soukromoprávních uživatelů údajů (SPUÚ) a dále umožnit bezpečné síťové prostředí pro zajištění komunikace a interoperability v rámci EU.

CMS/KIVS jako privátní síť veřejné správy využívá dedikovaných resp. pronajatých síťových prostředků pro bezpečné propojení úředníků orgánů veřejné správy (OVS) a SPUÚ pracujících v agendách veřejné správy s jejich vzdálenými agendovými informačními systémy, pro bezpečné síťové propojení agendových systémů navzájem a pro bezpečný přístup jednotlivých OVS do internetu. OVS a SPUÚ přistupují k CMS jedním ze čtyř možných způsobů:

- Krajská síť (Vysočina, Plzeňský, Karlovarský, Zlínský, Pardubický kraj).
- Metropolitních síť okresních měst (aktuálně cca 77 okresních měst).
- Komunikační infrastruktury veřejné správy (KIVS) s využitím komerčních nabídek soutěžených prostřednictvím Ministerstva vnitra, viz níže.
- Veřejný internet, a to přes zabezpečený tunel VPN SSL (Virtual Private Network Secure Sockets Layer) nebo VPN IPSec (Virtual Private Network Internet Protocol Security). Toto připojení slouží ke speciálním účelům, není možné pro rutinní provoz připojení k CMS.

Současnou novinkou pro rok 2022 a nadcházející roky je uvažovaná pátá možnost připojení nejmenších obcí do CMS/KIVS přes Webový aplikační firewall (WAF).

17.2 Komunikační infrastruktura veřejné správy

KIVS je jednotná komunikační infrastruktura pro podporu elektronického úřadování. Slouží k bezpečnému propojení orgánů veřejné správy mezi sebou a s veřejností. KIVS slouží ke garantované, bezpečné a auditovatelné výměně informací mezi jednotlivými orgány veřejné správy.

KIVS je navržena jako centralizovaná komunikační infrastruktura s Centrálním místem služeb, které je místem výměny dat mezi jednotlivými informačními systémy veřejné správy a zároveň místem propojení k veřejné síti internet a neveřejných sítí např. sítí Evropské unie.

17.3 Radiokomunikační systém PEGAS

Radiokomunikační systém PEGAS je základním komunikačním prostředím pro bezpečnostní a záchranné složky v České republice, zejm. integrovaný záchranný systém (Policie České republiky, Hasičský záchranný sbor, Zdravotnická záchranná služba) ve smyslu zákona č. 239/2000 Sb., o integrovaném záchranném sytému.

Systém umožňuje mobilní digitální komunikaci a je založen na standardu TETRAPOL vyvinutého přímo pro potřeby bezpečnostních složek. Architektura národní sítě je tvořena 14 regionálními sítěmi (kopírujícími současné územně právní členění státu), zajišťujícími rádiové pokrytí a řízení komunikace na území regionu i celého státu. Uživatelům mobilních i pevných terminálů poskytuje následující služby:

- hlasové služby – individuální hovory, skupinové komunikace, komunikace v přímém režimu, tísňová volání atd.,
- datové služby – odesílání krátkých zpráv, datové přenosy mezi aplikacemi standardním protokolem IP, dotazy do databází (např. do registrů osob, řidičů, vozidel).

Jedná se o plně digitální služby zabezpečené proti odposlechu způsobem konec – konec, a to především díky autentizačním a šifrovacím mechanismům. Systém PEGAS umožňuje propojení s dalšími externími komunikačními systémy, například s privátní i veřejnou telefonní sítí.

Hlavními výhody systému PEGAS oproti sítím komerčních operátorů spočívá v:

- umožnění řízeného provozu s komunikací v hovorových skupinách,
- vlastnictví veškeré technologie v rukou státu (MV), a tedy snížení rizika závislosti na dodavateli,
- poskytování vysokého zabezpečení hlasových a datových komunikací díky unikátní technologii,
- výrazně vyšším pokrytí území rádiovým signálem, a to včetně pohraničí a podzemních staveb,
- v licenčním modelu nezávislým na počtu klientů/uživatelů.

Otázky k procvičení:

1. Je komunikace mezi informačními systémy ČR a EU nějak technologicky podpořena?

Ano pro komunikaci informačních systémů s EU a jejími státy je vhodné užití služeb CMS/KIVS, kdy CMS je připojena na dílčí sítě EU.

2. Jaké jsou výhody sítě PEGAS?

Výhody plynou zejména ze specifické potřeby a použití tohoto systémy jako je pokrytí, zabezpečení, vlastnictví technologie, viz výše.

17.4 Doplňující část

Doplnění k možnosti připojení do CMS/KIVS: Současnou novinkou pro rok 2022 a nadcházející roky je uvažovaná možnost připojení nejmenších obcí do CMS/KIVS přes Webový aplikační firewall (WAF), tato varianta včetně prvních realizací, pokud se osvědčí, může finálně a elegantně dokončit proces připojování obcí do CMS/KIVS.

Doplnění k historickému vývoji CMS a KIVS – verze 2.0: Řízení využívání sílených služeb poskytovaných KIVS realizuje od roku 2006 Ministerstvo vnitra ČR (dále je „MV“). Hlavním záměrem projektu je sjednocení datových i hlasových služeb do jednotné sítě poskytující subjektům veřejné správy bezpečné připojení, vysoký standard nabízených služeb a úspory nákladů.

Do projektu KIVS je aktuálně zapojeno / jeho služby využívá více jak 250 subjektů státní správy a samosprávy od ústředních orgánů státní správy přes krajské úřady až po radnice, které uzavřely s MV Dohodu o centralizovaném zadávání, tedy zmocnily MV jako Centrálního zadavatele, aby jimi požadované služby soutěžil jejich jménem a na jejich účet.

K vlastním soutěžím využívá MV tzv. dynamického nákupního systému (**DNS**) definovaného § 138 a násl. zákonem č. 134/2016 Sb., o zadávání veřejných zakázek ve znění pozdějších předpisů, tedy vlastně elektronických aukcí, v nichž uchazeči nabízejí cenu za své služby.

Více informací lze nalézt na na www.cms2.cz a https://archi.gov.cz/nap:popisy:popis_cms_kivs.

Doplnění k systému PEGAS: Vlastníkem systému PEGAS je Ministerstvo vnitra, které ho vybudovalo v letech 1995 – 2003. Dodavatelem technologie Matracom 9600 byla tehdejší firma Matra Communications, dnes Airbus Defence α Space. V současnosti má systém cca 30 tisíc uživatelů.

Na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, byl systém PEGAS určen prvkem kritické informační infrastruktury státu.

17.4.1 Odkazy

- Komunikační infrastruktura veřejné správy a Centrální místo služeb na stránkách Ministersrva vnitra

https://www.mvcr.cz/clanek/komunikacni-infrastruktura-verejne-spravy-278660.aspx

- Komunikační infrastruktura veřejné správy a Centrální místo služeb na stránkách Národní architektury eGovernmentu:

https://archi.gov.cz/nap:komunikacni_infrastruktura_verejne_spravy

18 Kybernetická bezpečnost – obecný přehled

Související právní předpisy: zejména zákon č. 181/2014 Sb., zákon č. 127/2005 Sb., průřezově zákon č. 365/2000 Sb.

18.1 Obecný přehled – legislativa, terminologie

Kybernetickou bezpečností (KB) lze chápat jako souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru (typicky digitální prostředí tvořeno informačními systémy a jejich propojeními), jinak též zajištění bezpečnosti informací v kybernetickém prostoru

Kybernetická bezpečnost je v prostředí České republiky regulována zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB), který ukládá povinnosti v oblasti kybernetické bezpečnosti typicky správci nebo provozovateli systému (dále viz doplňující část).

Bezpečnost informací (a případně její úroveň) je vyjádřena pomocí třech základních atributů:

- Důvěrnost – informace je přístupná pouze oprávněným osobám;
- Integrita – informace je přesná a úplná a nedošlo k její neoprávněné změně;
- Dostupnost – informace je dostupná, odkud je třeba, kdy je třeba a jakou formou je třeba.

Dle zákona č. 181/2014 Sb., se rozumí

- **významnou sítí síť elektronických komunikací** (viz zákon č. 127/2005 Sb.) zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře,
- **kritickou informační infrastrukturou** prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy (případně viz zákon č. 240/2000 Sb. a Nařízení vlády č. 432/2010 Sb. v oblasti kybernetické bezpečnosti),
- **významným informačním systémem** informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
- **informačním systémem základní služby** informační systém, na jehož fungování je závislé poskytování základní služby.

Aktivem, případně bezpečnostním aktivem, se obecně rozumí cokoliv, co má pro organizaci určitou hodnotu. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, rozlišuje dva základní typy:

- **Primárním aktivem** je **informace** nebo **služba**, kterou zpracovává nebo poskytuje informační a komunikační systém.
- **Podpůrným aktivem** je **technické aktivum** – což je technické vybavení, komunikační prostředky a programové vybavení informačního a komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační a komunikační systém; nebo **zaměstnanci a dodavatelé** podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému. Podpůrná aktiva jsou navázána na aktiva primární.

Riziko je vyjádření kvantifikovatelné možnosti, že určitá **hrozba** (např. zemětřesení, ale i útok hackera/crackera), vyžije **zranitelnosti** (slabé místo podpůrného aktiva – např. server umístěný u aktivní sopky, nebo **bezpečnostního opatření** – jako je žádné omezení na délku hesla, kdy pak uživatelé užívají heslo: 123), a tím způsobí negativní následek – **dopad.**

Kybernetická bezpečnostní událost (KBU) je událost, která **může způsobit narušení** bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. **Kybernetický bezpečnostní incidentem** (KBI) je **narušení** bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Bezpečnostní opatření je souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru, kdy se může jednat o **organizační opatření** (např. školení, audit, politika hesel) nebo **technická opatření** (např. antivirus, šifrování, technické vynucení délky hesla)

Definovanými bezpečnostními rolemi jsou **Manažer kybernetické bezpečnosti**, **Architekt kybernetické bezpečnosti**, **Auditor kybernetické bezpečnosti**, **Garant aktiva**.

Mezi základní **nástroje kybernetické kriminality**, což je trestná činnost vyžívající technického (počítač) a programového vybavení (aplikace a její data) lze považovat: **Krádež/podvržení identity** (úvěrový podvod), **phishingové útoky** (vylákání citlivých informací jako jsou údaje kreditní karty), nebo **ransomware** (typicky aplikace, která požaduje výkupné, jinak zničí data).

Otázky k procvičení:

1. V rámci kybernetického útoku typu DoS (Denial of Service, česky odepření služby), dochází k přehlcení informačního systému, který následně přestane zcela odpovídat („zkolabuje/zamrzne“). Jaký atribut bezpečnosti informací je v této situaci dotčen?

Vzhledem k tomu, že systém neodpovídá, tak z něj nejdou dostat informace ani pro oprávněné uživatele dat. Rozhodně je tedy dotčena dostupnost. Dle popisovaného stavu však útočník nebyl schopen pravděpodobně získat přístup k serveru, tedy integrita by měla být zachována. A tím by měla být zachována i důvěrnost dat.

2. Útočníkovi se podařilo zmocnit serveru, kdy má administrátorská práva (práva číst, zapisovat, měnit záznamy a mazat je), na kterém je provozován informační systém veřejné správy. Jaké atributy bezpečnosti informací jsou dotčeny/ohroženy?

V této situaci dochází ke katastrofálnímu ohrožení všech atributů: integrita je narušena možností měnit zápisy, důvěryhodnost je ztracena kvůli neoprávněnému přístupy třetí osoby, samotná dostupnost je ohrožena – útočník může, když se mu zachce tento server (a tedy i informační systém) vypnout.

3. Užívá váš úřad, případně vy informační systémy klasifikované jako VIS či KII? O které se jedná, jaká jsou jeho primární a podpůrná aktiva?

Informační systém datových schránek – je dle informací KII, primárním aktivem bude např. služba zaslání datové zprávy. Podpůrným aktivem bude jistě MV a Česká pošta, a to konkrétní lidé…

18.2 Doplňující část

Doplnění k bezpečnosti informací: Krom představeného modelu triády (důvěrnost integrita bezpečnost) je užíván alternativní model, vlastností šesti, který přidává vlastnictví, užitnost, autenticitu.

Doplnění k subjektům ZoKB, ZoKB ukládá povinnosti:

- Správci a provozovateli informačního nebo komunikačního systému kritické informační infrastruktury (KII) – např. Ministerstvo vnitra (MV)
- Správci a provozovateli významného informačního systému (VIS) – např. MV, ale i Ministerstvo zahraničních věcí.
- Orgánu, nebo osobě zajišťující významnou síť.
- Poskytovateli služby elektronických komunikací a subjektu zajišťujícímu síť elektronických komunikací, pokud není orgánem nebo osobou zajišťující významnou sít. – odkaz na zákon č. 127/2005 Sb.
- Správci a provozovateli informačního systému základní služby, pokud nejsou správci nebo provozovateli KII nebo VIS.
- Provozovateli základní služby, pokud není správcem nebo provozovatelem informačního systému základní služby.
- Poskytovateli digitální služby.

Přehled dílčích legislativních aktů kybernetické bezpečnosti v prostředí ČR:

- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB).
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V kybernetické bezpečnosti se ještě setkáváme s pojmem **„Hybridní válka“** – druh ozbrojeného konfliktu vedeného útočníkem za kombinace konvekčních a nekonvekčních prostředků se synergickým efektem (nevojenské nástroje: kybernetické útoky, ekonomické sankce) a dále „**Kybernetická válka“** – operace v kybernetickém prostoru, jejichž cílem je informační vytížení, oslabení nebo úplné zničení informačních systémů protivníka (kybernetické útoky tzv. hackerů).

18.2.1 Odkazy

- Portál Národního úřadu pro kybernetickou a informační bezpečnost:

https://www.nukib.cz/

19 Kategorizace data a dokumentů (veřejné správy) z pohledu potřeby zajištění jejich ochrany

Související právní předpisy: zejména zákon č. 181/2014 Sb., zákon č. 365/2000 Sb., průřezově zákon č. 111/2009 Sb., Národní architektonický plán vydaný Ministerstvem vnitra.

19.1 Kategorizace dat a dokumentů

Každý informační systém IS obsahuje data a informace, tj. údaje, které představují cennou informační hodnotu. Ve veřejné správě dělíme údaje na **veřejné** a **neveřejné**.

Užitím dat (resp. údajů) do vytvořené formy vzniká dokument ať již tištěný, či digitální. **Vztah mezi daty a dokumentem je však duální** – z předchozí věty lze dovodit, že dokument obsahuje data. Na druhou stranu digitální dokument (třeba tato skripta) je realizován na vašem počítači jako binárním řetězec znaků – která lze považovat za data. Vždy je tedy potřeba rozlišovat z jakého úhlu pohledu se na problematiku dat a dokumentů hledí a k čemu jsou vlastně potřeba – pro statistické zpracování se hodí (digitální) data, pro pověšení si diplomu na zeď zase (fyzický) dokument.

Neveřejné údaje jsou údaje, u nichž existují právní překážky pro jejich zveřejnění (např. ochrana utajovaných informací, ochrana osobních údajů, ochrana osobního tajemství, případně jejich neveřejnost vyplývá z nějakého právního přepisu). Všechny ostatní údaje jsou **veřejné** a je možné o ně požádat na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Každá organizace pracuje s **velkým množstvím dat, která spolu vzájemně souvisí**. Aby mohla daná organizace data správně kategorizovat, je vhodné provést **datový audit**, tzn. identifikovat:

- jaká data má k dispozici ve svých informačních systémech,
- co tato data znamenají,
- jak spolu souvisí,
- jak se přenáší a transformují mezi informačními systémy,
- a zda jsou veřejná či neveřejná.

Jako prostředku pro identifikaci pojmů jejich vazeb a smyslu lze užít pokročilého přístupu **konceptuálního datového modelování**.

Předpokladem pro zajištění ochrany dat je správné určení veřejnosti a neveřejnosti údajů a jejich registrace do **registru práv a povinností** ohlašovatelem agendy včetně oprávnění přístupu. Pokud má orgán veřejné moci (OVM) či soukromoprávní uživatel údajů (SPUÚ) příslušné oprávnění přístupu k datům z IS, jehož není správcem, může je čerpat skrze propojený datový fond. Veřejné údaje je možné publikovat a získat přes veřejný datový fond např. skrze otevřená data.

Otevřená data (zákon č. 106/1999 Sb., o svobodném přístupu k informacím) jsou informace veřejného sektoru zveřejněná na internetu v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není omezen a které jsou evidovány v národním katalogu otevřených dat (informační systém spravovaný MV).

S problematikou neveřejnosti souvisí oblast osobních údajů a možnosti jejich zpracování a práci s nimi (zpracovat a správce dat), viz obecná část úřední zkoušky a **problematika GDPR**. Dalším bodem, který je zde okrajově zmíněn, je oblast **utajovaných informací** (zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti), a členění na stupeň utajení: vyhrazené (V), důvěrné (D), tajné (T), přísně tajné (PT).

Ochrana informací (ať již utajovaných, či obecně neveřejných informací) může být zajišťována:

- **personální bezpečností**:
  - výběr fyzických osob, které mají mít přístup k informacím,
  - ověřování podmínek pro jejich přístup k informacím,
  - jejich výchova a ochrana,
- **průmyslovou bezpečností**:
  - systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k informacím,
  - zajištění nakládání s informací u podnikatele v souladu se zákonem/smlouvou,
- **administrativní bezpečností**:
  - systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s informacemi,
- **fyzickou bezpečností**:
  - systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k informacím, popřípadě přístup nebo pokus o něj zaznamenat,
- **bezpečností informačních nebo komunikačních systémů**:
  - systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost informací, s nimiž tyto systémy nakládají,
  - odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému,
- **kryptografickou ochranou**:
  - systém opatření na ochranu informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání informací.

Otázky k procvičení:

1. Jakým způsobem přispívá Registr práv a povinností (RPP) při sdílení údajů napříč veřejnou správou?

Pomocí registrace těchto údajů do RPP je možno stanovit jejich veřejnost/neveřejnost a dále v případě neveřejnosti definovat množinu subjektů, které mohou k těmto datům přístup včetně kontroly daného přístupu.

2. Jakým způsobem na pracovišti zabezpečujete kategorizace dat a dokumentů?

Například každý původce dat a dokumentů definuje jaké bezpečnostní úrovně nebo stupně utajení dosahují tato jednotlivá data či dokumenty. Např. útvar tisku a public relations bude pracovat typicky s veřejnými informacemi, které může vydat – tiskové zprávy, ale i třeba potisk reklamních předmětů s logy včetně věnování či publikaci výročních zpráv.

19.2 Doplňující část

Doplnění k otevřeným datům a ochraně osobních údajů: Jak bylo zmíněno, otevřená data specifikuje zákon č. 106/1999 Sb., o svobodném přístupu k informacím, a dále pak nařízení vlády č. 425/2016, o seznamu informací zveřejňovaných jako otevřená data. Otevřenost a transparentnost je zároveň jedním z architektonických principů eGovernmentu definovaných Informační koncepcí České republiky. Tento princip je převzatý ze strategických dokumentů Evropské unie a na národní úrovni jej doplňuje princip otevřená data jako standard. Pro dodržení těchto principů musí organizace veřejné správy publikovat veřejné údaje evidované ve svých informačních systémech jako otevřená data. Pro neveřejné údaje musí být jako otevřená data zveřejňována jejich anonymizovaná podoba, souhrn nebo statistika, nebo obdobná forma, pokud může mít význam pro uživatele těchto dat. Potřebnost publikace otevřených dat zmiňuje i programové prohlášení Vlády ČR z června 2018 a mezinárodní iniciativa Partnerství pro otevřené vládnutí.

V souladu s tzv. "FAIR principy" by otevřená data měla být zpracována tak, aby byla vyhledatelná (Findable), dostupná (Accessible), interoperabilní (Interoperable) a opětovně využitelná (Reusable). Vyhledatelnost otevřených dat je zajištěna jejich registrací do Národního katalogu otevřených dat (dále jen „NKOD") a vyplněním všech povinných položek metadat, které popisují publikovaná data. Veškeré informace týkající se standardů publikace a katalogizace otevřených dat, vzorových publikačních plánů, včetně otevřených formálních norem udržuje Ministerstvo vnitra na Portálu otevřených dat (dále jen „POD") - https://data.gov.cz/

Národní katalog otevřených dat (NKOD) je informační systém veřejné správy přístupný způsobem umožňujícím dálkový přístup sloužící k evidování a katalogizaci informací zveřejňovaných jako otevřená data. Podle § 3 odst. 11 zákona č. 106/1999 Sb., o svobodném přístupu k informacím jsou otevřená data institucí veřejné správy v NKOD katalogizována povinně. Slouží uživateli pro snazší orientaci a vyhledávání v otevřených datech publikovaných veřejnou správou ČR z jednoho místa.

Při práci s daty je nutné myslet i na ochranu osobních údajů. Agendové a identifikační údaje by měly být odděleny z důvodu snížení rizika neoprávněného nakládání s osobními údaji a snížení rizika neoprávněného spojování osobních údajů. Zákonem č. 111/2009 Sb., o základních registrech byl zaveden základní princip pseudonymizace ve veřejné správě formou Agendového identifikátoru fyzické osoby (AIFO). Požadavky na zpracování osobních údajů podrobně definuje zákon č. 110/2019 Sb., o zpracování osobních údajů.

Základní pojmy, ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů se rozumí:

- **Osobním údajem** jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
- **Citlivým údajem** osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů

a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

- **Zveřejněným osobním údajem** osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu, např. otevřená data. Nelze zveřejnit osobní údaje, pokud k tomu není zákonné zmocnění nebo není dostatečně významný veřejný zájem na zveřejnění.
- **Anonymním údajem** takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů, anonymizace je mnohdy podmínkou pro zveřejnění některých údajů.
- **Pseudonymizovaným** údajem anonymizovaný údaj, přičemž ale použitý anonymizační klíč (postup procesu) je bezpečně uložen (tj. s vysoce zabezpečenými přístupovými právy) pro případ potřeby zpětné autentizace (= reverze anonymizace).
- **Subjektem osobních údajů** fyzická osoba, k níž se osobní údaje vztahují.
- **Zpracováním osobních údajů** jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.
- **Shromažďováním osobních údajů** systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.
- **Uchováváním osobních údajů** udržování údajů v takové podobě, která je umožňuje dále zpracovávat.
- **Evidencí nebo datovým souborem osobních údajů** (datový soubor) jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.
- **Blokováním osobních údajů** operace nebo soustava operací, kterými se na stanovenou dobu omezí způsob nebo prostředky zpracování osobních údajů, s výjimkou nezbytných zásahů.
- **Likvidací osobních údajů** se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.
- Správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.
- **Zpracovatelem** každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.
- **Souhlasem subjektu údajů** svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.
- **Příjemcem** každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).

Pravidla / zásady pro zpracování a ochranu osobních údajů:

- Pro požadování osobních údajů, musí být k jejich využití souhlas nebo ke shromažďování osobních údajů musí opravňovat zákon.

- Osobních údaje mohou být dále využívány jen na základě podepsaných a odsouhlasených podmínek (vyjma případů kdy podmínky stanovuje zákonné oprávnění).
- Souhlas s poskytnutím osobních údajů musí být vědomý, svobodný a informovaný.
- Každý má právo vědět, jaké osobní údaje o něm dotčený subjekt shromažďuje a má právo požadovat jejich blokování, opravu, doplnění či výmaz.
- Osobní údaje smí být uchovávány pouze po dobu, která je nezbytně nutná pro naplnění účelu jejich zpracování.
- Je zakázáno pořizovat jakýmikoliv prostředky kopie osobních dokladů (občanský průkaz, cestovní doklad) bez souhlasu, vyjma zákonem stanovených případů (zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu).
- Pro evidenci vstupu do budov nesmí být vyžadováno rodné číslo, plně dostačující je jméno a příjmení, případně číslo občanského průkazu (v případě pracovního jednání služebního průkazu).
- Osobní údaje, které mohly být uloženy na nějakém záznamovém zařízení (např. počítačový pevný disk), musí být před případným prodejem důkladně smazány pomocí zvláštních programových prostředků. Běžné přeinstalování či jednoduché smazání není dostatečnou zárukou zničení uložených údajů.
- Buďte opatrní při zasílání osobních údajů pomocí elektronických prostředků. Mějte vždy na paměti, že komunikační kanály mohou být „odposlouchávány“ neoprávněnou osobou. Pokud již musíte takovou formu přenosu použít, využívejte v co největší míře standardní prostředky šifrování nebo certifikace (SSL protokoly, podpisové certifikáty nebo jednorázová zabezpečovací hesla).
- Vždy musíte být upozorněni, ve většině případů alespoň nástěnným piktogramem, že se pohybujete v prostoru sledovaném kamerovými systémy. Kamerové sledování je nepřípustné v prostorách určených pro ryze intimní úkony (např. toalety, koupelny, prostory vyhrazené k převlékání apod.).

Dohled a kontrola nad dodržováním ochrany osobních údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, jsou vykonávány Úřadem pro ochranu osobních údajů.

Správce osobních údajů je povinen:

- Stanovit účel, k němuž mají být osobní údaje zpracovány.
- Stanovit prostředky a způsob zpracování osobních údajů.
- Zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje.

Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje.

Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6.11) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, tj. správce musí nepřesné osobní údaje označit a informaci o jejich blokování, opravě, doplnění nebo likvidaci bez zbytečného odkladu předat všem příjemcům.

- Shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu.
- Uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné.
- Zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, nebo pokud k tomu dal subjekt údajů předem souhlas.
- Shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti.
- Nesdružovat osobní údaje, které byly získány k rozdílným účelům.

19.2.1 Odkazy

- Portál otevřených dat:

https://data.gov.cz/

- Veřejně dostupný seznam agend Registru práv a povinností:

https://rpp-ais.egon.gov.cz/gen/agendy-detail/

20 Způsoby a prostředky ochrany informačních aktiv

Související právní předpisy: průřezově všechny ze seznamu odborné literatury, významné zejména zákon č. 181/2014 Sb.

20.1 Absolutní bezpečnost

V praxi **nelze dosáhnout absolutní bezpečnosti**, naopak zmíněná triáda v některých případech funguje protikladně, tedy např. požadavkem na zvýšení dostupnosti (stejná data budou uložena na vícero místech/zálohách) je snížení důvěryhodnosti (každé umístění zvyšuje riziko, že se k datům dostane někdo jiný. Z toho plyne, že **ne všechna rizika lze potlačit**, ale mělo by být možné je **mitigovat** , tedy snížit na takovou úroveň, kterou organizace považuje za dostatečnou a toto riziko bude **akceptovat**.

Zajištění kybernetické bezpečnosti je stále živoucí proces, kdy platí, že implementace pouze technických, byť nejmodernějších prostředků sama o sobě nestačí. **Lidský faktor** (lidi) je v tomto ohledu jedním z největších rizik. Bez souběžného zavedení odpovídajících organizačních opatření je i sebelepší trezor k ničemu, pokud jeho obsluha všem vyzradí přístupové údaje, nebo trezor z pohodlnosti vůbec nezamyká.

Způsoby a prostředky ochrany informačních aktiv, viz kapitola 18, lze definovat pomocí technických a organizačních opatření, která mají zamezit ztrátě důvěrnosti, integrity a dostupnosti daného informačního aktiva. V kapitolách níže jsou popsaný vybrané způsoby a prostředky po atributech bezpečnosti informací. Pro každý způsob a prostředek byla zvolena hlavní kategorie, ale typicky mohou ovlivňovat i vícero atributů bezpečnosti informací zároveň.

20.2 Zajištění důvěrnosti

Důvěrnost lze definovat jako zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni. Ztráta důvěrnosti může vést např. ke ztrátě důvěry zákazníků, právní odpovědnosti, ohrožení osobní bezpečnosti nebo finanční ztrátě.

- **Oddělení sítí** (**segmentace sítí**) – jednotlivá zařízení spolu komunikují pouze po jasně definovaných sítích (ať již fyzických – dráty, tak logických – aplikačně definovaná spojení), protokolech a portech.
- **Šifrování** – data jsou při komunikaci mezi odesílatelem a příjemcem zašifrována, útočník tedy i při odposlechnutí datového přenosu nemá možnost zjistit obsah přenášené zprávy.
- **Komunikace po virtuálním kanálu / užití virtuální privátní sítě** (VPN) – prvek mimo interní síť je pomocí aplikace schopen komunikovat s interní sítí, jako kdyby mimo interní síť nebyl. Např. připojení do IS elektronické spisové služby úřadu pomocí domácího počítače přes VPN.
- **Bezpečnostní komunikační protokol** – užití technického protokolu Transport Layer Security (TLS), který je užíván jako součást HTTPS (Hypertext Transfer Protocol Secure) volání zabezpečené spojení a komunikaci mezi prohlížečem a webovou stránkou.
- **Identifikace, autentizace a autorizace** – více viz kapitola 7, vstup a práce se systém povolena pouze takové identitě (uživatelskému účtu), který se autentizoval (prokázal např. heslem, či

vícero prostředky zároveň, tj. užil vícefaktorová autentizace – např. heslo a SMS) a má právo konat (má potřebné uživatelské oprávnění).

- **Pořizování záznamů** (**logování**) – opatření záznamu či auditní stopy, ať již pro případ chyby systému, tak případné nekalé úmyslné chování.

20.3 Zajištění integrity

Integritu lze definovat jako zajištění přesnosti (správnosti) a úplnosti. V případě, že dojde k narušení integrity (např. dojde k nežádoucí změně dat), nemusí být tato změna vůbec odhalena a může uplynout značná doba, než je porušení integrity zjištěno. Ztráta integrity může vést například k přijetí nesprávných rozhodnutí, rozpadu funkčnosti organizace.

- **Hashovací** (**kryptografická**) **funkce** – je typicky taková funkce, které převede vstup o jakékoliv délce na výstup (hash) o předem definované délce. Smysl je takový, že stejný vstup vygeneruje vždy stejný výstup (hash). Nicméně na základě výstupu (hashe) nelze (lehce) zrekonstruovat vstup. Hashovací funkce je tzv. ireverzibilní. Užití hashovací funkce je široké, od šifrování, elektronický podpis (viz kapitola 16), přes detekci konzistence souborů či databáze až po užití v blokchainu a kryptoměnách.
- **Elektronické podpisy, pečetě a časová razítka** definuje nařízení eIDAS, viz kapitola 4, dále pak pro konkrétní provedení elektronického podpisu a související viz kapitola 16.

20.4 Zajištění dostupnosti

Dostupnost lze definovat jako zajištění, že informace je pro oprávněné uživatele přístupná a použitelná v okamžiku její potřeby. Narušení dostupnosti může vést například k neschopnosti vykonávat kritické činnosti organizace.

- **Dedikované ukládací prostředí** – ukládání dokumentů na zabezpečené síťové úložiště, kde lze v případě potřeby dokument (např. s kolegy) sdílet.
- **Zálohování** – replikace/uložení dat na jiném fyzickém místě a fyzickém nosiči. V případě ztráty primárních dat lze užít tuto záloha a nedochází tak k zásadní ztrátě dat
- **Zajištění kontinuity činností** – strategicko-taktická schopnost organizace plánovat a reagovat na mimořádné situace a narušení jejího chodu. Příkladem je tzv. disaster recovery – obnova do produkčního stavu v případě celkové selhání informačního systém (i jeho sekundárních lokací).

Otázky k procvičení:

1. Splňuje vaše emailové schránka atributy bezpečnosti informací?

Předpokládejme, že plně důvěřujeme poskytovateli služby e-mailu. K e-mailové schránce se budete moci dostat pouze vy pomocí hesla, které znáte pouze vy – faktor důvěrnosti. Vzhledem k tomu, že nikdo jiný se nedovede přihlásit a měnit tak obsah zpráv, tak bude schránka splňovat i faktor integrity. Úroveň atributy dostupnost bude dán způsoby, jak se budete moci připojit, pokud je schránka dostupná i přes internetové rozhraní a služba běží v režimu vysoké dostupnosti, tak bude i tento atribut splněn.

20.5 Doplňující část

Doplnění k termínu šifrování: Jedním ze základních technických opatření pro zajištění důvěrnosti je šifrování. Jde o mechanismus zaměřený na ochranu obsahu zprávy, který využívá kryptografických prostředků pro transformací dat do takové podoby, jež je učiní pro neoprávněné subjekty nečitelnými. Účelem kryptografických prostředků je zajištění ochrany informací před zneužitím a neoprávněnou modifikací. Všechny informace, které mohou být takto ohroženy, musí být chráněny vhodnými kryptografickými prostředky.
Základní dělení kryptografických prostředků:

- Symetrická kryptografie – stejný klíč, který použil odesílatel k zašifrování zprávy, se použije příjemcem i pro dešifrování této zprávy. Šifrovací klíč je nutné předat důvěryhodným kanálem ještě před zahájením komunikace. Symetrická kryptografie se využívá např. pro šifrování dokumentů.
- Asymetrická kryptografie – na rozdíl od symetrické kryptografie se používá dvojice klíčů. Veřejný klíč lze zveřejnit, soukromý klíč je nutné udržet v tajnosti a bezpečí. Princip asymetrické kryptografie spočívá v tom, že data zašifrovaná veřejným klíčem lze v rozumném čase dešifrovat pouze se znalostí soukromého klíče. Elektronický podpis, který byl vytvořen soukromým klíčem, lze ověřit pomocí veřejného klíče.

Správu a distribuci veřejných klíčů řeší certifikační autorita, která při vzájemné komunikaci dvou subjektů vystupuje jako třetí nezávislý a důvěryhodný subjekt. Prostřednictvím digitálních certifikátů, což jsou elektronicky podepsané veřejné klíče, jednoznačně svazuje identifikaci subjektu s jeho dvojicí klíčů.

Šifrovat lze jednotlivé soubory a dokumenty, diskové oddíly či celá paměťová média. Bezpečnostní komunikační protokoly pomocí šifrování zajistí například bezpečné odeslání přihlašovacího formuláře na webových stránkách. Šifrování je také nezbytné pro bezpečnou komunikaci po virtuálním kanálu například pro vzdálený přístup do jiné sítě.

Doplnění k zajištění důvěrnosti – elevace práv a privilegované účty: Privilegované účty umožňují takřka neomezený přístup ke zdrojům příslušných systémů včetně dat, a proto jsou významným bezpečnostním rizikem. Oprávnění disponovat takovým účtem mají jak interní zaměstnanci, tak externí dodavatelé a takové oprávnění často není nijak evidováno. Znalost přihlašovacích údajů je navíc zpravidla sdílena mezi více uživateli, tudíž odpovědnost za případné zneužití je velice těžko dohledatelná, nebo dokonce není vůbec prokazatelná. Toto riziko se vztahuje na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky až na komplexní informační systémy distribuované jako produkt, nebo vyvinuté na míru.

Z tohoto důvodu je nutné zavést správu přístupu k těmto účtům a monitoring veškeré aktivity účtů s vazbou na konkrétní osobu, která jím právě disponuje. Řešením správy privilegovaných účtu je nasazení tzv. Privileged Identity Management systému (PIM), nebo také Privileged Account Management (PAM).

Doplnění k elektronickým podpisům razítkům a pečetím: Technologie elektronických podpisů a pečetí staví na principech asymetrické kryptografie. Pomocí soukromého klíče se vytváří elektronický podpis či elektronická pečeť. Veřejný klíč je součástí certifikátu a používá se k ověření

elektronického podpisu nebo pečeti. Při podepisování (pečetění) je nejprve pomocí hashovací funkce vytvořen otisk dat daného dokumentu (viz kapitola 20.2.1). Tento otisk je poté zašifrován soukromým klíčem, čímž vznikne elektronický podpis (pečeť). Je-li potřeba ověřit elektronický podpis (pečeť), je nutné dešifrovat otisk dat pomocí veřejného klíče. Dešifrovaný otisk musí odpovídat otisku původního dokumentu.

Řízení kontinuity činností vyžaduje komplexní porozumění organizací vykonávaným činnostem. Nezbytnou součástí je analýza dopadů, jejímž výstupem je identifikace možných rizik, odhad následků havarijní události na organizaci a určení požadavků na strategii obnovy klíčových procesů a minimální potřebné úrovně pro alespoň omezené fungování. Na základě provedené analýzy se vytvoří strategie definující základní východiska, která stanoví přístup k zajištění kontinuity činností organizace.

Jedním z hlavních výstupů řízení kontinuity činností jsou plány zachování kontinuity činností, které minimalizují následky mimořádných situací a zároveň umožňují rychlé uvedení fungování do normálního stavu. Plán zachování kontinuity činností by měl poskytnout návod a postup pro reakci na mimořádnou situaci. Plán obnovy po havárii zkracuje dobu potřebnou.

20.5.1 Odkazy

- Minimální bezpečností standard:

https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

Závěr

Skripta jsou pouze jedním ze způsobů získávání znalostí. Dá se samozřejmě říci, že jsou informace kondenzované, ale samotnou kondenzací ubírají na celkovém zážitku. Přestože nelze považovat skripta za nudná, tak poznávání samotného eGovernmentu pomocí jeho prožití – přihlášení se do portálu občana, kontrola bodového konta řidiče, či vyzvednutí léku pomocí eReceptu – je minimálně interaktivnější a případně zábavnější.

Představená materie v předcházejících dvaceti kapitolách představuje slušný rozhled. Je již pouze na vás, zda se z této pozice budete chtít porozhlédnout dále. Per aspera ad astra.

Seznam literatury

EVROPSKÝ ÚČETNÍ DVŮR, 2017. Manuál pro audit výkonnosti – Ředitelství pro řízení kvality auditu [online]. Získáno z: https://www.eca.europa.eu/Lists/ECADocuments/PERF_AUDIT_MANUAL/PERF_AUDIT_MANUAL_CS.PDF

WIEGERS, Karl Eugene a Joy BEATTY, 2013. Software requirements. Third edition. Redmond, Washington: Microsoft Press, s division of Microsoft Corporation. ISBN 978-0-7356-7966-5.

JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J.: Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, Česká pobočka AFCEA, NBÚ, 2015, 240s. ISBN 978-80-7251436-9-6. Dostupné také na http://www.cybersecurity.cz/data/slovnik_v310.pdf k volnému stažení.

BUDIŠ, P. Elektronický podpis a jeho aplikace v praxi, ANAG.

BOSÁKOVÁ, D. - Elektronický podpis, přehled právní úpravy, ANAG.

ŠPAČEK, D. eGOVERNMENT - Cíle, trendy a přístupy k jeho hodnocení, C.H.BECK.

Přílohy

Seznam otázek zvláštní části úřednické zkoušky oboru státní služby 28

Tabulka 12 – Otázky zvláštní části úřednické zkoušky oboru státní služby 28

Pořadové číslo	Znění otázky
1	Informační a komunikační technologie – základní pojmy, etika
2	Rozhodující trendy v současném ICT
3	ICT veřejné správy – smysl, očekávání, rizika, prostředky
4	Právní normy, standardy a doporučení v oblasti ICT veřejné správy
5	Ekonomická výhodnost ICT veřejné správy
6	eGovernment – principy, směry rozvoje, klíčové dokumenty
7	Identifikace / autentizace uživatelů digitálních služeb
8	Řízení eGovernmentu – úrovně řízení a kompetenční útvary
9	Význam ICT architektury veřejné správy
10	Životní cyklus digitální služby
11	Klíčové role ICT veřejné správy
12	Registr práv a povinností – metainformační systém státu pro výkon veřejné správy
13	IS Czech POINT a kontaktní místa veřejné správy
14	Informační systém datových schránek
15	Portál veřejné správy a portál občana
16	Elektronická komunikace VS
17	Centrální místo služeb, komunikační infrastruktura veřejné správy a radiokomunikační systém PEGAS
18	Kybernetická bezpečnost – obecný přehled
19	Kategorizace dat a dokumentů (veřejné správy) z pohledu potřeby zajištění jejich ochrany
20	Způsoby a prostředky ochrany informačních aktiv

Seznam právních předpis zvláštní části úřednické zkoušky oboru státní služby 28

Tabulka 13 – Právní předpisy zvláštní části úřednické zkoušky oboru státní služby 28

Právní předpis	Druh právního předpisu
Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES	Nařízení EU
směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, d) zákon o svobodném přístupu k informacím	Směrnice EU
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy	Zákon ČR
Zákon č. 111/2009 Sb., o základních registrech	Zákon ČR
Zákon č. 12/2020 Sb., o právu na digitální služby	Zákon ČR
Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů	Zákon ČR
Zákon č. 499/2004 Sb., o archivnictví a spisové službě	Zákon ČR
Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce	Zákon ČR
Zákon č. 250/2017 Sb., o elektronické identifikaci	Zákon ČR

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti	Zákon ČR
Zákon č. 127/2005 Sb., o elektronických komunikacích	Zákon ČR
Zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů	Zákon ČR
Zákon č. 340/2015 Sb., o registru smluv	Zákon ČR
Zákon č. 134/2016 Sb., o zadávání veřejných zakázek	Zákon ČR
Zákon č. 480/2004 Sb. Zákon o některých službách informační společnosti	Zákon ČR
Zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací	Zákon ČR
Národní architektonická plán vydaný Ministerstvem vnitra	Na úrovni usnesení vlády