Informační koncepce Úřadu pro ochranu osobních údajů 2023–2028

v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, a vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy

Praha, říjen 2023

OBSAH

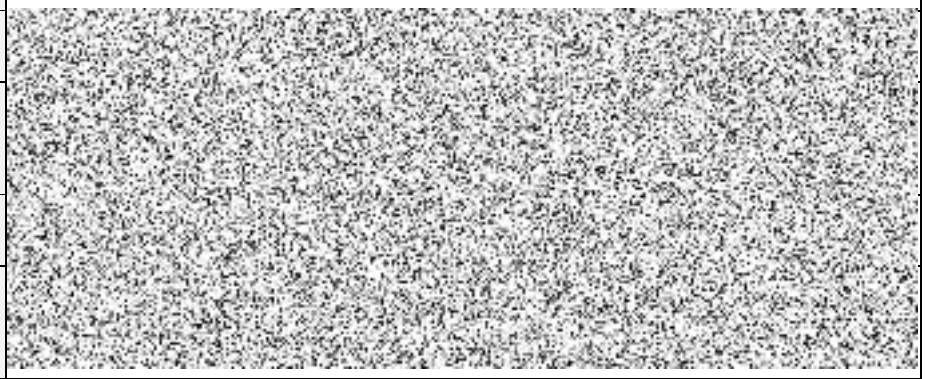
ÚVOD

1 Identifikace Informační koncepce

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) vydává tuto Informační koncepci ÚOOÚ (dále jen „IK ÚOOÚ“) v souladu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (§ 5a). V Informační koncepci stanovuje své dlouhodobé cíle v oblasti řízení architektury ÚOOÚ, řízení ICT služeb a vizi rozvoje digitalizace některých služeb.

ÚOOÚ je z pohledu eGovernmentu zásadní zejména tím, že provozuje Kritický systém informační infrastruktury IS ORG, který je klíčovou částí Základních registrů, protože zajišťuje anonymizaci pohybu osobních údajů v rámci tohoto systému.

1.1 Základní údaje IK ÚOOÚ

Název orgánu veřejné správy	**Úřad pro ochranu osobních údajů**
IČO	**70837627**
Typ organizace	**Orgán státní správy**
Adresa sídla	**Pplk. Sochora 727, 170 00 Praha 7- Holešovice**
Verze IK ÚOOÚ	**1.0**
Datum vzniku	**1. 10. 2023**
Datum schválení	**8. 11. 2023**
Počátek platnosti	**8. 11. 2023**
Autor verze	
Organizační útvar / organizace	
Verzi schválil	
Organizační útvar / organizace	
Název souboru	**IK_UOOU**
Počet stran	**97**

2 Manažerské shrnutí

2.1 Nejstručnější rekapitulace závěrů IK ÚOOÚ

IK ÚOOÚ identifikuje celou řadu oblastí, v nichž bude potřeba provést změny. Maximální důraz bude kladen zejména na 3 pilíře IK ÚOOÚ:

1) Digitalizace vnitřních procesů a evidence zásadních dokumentů;
2) Maximální využití cloudových technologií (státního či komerčního cloudu);
3) Dlouhodobá udržitelnost zvolených technických řešení a maximální využívání pilotního ověřování jednotlivých řešení.

Tyto pilíře se musí opírat o dodržování všech pravidel pro provoz IT vyplývajících ze zákonů a vyhlášek, tedy o dodržování pravidel kybernetické bezpečnosti a pravidel dle vyhlášek či zákonů upravujících provoz a rozvoj informačních systémů.

2.2 Základní zodpovědnosti a kompetence ÚOOÚ

V primární působnosti ÚOOÚ je ochrana osobních údajů. Obecná působnost ÚOOÚ v ochraně osobních údajů je konkrétně vymezena v článku 57 obecného nařízení o ochraně osobních údajů jako „úkoly“ (angl. tasks) a ÚOOÚ má k tomu v článku 58 obecného nařízení o ochraně osobních údajů „pravomoci“ (angl. powers). ÚOOÚ je jediným dozorovým úřadem s obecnou působností v České republice. Z jeho působnosti je na jedné straně vyňato zpracování osobních údajů některými skupinami správců, na straně druhé jeho role zahrnuje ochranu osobních údajů v oblastech nespadajících do působnosti obecného nařízení o ochraně osobních údajů (GDPR).

Vedle ochrany osobních údajů je dalším pilířem činnosti ÚOOÚ agenda svobodného přístupu k informacím, v níž je ÚOOÚ svěřena dílčí působnost nadřízeného, přezkumného a nečinnostního orgánu v rozsahu vymezeném ustanoveními § 16b a § 20 odst. 5 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Třetím pilířem činnosti ÚOOÚ je provozování kritického informačního systému poskytujícího zdrojové a agendové identifikátory fyzických osob (elektronické identifikátory podle § 11 zákona č. 111/2009 Sb., o základních registrech). Uzavřený a organizačně oddělený systém (IS ORG) funguje jako součást základních registrů.

2.3 Shrnutí stávajícího stavu ÚOOÚ a jeho architektury

Stávající stav digitalizace v rámci ÚOOÚ je uspokojivý. IT podporuje fungování ÚOOÚ do míry, která je pro běžný provoz postačující. Bude nutné vyřešit kontinuitu digitalizace agendy nevyžádaných obchodních sdělení. Zároveň je potřeba zamyslet se nad větší digitalizací procesů spojených s nejzásadnějšími agendami typu kontrol v oblasti ochrany osobních údajů a v rámci působnosti ÚOOÚ v agendě spojené se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím.

IS ORG funguje stabilně a bez větších problémů. Při jeho provozu jsou hlavními prioritami bezpečnost a stabilita.

Architektura ÚOOÚ je postavena na využívání on-premise infrastruktury pro vnitřní IT i IS ORG. ÚOOÚ vlastní z tohoto důvodu velké množství hardwaru a nedisponuje v rámci svých rozvojových plánů příliš velkou flexibilitou.

2.4 Klíčové transformační cíle

1. **Digitalizace fungování nejdůležitějších agend**

Z analýzy stávajícího stavu vychází, že současný stav digitalizace fungování agend ÚOOÚ není dostatečný. Pro naplnění výše popsaných cílů organizace je zásadní, aby vznikl Agendový informační systém, který bude sloužit evidenci nejzásadnějších dokumentů, a zároveň bude definovat a podporovat potřebné workflow. Agenda ÚOOÚ není z pohledu procesů příliš komplikovaná. V zásadě se jedná o přijetí podání, jeho vyhodnocení a vydání následného rozhodnutí. Pro každé konkrétní podání se však liší zákon, na jehož základě je podání učiněno. Do procesu zpracování však tento rozdíl zasahuje jen minimálně. Z toho důvodu se je vhodným řešením vytvoření jednoho většího agendového informačního systému, který bude evidovat všechny dokumenty potřebné pro fungování agend ÚOOÚ a definovat všechna workflow. Workflow se budou na základě legislativního ukotvení lišit, dokumenty však mohou být v jedné databázi, kde se bude dle podkladového zákona pouze filtrovat. Vedle toho by bylo vhodné v rámci AIS vytvořit elektronické formuláře umožňující automatický import dat přímo do AIS, které by bylo možné vyplnit na webových stránkách. Vzhledem k rozsahu takového systému bude preferována varianta postupného vývoje a rozvoje po menších částech.

Dále je pro digitalizaci fungování nejdůležitějších agend nutné zavést podpůrné procesy typu projektového řízení a řízení změnových požadavků.

2. **Maximalizovat využití cloudových technologií**

Jedním z cílů ÚOOÚ je dlouhodobě více podporovat práci z domova, a zároveň umožnit větší možnosti kontrol a působení v terénu. Pro naplnění těchto cílů je ideální využít cloudových technologií. Na ÚOOÚ je již nasazeno cloudové řešení pro kancelářské aplikace a e-mailový server. Vedle toho byla na ÚOOÚ úspěšně nasazena dvě řešení postavená na cloudové technologii pro Evidenci smluv a Informační hub.

Z analýzy stávajícího stavu navíc vyplynula řada problémů se současným fungováním IT infrastruktury ÚOOÚ. V roce 2019 byla vypovězena provozní smlouva na správu datového centra ÚOOÚ, která nebyla adekvátně nahrazena. HW v datovém centru ÚOOÚ nebyl dlouhodobě obnovován, z čehož vyplývá nutnost ho co možná nejrychleji nahradit. Nabízí se tedy spojit byznysové cíle s řešením těchto problémů a začít vypracovávat podrobný plán přesunu maximálního počtu aplikací a infrastrukturních prvků na cloud.

Pro naplnění tohoto cíle bude nutné vyřešit nejasnosti spojené s evropským stanoviskem k využívání komerčního cloudu, a to využitím šifrování klíči ve správě ÚOOÚ a správnou kategorizací dat dle citlivosti.

2.5 Klíčové vnitřní potřeby ICT

Klíčové pro provoz ICT budou z pohledu zpracovatele IK ÚOOÚ spíše principy než jednotlivé potřeby, proto je zde zmíníme.

Vnitřní motivací pro řízení ICT je snaha provozovat IT efektivně a spolehlivě za dodržování všech zákonů a vyhlášek, které na ICT dopadají. Realita malého úřadu s nevelkými finančními prostředky a omezenými personálními kapacitami dovedla OIT k několika základním principům, kterými se bude v dalších 5 letech řídit a které budou rámovat naplňování externích i byznysových cílů.

1) Maximální využívání pilotního provozu a postupné nasazování nových technologií

Jednou z mála výhod malého úřadu je možnost o něco snáz nasazovat nové technologie. Tyto technologie se ale musí nasazovat s jasnou představou, co takové nasazení pro organizaci znamená. Ideální je vyzkoušet nástroj na omezeném počtu uživatelů, a až následně uvažovat o jeho nasazení. Takový pilotní provoz zpravidla trvá 1–3 měsíce a je ukončen vyhodnocením a návrhem dalšího postupu schvalovaným vedením ÚOOÚ.

2) Maximální využívání již nakoupeného SW a licencí (včetně licencí zdarma)

Je důležité si být vědomi všech služeb a aplikací, které organizace má dlouhodobě či historicky zasmluvněné. V průběhu let se často podoba jejich využití mění nebo personálními změnami ztrácí, a je tedy nutné ji pravidelně obnovovat a být si vědomi všech součástí portfolia. Důležité je to nejvíce ve spolupráci s velkými korporátními partnery typu Microsoft, jejichž licenční politika se často mění, a tím pádem se mění rozsah a možnosti využívaných aplikací. Vedle toho je výhodné sledovat trh a hledat možnosti využívání SW zdarma, minimálně v rámci pilotního provozu, a tím pádem snížit náklady na pilotní provozy.

3) Postupný ústup od provozování HW na ÚOOÚ

Pro úřady malé velikosti je provozování HW velmi nákladnou záležitostí, a je tak nutné přemýšlet o alternativních řešení. Dlouhodobým cílem pro IT ÚOOÚ tak je omezovat využívání on-premise HW a přechod na cloud. V rámci aplikací nutných pro provoz ÚOOÚ, a v případě dokumentů a dat, která jsou jakýmkoliv způsobem citlivá (dle DLP Red a Amber Strict/Amber), je možné uvažovat o využití šifrování pro zajištění bezpečnosti těchto dat. V případě systému IS ORG je preferovanou variantou využití státního cloudu.

4) Velký důraz na strategické řízení a dlouhodobou udržitelnost

Vzhledem k systému fungování veřejné správy a náročnosti jejích administrativních procesů je nutné veškeré změny plánovat s dostatečným předstihem. Každou změnu pak hodnotit nejen z pohledu krátkodobých, například investičních nákladů, ale i z pohledu dlouhodobé udržitelnosti a náročnosti na správu takových systémů.

5) Využívání externích služeb za účelem rozšíření know-how organizace a outsourcingu expertních služeb

Vzhledem k velikosti ÚOOÚ není možné veškeré činnosti potřebné pro řízení ICT vykonávat interními zaměstnanci. Pro rozvoj bude nutné nejen získat nové zaměstnance schopné vytvářet návrhy koncepčních změn, ale také spolupracovat s partnery ze soukromého sektoru, kteří mají znalosti nejnovějších technologií a jsou schopni pomoci vybrané projekty realizovat.

2.6 Shrnutí vize cílového stavu ÚOOÚ a jeho architektury

Vizi cílového stavu architektury lze shrnout do několika málo bodů:

1. vnitřní procesy ÚOOÚ jsou digitalizované, výkon klíčových agend je podporován Agendovým informačním systémem;
2. ÚOOÚ se prezentuje novým moderním webem, který respektuje jednotnou vizuální identitu státu;
3. ÚOOÚ provozuje minimum HW, využívá cloudových služeb a v datovém centru běží pouze Firewall, HSM pro generování vlastních šifrovacích klíčů a síťová infrastruktura;
4. všechny informační systémy jsou provozovány bezpečně a dle pravidel stanovených ve vyhláškách a zákonech upravujících provoz a rozvoj informačních systémů veřejné správy;
5. IS ORG běží stabilně a bezpečně na podporovaném HW ve státním cloudu nebo na infrastruktuře ÚOOÚ.

2.7 Výběr klíčových změnových záměrů / projektů

Klíčové projekty pro naplnění vize jsou následující:

- AIS ÚOOÚ – Evidence stížností, podnětů, záznamů, rozhodnutí a kontrol, včetně DMS a definic workflow;
- Nový web ÚOOÚ a jeho rozvoj;
- Vyhodnocení výhodnosti a náročnosti přechodu informačních systémů ÚOOÚ do cloudu;
- Analýza možného řešení pro nahrazení modulu NOS (nevyžádaná obchodní sdělení);
- Projekt na uvedení ICT do souladu s novou VoDŘISVS;
- Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ;
- Obnovení HW IS ORG;
- Analýza přesunu provozu IS ORG na eGovernment Cloud.

2.8 Výběr klíčových změn v řízení ICT

Klíčové změny v řízení ICT:

- vznik řídícího výboru pro IT architekturu ÚOOÚ (dále jen ŘV ITA) jako zastřešující struktury pro řízení IT;
- strategické řízení IT na základě cílů stanovených v IK ÚOOÚ;
- přechod na nový systém IT podpory, který umožní lepší sledování a rychlejší podporu jednotlivých požadavků.

2.9 Základní podmínky realizovatelnosti změn

Zásadní pro realizaci vize IK ÚOOÚ je rozšíření útvaru IT o dvě vysoce odborné pracovní pozice:

1. Architekt kybernetické bezpečnosti;
2. IT architekt.

Dále je to přidělení finančních prostředků na provoz ÚOOÚ v řádech jednotek milionů korun ročně.

2.10 Jak číst IK ÚOOÚ

Dokument IK ÚOOÚ se skládá z několika částí, které postupně popisují danou problematiku.

- Část A: Koncepce architektury ***Část A: Koncepce architektury ÚOOÚ*** je o fungování úřadu jako celku. Popisuje činnosti ÚOOÚ v rámci jeho agend („co dělám a proč“) a jejich podporu informačními systémy a technologiemi („s čím to dělám“).
- Část B: Koncepce řízení služeb ICT***Část B: Koncepce řízení služeb ICT*** se zaměřuje na fungování ICT útvaru ÚOOÚ. Popisuje služby, které ICT poskytuje ostatním složkám úřadu, a způsob jejich řízení.

  Obě části (A i B) jsou členěny do čtyř kapitol, z nichž první poskytuje přehled stávajícího stavu, druhá popisuje motivace ke změnám (co je potřeba změnit a proč), třetí obsahuje high-level návrh cílového stavu (jak to bude vypadat po změnách) a čtvrtá definuje plán realizace popsaných změn (jakými projekty a kdy budou změny realizovány).
- *Část C* je o tom, jak bude tento dokument řízen a jak bude naplňován – postupy realizace změn, kontroly a vyhodnocování změn a odpovědnosti za plnění.
- *Část D* obsahuje různé dodatky, přílohy apod., ve kterých může čtenář najít vysvětlení, upřesnění nebo rozšíření informací z předchozích částí dokumentu.

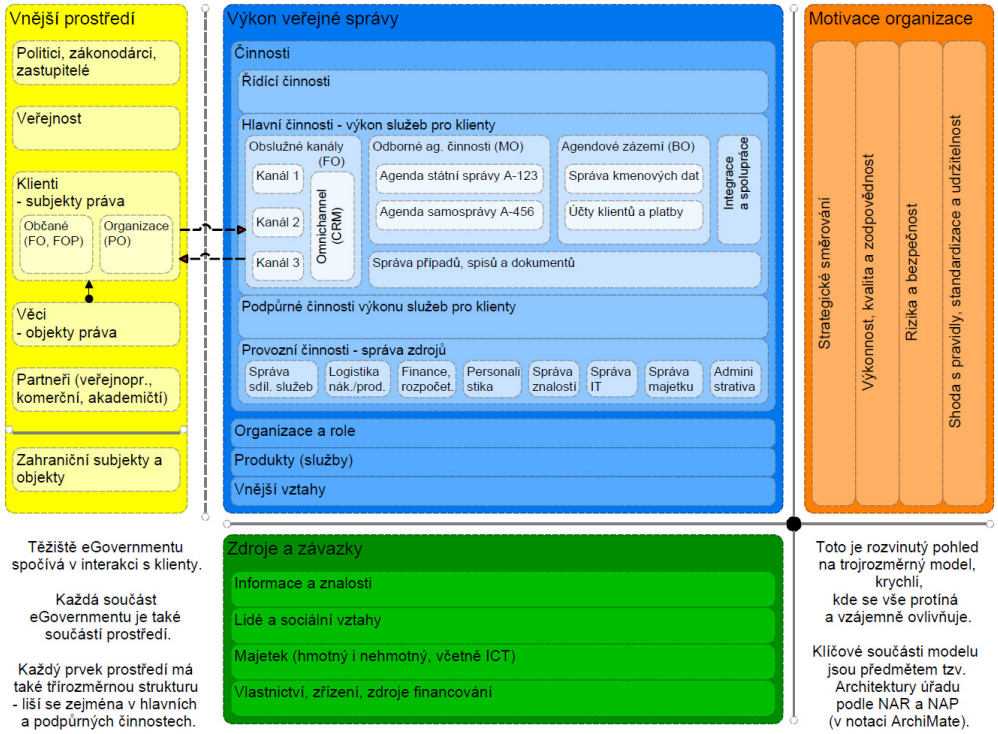
  Tato část obsahuje také přehled základních pojmů a zkratek ke snadnější orientaci v dokumentu.

ČÁST A: Koncepce architektury ÚOOÚ

Úvod do architektury ÚOOÚ

Pro popis organizace veřejné správy za účelem její digitální transformace a dlouhodobého řízení jejích informačních systémů se využívá manažerská metoda zvaná Architektura úřadu (EA).

Každou organizaci lze členit na Motivační část (oranžová), Výkonnou část (modrá) a část Správy zdrojů (zelená), které společně slouží klientům a ostatním zainteresovaným subjektům z Vnějšího prostředí (žlutá). Různé části mají pro konkrétní organizaci a konkrétní situaci různou důležitost, některými se zabývá více, jinými méně. Žádnou z nich ale nelze zcela pominout.



Obrázek 1: Celkový pohled na jakoukoli organizaci veřejné správy

Výše uvedené členění budeme v IK ÚOOÚ aplikovat a popisovat podle doporučení a metodiky Národního architektonického rámce (NAR): tj. domény (vrstvy) architektury výkonu veřejné správy rozdělením do čtyř architektonických vrstev, čtyř motivačních oblastí prostupujících všemi vrstvami, a transverzální vrstvou řízení.

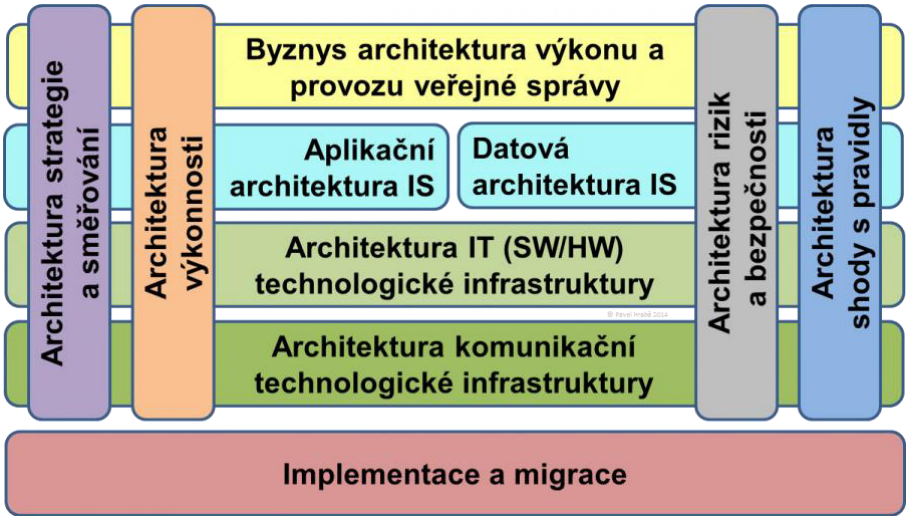
Jednotlivé vrstvy popisují:

- *byznys, jeho klienty a jim poskytované služby; nezbytné schopnosti a lidské, finanční a kapacitní zdroje,*
- *architekturu informačních systémů a dat v nich zpracovávaných,*
- *vrstvu IT technologické infrastruktury,*
- *vrstvu komunikační a síťové infrastruktury.*

Čtyři vertikální oblasti motivační architektury představují:

- *strategii a směrování úřadu, jeho cíle, účel a důvod existence,*
- *měření výkonnosti a efektivity, měření plnění strategie a provozní efektivity,*
- *řízení rizik a bezpečnosti, včetně (ale nejenom) té kybernetické,*
- *řízení shody s pravidly, naplňování zákonů, regulací, standardizace a dlouhodobá udržitelnost.*

Vrstva Implementace a migrace je transverzální vrstvou popisující řízení změn ve všech vrstvách a oblastech.



Obrázek 2: Struktura domén architektonického rámce NAP

Jednotlivé vrstvy a oblasti nejprve popíšeme z pohledu stávajícího stavu, identifikujeme silná a slabá místa a potřeby změn. Následně popíšeme ideální cílový stav.

Rozdíl mezi cílovým a aktuálním stavem potom definuje množinu změn, projektů, času, úsilí a zdrojů, nezbytných pro jeho dosažení. Je téměř jisté, že ne všeho lze dosáhnout hned a jednou velkou změnou, proto je třeba jednotlivé aktivity prioritizovat a seřadit do uskutečnitelné roadmapy.

1 PŘEHLED STÁVAJÍCÍHO STAVU

1.1 Zodpovědnosti a kompetence ÚOOÚ

ÚOOÚ, IČO 70837627, se sídlem Pplk. Sochora 727/27, 170 00 Praha 7, byl zřízen zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, s účinností od 1. června 2000. Tento právní základ byl dne 24. dubna 2019 transformován na zákon č. 111/2019 Sb., o zpracování osobních údajů (dále jen „zákon o zpracování osobních údajů“).

Podle § 50 odst. 1 zákona o zpracování osobních údajů je ÚOOÚ ústřední správní úřad pro oblast ochrany osobních údajů. To, že je úřad, znamená, že stát zákonem stanoví působnost (oblast činnosti) a pravomoci – souhrnně tedy kompetenci – a dá k tomu předpoklady materiální (budova, vybavení) i personální (zaměstnanci a prostředky na jejich platy). To, že je správní, znamená, že je součástí exekutivy (výkonné moci) a postupuje prostředky správního práva, primárně vydáváním rozhodnutí (správních aktů). To, že je ústřední, znamená, že pro celou Českou republiku je jen jeden. A konečně je ÚOOÚ dozorový úřad, což znamená, že porovnává ideální stav s reálným a vydává o tom autoritativní rozhodnutí, v čemž se řídí zákonem č. 255/2012 Sb., o kontrole (kontrolní řád).

Dozorový úřad monitoruje dodržování právních předpisů v oblasti ochrany osobních údajů a vymáhá je. ÚOOÚ se dále řídí i právními předpisy pro činnost správních úřadů, jako je zákon č. 500/2004 Sb., správní řád, a zákon č. 234/2014 Sb., o státní službě. Soudní spory, ve kterých je ÚOOÚ stranou, í se řídí zákonem č. 150/2002 Sb., soudní řád správní, a podpůrně rovněž zákonem č. 99/1963 Sb., občanský soudní řád.

Podle článku 52 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, GDPR) a § 51 zákona o zpracování osobních údajů je ÚOOÚ zcela nezávislý. To, že je nezávislý, znamená, že mu vláda nesmí udílet žádné pokyny, ani jeho činnost přímo ovlivňovat. Příslovečné určení „zcela“ znamená, že nezávislost ÚOOÚ nesmí být vládou ohrožena ani nepřímo, tj. takovým opatřením, které by mělo tyto důsledky.

Působnost

V primární působnosti ÚOOÚ je ochrana osobních údajů. Podle § 1 zákona o zpracování osobních údajů jsou k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravena práva a povinnosti při zpracování osobních údajů. Soukromí patří mezi obecné osobní projevy, které jsou jedním z prvků ochrany osobnosti jako nehmotného statku. Obecná působnost ÚOOÚ v ochraně osobních údajů je konkrétně vymezena v článku 57 obecného nařízení o ochraně osobních údajů jako „úkoly“ (angl. tasks) a ÚOOÚ má k tomu v článku 58 obecného nařízení o ochraně osobních údajů „pravomoci“ (angl. powers), které se promítají do § 54 zákona o zpracování osobních údajů jako „činnosti ÚOOÚ“, přičemž pouze odstavec 1 a částečně odstavec 3 jsou promítnutím obecného nařízení o ochraně osobních údajů. Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (dále jen „směrnice (EU) 2016/680“) stanoví v čl. 46 rovněž působnost ÚOOÚ v oblasti zpracováních osobních údajů za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a

ochranných opatření, zajišťování bezpečnosti státu nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, přičemž transpozici úkolů ÚOOÚ nalezneme v § 54 odst. 2 zákona o zpracování osobních údajů.

Ochrana osobních údajů má mezinárodní základ v Úmluvě Rady Evropy č. 108 z roku 1981 a jejích protokolech, článku 8 Charty základních práv EU a článku 16 Smlouvy o fungování Evropské unie. V Evropském hospodářském prostoru a Švýcarské konfederaci tak vzniklo území unifikované ochrany osobních údajů. V národním právu jsou základem články 7, 10 odst. 3 a 13 Listiny základních práv a svobod a zákon č. 89/2012 Sb., občanský zákoník.

Obecná regulace ochrany osobních údajů spočívá v obecném nařízení o ochraně osobních údajů, směrnici (EU) 2016/680 a prováděcím (adaptačním) a transpozičním zákoně č. 110/2019 Sb., o zpracování osobních údajů.

ÚOOÚ je jediným dozorovým úřadem s obecnou působností v oblasti ochrany osobních údajů v České republice. Z jeho působnosti je na jedné straně vyňato zpracování osobních údajů některými skupinami správců, na straně druhé jeho role zahrnuje ochranu osobních údajů v oblastech nespadajících do působnosti obecného nařízení o ochraně osobních údajů.

Jedním z úkolů ÚOOÚ je napravit chybné procedury zpracování osobních údajů správci nebo zpracovateli osobních údajů. ÚOOÚ se rovněž zabývá nedostatečnou ochranou osobních údajů, která má systémový přesah, tj. z její nápravy bude profitovat větší množství subjektů údajů. Ke zkvalitnění a prohloubení ochrany osobních údajů v mikrosvětě správců osobních údajů existuje řada nových nástrojů, k nimž mimo jiné patří regulace předávání osobních údajů do třetích zemí a mezinárodním organizacím, posuzování vlivu na ochranu osobních údajů, kodexy chování a vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů.

ÚOOÚ se originárně nezabývá těmi zpracováními osobních údajů, u nichž je normotvorba v působnosti regulátora sektoru – ministerstva. Regulátoři stanoví pravidla správcům a zpracovatelům osobních údajů pro sektorová zpracování osobních údajů a ÚOOÚ nad tím jen dozírá. Nejedná-li se o obecné zpracování osobních údajů, je v takové věci nutné se obrátit na gestora právní oblasti (ministerstvo), který má k tomu jmenovaného pověřence pro ochranu osobních údajů (DPO). Ministerstvo řídí jím spravovanou oblast i v otázkách ochrany osobních údajů, které jsou různou měrou upraveny zvláštními právními předpisy. Do systémového selhání regulátora ÚOOÚ jako dozorový úřad v oblasti ochrany osobních údajů obvykle vstupuje až následně. Neposkytuje tedy detailní vyjádření týkající se ochrany osobních údajů v daných sektorech, aniž by příslušnému gestorovi umožnil možnost nápravy, například tvorbou či změnou pravidel, včetně zpracování soupisu vhodných pravidel, zohledňujících specifika daného odvětví, jež se promítají do práce s osobními údaji. Má-li subjekt údajů ke správci osobních údajů přímý právní vztah, měl by se nejdříve obrátit na něj, a teprve tehdy, je-li nespokojen s vyřízením své žádosti, na ÚOOÚ.

Podle článku 57 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů je působností ÚOOÚ zvyšovat povědomí veřejnosti o ochraně osobních údajů (osvětová role) a podle písmene c) veřejnému sektoru a zástupcům odborných, profesních a průmyslových sdružení poskytovat konzultace k aplikaci obecného nařízení o ochraně osobních údajů (konzultační role). ÚOOÚ se především se vyjadřuje k návrhům postupů při plnění povinností uložených správcům, včetně jejich vztahu s osobami, jejichž osobní údaje tito správci zpracovávají. Konzultace poskytuje jednotlivým správcům a rovněž osobám, které se domnívají, že jejich osobní údaje jsou zpracovávány v rozporu s právními předpisy. Šířeji

využitelné výstupy z konzultací zveřejňuje ÚOOÚ na svých webových stránkách a v odůvodněných případech organizuje veřejnou diskusi k návrhům metodik určených obecně správcům.

ÚOOÚ rovněž zveřejňuje překlady dokumentů z oblasti ochrany osobních údajů Globálního shromáždění pro ochranu soukromí (GPA) a k jednotlivým aplikačním otázkámobecného nařízení o ochraně osobních údajů, na jejichž vypracování se spolupodílí jako člen Evropského sboru pro ochranu osobních údajů (EDPB), nebo které vypracoval Evropský inspektor ochrany údajů (EDPS). V rámci poradenství se ÚOOÚ vyjadřuje k návrhům právních předpisů, je – li o to požádán ministerstvem, vládou nebo Parlamentem, případně i z vlastního iniciativy.

Vedle ochrany osobních údajů je dalším pilířem činnosti ÚOOÚ agenda svobodného přístupu k informacím, v níž je ÚOOÚ svěřena dílčí působnost nadřízeného, přezkumného a nečinnostního orgánu v rozsahu vymezeném ustanoveními § 16b a § 20 odst. 5 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Třetím pilířem činnosti ÚOOÚ je provozování kritického informačního systému poskytujícího zdrojové a agendové identifikátory fyzických osob (elektronické identifikátory podle § 11 zákona č. 111/2009 Sb., o základních registrech). Uzavřený a organizačně oddělený systém (IS ORG) funguje jako součást základních registrů.

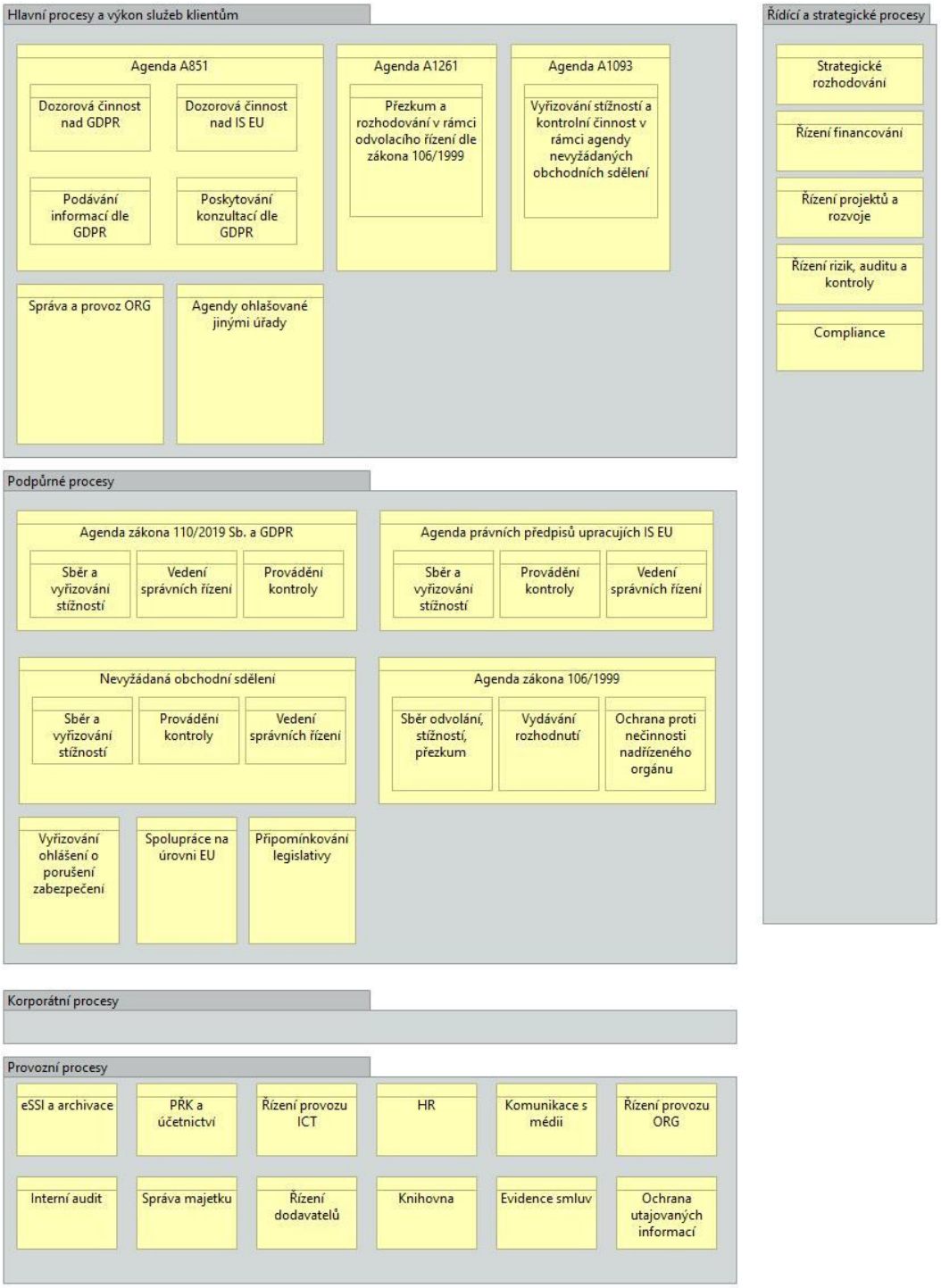
Další oblasti, ve kterých ÚOOÚ plní úkoly svěřené mu zákonem:

1) šíření obchodních sdělení podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti),

2) zvláštní dozor, například § 80b odst. 3 věta druhá a § 80c odst. 4 věta první zákona č. 273/2008 Sb., o Policii České republiky, a

3) zvláštní správní trestání, například porušení zákazu zveřejnění osobních údajů podle § 61 zákona o zpracování osobních údajů, § 7 písm. f) zákona č. 40/1995 Sb., o regulaci reklamy a o změně a doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů, § 34a odst. 4 a § 34c odst. 4 zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb, o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), § 17e odst. 6 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), § 25 odst. 2 zákona č. 159/2006 Sb., o střetu zájmů, a § 61 zákona o zpracování osobních údajů.

1.2 Přehled byznys architektury



Obrázek 3: Nejvyšší úroveň procesní dekompozice podle referenčního modelu NAR

1.2.1 Hlavní a podpůrné procesy

1.2.1.1 Stav agend ohlašovaných ÚOOÚ

V rámci mapování stavu digitalizace byla z pohledu metodiky doporučena cesta stanovení stupňů, a jejich pomocí následně kategorizace míry digitalizace v rámci jednotlivých agend, procesů a organizačních celků. Tyto stupně tak budou aplikovány i v dalších kapitolách IK ÚOOÚ.

Stupeň digitalizace	Popis
0	Papírová pošta, předávání papírových spisů, nulová míra digitalizace fungování ÚOOÚ.
1	Využívání kancelářských aplikací, e-mailu a nástrojů na spolupráci pro řešení pracovních úkolů.
2	Oběh dokumentů zajištěný spisovou službou, využívání datových schránek pro digitalizaci úkonů.
3	Využívání agendových informačních systémů pro optimalizaci výkonu agendy, digitalizace vnitřních procesů do jisté míry.
4	Kompletní digitalizace vnitřních procesů, optimální výkon ÚOOÚ.
5	Kompletní digitalizace vnitřních i vnějších procesů a komunikace ÚOOÚ s občany.

Tabulka 1: Přehled ohlášených agend

Ohlášená agenda	Odbor správce agendy	Agendový IS	Stav digitalizace
A 851	ÚOOÚ jako celek	Neexistuje	Jediným elektronickým nástrojem využívaným při vykonávání agendy jsou datové schránky a elektronická pošta. Používáme pro výkon agendy spisovou službu. Stupeň digitalizace: 2

1.2.1.2 Stav agend, v nichž ÚOOÚ působí, ale neohlašuje je

Tabulka 2: Přehled agend působení ÚOOÚ - vedle ohlášených

Agenda působení	Odbor správce agendy	Agendový IS	Stav digitalizace
A1261	MV	Neexistuje	Je digitalizováno ve formě formuláře na Portálu občana, který je volně k dispozici s přihlášením i bez. V případě přihlášení elektronickou identitou je předvyplněn ze základních registrů.

			Používáme pro výkon agendy spisovou službu. Stupeň digitalizace: 2
A1093	MPO	Neexistuje	Již nepodporovaný systém IS ÚOOÚ má poslední funkční modul NOS pro nevyžádaná obchodní sdělení, který automaticky generuje spis do spisové služby a vytváří seznam stížností na nevyžádaná obchodní sdělení. Je však nutná jeho revitalizace. Stupeň digitalizace: 3
A1083	MPO	Neexistuje	Vykonáváme v rámci hlavního procesu Dozorová činnost nad GDPR. Používáme pro výkon agendy spisovou službu. Stupeň digitalizace: 2
A115	MV	Neexistuje	Speciální dozorová pravomoc, vykonávána v rámci hlavního procesu Dozorová činnost nad GDPR. Stupeň digitalizace: 2
A117	MV	Neexistuje	Zastaralé ohlášení agendy ze strany MV, v současně platném předpisu již ÚOOÚ nefiguruje.
A118	MV	Neexistuje	Speciální dozorová pravomoc, vykonávána v rámci hlavního procesu Dozorová činnost nad GDPR. Stupeň digitalizace: 2
A1761	MV	Neexistuje	Máme právo nahlížet do osobního spisu, opět využíváno v rámci hlavního procesu Dozorová činnost nad GDPR. Stupeň digitalizace: 2
A1941	MV	Neexistuje	Zákon o střetu zájmů, ÚOOÚ řeší přestupky, vykonáváno v rámci hlavního procesu Dozorová činnost nad GDPR. Stupeň digitalizace: 2
A304	MV	Neexistuje	Máme ohlášenou působnost, ale pouze plníme povinnosti, které platí pro všechny úřady.
A750	MPO	Neexistuje	Vykonáváno v rámci hlavního procesu Vyřizování stížností a kontrolní činnost

			v rámci agendy nevyžádaných obchodních sdělení. Stupeň digitalizace: 3

1.2.1.3 Jiné činnosti při výkonu veřejné správy

Žádné jiné činnosti dle definice v rámci IK ÚOOÚ nevykonává.

1.2.1.4 Shoda skutečnosti a záznamů v RPP

V současnosti jsou ohlášeny v rámci agendy A851 služby a úkony veřejné správy. Vedle toho ÚOOÚ má ohlášen i významný IS pod názvem IS ÚOOÚ. Ohlášení agendy je aktuální.

Ohlášení informačních systémů však bude vyžadovat revizi. Ohlášení IS ÚOOÚ bylo vytvořeno do jisté míry účelově a není přehledné. V souvislosti s aktivitami spojenými s kybernetickou bezpečností je v plánu ohlášení změnit. Stejně tak je nutné se v rámci ohlášení IS nějakým způsobem postavit k IS ORG, který do této chvíle nebyl nijak ohlášen. V tuto chvíli počítáme s ohlášením nové agendy, přímo pro IS ORG.

Ohledně digitalizace deklarovalo ÚOOÚ v rámci katalogu služeb, že naprostá většina úkonů může být provedena elektronicky. ÚOOÚ má specifickou agendu, která umožňuje podávání stížností a podnětů bez nutnosti identifikace, z čehož vyplývá i možnost využití například e-mailu. Každopádně všechny služby, které poskytujeme občanům lze podat přes datovou schránku. V případě agendy Nevyžádaných obchodních sdělení je pak možné podat i přes elektronický formulář, a zároveň se v průběhu řízení i dozvědět stav podání. Tyto informace jsou v katalogu služeb obsaženy.

1.2.2 Stav řídících, provozních a korporátních činností a jejich IT podpory

Tabulka 3: Přehled řídících, provozních a korporátních činností

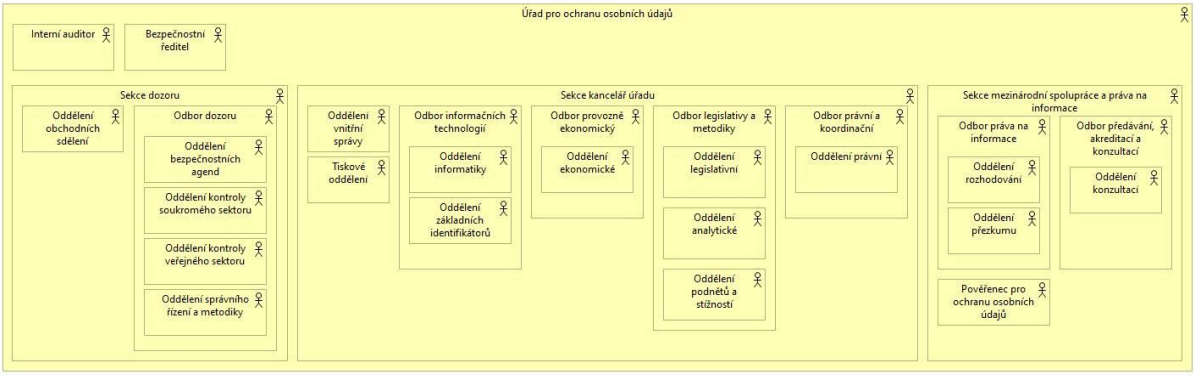
Činnost	Odpovědný odbor	IS	Stav digitalizace
Strategické rozhodování	Sekce kancelář úřadu ve spolupráci s dalšími sekcemi	• Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu. Stupeň digitalizace: 2
Řízení financování	Odbor provozně ekonomický	• Croseus, EIS JASU	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK a SW na správu účetnictví. Stupeň digitalizace: 3
Řízení projektů a rozvoje	Odbor informačních technologií	• Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS

			Outlook. Dále využívá elektronickou spisovou službu. Stupeň digitalizace: 2
Personální správa	Oddělení vnitřní správy	• Avensio	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Využívá elektronickou spisovou službu, SW pro výkon PŘK. Dále využívá software pro podporu procesů personální správy a zejména výpočtu a zpracování platů zaměstnanců Úřadu. Stupeň digitalizace: 2
Řízení rizik, auditů a kontroly	Interní auditor a Bezpečnostní ředitel	• Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu. Stupeň digitalizace: 2
Compliance	Odbor informačních technologií	• Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu. Stupeň digitalizace: 2

1.2.2.1 Procesy zaměřené na spolupráci

Na ÚOOÚ funguje cloudová technologie Microsoft 365, byla zavedena primárně v reakci na přijatá mimořádná opatření v souvislosti s vypuknutím pandemie onemocnění Covid-19. Její funkce typu kolaboračního SW MS Teams a MS Sharepoint jsou využívány v omezeném rozsahu. Do budoucna plánujeme jejich zásadnější využití. Tomuto kroku ale bude předcházet analýza aktiv, která určí, jaká data jsou vhodná pro ukládání na cloud a jaká ne.

1.2.3 Přehled digitalizace z pohledu organizační struktury



Obrázek 4: Organizační struktura ÚOOÚ.

Tabulka 4: Přehled dle organizační struktury ÚOOÚ a míry digitalizace útvarů

Útvar / odbor	Činnost působení, předpis, zákon	IS	Stav digitalizace
Interní auditor	Společně s bezpečnostním ředitelem zajišťuje strategický a řídící proces Řízení rizik, auditu a kontroly. Zajišťuje provozní proces Interní audit.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK a SW na správu účetnictví. Stupeň digitalizace: 2
Bezpečnostní ředitel	Zajišťuje výkon činností týkajících se administrativní bezpečnosti, registru utajovaných informací a povinností SBS v oblasti informačních systémů veřejné správy. Společně s interním auditorem zajišťuje strategický a řídící proces Řízení rizik, auditu a kontroly. Zároveň vykonává roli manažera kybernetické bezpečnosti.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Stupeň digitalizace: 2
Oddělení obchodních sdělení	Vykonává působnost ÚOOÚ v agendě A1093, zajišťuje hlavní proces vyřizování stížností a kontrolní činnost v rámci agendy nevyžádaných obchodních sdělení. Zajišťuje i s tím související podpůrné procesy: Sběr a vyřizování stížností v rámci NOS; Provádění kontroly v rámci NOS a Vedení správních řízení v rámci NOS.	IS ÚOOÚ	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Vedle toho je agenda digitalizována speciálním modulem v IS ÚOOÚ, který automaticky vytváří z podnětů spis do GINIS a vede statistiky. Stupeň digitalizace: 3
Odbor dozoru	Vykonává působnost ÚOOÚ v oblasti agendy A851, konkrétně Dozorovou činnost nad GDPR a dozorovou činnost nad IS EU. Zároveň zajišťuje všechny s tím související podpůrné procesy.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK.

			Stupeň digitalizace: 2
Tiskové oddělení	Zajišťuje primárně provozní proces Komunikace s médii. Dále zajišťuje provozní proces Knihovna.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Dále využívá SW na správu knihovních výpůjček. Stupeň digitalizace: 2
Oddělení vnitřní správy	Zajišťuje provozní proces personální správy a provozní proces příjmu podání a vyřazování písemností a komponent v rámci skartačního řízení v eSSL včetně zajištění výkonu spisovny. Dále zajišťuje provozní proces veřejných zakázek/řízení dodavatelů.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Dále využívá software pro podporu personální správy. Stupeň digitalizace: 2
Odbor legislativy a metodiky	Zajišťuje podpůrné procesy Připomínkování legislativních i nelegislativních materiálů, včetně interních aktů řízení, Sběr a vyřizování stížností a podnětů na základě zákona č. 110/2019 Sb. a GDPR a Vyřizování ohlášení o porušení zabezpečení. Nad rámec této činnosti zajišťuje plnění povinností vyplývajících Úřadu jako povinnému subjektu ze zákona č. 106/1999 Sb.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Stupeň digitalizace: 2
Odbor provozně ekonomický	Zajišťuje provozní procesy PŘK a účetnictví, Správa majetku a Řízení dodavatelů. Zároveň zajišťuje řídící a strategický proces Řízení financování a podílí se na řídícím a strategickém procesu Řízení rizik, auditu a kontroly.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK a SW na správu účetnictví. Stupeň digitalizace: 3

Odbor informačních technologií	Zajišťuje hlavní proces Správa a provoz IS ORG, dále zajišťuje vedlejší procesy Řízení provozu ICT, Řízení provozu IS ORG a Řízení dodavatelů. Významně se podílí na řídících a strategických procesech Řízení projektů a rozvoje a Compliance. Zajišťuje technickou část provozního procesu Evidence smluv.	IS ÚOOÚ, IS ORG	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Kompletně digitalizován je i provoz IS ORG, za využití Service desku a Řídícího pracoviště, z nějž je možný vzdálený přístup ke správě systému. Stupeň digitalizace: 3
Odbor právní a koordinační	Zajišťuje činnost rozkladové komise pro hlavní procesy a podpůrné procesy v rámci agendy A851. Zajišťuje metodickou a výkonnou část provozního procesu Evidence smluv.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Metodicky vede a využívá systém evidence smluv. Stupeň digitalizace: 2
Odbor práva na informace	Zajišťuje výkon působnosti v rámci agendy A1261 Přezkum a rozhodování v rámci odvolacího řízení dle zákona 106/1999, a s tím související podpůrné procesy, tedy sběr odvolání, stížností a přezkum, vydávání rozhodnutí a ochranu proti nečinnosti nadřízeného orgánu.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Stupeň digitalizace: 2
Odbor předávání, akreditací a konzultací	Zajišťuje subprocesy v rámci hlavního procesu výkonu agendy A851, konkrétně subproces Podávání informací dle GDPR a Poskytování konzultací dle GDPR.	Není	Digitalizována běžná činnost formou elektronické pošty zajištěné aplikací MS Outlook. Dále využívá elektronickou spisovou službu, SW pro výkon PŘK. Stupeň digitalizace: 2

Výše uvedená tabulka je organizována dle odborů, zmíněné odbory zahrnují i jim podřízená oddělení. Výjimku tvoří oddělení podřízená přímo ředitelům sekcí, ta jsou zmíněna taktéž speciálně.

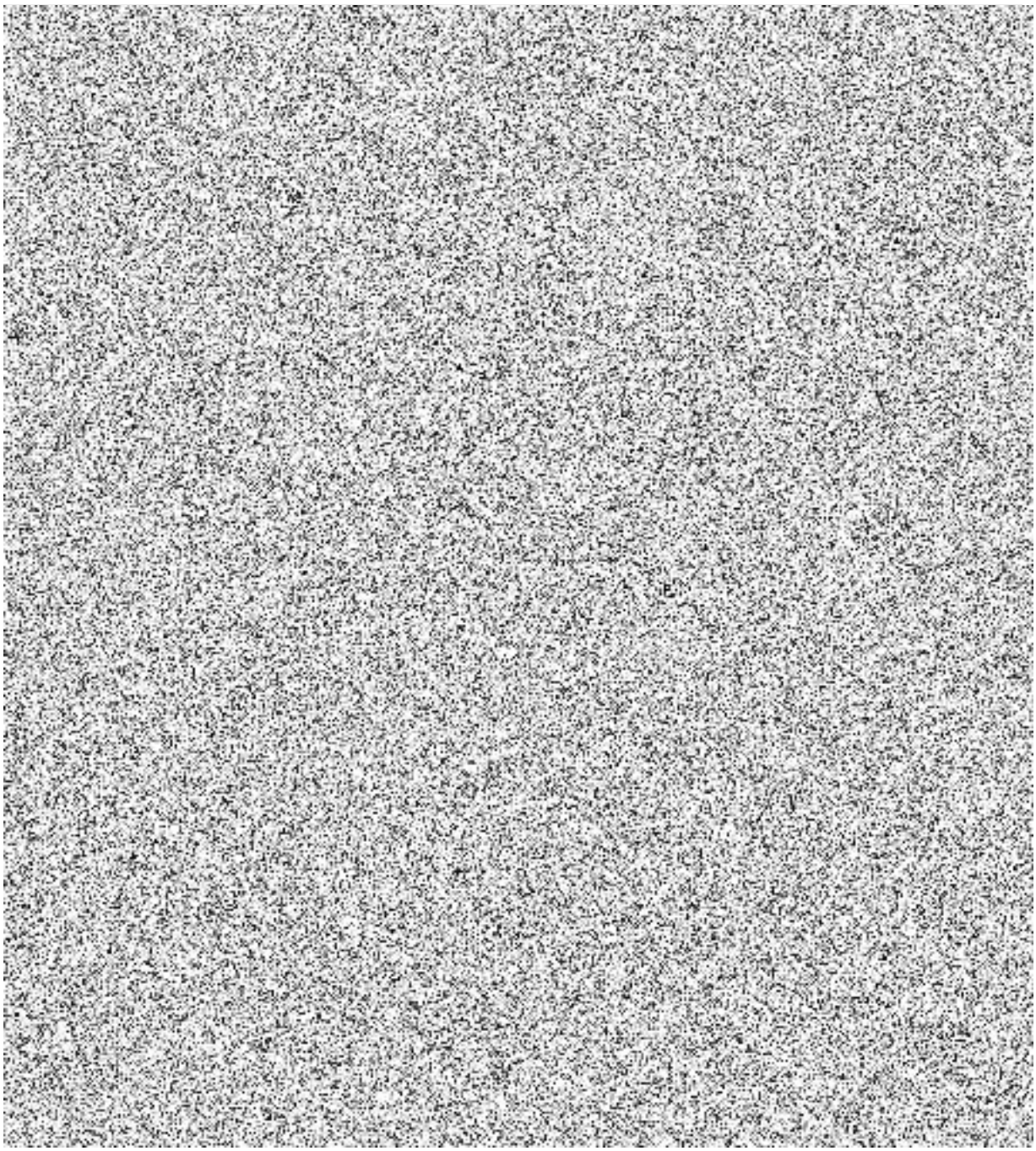
1.2.4 Shrnutí potřeb ze stávajícího stavu byznys architektury

Ze zjištěného vyplývá potřeba rozšířit počet digitalizovaných procesů. V rámci hlavních procesů jsou digitalizovány pouze činnosti související s výkonem agendy v oblasti Nevyžádaných obchodních sdělení, je to však způsobem, který není dlouhodobě udržitelný, a bude nutné hledat nová řešení. Ostatní procesy, zejména Dozorová činnost nad GDPR a Dozorová činnost nad IS EU jsou digitalizovány velmi omezeně. Vzhledem k tomu, že tyto činnosti jsou z pohledu byznys architektury těmi nejzásadnějšími a obecně strategicky jsou považovány za primární účel fungování ÚOOÚ, měla by jim být věnována dostatečná pozornost i v rámci digitalizace.

Ohledně dosahovaných stupňů digitalizace je obecným strategickým cílem ÚOOÚ dosáhnout na stupeň 4. Nicméně vzhledem k finančním, personálním a časovým možnostem ÚOOÚ bude primární důraz kladen na zvýšení stupně digitalizace na 3 u hlavních agend ÚOOÚ, zejména u procesů spojených s GDPR a odborem dozoru. V těchto procesech chybí jednotná evidence primárních dat. Pro zvýšení efektivity fungování ÚOOÚ by bylo vhodné vytvořit jednotnou databázi kontrol, rozhodnutí, podnětů i stížností a dalších podání Ta by pak měla sloužit jako prostředí pro zajištění jednotného rozhodování ÚOOÚ v obdobných případech, lepšímu přehledu o činnosti ÚOOÚ a zjednodušení dohledání starších, ale zásadních případů.

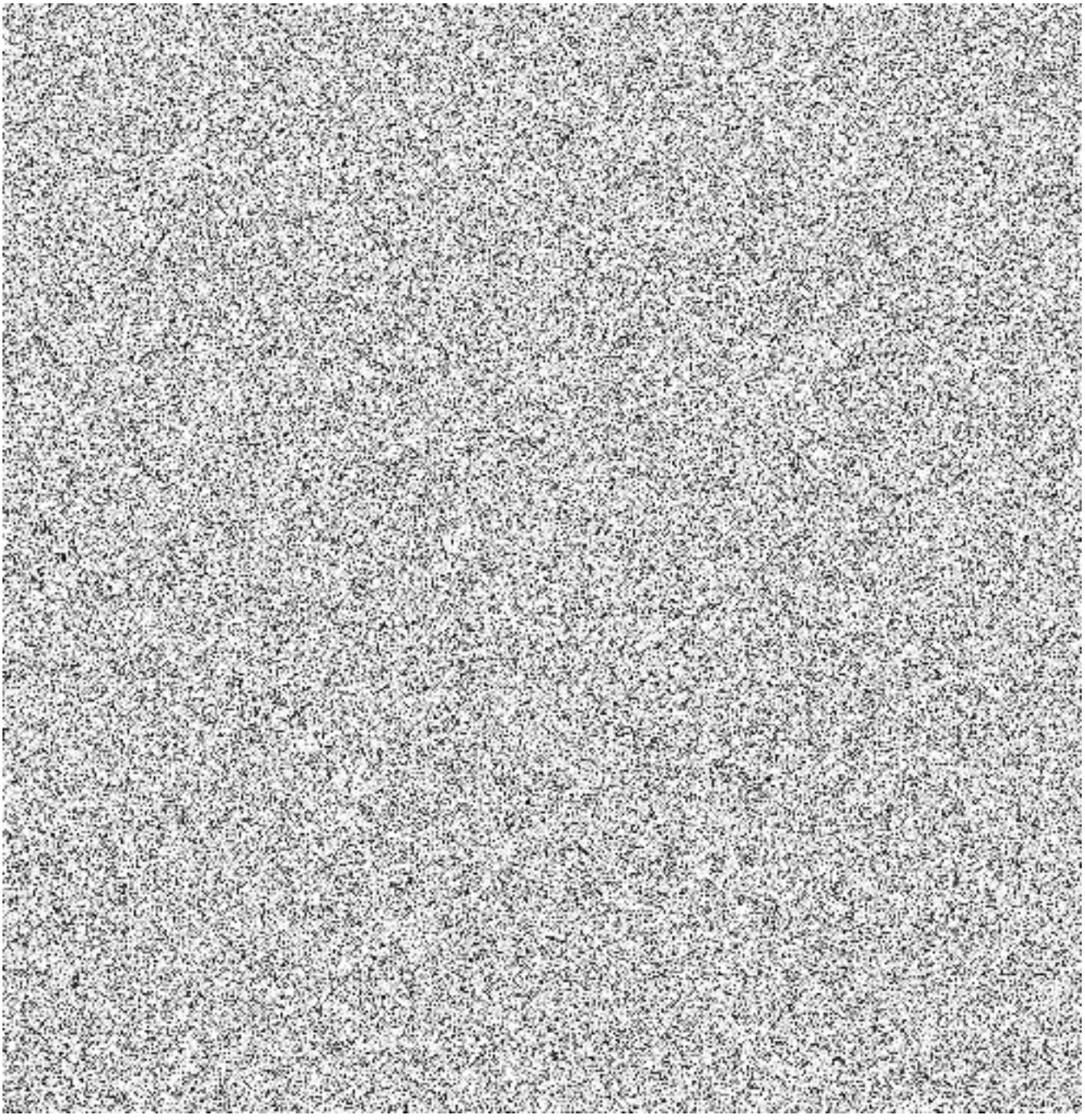
1.3 Aplikační architektura informačních systémů ÚOOÚ

1.3.1 Přehled a klasifikace všech informačních systémů ÚOOÚ



Obrázek 5: Rozdělení aplikací podle funkčních oblastí

1.3.2 Přehled ISVS a provozních ISVS ve správě ÚOOÚ



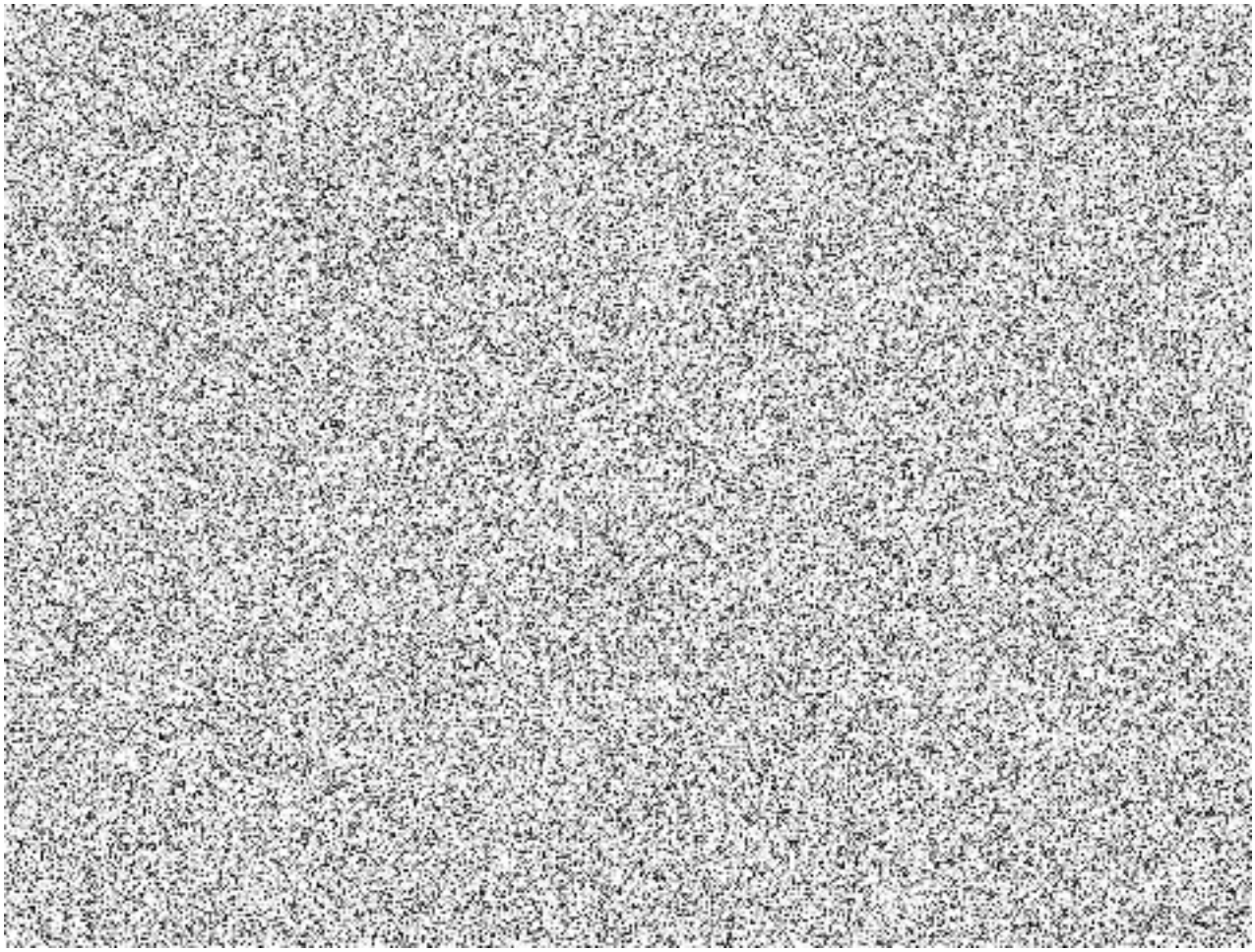
1.3.4 Nástroje podporující spolupráci

Na ÚOOÚ funguje cloudová technologie Microsoft 365, byla zavedena primárně v reakci na mimořádná vládní opatření přijatá v souvislosti s pandemií Covid-19. Její funkce typu kolaboračního SW MS Teams a MS Sharepoint jsou využívány v omezeném rozsahu. Do budoucna plánujeme jejich zásadnější využití. Tomuto kroku ale bude předcházet analýza aktiv, která určí, jaká data jsou vhodná pro ukládání na cloud a jaká ne.

Bezpečnost dat samotných je zajišťována formou smlouvy s dodavatelem. Sekundárním bezpečnostním prvkem se pak stane v rozřazení jednotlivých datových prvků do skupin dle jejich

citlivosti. Obecně počítáme s tím, že budou v cloudu ukládány pouze datové prvky označené jako „white“ a „green“, tedy ty, u nichž riziko zneužití není velké. Datové prvky označené jako „amber“ a „red“ budeme držet mimo cloudové technologie na infrastruktuře ÚOOÚ či na cloudovém úložišti zašifrovaném klíči ve správě ÚOOÚ.

1.3.5 Využití klíčových sdílených služeb eGovernmentu a externích IS



1.3.6 Využití cloud řešení

V současnosti ÚOOÚ využívá Microsoft 365 v jeho cloudové verzi. K přechodu na kompletní cloudové řešení elektronické pošty došlo v souvislosti s pandemií Covid-19. Licence obsahuje kompletní poskytování emailových služeb, využívání kancelářských aplikací a nástrojů pro týmovou spolupráci, jako je MS Teams a Onedrive.

Obecně je potenciál pro využití cloudu v rámci interního IT obrovské. Není příliš efektivní udržovat vlastní datové centrum ÚOOÚ při velikosti organizace do cca 150 zaměstnanců. V současnosti však probíhá analýza aktiv ÚOOÚ, ze které vyplyne, jaká data jsou pro ÚOOÚ citlivá. Obecně počítáme s tím, že budou v cloudu ukládány pouze datové prvky označené jako „white“ a „green“, tedy ty, u nichž riziko zneužití není velké. Datové prvky označené jako „amber“ a „red“ budeme držet mimo cloudové technologie na infrastruktuře ÚOOÚ či na cloudovém úložišti zašifrovaném klíči ve správě ÚOOÚ.

Co se týče infrastruktury, lze konstatovat, že bude potřeba vyšší výpočetní výkon pro jakýkoliv rozvoj IT a digitalizace procesů či služeb. I zde by pro organizaci velikosti ÚOOÚ bylo daleko hospodárnější využít cloud, než dále rozšiřovat a provozovat své datové centrum. Opět je ale zásadní citlivá data šifrovat klíči ve správě ÚOOÚ.

Pro dlouhodobé fungování ÚOOÚ je nutné si uvědomit také neustále stoupající nároky na jednotlivé odbory IT ze strany centrálního eGovernmentu a plnění nových zákonných povinností. Pokud není vizí celé české veřejné správy stále zvyšovat počet pracovníků IT na jednotlivých úřadech, jeví se využívání externích služeb jako cloud jednou z reálných cest.

1.3.7 Integrační model aplikační architektury

ZR pro potřeby agendy A851, toto napojení je technicky realizováno za využití spisové služby. Vedle toho je ÚOOÚ napojen na CMS a KIVS primárně pro potřeby skládání úřednických zkoušek.

V rámci IS ORG je ÚOOÚ napojen na CMS a KIVS taktéž, ale toto napojení je naprosto oddělené od napojení pro potřeby vnitřního IT ÚOOÚ. IS ORG komunikuje pouze s ISZR.

ÚOOÚ neposkytuje žádné aplikační služby třetím stranám, ani v tuto chvíli nevyužívá možnosti propojeného datového fondu. Důvodem je specifikum ÚOOÚ, kdy se klienti nemusí ve styku s ÚOOÚ identifikovat, ale mohou podávat podání i anonymním způsobem. Na druhou stranu ÚOOÚ nemá žádná strukturovaná data, která by mohl sdílet.

1.3.8 Shrnutí potřeb ze stávajícího stavu aplikační architektury

První nepochybnou aplikační potřebou je maximalizovat využití nástrojů a systému již nakoupených a funkčních. Možnosti cloudových produktů společnosti Microsoft nejsou využity na maximum. To se týká zejména aplikace Sharepoint Online. Předpokladem rozvoje tímto směrem je jasná definice datových sad, které budeme z pohledu bezpečnosti ochotni v cloudu uchovávat.

Prostor pro zlepšení je také v ohlášení IS do RPP. Je nutné vypořádat se s ohlášením IS ORG a změnit parametry ohlášení IS ÚOOÚ, který se bude razantně měnit.

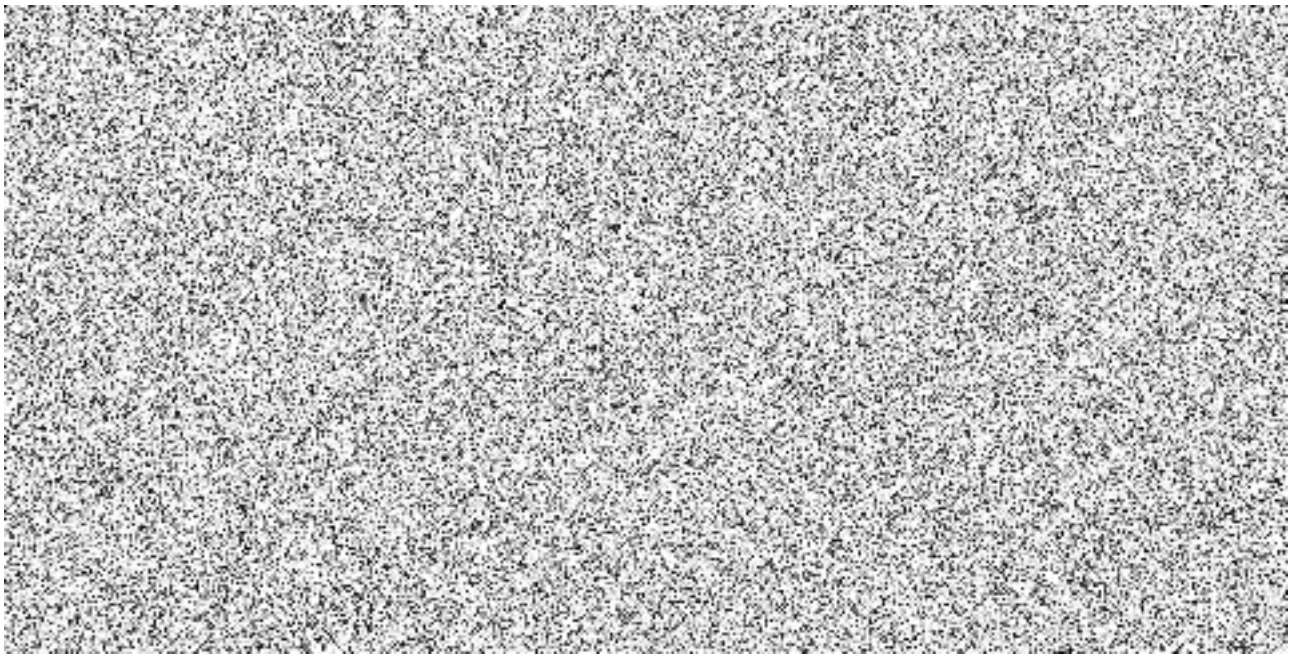
Důležitým zjištěním a potřebou je také nutnost zajištění kontinuity, tedy nahrazení funkcí IS ÚOOÚ. Tento systém v současnosti není podporován i přes to, že je využíván pro agendu Nevyžádaných obchodních sdělení. Nahrazení tohoto systému, případně udržení jeho funkčnosti, je zásadním úkolem IK ÚOOÚ.

1.4 Datová architektura informačních systémů ÚOOÚ

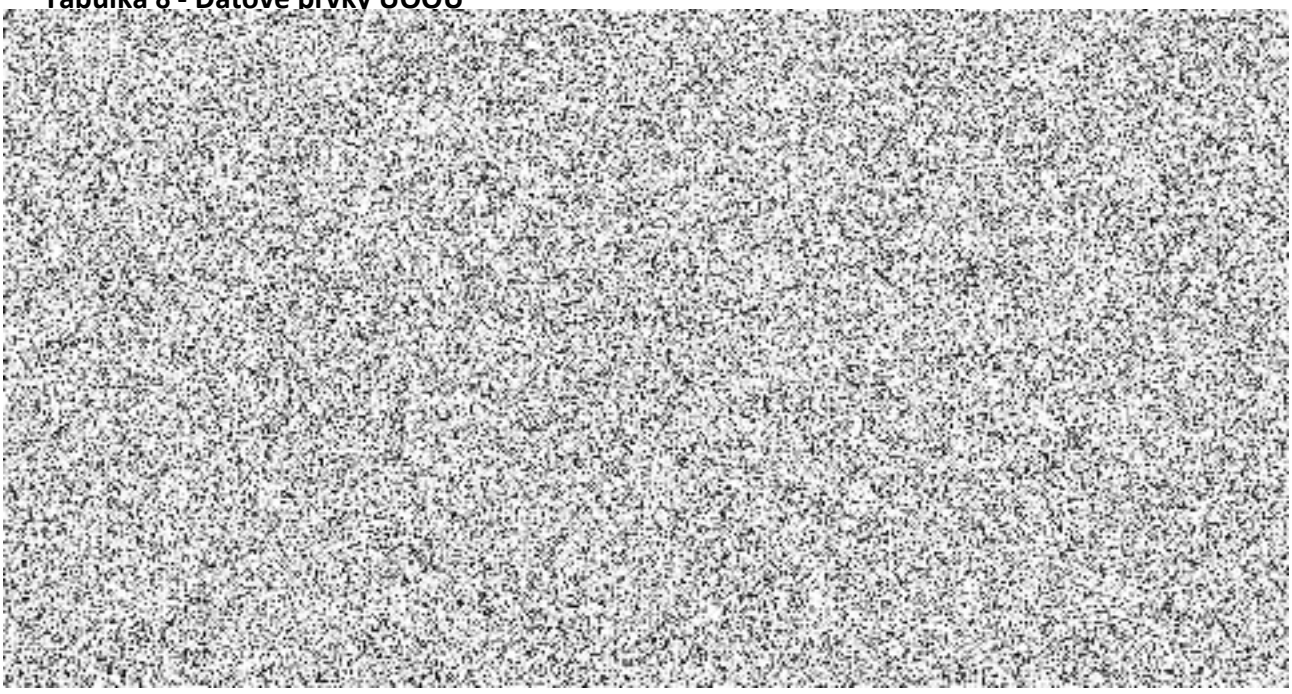
1.4.1 Základní charakteristiky datové architektury

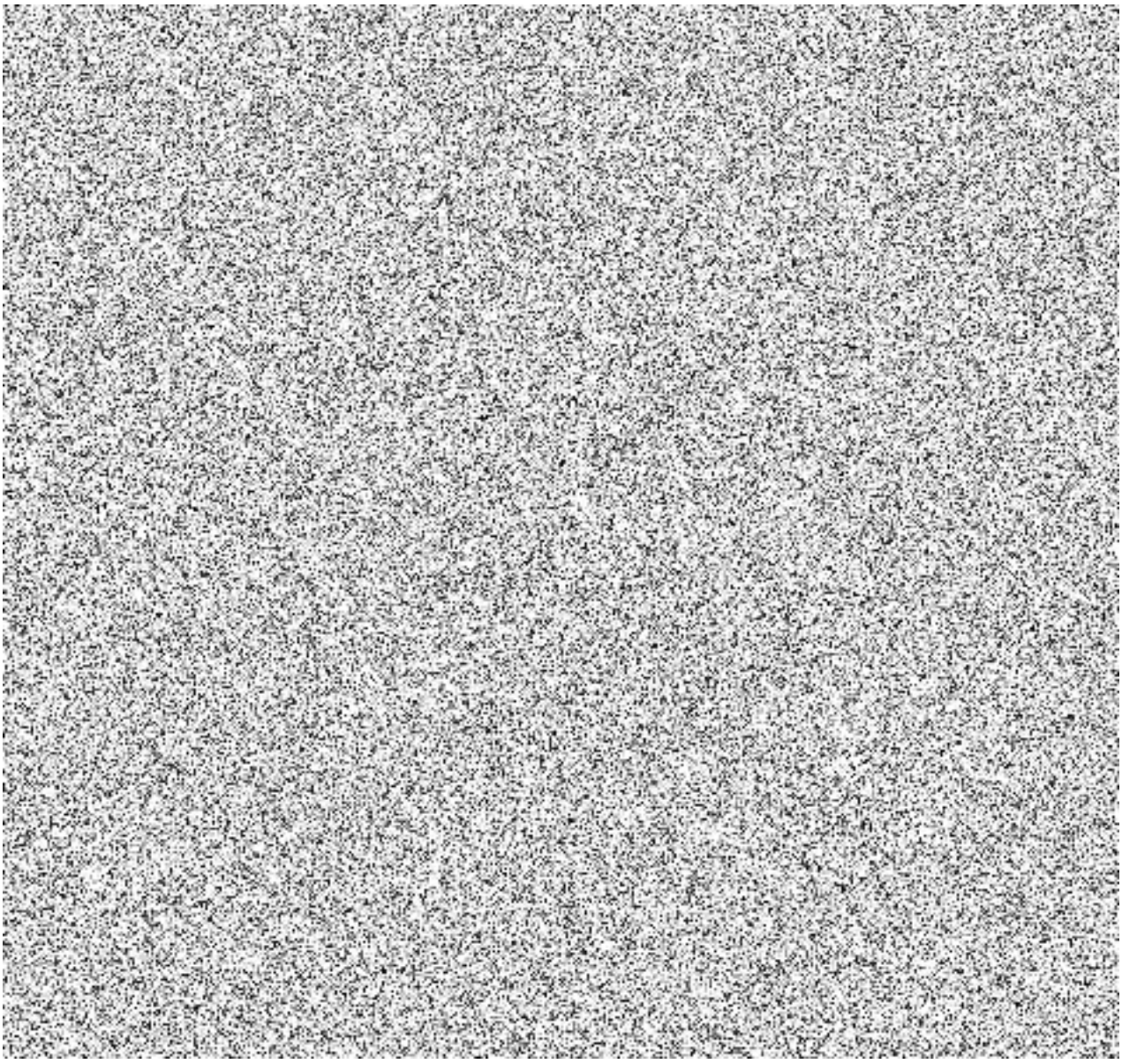
Před začátkem vytváření IK ÚOOÚ datové modely v rámci ÚOOÚ neexistovaly. V rámci tvorby IK ÚOOÚ byly vytvořeny základní konceptuální datové modely. Pro potřeby kybernetické bezpečnosti a posouzení citlivosti jednotlivých datových prvků bude vytvořen v rámci implementace IK ÚOOÚ soupis datových aktiv, která budou rozřazena do jednotlivých stupňů dle citlivosti. Tuto aktivitu chápeme jako zásadní pro další nakládání s jednotlivými datovými prvky pro potřeby rozvoje IT systémů ÚOOÚ.

1.4.2 Konceptuální datový model ÚOOÚ



Tabulka 8 - Datové prvky ÚOOÚ

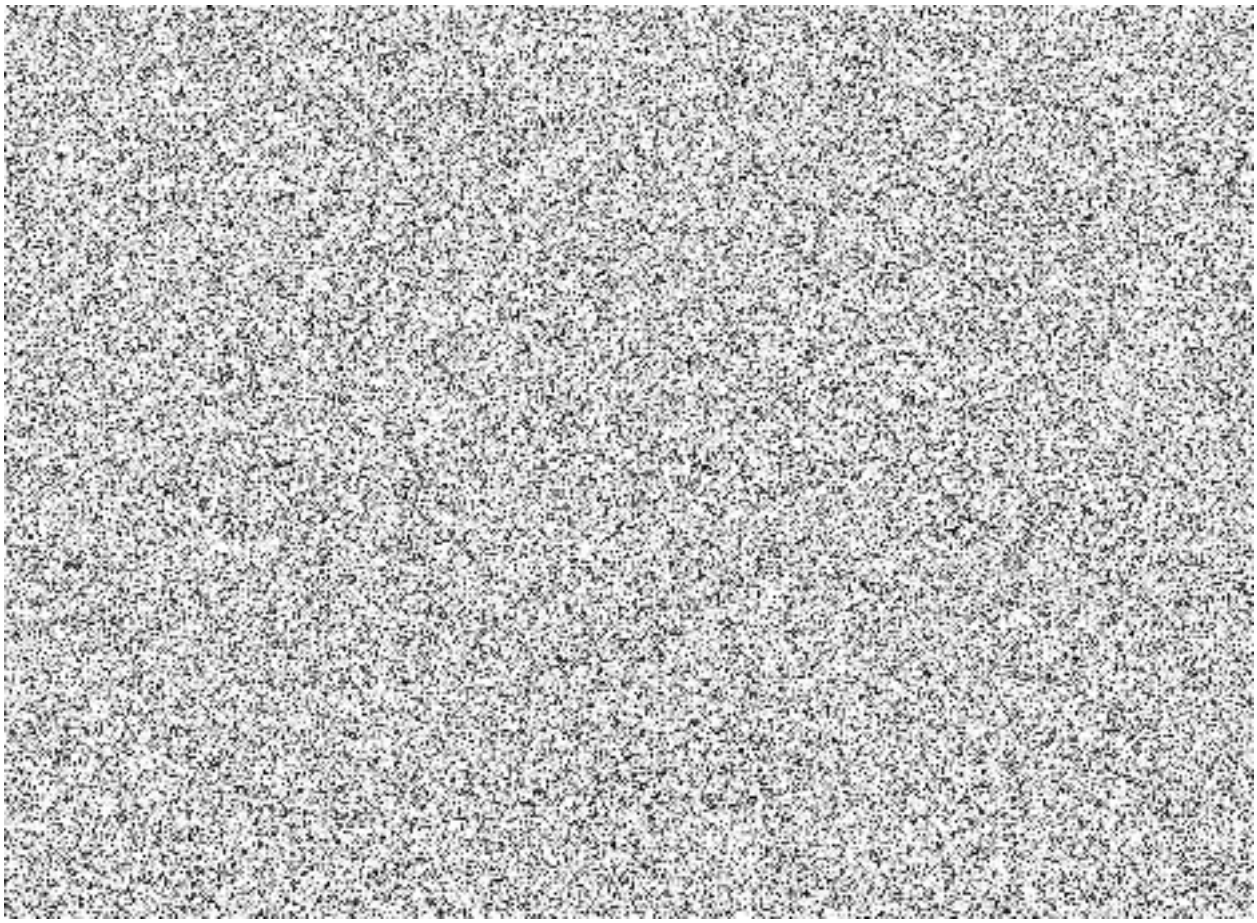




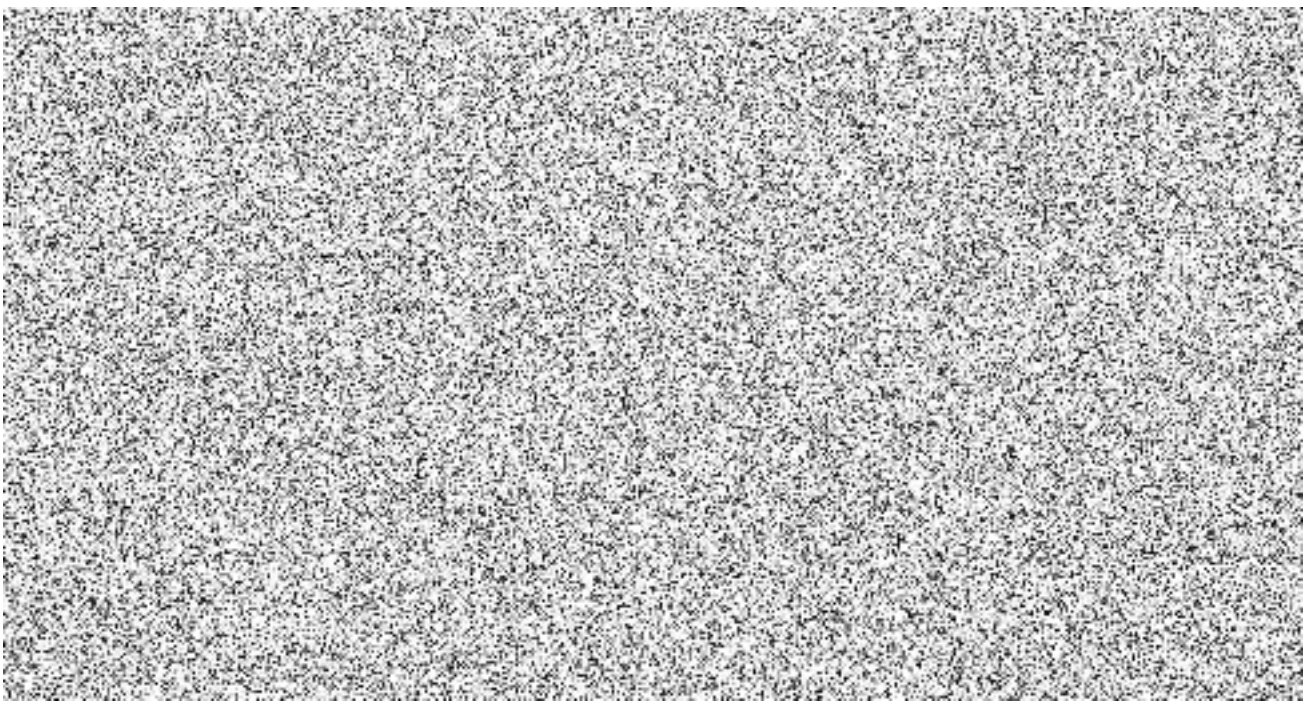
1.4.3 Kategorie údajů ÚOOÚ

Vzhledem ke specifičnosti agendy ÚOOÚ neevidujeme žádné údaje, které by bylo vhodné/možné sdílet. Všechny datové zdroje ÚOOÚ jsou používány buď pro vnitřní fungování nebo pro technický dohled nad fungováním informačních systémů.

Výjimku tvoří IS ORG, který naopak vede velmi citlivé údaje o všech občanech ČR a o jejich identifikačních číslech v rámci agend. Tyto informace jsou ale neveřejné a využívané pro anonymizaci pohybu osobních údajů v rámci ZR. Tyto údaje tak spotřebovávají velké množství výpočetního výkonu. I z tohoto důvodu jsme do této kapitoly vložili umístění jednotlivých datových prvků dle infrastruktury. Umístění dat je důležité pro ÚOOÚ i z pohledu dalšího rozvoje. Vzhledem k agendě, kterou ÚOOÚ vykonává je kladen zvláštní důraz na bezpečnost dat a je respektováno omezení ve využití cloudových služeb vyplývající z nejistoty možnosti předávání dat z cloudů třetím stranám, případně nutnost tato data šifrovat klíči ve správě ÚOOÚ.



Obrázek 9: Kategorizace z pohledu rozdělení procesů



Obrázek 12: Kategorizace z pohledu fyzického umístění dat

1.4.4 Otevřená data

ÚOOÚ poskytuje otevřená data jen v podobě úřední desky na webu. Jiná otevřená data neposkytuje. V současnosti je nejasné, zda ÚOOÚ disponuje nějakými obecně využitelnými daty. Nejzásadnějším produktem ÚOOÚ jsou rozhodnutí a stanoviska, která by ale nebyla vhodná k jakémukoliv štěpení na strojově čitelné části.

Zároveň však ÚOOÚ plánuje rozvoj ve vytváření metadat o jednotlivých rozhodnutích a stanoviscích, která by poté mohla sloužit pro snazší orientaci ve výstupech ÚOOÚ. Nebráníme se tedy diskuzi o možnostech publikování otevřených dat v budoucnu.

Koordinátorem otevřených dat bude v podmínkách ÚOOÚ nejspíše ředitel odboru informačních technologií. V rámci implementace IK a jejích projektů bude přistoupeno k jeho jmenování.

1.4.5 Shrnutí potřeb ze stávajícího stavu datové architektury

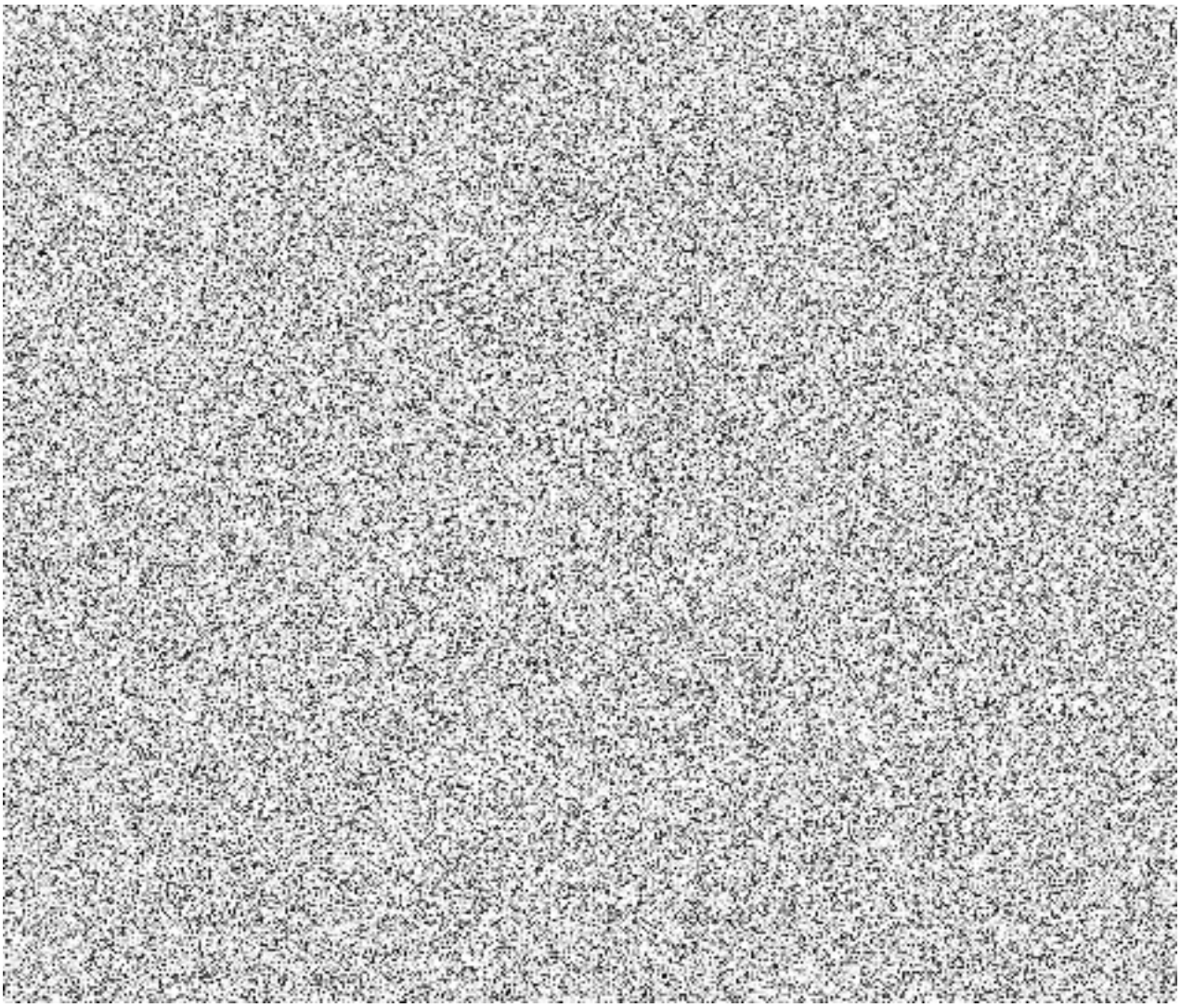
Velkou výzvou pro další směřování ÚOOÚ a jeho datové architektury je rozhodnutí, zda a do jaké míry využívat cloudové technologie. Vzhledem k velikosti ÚOOÚ a jeho personálním kapacitám je nutné se nad využíváním cloudu hluboce zamyslet i z pohledu ukládání a využívání dat. Jisté je, že musí být lépe definováno, jaká data mohou/nemohou v cloudu být či jaká data musí být šifrována s využitím klíčů ve správě ÚOOÚ, což bude učiněno výše zmíněnou analýzou aktiv ÚOOÚ. Datová architektura je pro ÚOOÚ zásadní otázkou i proto, že drží gesci nad Posouzením vlivu na ochranu osobních údajů a musí tedy velmi citlivě a pečlivě chránit data, která sám zpracovává, a dodržovat pravidla v metodikách obsažená.

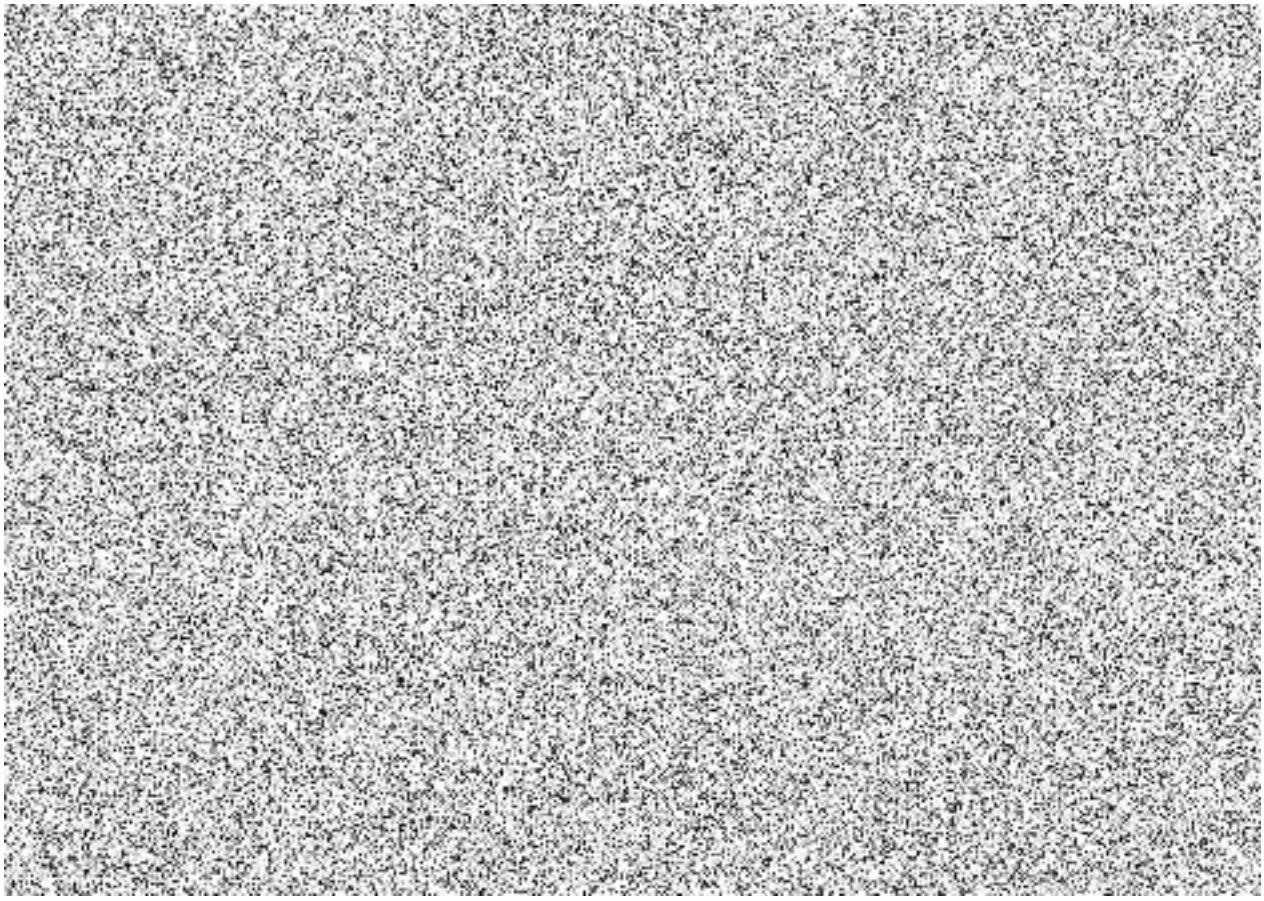
Jasně poté z analýzy současného stavu vyplývá, že se ÚOOÚ bude muset hlouběji zabývat problematikou otevřených dat, určit si koordinátora otevřených dat a nastartovat spolupráci s MV.

Vedle toho bude nutné v rámci rozvoje promyslet, jak data dále využívat a jak je strukturovat. Ze současného stavu byznys vrstvy enterprise architektury vyplynula potřeba tvorby databází zásadních dokumentů a podání v rámci ÚOOÚ. Tento záměr pak bude zásadní pro práci s daty ÚOOÚ. Stejně tak z analýzy současného stavu vyplynula potřeba lepšího přístupu vedení k datům ÚOOÚ a širší možnosti reportingu činností ÚOOÚ, případně jednodušší získávání strukturovaných dat pro Výroční zprávu ÚOOÚ.

1.5 Architektura IT infrastruktury ÚOOÚ

1.5.1 Architektura serverové infrastruktury





Obrázek 7: Infrastruktura ÚOOÚ - topologie, SW a HW

1.5.1 Infrastrukturní architektura koncových zařízení

Koncová zařízení jsou spravována oddělením Informatiky, monitoring na nich v tuto chvíli není prováděn. V rámci kybernetické bezpečnosti však plánujeme základní monitoring zavést, bude to jedním z úkolů vyplývajících z této koncepce.

Obecně BYOD (Bring Your Own Device – využívání vlastních zařízení) zařízení nejsou podporována. Přístup do vnitřní sítě je omezený pouze na přístup do Spisové služby a aplikace pro provádění předběžné řídící kontroly za využití dvoufaktorové autentizace a identity pro přístup do prostředí Microsoft 365. VPN je využívána pouze pracovníky OIT a pouze výjimečně pro případy nutnosti řešit některé úkony spojené s administrací IT vzdáleně a v mimo pracovní dobu.

Z osobních zařízení je možné do prostoru Microsoft 365 a do aplikací, které sdílí jeho identitní prostor, tedy Spisovou službu a předběžnou řídící kontrolu. Základní zabezpečení tohoto přístupu je zajištěno dodavatelem Microsoft 365.

1.5.2 Shrnutí potřeb ze stávajícího stavu Infrastrukturní architektury

Otázka infrastruktury je zásadní pro jakýkoliv rozvoj IT na ÚOOÚ. V tuto chvíli ÚOOÚ sice disponuje dostatečným výpočetním výkonem pro zachování současného fungování, nikoliv však pro rozvoj. Shrnutí současného stavu je nutné rozdělit na dva základní bloky: IS ORG a vnitřní IT ÚOOÚ.

Co se týče IS ORG je infrastruktura v dobrém stavu. Díky jeho strategickému významu se dlouhodobě daří financovat postupnou odměnu HW prvků a lehké zvyšování výkonu HW IS ORG. Náklady na investice jsou značné, nicméně vzhledem k charakteru dat, které IS ORG uchovává je bezpečnost na

prvním místě. Z tohoto pohledu je nejbezpečnější provozovat IS ORG na infrastruktuře ve vlastnictví ÚOOÚ, případně v zabezpečeném státním cloudu. Bude nutné počítat s tím, že do budoucna bude potřeba navýšení výkonu IS ORG nadále stoupat, zejména s ohledem na postupující digitalizaci jednotlivých agend a s tím související větší využívání propojeného datového fondu.

V rámci interního IT ÚOOÚ je situace odlišná. Obnova HW v rámci datového centra ÚOOÚ nebyla realizována. HW je ve své většině stále původní z doby zavádění IS ÚOOÚ, tedy z roku 2013. ÚOOÚ stojí před zásadním rozhodnutím, zda tuto infrastrukturu obnovovat či zda provést migraci do cloudového řešení. Musí být provedena analýza, co by přechod do cloudu znamenal a zda je pro ÚOOÚ technicky i nákladově reálný. Pro datové prvky, které jsou citlivé, se počítá s tím, že by měly zůstat v rámci interní infrastruktury ÚOOÚ, či šifrovány vlastními klíči v rámci cloudu, necitlivá data by výhledově mohla být v cloudu.

1.6 Architektura komunikační infrastruktury ÚOOÚ

ZR jsou využívány pro potřeby agendy A851, toto napojení je technicky realizováno za využití spisové služby. Vedle toho je ÚOOÚ napojen na CMS a KIVS primárně pro potřeby skládání úřednických zkoušek.

V rámci IS ORG je ÚOOÚ napojen na CMS a KIVS taktéž, ale toto napojení je naprosto oddělené od napojení pro potřeby ÚOOÚ. IS ORG komunikuje pouze s ISZR.

ÚOOÚ neposkytuje žádné aplikační služby třetím stranám, ani v tuto chvíli nevyužívá možnosti propojeného datového fondu. Důvodem je specifikum ÚOOÚ, kdy se klienti nemusí ve styku s ÚOOÚ identifikovat, ale mohou podávat podání i anonymním způsobem. Na druhou stranu ÚOOÚ nemá žádná strukturovaná data, která by mohl sdílet.

1.6.1 Shrnutí potřeb ze stávajícího stavu Architektury komunikační infrastruktury ÚOOÚ

Ze současného stavu architektury komunikační infrastruktury ÚOOÚ v tuto chvíli nevyplývá příliš velké množství potřeb. Ty by se mohly změnit za předpokladu, že bude vize upustit od anonymních podání, a tím pádem bude preferována cesta podání formou elektronických formulářů. V takové chvíli by bylo nutné začít přemýšlet o napojení na Propojený datový fond a tvorbě inteligentních formulářů ve spojitosti s výše popsanou vizí vytvoření strukturovaných databází podání a vyřízení.

1.7 Přehled projektů

Tabulka 9: Přehled projektů

Kód a název projektu	Předmět projektu	Fáze projektu	Odpovědný útvar	Termín zahájení	Termín dokončení	DČ
P1 - Vega D2-G	Implementace systému Vega D2-G pro potřeby tvorby a práce s utajovanými dokumenty do výše režimu utajení „Důvěrné“	Běží	OIT	06/2022	11/2023	Ne
P2- Docházkový systém	Implementace nového Docházkového systému s dotykovými terminály.	Běží	OVS	11/2022	3/2024	Ne

Kód a název projektu	Předmět projektu	Fáze projektu	Odpovědný útvar	Termín zahájení	Termín dokončení	DČ
P3- eSIAŘ	Implementace systému na evidenci a seznamování se s interními akty řízení ÚOOÚ.	Běží	OIT	06/2021	06/2023	Ne
P4 - Analýza aktiv ÚOOÚ	Analýza aktiv ÚOOÚ, s důrazem na datové prvky.	Běží	BŘ	01/2023	09/2023	Ne
P5 - Nový web ÚOOÚ	Implementace nového webu ÚOOÚ v souladu s Design systémem gov.cz.	Běží	TO/OIT	01/2021	10/2023	Ne

2 Přehled motivací ÚOOÚ ke změnám architektury

2.1 Poslání ÚOOÚ, strategické cíle a byznys požadavky

2.1.1 Poslání a kompetence ÚOOÚ

V rámci budoucích kompetencí ÚOOÚ, které by vyplývaly z legislativy, je nyní možné zmínit povinnosti vyplývající z věcného záměru zákona o správě dat veřejného sektoru, kde bude ÚOOÚ v souladu se svými kompetencemi oprávněn k ukládání sankcí za porušení povinností souvisejících s dalším užitím dat, které budou poskytovány řízeným přístupem. Vzhledem k tomu, že v takovém případě půjde o porušení norem GDPR, je ÚOOÚ jako instituce pro ukládání těchto sankcí již nyní oprávněn. Navýšení agendy bude vyžadovat rozšíření počtu systemizovaných míst na ÚOOÚ. Tato novinka bude realizována za využití stávajících zdrojů a jediným dopadem do budoucna může být rozšíření informační báze budoucího systému pro evidenci dokumentů ÚOOÚ.

Jiné změny v tuto chvíli neočekáváme, nicméně pokud by nastaly, budou průběžně doplňovány v rámci aktualizací IK ÚOOÚ.

2.1.2 Strategické cíle ÚOOÚ

Vize a mise ÚOOÚ: Zajistit konzistentní aplikaci práva upravujícího ochranu osobních údajů skrze zapojení klíčových aktérů v rámci veřejné správy i soukromého sektoru, vykonávání dohledu nad subjekty práva a vynucování dodržování základních legislativních pravidel ochrany osobních údajů v podmínkách provozování systému kritické informační infrastruktury IS ORG a budování výkonu agendy vykonávané dle zákona č. 106/1999 Sb.

Primárními cíli ÚOOÚ jsou:

1) Služba veřejnosti v oblasti ochrany osobních údajů.
2) Naplňování evropských úkolů v oblasti ochrany osobních údajů.
3) Metodická pomoc správcům a zpracovatelům osobních údajů.
4) Ochrana veřejných subjektivních práv v oblasti svobodného přístupu k informacím.
5) Provoz a rozvoj IS ORG.

Vize a cíle budou naplňovány následujícími aktivitami:

1) Aktivním zapojením se do fungování EDPB a implementace jeho závěrů do praxe ÚOOÚ.
2) Spravedlivým a přiměřeným trestáním pochybení v dodržování legislativy týkající se ochrany osobních údajů.
3) Spravedlivým a vyváženým posuzováním stížností.
4) Transparentní komunikací s klíčovými aktéry a veřejností.
5) Udržením expertních kapacit pro plynulé a efektivní fungování ÚOOÚ.
6) Vybudováním zdrojů a kapacit pro vyvážené a spravedlivé posuzování odvolání v rámci agendy zákona 106/1999.

7) Rozvojem kompetencí a prostředků ÚOOÚ pro výkon dozoru a nakládání s informacemi v režimu utajení.

8) Vzděláváním klíčových aktérů (např. pověřenců) z pohledu jejich práv a povinností.

Pro podpoření těchto cílů je nutné provést změny v IT architektuře ÚOOÚ. Ty se budou týkat například nakládání s informacemi v rámci ÚOOÚ. Aby bylo možné spravedlivě, vyváženě a přiměřeně trestat nebo posuzovat stížnosti, je nutné udržovat všechny zásadní dokumenty na ÚOOÚ dostupné všem relevantním subjektům. Zde bude tedy nutné postupně vytvořit nový informační systém, který tuto činnost zajistí.

Vzdělávání a komunikace pak musí být podpořena atraktivnějším prostředím pro sledování novinek a získávání informací. Z tohoto důvodu budeme v rámci naplňování cílů IK ÚOOÚ implementovat nový web.

2.1.3 Externí byznys požadavky

1) Požadavky na kybernetickou bezpečnost; jedná se obyvkle o menší změny, které ale vyžadují investice nebo změnu fungování některých prvků enterprise architektury.

Zároveň je možné, že určité byznys požadavky si vyžádá i přesun SZR na Digitální a informační agenturu a případné nová koncepce rozvoje ZR.

2.1.4 Interní byznys požadavky

Na podzim 2022 proběhl v rámci ÚOOÚ výzkum mezi zaměstnanci, kteří mají na starosti klíčovou agendu kontroly dodržování ustanovení GDPR a dalších předpisů týkající se ochrany osobních údajů. Výzkum se konkrétně týkal hlavních procesů v rámci agendy A851.

Předmětem zkoumání byly konkrétní procesy přijímání a vyřizování podnětů a stížností a proces kontroly subjektů různého zaměření. Výsledné požadavky jsou sestaveny na základě zjištění z kvalitativního výzkumu mezi úředníky, kteří kontrolu a dozor nad subjekty zajišťují.

Jako metody výzkumu byly využity kontextový rozhovor s experty, uživatelský výzkum a průchod službou. V rámci průzkumu bylo osloveno 7 respondentů ze Sekce dozoru a Odboru legislativy a metodiky.

Z výzkumu vyšly byznys požadavky obsažené v tabulce níže.

Tyto požadavky jsou blíže definovány v rámci přílohy č. 1 IK ÚOOÚ: Možnosti digitalizace vybraných agend ÚOOÚ.

Vedle výše zmíněných požadavků evidujeme i další požadavky ze strany vedení ÚOOÚ, primárně od předsedy ÚOOÚ a místopředsedů, které jsou také uvedeny v tabulce a jejich konkrétní naplňování bude zmíněno v jednotlivých projektech.

Id	Autor	Název
P1	OD	Úplnost vedení záznamů
P2	OD	Kontinuita řešení podnětů
P4	OD	Sjednocení vedení záznamů

P5	OD	Základní přehled o podnětech a kontrolách napříč úřadem
P6	OD	Propojenost databází případů
P7	OD	Upozornění na lhůty
P8	OD	Kvantitativní a kvalitativní vyhledávání v podnětech
P9	OD	Aktualizace stavu na webu
P10	OD	Napojení na GINIS
P11	OD	Proškolení personálu v oblasti vedení záznamů v systému
P12	OD	Možnosti exportu dat
P13	OD	Zvýšení rychlosti výměny informací
P14	OD	Nezávislý přístup k datům
P15	OD	Omezení spotřeby papíru na tisk jednotlivých spisů
P16	SMSPI	Vedení evidence pověřenců na ochranu osobních údajů
P17	OD	Jednotná evidence ukončených a běžících kontrol a sledování stavu rozpracovanosti jednotlivých kontrolních akcí
P18	Předseda ÚOOÚ	Rozvoj digitálních kompetencí v rámci ÚOOÚ
P19	Předseda ÚOOÚ	Rozvoj možností spolupráce s dozorovými úřady napříč EU
P20	Předseda ÚOOÚ	Klást zvýšený důraz na bezpečnost informací
P21	Předseda ÚOOÚ	Digitální a mobilní kancelář (pro kontroly v terénu)
P22	Předseda ÚOOÚ	Plnohodnotná a bezpečná práce z jiného místa než z pracoviště ÚOOÚ
P23	Předseda ÚOOÚ	Zavedení šifrování pro vybranou komunikaci

2.2 Dopady a požadavky na ICT

2.2.1 Byznys požadavky na změny

- Primární požadavky na změny v IT vyplývají z výše umíněných byznys požadavků. Většinu výše zmíněných požadavků řeší nějaká forma evidence podnětů, stížností nebo rozhodnutí. Jedním z hlavních cílů IK ÚOOÚ bude právě dopracování definice a zavedení evidence, která bude plnit co největší množství výše popsaných požadavků. Ta bude přesněji definována v rámci konkrétního projektu.

- Jako změnu v existujících řešeních je nutné zmínit také funkcionality související s agendou Nevyžádaných obchodních sdělení. Nejedná se ani tak o změny, jako spíše o udržení kontinuity současného řešení, které již není podporováno. Dalším cílem IK ÚOOÚ bude zpracovat návrh, jak a čím toto řešení nahradit.
- Dalším požadavkem je přechod na novou verzi intranetu, v současnosti na již nepodporované technologii Sharepoint 2010. Zároveň by měl být obohacen o nové funkcionality jako „Evidence smluv“ či „Informační hub“.
- Nástroj pro tvorbu formulářů – pro různé potřeby (přihlašování na školení, elektronická podání) ÚOOÚ – je nutné pořídit komplexní řešení na tvorbu formulářů pro nový web, případně rozvinout současné řešení do použitelné podoby.

2.2.2 Vnitřní ICT potřeby

2.2.2.1 HW potřeby

I v následujících 5 letech bude nutné investovat do obnovy HW na IS ORG i v rámci interního IT. IS ORG má v této oblasti zpracovanou Strategii a je připravována strategie na roky 2024-2028. Počítá se s investicemi v celkové hodnotě cca 75 000 000,- Kč. V rámci interního IT je nutné počítat s nutností investic v hodnotě 10 000 000,- Kč v rámci dalších 5 let, aby bylo možné provozovat aplikace nutné pro chod ÚOOÚ. Tyto investice ale proběhnou jen za předpokladu, že se neukáže využití výpočetního výkonu v cloudu jako efektivnější řešení.

2.2.2.2 SW potřeby

1. Nový service desk – v rámci fungování ÚOOÚ je v plánu vytvořit nový service desk, ideálně na technologii Sharepoint Online a posléze jeho využívání jako primárního kanálu pro hlášení technických problémů.
2. Pro potřeby kybernetické bezpečnosti bude nutné zajistit pořízení nástroje na sběr logů a bezpečnostní monitoring pro aplikace, které spadnou do režimu VIS.

2.2.2.3 Personální potřeby

V rámci Odboru informačních technologií chybí personální zajištění zejména dvou rolí: architekt kybernetické bezpečnosti a IT architekt. Obě role jsou naprosto zásadní pro rozvoj IT služeb. Jednalo by se tedy o dvě systemizovaná místa.

2.2.3 Výjimky OHA

V rámci ÚOOÚ nejsou aplikovány žádné výjimky.

2.3 Shoda s cíli Informační koncepce ČR

2.3.1 Dopady cílů Informační koncepce ČR v prostředí ÚOOÚ

Tabulka 10: Posouzení dopadů cílů Informační koncepce ČR

Cíl IK ČR	Dopady cíle IK ČR na ÚOOÚ
1 - UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	
1.1 Národní katalog služeb	ÚOOÚ má řádně ohlášeny služby i úkony. Bude dopracován detailní popis služeb.
1.2 Centrální informační místo	Detailní popis bude dopracován v souladu s cíli IK ÚOOÚ.
1.3 Univerzální obslužné kanály	Nerelevantní
1.4 Digitální služby resortů	Nerelevantní
1.5 Národní katalog otevřených dat	Bude provedena analýza možností publikace otevřených dat.
1.6 Role správců služeb	Bude vytvořena role správců služeb a správců obslužných kanálů, napříč agendami.
1.7 Zpětná vazba klientů	Bude doplněn zpětnovazební formulář na web.
1.8 Jednotné UX/UI	Nový web ÚOOÚ bude v souladu s Design systémem gov.cz.
1.9 Proaktivní poskytování služeb	Bude podpořeno tvorbou nových formulářů v rámci Z3.
2 - DIGITÁLNĚ PŘÍVĚTIVÁ LEGISLATIVA	
2.1 Digitální dopady navrhované legislativy	Řešíme s gestory jednotlivých zákonů, které upravují naši činnost.
2.3 eSbírka a eLegislativa	Nerelevantní
2.4 Průběžná aktualizace platné legislativy	Řešíme s gestory jednotlivých zákonů, které upravují naši činnost.
2.5 Právo na digitální služby	Splňujeme. Služby, které dnes poskytujeme, poskytujeme digitálně.
2.6 Revize legislativy eGovernmentu	Nerelevantní
2.7 Soukromé a veřejnoprávní služby	Nerelevantní

Cíl IK ČR	Dopady cíle IK ČR na ÚOOÚ
2.8 Metodika pro veřejné zakázky v oblasti ICT	Nerelevantní
2.9 Nová legislativa eGovernmentu	Nerelevantní
2.10 Legislativní podpora proaktivního poskytování služeb	Nerelevantní
3 - ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	
3.1 Čerpání mimorozpočtových zdrojů	Budu analyzováno, zda je ÚOOÚ schopen zvládnout přípravné a provozní práce v rámci čerpání z mimorozpočtových zdrojů.
3.2 Digitalizace dosud nedigitalizovaného obsahu	Nerelevantní
3.3 Digitální archivy	Bude řešeno projektem Digitální archiv.
3.4 Základní registry	Probíhá, jsme správce IS ORG, který se řídí strategií IS ORG. Data ze ZR čerpáme.
3.5 Komunikační infrastruktura	Je využívána. Jsme napojeni na CMS i KIVS.
3.6 Elektronická identifikace	Bude provedena analýza nutnosti zavedení elektronické identifikace v rámci agend ÚOOÚ.
3.7 Digitální mapa veřejné správy	Nerelevantní
03.08 Kybernetická bezpečnost	Proběhne kompletní revitalizace kybernetické bezpečnosti v rámci IS ÚOOÚ.
3.9 Přeshraniční elektronická identifikace	Nerelevantní
3.10 Digitální oprávnění a zmocnění	Nerelevantní
3.11 Elektronické platby	Nerelevantní
3.12 Stavebnice sdílených řešení	Nerelevantní
4 - ZVÝŠENÍ KAPACIT A KOMPETENCÍ ZAMĚSTNANCŮ VE VEŘEJNÉ SPRÁVĚ	
4.1 Systemizace expertních profesí	ÚOOÚ bude žádat 2 nová místa na IT.

Cíl IK ČR	Dopady cíle IK ČR na ÚOOÚ
4.2 Získání, udržení a rozvoj klíčových specialistů	ÚOOÚ se snaží dělat v rámci svých kompetencí a finančních možností, například nabídkou školení a pružných pracovních podmínek. Nastavení zdravé firemní kultury.
4.3 Absolventi ve státním sektoru	ÚOOÚ se zaměstnávání absolventů nebrání, ale vzhledem k jeho velikosti to není ucelenou strategií ÚOOÚ v personální oblasti.
4.4 Využití kompetenčních center	Plánujeme využití kompetenčních center pro realizaci níže vypsaných záměrů.
4.5 Ustavení transformačních útvarů	V případě ÚOOÚ počítáme s tím, že transformačním útvarem bude OIT.
4.6 Kapacity pro realizaci změn	Nejsou dostatečné, ÚOOÚ bude žádat o jejich navýšení.
4.7 Naplnění expertních míst	Potřebujeme posílit zejména na výše pospaných pozicích Architekta KB a IT architekta.
4.8 Rozvoj digitálních kompetencí	Probíhá formou externích školení. Zároveň je podporován přenos know-how uvnitř ÚOOÚ s velkou podporou manažera kybernetické bezpečnosti.
5 - EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	
5.1 Řízení realizace IKČR	Nerelevantní
5.2 Zdroje na realizaci IKČR	Nerelevantní
5.3 Architektura veřejné správy	Začne probíhat po schválení IK ÚOOÚ.
5.4 Koordinace státního ICT	Nerelevantní
5.5 eGovernment cloud	Nerelevantní
5.6 Národní ICT autorita	Nerelevantní
5.7 Agendy v přenesené působnosti	Nerelevantní
5.8 Sdílená řešení pro malé agendy a úřady	Nerelevantní
5.9 Propojený datový fond	Nerelevantní
5.10 Veřejný datový fond	Proběhne analýza dat a na jejím základě bude stanoveno, jaká data mohou či nemohou být publikována.
5.11 Systémy prostorových dat	Nerelevantní

Cíl IK ČR	Dopady cíle IK ČR na ÚOOÚ
5.12 Měření a vyhodnocení realizace IK ČR	Nerelevantní
5.13 Agendové informační systémy	Bude probíhat v rámci záměru Z1.
6 - EFEKTIVNÍ A PRUŽNÝ DIGITÁLNÍ ÚŘAD	
6.1 IT podpora práce úředníků	Záměr Nový intranet ÚOOÚ má za cíl naplnit tento cíl a vytvořit jakýsi portál pro úředníka.
6.2 Vnitřní digitalizace ÚOOÚ	V rámci záměrů Z1 a Z2 viz níže bude značně zdigitalizována výměna informací.
6.3 Nové metody řízení ÚOOÚ	Postupně zaváděno v rámci začínající realizace projektů. IK ÚOOÚ bude zásadním nástrojem pro zavádění nových metod.
6.4 Modernizace provozních IS	Realizováno záměry Z4, Z5 a Z10, tedy nahrazením současného řešení agendy Nevyžádaných obchodních sdělení.
06.5 Modernizace digitální infrastruktury	Realizováno v rámci záměrů souvisejících s obnovou HW.

2.4 Dopady principů Informační koncepce ČR do digitalizace ÚOOÚ

Tabulka 11: Posouzení dopadů principů IK ČR

ID	Název principu	Dopady principu IK ČR na ÚOOÚ
P1	Standardně digitalizované (Digital by default)	Bude podpořeno Záměrem Z3 Formulářový server ÚOOÚ.
P2	Pouze jednou (Once only)	Vzhledem k charakteru agendy ÚOOÚ není tento princip příliš relevantní.
P3	Podpora začlenění a přístupnost (Inclusiveness and Accessibility)	Změny k lepší přístupnosti budou implementovány v rámci záměru Z8 Zavedení nového webu ÚOOÚ se zpětnovazebním formulářem.
P4	Otevřenost a transparentnost (Openness and Transparency)	Budou analyzovány možnosti větší transparentnosti.

ID	Název principu	Dopady principu IK ČR na ÚOOÚ
P5	Přeshraniční přístup jako standard (Crossborder interoperability)	V tuto chvíli neplánujeme žádný projekt pro mezinárodní spolupráci, ale vidíme ve spolupráci s ostatními dozorovými úřady napříč EU velký potenciál.
P6	Interoperabilita jako standard (Interoperability by design)	Nerelevantní
P7	Důvěryhodnost a bezpečnost (Security by design)	Prohlubováno v rámci záměru Z5 Zajištění kybernetické bezpečnosti IS ÚOOÚ.
P8	Jeden stát (Whole-of-Government)	Služby ÚOOÚ jsou specifické, ale v rámci záměru Z8 Zavedení nového webu ÚOOÚ se zpětnovazebním formulářem plánujeme využít jednotný vizuální styl VS.
P9	Sdílené služby veřejné správy (Shared Services)	Sdílené služby jsou využívány, jejich budování neplánujeme. Zároveň ÚOOÚ provozuje IS ORG jako sdílenou službu pro ZR.
P10	Připravenost na změny (Flexibility)	Dlouhodobě cílem.
P11	eGovernment jako platforma (Embeded eGovernment)	Takové projekty v tuto chvíli neplánujeme.
P12	Vnitřně pouze digitální (Inside only digital)	Realizováno několika záměry, např. Z1, Z2, Z4 či Z10.
P13	Otevřená data jako standard (Open Data by default)	Proběhne analýza dat a na jejím základě padne rozhodnutí, zda je možné některé poskytnout, či ne.
P14	Technologická neutralita (Technological neutrality)	Dlouhodobý cíl, v podmínkách malého úřadu je však nesnadné ho implementovat.
P15	Uživatelská přívětivost (User-friendliness)	Zohledněno při realizaci záměru Z8 a je vize zohledňovat uživatelskou přívětivost u všech služeb.
P16	Konsolidace a propojování (IT Consolidation)	Rozhodně plánujeme využívat možností sdílení řešení mezi úřady.
P17	Omezení budování monolitických systémů	Dlouhodobě naplňováno, zejména s ohledem na systémy pro personální správu, účetnictví a PŘK.
P18	Datová suverenita a nezávislost	Dlouhodobě naplňováno napříč IS ÚOOÚ.

ID	Název principu	Dopady principu IK ČR na ÚOOÚ
P19	Otevřená řešení (Open source)	Bude realizováno v rámci nových projektů a řešení.
P20	Metriky digitálních služeb	Plánujeme u nových systémů.

2.5 Shrnutí a interpretace potřebných změn architektury

Záměry dělíme do 4 fází rozpracovanosti:

1. V přípravě – probíhá definice uživatelských požadavků a potřeb ÚOOÚ, diskuse o gestorech a projektovém týmu.
2. Záměr schválen – záměr schválen vedením ÚOOÚ v nadefinované podobě.
3. Příprava plánu projektu – na základě schváleného záměru probíhá příprava projektu.
4. Záměr přesunut do projektu – u záměru byla dopracována projektová dokumentace, přesunut ke schválení a realizaci v rámci projektového řízení, tedy stal se z něho projekt.

Zároveň v tabulce proběhla jedna změna - technicky bude za všechny projekty zodpovědným útvarem OIT, v případě jednotlivých záměrů se bude lišit pouze věcná gesce, kolonka „odpovědný útvar“ tak byla nahrazena formulací „věcně odpovědný útvar“.

Tabulka 12: Přehled identifikovaných záměrů

Kód a název záměru	Předmět záměru	Fáze záměru	Věcně odpovědný útvar	Termín zahájení	Termín dokončení záměru	DČ
Z1	AIS ÚOOÚ	V přípravě	SMI, SD, SKANC	Q3 2023	Q2 2026	Ano, projektový záměr je v Archirepu DČ
Z2	Evidence pověřenců	V přípravě	SMI	Q1 2024	Q3 2024	Ne
Z3	Zavedení projektového řízení pro ICT projekty	V přípravě	OIT	Q3 2023	Q1 2024	
Z4	Nový intranet ÚOOÚ	V přípravě	OIT	Q4 2023	Q4 2024	Ne
Z5	Interní a externí databáze rozhodnutí (INROK/EXROK)	V přípravě	SMI	Q1 2024	Q4 2024	

Kód a název záměru	Předmět záměru	Fáze záměru	Věcně odpovědný útvar	Termín zahájení	Termín dokončení záměru	DČ
Z6	Rozvoj webu ÚOOÚ o zpětnovazební formulář	Záměr přesunut do projektu	TO	Q4 2023	Q4 2024	Ne
Z7	Dopracování ohlášení detailního popisu služeb a údajů do RPP	V přípravě	OLM	Q3 2023	Q2 2024	Ne
Z8	Analýza možného řešení pro nahrazení modulu NOS	V přípravě	SD, oddělení NOS	Q3 2023	Q2 2024	Ne
Z9	Plán rozvoje spisové služby	V přípravě	OVS	Q1 2024	Q2 2024	Ne
Z10	Zajištění systému pro hybridní (on-line a zároveň prezenční) vzdělávání odborné veřejnosti (pověřenců)	V přípravě	OIT	Q2 2024	Q4 2024	Ne
Z11	Uvedení praxe ÚOOÚ do souladu se zákonem č. 12/2020 Sb., o právu na digitální služby dle nových výkladů DIA	Zajištění procesů a digitalizačních kroků v rámci ÚOOÚ do souladu se zákonem č. 12/2020 Sb., o právu na digitální služby dle nových výkladů DIA	V přípravě	OLM	Q2 2024	Q2 2025

3 Návrh cílového stavu

3.1 Architektonická vize ÚOOÚ

Digitální transformace pro ÚOOÚ znamená 2 základní kroky:

1) Digitalizovat fungování nejdůležitějších agend ÚOOÚ
2) Maximalizovat využití cloudových technologií

Digitalizace fungování nejdůležitějších agend

Z analýzy stávajícího stavu vychází, že současný stav digitalizace fungování agend ÚOOÚ není dostatečný. Pro naplnění výše popsaných cílů organizace je zásadní, aby vznikl Agendový informační systém, který bude sloužit evidence nejzásadnějších dokumentů, a zároveň bude definovat a podporovat potřebné workflow. Agenda ÚOOÚ není z pohledu procesů příliš komplikovaná. V zásadě se jedná o přijetí podání, jeho vyhodnocení a následného rozhodnutí. U každého konkrétního podání se liší zákon, na jehož základě je podáno, do procesu však tento rozdíl zasahuje jen minimálně. Z toho důvodu se nabízí vytvořit jeden větší agendový informační systém, který bude evidovat všechny dokumenty potřebné pro fungování agend ÚOOÚ a definovat všechna workflow. Workflow se budou na základě legislativního ukotvení lišit, dokumenty však mohou být v jedné databázi, která se bude dle legislativy pouze filtrovat. Vedle toho by bylo vhodné v rámci AIS vytvořit elektronické formuláře, které by se vyplňovaly na webu a automaticky by umožnily import dat přímo do AIS. (Projektový záměr Z1). Vzhledem k rozsahu takového systému bude preferována varianta postupného vývoje a rozvoje po menších částech.

Dále je pro digitalizaci fungování nejdůležitějších agend nutné zavést podpůrné procesy typu projektového řízení (projektový záměr Z3) a řízení změnových požadavků (provozní projektový záměr PZ3).

Maximalizovat využití cloudových technologií

Jedním z cílů ÚOOÚ je dlouhodobě více podporovat práci z domova a zároveň umožnit větší možnosti kontrol a působení v terénu. Pro naplnění těchto cílů je ideální využít cloudových technologií. Na ÚOOÚ je již nasazeno cloudové řešení pro kancelářské aplikace a e-mailový server. Vedle toho byla na ÚOOÚ úspěšně nasazena dvě řešení postavená na cloudové technologii pro Evidenci smluv a Informační hub.

Z analýzy stávajícího stavu navíc vyplynula řada problémů se současným fungováním IT infrastruktury ÚOOÚ. V roce 2019 byla vypovězena provozní smlouva na správu datového centra ÚOOÚ, která nebyla adekvátně nahrazena. HW v datovém centru ÚOOÚ nebyl dlouhodobě obnovován, z čehož vyplývá nutnost ho co možná nejrychleji nahradit. Nabízí se tedy spojit byznysové cíle s řešením těchto problémů a začít vypracovávat podrobný plán přesunu maximálního počtu aplikací a infrastrukturních prvků na cloud.

Největší překážkou tohoto řešení jsou nejasnosti spojené s evropským stanoviskem k využíváním komerčního cloudu, které se snažíme vyřešit za využití šifrování či správnou kategorizací dat dle citlivosti.

3.2 Návrh cílové byznys architektury

Vzhledem k malým změnám ve fungování ÚOOÚ, které v dalších letech očekáváme, nebudou změny v byznys architektuře nijak výrazné. Stejná činnost bude pouze prováděna jinými prostředky.

Služby externím klientům budou více využívat webových stránek a interaktivních formulářů. Řadu nových služeb získají interní klienti ve formě evidence zásadních dokumentů a informací o podání a jednodušší práce s nimi. Samotný charakter procesů ale zůstane spíše podobný, protože jsou dány přímo ze zákonů, které nemá ÚOOÚ v gesci.

Portály a obslužné kanály budou více využívány ve formě větší propagace formulářů a jejich napojení na nový AIS.

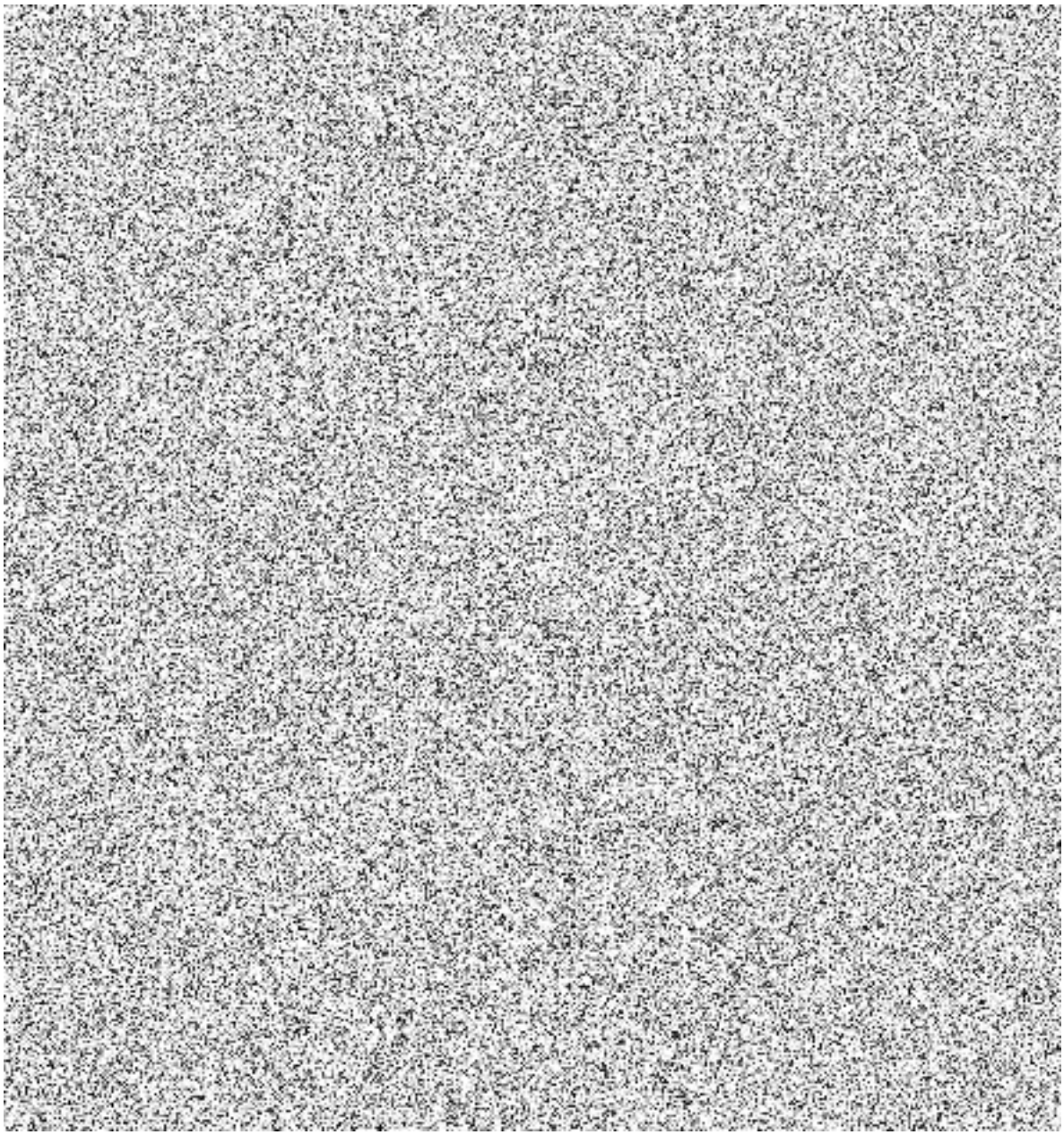
Procesy ÚOOÚ jsou upraveny v právních předpisech, které nemá ÚOOÚ v gesci.

3.3 Návrh cílové aplikační a datové architektury

Aplikační architektura

Na úrovni aplikací je zásadní změnou vznik nového AIS se třemi moduly: dokument management systém, modul formuláře a modul workflow. Dále zvažujeme rozšíření IS ORG o analytický modul, který by byl schopen dávat podklady pro případnou kontrolu nakládání s daty základních registrů, zejména ze strany soukromoprávních uživatelů údajů.

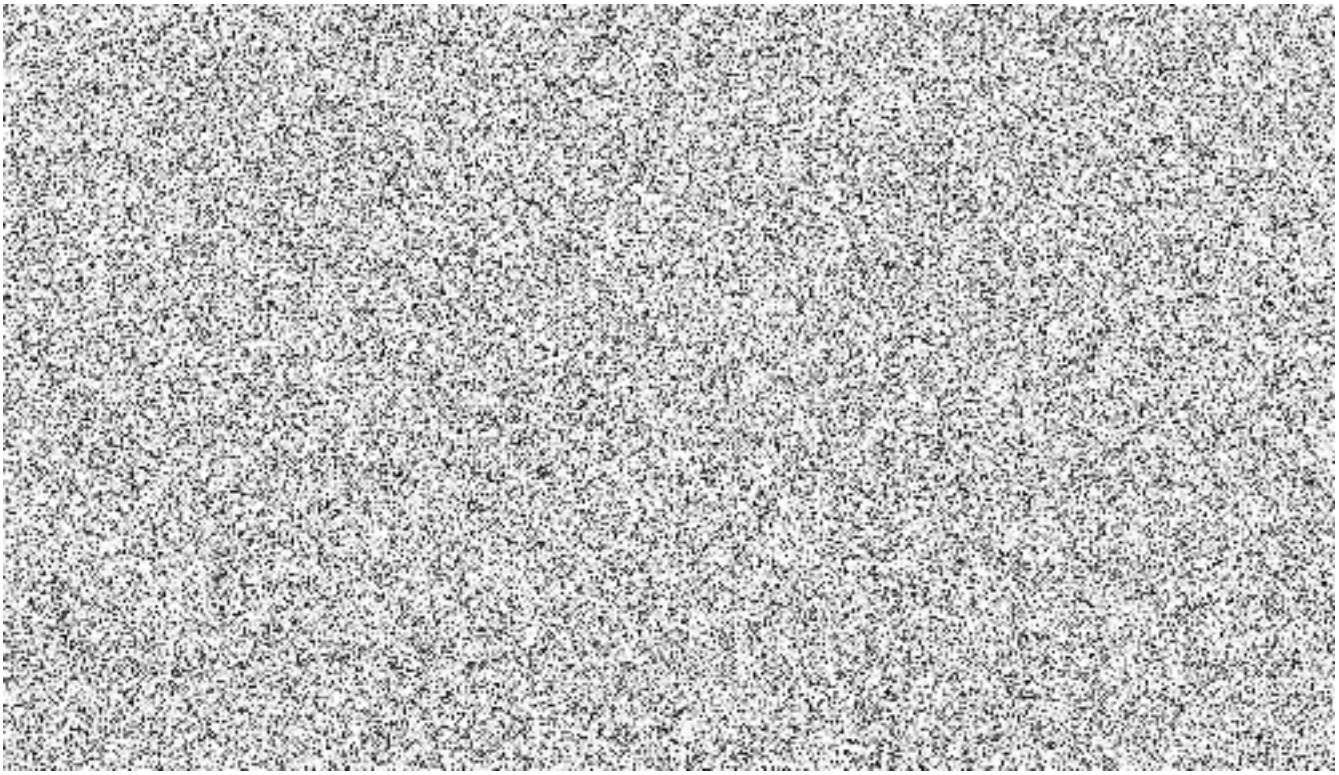
Další změny jsou pouze kosmetické, plánujeme revizi fungování Service desku a přechod na pokročilejší SW, umožňující také Change management. Vedle toho plánujeme přesunout intranet z již nepodporované verze Sharepoint 2010 a nejnovější cloudovou verzi aplikace.



Datová architektura

Změny v datové architektuře se opět budou týkat primárně vzniku AIS ÚOOÚ. V této chvíli ještě není k dispozici kompletní architektura informačního systému, ale je vcelku jasné, že bude systém evidovat nějaká transakční data, nějaké subjekty, jichž se dokumenty týkají a dokumenty, rozhodnutí a stanoviska ÚOOÚ. To bylo zohledněno v To-Be modelu datového fondu ÚOOÚ.

Změny v datovém fondu IS ORG se týkají primárně analytického modulu, který by měl být schopen dávat podklady pro případnou kontrolu nakládání s daty základních registrů, zejména ze strany soukromoprávních uživatelů údajů. Jedná se o doplnění Analyzovaných institucí do subjektů v rámci datového kmene IS ORG, analytických transakčních dat a analytických reportů.



3.4 Využití klíčových sdílených služeb eGovernmentu a externích IS

Tabulka 13: Přehled změn ve využití sdílených služeb

Sdílená služba	Informační systém
Autentizace NIA	neočekáváme
Základní registr ROB	AIS ÚOOÚ/GINIS
Základní registr ROS	AIS ÚOOÚ/GINIS
Základní registr RPP	neočekáváme
Kompozitní služby – evidence obyvatel	AIS ÚOOÚ/GINIS
Kompozitní služby – evidence cizinců	AIS ÚOOÚ/GINIS
Čerpání dat z PPDF (ISSS)	AIS ÚOOÚ

3.5 Návrh cílové IT technologické architektury

Na základě analýzy současného stavu a vyhodnocení personálních i finančních možností ÚOOÚ v rámci implementace IK ÚOOÚ budou vyhodnoceny 2 možnosti, jak do budoucna řešit IT infrastrukturu ÚOOÚ.

1) Infrastruktura kompletně v cloudu

V případě, že se podaří najít řešení finančně i právně způsobilé, byl by první volbou kompletní přechod na cloud. Důsledkem by byla minimalizace provozu infrastruktury v místním datovém centru (reálně pouze firewall). V rámci implementace IK ÚOOÚ bude analyzováno, zda je možné z pohledu kybernetické bezpečnosti a ochrany osobních údajů přejít na cloud kompletně. Počítáme s využitím šifrování, pro citlivá data i s využíváním vlastních šifrovacích klíčů.

IS ORG v rámci implementace IK ÚOOÚ začne analyzovat možnosti přechodu do státního cloudu či ke státnímu infrastrukturnímu provozovateli. Je vysoce pravděpodobné, že kritické informační systémy budou v následujících letech povinně přesunuty a provozovány centrálně.

2) Hybridní model – část v cloudu, část on-premise

Druhou variantou je částečný přechod na cloud, kdy by citlivá data a bezpečnostně nejrizikovější aktiva byla stále ukládána a provozována v rámci on-premise infrastruktury. Zbytek dat a aplikací by však byl provozován na cloudu. Není to preferovaná varianta, ale je možné, že buď z finančních důvodů nebo z důvodů bezpečnostně legislativních bude nutné takto postupovat.

IS ORG by i v případě této varianty postupoval stejně jako v prvním případě.

3.6 Návrh cílové komunikační technologické architektury

Komunikační infrastruktura projde v případě implementace AIS ÚOOÚ zásadní změnou. Dosud byla data ze základních registrů čerpána za využití spisové služby. Do budoucna by takovou funkci měl obsahovat AIS ÚOOÚ. Stejně tak očekáváme v rámci jeho vzniku napojení na ISSS a poskytováním dat do propojeného datového fondu.

Podoba AIS ÚOOÚ ale bude kompletněji popsána až v rámci implementace IK ÚOOÚ.

Pro komunikační technologickou architekturu z toho vyplývá připojení na CMS a publikace dat v PPDF.

4 Plán realizace změn v architektuře ÚOOÚ

4.1 Návrh strategie implementace

Implementace strategie bude probíhat v souvislosti s naplňováním IK ÚOOÚ. Bude využívat mechanismů popsaných v části C IK ÚOOÚ.

V praxi to znamená, že na ÚOOÚ bude implementováno zjednodušené projektové a programové řízení. Pro projektové řízení vznikne jednoduchá metodika, která bude povinná pro projekty realizované v rámci implementace IK ÚOOÚ. Ta bude zároveň sloužit jako programový dokument pro programové řízení.

Již v rámci tvorby IK ÚOOÚ byly všechny projektové záměry startující hned po jejím schválení rozpracovány do formy projektové karty, zhodnoceny z pohledu priorit a poskládány do konkrétního harmonogramu projektů. Postup v realizaci projektů bude průběžně reportován níže popsanému ŘV ITA každých 6 měsíců a předsedovi ÚOOÚ každých 12 měsíců.

Případné změny a posuny v harmonogramech pak budou schvalovány vedením ÚOOÚ a zapracovávány do IK ÚOOÚ.

4.2 Přehled všech běžících i plánovaných projektů/programů

Tabulka 14: Přehled všech běžících i plánovaných projektů/programů

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
P1	Vega D2-G	Implementace systému Vega D2-G pro potřeby tvorby a práce s utajovanými dokumenty do výše režimu utajení „Důvěrné“.	Běží	OIT	06/2022	11/2023
P2	Docházkový systém	Implementace nového Docházkového systému s dotykovými terminály.	Běží	OVS	11/2022	03/2024
P3	eSIAŘ	Implementace systému na evidenci a seznamování se s interními akty řízení ÚOOÚ.	Běží	OIT	06/2021	06/2023
P4	Analýza aktiv ÚOOÚ	Analýza aktiv ÚOOÚ, s důrazem na datové prvky.	Běží	BŘ	01/2023	04/2023

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
P5	Nový web ÚOOÚ	Implementace nového webu ÚOOÚ v souladu s Design systémem gov.cz.	Běží	TO/OIT	01/2021	06/2023
Z1	AIS ÚOOÚ	Systém zabezpečující pro všechny dílčí agendy (ochrana osobních údajů, svobodný přístup k informacím, nevyžádaná obchodní sdělení, konzultace aj.) ve spojení se stávající spisovou službou Ginis (nebo namísto ní, při zajištění ostatních funkcionalit spisové služby) příjem podání a podnětů všemi elektronickými kanály (včetně příjmu skrze webové formuláře), jejich evidenci a vyhodnocení, správu a úložiště dokumentů, funkcionality elektronického spisu a jeho elektronického oběhu (DMS), podporu tvorby vlastních dokumentů a management procesního workflow správních řízení, výkonu kontroly, včetně instancí a soudních řízení, a dalších procesů. Systém bude počítat	V přípravě	SMI, SD, SKANC	Q3 2023	Q4 2026

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
		s existencí došlých analogových dokumentů, které nelze konvertovat, a samostatných externích nosičů. Systém bude zobrazovat souvislosti mezi spisy navzájem, umožňovat lustrace (při zohlednění různých procesních rolí subjektu) a rešerše v metadatech (a určených dokumentech), analyticky zobrazovat vstupy (nápad) a navazující procesy, statisticky vykazovat definované procesy, dokumenty a časové údaje (plynutí lhůt, časové intervaly). Systém bude integrovat rozhraní pro dálkové nahlížení účastníků do spisu. V závislosti na vyhodnocení vztahu k jiným záměrům bude tyto integrovat: Z2 [Evidence pověřenců] a Z8 [modul NOS]; případně propojovat: Z5 [Interní a externí databáze rozhodnutí (INROK/EXROK)].				
Z2	Evidence pověřenců	Databáze pověřenců, součástí projektu bude	V přípravě	SMI	Q1 2024	Q3 2024

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
		volba vhodného technického řešení, definice rozsahu ukládaných údajů a import současných dat.				
Z3	Zavedení projektového řízení pro ICT projekty	Vytvoření metodiky projektového řízení pro projekty implementující informační koncepci. Metodika nebude závazná, bude doporučeným postupem.	V přípravě	OIT	Q3 2023	Q1 2024
Z4	Nový intranet ÚOOÚ	Nahrazení současného řešení intranetu novou verzí.	V přípravě	OIT	Q4 2023	
Z5	Interní a externí databáze rozhodnutí (INROK/EXROK)	Návrh technického řešení a vyřešení vztahu projektu s projektem Z1 - AIS. Jedná se o databáze rozhodnutí dle návrhu sekce SMI.	V přípravě	SMI	Q1 2024	Q4 2024
Z6	Rozvoj webu ÚOOÚ o zpětnovazební formulář	Rozvoj nového webu ÚOOÚ, doplnění zpětnovazebního formuláře a další rozvoj webu ÚOOÚ do konce roku 2024.	Záměr přesunut do projektu	TO	Q4 2023	Q2 2024
Z7	Dopracování ohlášení detailního popisu služeb a údajů do RPP	Naplnění požadavků zákona v oblasti ohlášení agend ÚOOÚ do RPP. Tedy sepsání detailního popisu služeb u všech ohlášených služeb na ÚOOÚ.	V přípravě	OLM	Q3 2023	Q2 2024
Z8	Analýza možného řešení pro nahrazení modulu NOS	Analýza s variantním návrhem řešení pro kontinuitu digitalizace agendy nevyžádaných obchodních sdělení.	V přípravě	SD, oddělení NOS	Q3 2023	Q2 2024

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
Z9	Plán rozvoje spisové služby	Vytvoření plánu rozvoje spisové služby za účelem implementace pravidel stanovených vyhláškou o podrobnostech výkonu spisové služby.	V přípravě	OVS	Q1 2024	Q2 2024
Z10	Zajištění systému pro hybridní (on-line a zároveň prezenční) vzdělávání odborné veřejnosti (pověřenců)	Zajištění profesionálního řešení pro pořádání hybridních jednání typu workshopu, konference nebo přednášky.	V přípravě	OIT	Q2 2024	Q4 2024
Z11	Uvedení praxe ÚOOÚ do souladu se zákonem č. 12/2020 Sb., o právu na digitální služby dle nových výkladů DIA	Zajištění procesů a digitalizačních kroků v rámci ÚOOÚ do souladu se zákonem č. 12/2020 Sb., o právu na digitální služby dle nových výkladů DIA	V přípravě	OLM	Q2 2024	Q2 2025
PZ1	Projekt na uvedení ICT do souladu s novou VoDŘISVS	Vytvoření plánu prací pro naplnění požadavků novely vyhlášky č. 529/2006 Sb., tento plán bude následně naplňován navazujícím projektem.		INF	Q3 2023	Q2 2024
PZ2	Vyhodnocení výhodnosti a náročnosti přechodu informačních systémů ÚOOÚ do cloudu	Vytvoření analýzy náročnosti a finanční výhodnosti přesunutí aplikací provozovaných na infrastruktuře ÚOOÚ do cloudové infrastruktury, včetně návrhu plánu případné migrace.		INF	Q3 2023	Q1 2024
PZ3	Maximalizace možností práce z domova	Vytvoření materiálu shrnujícího všechny prostředky, které mohou napomoci zaměstnancům ÚOOÚ pracovat ze svých		INF	Q1 2024	Q4 2024

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
		domovů. Výstupem projektu bude návrh potřebných kroků a harmonogram jejich realizace.				
PZ4	Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ	Aktualizace dokumentace týkající se kybernetické bezpečnosti IS Provoz ÚOOÚ. Součástí projektu bude tvorba daných dokumentů, nakoupení potřebných technických prostředků a externích služeb pro složitější úlohy.	V přípravě	INF	Q3 2023	Q1 2024
PZ5	Obnovení HW IS ORG	Dlouhodobý projekt na obnovu HW IS ORG, kterému skončila podpora od výrobce.	V přípravě	OZI	Q3 2023	Q4 2028
PZ6	Obnovení HW IS ÚOOÚ	Dlouhodobý projekt, který bude realizován pouze v případě, že se ukáže, že cloudové řešení není pro ÚOOÚ buď finančně nebo technicky realizovatelné.	V přípravě	INF	zrušeno!	
PZ7	Vytvoření řešení pro správu a tvorbu formulářů	Vytvoření prostředí, ve kterém bude možné jednoduše vytvářet a spravovat formuláře. Součástí projektu bude návrh technického řešení	V přípravě	INF	Q4 2023	
PZ8	Analýza přesunu provozu IS ORG na eGovernment Cloud	Výstupem projektu bude hypotetická analýza přesunu provozu IS ORG na cloudové řešení. Cílem je navrhnout konceptuální architekturu nového	V přípravě	OZI	Q3 2023	Q2 2024

Kód projektu	Název projektu	Předmět projektu	Stav projektu	Gestor	Termín zahájení	Termín dokončení
		řešení a identifikovat rizika, hrozby a příležitosti.				
PZ9	Nasazení nové technologie pro Service Desk	Projekt bude obsahovat analýzu potřebnosti nového Service Desku, plán jeho případného nasazení a směr rozvoje.	V přípravě	INF	Q1 2024	Q3 2024

4.3 Předpoklady úspěšné realizace plánovaných projektů/programů

Předpoklady pro úspěšnou realizaci plánovaných projektů jsou následující:

1) Úspěšné zapojení věcných gestorů do realizace digitalizačních aktivit.

ÚOOÚ v posledním období velmi postrádá konkrétní a přesně metodicky popsané zapojení věcných útvarů do digitalizačních aktivit. Změnu tohoto stavu by mělo přinést zavedení organizačních postupů vedoucích k přímému zapojení do projektových týmů, řídící struktury projektů a ŘV ITA.

2) Personální posílení IT útvaru a ekonomických útvarů

Pro naplnění dlouhodobých cílů IK ÚOOÚ bude nutné, aby bylo IT na ÚOOÚ posíleno minimálně o dvě pozice: architekt kybernetické bezpečnosti a IT architekt. V současnosti disponuje ÚOOÚ pouze pozicemi určenými pro provoz IT ÚOOÚ a provoz IS ORG. Odborné pozice potřebné pro rozvoj digitálních služeb chybí. Vedle toho je nutné zvážit přijetí jedné nové pozice pro finanční administraci případných projektů ze strukturálních fondů.

3) Získání finančních zdrojů

Při naplňování cílů IK ÚOOÚ bude kladen maximální důraz na dlouhodobou udržitelnost, proto je zásadní, aby byl ÚOOÚ schopen provoz nových digitálních služeb financovat ze státního rozpočtu ideálně bez jeho výraznějšího navyšování. Proto budeme v první fázi hledat možnosti úspor ve vlastním rozpočtu. Ve druhé fázi je ale možné, že bude nutné na některé projekty finance získat. Vzhledem k malému počtu zaměstnanců na ÚOOÚ budeme v první fázi usilovat o finance přímo ze státního rozpočtu. Ve druhé fázi a při neúspěchu bychom se pokusili získat prostředky i ze strukturálních fondů či jiných dotačních titulů.

4.4 Způsob financování projektů/programů a provozu ICT

4.4.1 Plán financování projektů

Tabulka 15: Plán přímých investičních nákladů na projekty.

Rok	Investiční výdaje (Kč)	Zdroje financování
2024		
2025	20 000 000 Kč	Státní rozpočet
2026	60 000 000 Kč	Státní rozpočet/evropské fondy
2027	10 000 000 Kč	Státní rozpočet
2028		

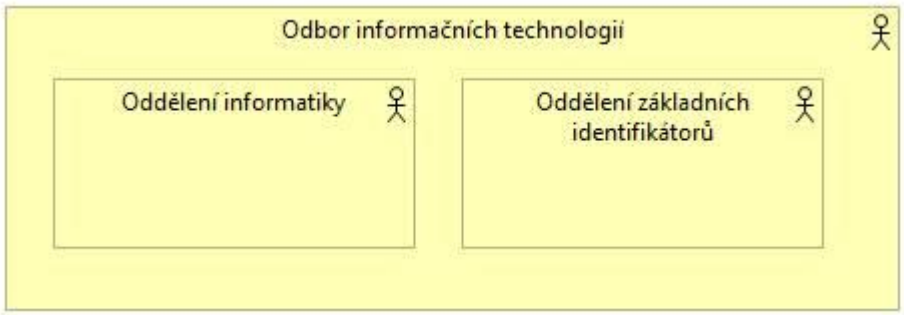
4.4.2 Plán financování provozu ICT

Tabulka 16: Plán mandatorních výdajů

Rok	Mandatorní výdaje	Zdroje financování
2024	10 000 000 Kč	Státní rozpočet
2025	12 000 000 Kč	Státní rozpočet
2026	12 000 000 Kč	Státní rozpočet
2027	12 000 000 Kč	Státní rozpočet
2028	13 000 000 Kč	Státní rozpočet

ČÁST B: Koncepce řízení služeb ICT

1 Zhodnocení stávajícího stavu řízení ICT



Obrázek 8: Organizační struktura ICT útvaru ÚOOÚ

1.1 Zhodnocení stavu a metod řízení životního cyklu IS

1.1.1 Strategie, plánování změn

ÚOOÚ se podílí na připomínkování dokumentů souvisejících s rozvojem základních registrů. Je členem Rady ZR a Rady vlády pro informační společnost. Pravidelně vyhodnocuje dopady jednotlivých strategických rozhodnutí na centrální úrovni směrem k fungování ÚOOÚ.

Pro IS ORG funguje strategické řízení ve formě pravidelných Strategií rozvoje a provozu, které jsou schvalovány Výborem pro kybernetickou bezpečnost ÚOOÚ (dále jen VKB) a vedením ÚOOÚ.

V současnosti neexistuje strategie pro Významný informační systém IS Provoz ÚOOÚ, stejně tak není přesně a dle pravidel kybernetické bezpečnosti definován proces plánování a schvalování změn.

1.1.2 Realizace změn a předání do provozu

Realizace a předání do provozu v rámci IS ORG jsou přesně definovány v rámci politik provozu IS ORG. V rámci interního IT není zatím proces změn přesněji definován. Jeho definice bude jedním z hlavních cílů K ÚOOÚ.

ÚOOÚ obecně funguje výhradně na dodavatelských řešeních. Proto probíhá předání do provozu klasickým akceptačním protokolem nebo akceptační procedurou dle smlouvy vzešlé z veřejné zakázky.

1.1.3 Produkční provoz

Provoz je řízen dle platného smluvního závazku akceptací předávacích či akceptačních protokolů pro daný IS nebo SW řešení. Část řešení běží na infrastruktuře dodavatele, zde jsou definována SLA. Část je pak provozována na infrastruktuře ÚOOÚ za využití služeb podpory od dodavatele a licenčních ujednání. U těchto systémů jsou smluvně zajištěny pouze odezvy v případě potřeby podpory, nikoliv celkové SLA. Jeho hlubší definice bude předmětem změn v rámci realizace cílů IK ÚOOÚ.

1.1.4 Vyhodnocování, optimalizace

V oblasti vyhodnocování a optimalizace IS jsou na ÚOOÚ rezervy. V současnosti probíhá spíše živelné vyhodnocování. Změny se dějí na základě provozních událostí nebo častých výpadků IS. Většina IS, které ÚOOÚ provozuje jsou ze zákona povinné nebo nutné pro fungování ÚOOÚ.

1.1.5 Ukončení provozu

Ukončení provozu IS se v rámci ÚOOÚ primárně řídí smluvními podmínkami daného IS. Neexistuje metodika správného procesu při ukončení provozu IS.

1.2 Zhodnocení stavu a metod řízení schopností ICT útvaru

1.2.1 Personální politika a rozvoj lidských zdrojů

Personální politika je v rámci OIT na ÚOOÚ velmi ovlivněna platovými možnostmi útvaru. Mimo řídících pracovníků jsou všichni na referentských pozicích v nízkých platových třídách. To znamená z pohledu IT trhu velice nízké platové ohodnocení, ale přesto je k nástupu na tuto třídu nutné vysokoškolské vzdělání alespoň v bakalářském studijním programu. Tato skutečnost velmi razantně omezuje možnosti OIT nabírat nové zaměstnance. Z těchto důvodů je kladen velký důraz na firemní kulturu, snažíme se v útvaru vytvářet prostředí, ve kterém je v rámci možností příjemné působit, snažíme se zaměstnancům vycházet vstříc, pracovat na jejich osobním rozvoji a respektovat jejich potřeby a limity. Co se týče náboru nových zaměstnanců, tak obecně je zaměstnání na ÚOOÚ zajímavé pro absolventy oborů, které nejsou IT, a kteří chtějí rozšířit své možnosti na trhu práce, přičemž počítáme s tím, že je pravděpodobné, že po rekvalifikaci ÚOOÚ opustí a my budeme hledat znovu. Druhou kategorií jsou zaměstnanci, kteří mají jiné priority než platové ohodnocení, a právě třeba firemní kultura je proto nejzásadnější.

1.2.2 Ekonomické a finanční řízení ICT

Ekonomické a finanční řízení ICT probíhá ve formě ročních plánů. Jako každý úřad sestavujeme každoročně rozpočet zhruba v srpnu předchozího roku. Tento rozpočet je poté schvalován vládou. Konkrétní schválené částky se pak dozvíme většinou na začátku daného kalendářního roku. To jsou i zásadní milníky pro finanční řízení OIT. Pro obě oddělení vznikají oddělené rozpočtové plány. Ty se ještě dělí na rozpočet na služby a rozpočet na investice. Finální verze těchto rozpočtů jsou finalizovány na začátku daného kalendářního roku.

Vedle toho pravidelně vyhodnocujeme současné smluvní vztahy a v rámci strategického řízení řešíme, kam alokovat finanční prostředky v dalších letech. Přesto lze konstatovat, že většina finančních prostředků míří do udržení současných IS v provozu, do rozvoje se investuje jen velmi malá část finančních prostředků. Největší část rozpočtu OIT pak míří do obnovy HW.

1.2.3 Správa vlastních informačních systémů ICT

Správa vlastních informačních systémů probíhá v úzké spolupráci s provozovateli informačních systémů. Vzhledem k personální situaci na OIT je nutné naprostou většinu činností spojených se správou IS vykonávat s podporou provozovatele. Proto většina IS na ÚOOÚ je buď nakupována jako služba s podporou od výrobce nebo (jako v případě IS ORG) vlastní ÚOOÚ HW a zdrojové kódy, systém je provozován na infrastruktuře ÚOOÚ, ale většinu úkonů spojených s provozem vykonává dodavatel.

1.2.4 Strategické plánování a řízení ICT OVS

Strategické plánování není na ÚOOÚ na vysoké úrovni, z toho důvodu je i velký důraz kladen na vytvoření IK ÚOOÚ. Obecně byl rámcově řízen pouze provoz IS ORG. Zbytek IS v rámci ÚOOÚ strategii v tuto chvíli postrádá. V minulosti proběhla s vidinou ušetření finančních prostředků i velká řada značně nekoncepčních kroků. Z toho důvodu je nyní nutné vytvořit nové řídící dokumenty, aktualizovat dokumentaci týkající se kybernetické bezpečnosti a všechny tyto činnosti v nových strategiích IS zohlednit.

Řízení ICT OVS je v tuto chvíli řešeno za pomoci půlročních plánů, jejich reportingu útvaru předsedy ÚOOÚ a následného půlročního vyhodnocování dosaženého pokroky. Dokument, který vzniká vždy na začátku pololetí se jmenuje „Směřování OIT“, tento dokument stanoví krátkodobé cíle a sleduje již známé úkoly. Jednou za zhruba dva týdny je reportován pokrok tomto směřování a případné změny v plánovaných termínech. Směřování je vytvářeno ve spolupráci se všemi představenými v rámci OIT a následné reporty jsou taktéž sdíleny. V rámci interního řízení probíhají každý týden pravidelné porady odboru, kde jsou primárně probírány úkoly ze „Směřování OIT“, případně jiné ad hoc záležitosti.

1.2.5 Řízení identifikace a realizace změn ICT ÚOOÚ

V tuto chvíli neexistuje na ÚOOÚ jasně definovaný proces identifikace a realizace změn v ICT. Vzhledem k absenci strategických materiálů probíhá identifikace změn živelně. Většinou ze strany řídících pracovníků přijde požadavek, který je nutné v co nejkratší době zrealizovat. Často je při identifikaci těchto požadavků opomíjen kontext zbytku IT a tlakem na rychlou realizaci dochází ke zkratkovitým a nekoncepčním řešením. Je jedním ze zásadních cílů IK ÚOOÚ tento stav změnit a proces řízení změn definovat a promítnout do interních aktů řízení.

1.2.6 Řízení provozu IS a dodávky služeb

Řízení provozu IS je prováděno v úzké spolupráci s dodavateli. Probíhají pravidelné schůzky se všemi významnými dodavateli, z nichž vznikají zápisy nebo seznamy úkolů.

1.2.7 Řízení rizik a bezpečnosti v ICT útvaru

Řízení rizik a bezpečnosti je velmi podrobně a precizně zpracováno pro IS ORG. Existuje analýza rizik a řada bezpečnostních politik a dokumentace dle platné VoKB. IS ORG prošel i certifikací na ISO 27001. V rámci interního IT je situace jiná. Zde chybí aktualizovaná analýza rizik a část bezpečnostních dokumentů. V rámci projektového záměru Z5 plánujeme tento stav napravit.

1.2.8 Standardizace v řízení ICT

Vzhledem k velikosti ÚOOÚ není standardizace velkým tématem. Jak bylo řešeno výše, IS ORG je certifikován dle ISO 27001, což je v jistém smyslu standardizace.

1.2.9 Řídící dokumentace, včetně bezpečnosti

Řídící dokumentace, včetně bezpečnostních dokumentů, je vedena v GINIS.

1.3 Zhodnocení stavu a metod řízení disciplín ve spolupráci s ostatními útvary ÚOOÚ

1.3.1 Podpora útvarů péče o klienty služeb ÚOOÚ - Integrovaný externí ServiceDesk

ÚOOÚ provozuje pouze interní Service Desk, kde řeší podporu uživatelů ICT v rámci ÚOOÚ. Externí Service Desk v nějaké sofistikované podobě neexistuje, na druhou stranu běží infolinka, kam je možné zavolat a na nutné věci se doptat. Nicméně ÚOOÚ se nesetkává s příliš velkým množstvím technických dotazů na funkčnost ICT služeb. Důvodem je relativní jednoduchost a přímočarost služeb, které ÚOOÚ poskytuje. Téměř všechny jdou řešit e-mailem či datovou schránkou, dotazy na ÚOOÚ tak spíše míří na metodiku v rámci řešených agend a většinou chodí formou žádosti dle zákona č. 106.

1.3.2 Přístup k legislativní podpoře informatizace VS - Digitálně přívětivá legislativa

ÚOOÚ samo o sobě není autorem zákonů, v drtivé většině případů je pouze připomínkovým místem. Vzhledem k současným trendům a agendě ÚOOÚ pak funguje spíše jako kontrola, zda už digitalizace nezasahuje do ochrany osobních údajů.

1.3.3 IT bezpečnost a ochrana údajů

IT bezpečnost je v IS ORG na vysoké úrovni. V rámci interního IT jsou rezervy, které budou adresovány v rámci projektového záměru Z5. Co se týče ochrany údajů, tak v období, kdy je zpracovávána IK ÚOOÚ, probíhá definice datových aktiv ÚOOÚ a jejich klasifikace. V rámci této klasifikace bude rozhodnuto, jakým způsobem bude k jakým údajům přistupováno. Je nutné definovat technické řešení tohoto problému.

1.3.4 Podíl IT na celkové bezpečnosti ÚOOÚ

ICT útvar se významně podílí na celkové bezpečnosti ÚOOÚ, ředitel OIT i vedoucí obou oddělení jsou součástí krizového štábu ÚOOÚ, který je rozhodujícím orgánem pro řízení bezpečnosti ÚOOÚ. Probíhají pravidelná jednání s bezpečnostním ředitelem na týdenní bázi, kde se řeší bezpečnostní hrozby a reakce na ně.

1.3.5 Podíl IT na ochraně údajů a GDPR

ICT útvar se významně podílí na ochraně údajů a GDPR. V případě nutnosti vytváření DPIA je primárním autorem technických částí dokumentace a partnerem do diskuze pro pověřence na ochranu osobních údajů. Vzhledem k tomu, že GDPR je jednou z hlavních agend ÚOOÚ, jsou nároky na ICT útvar v rámci ochrany osobních údajů velmi vysoké a probíhají časté debaty na toto téma. Někdy tyto debaty výrazně zdržují realizaci technických řešení.

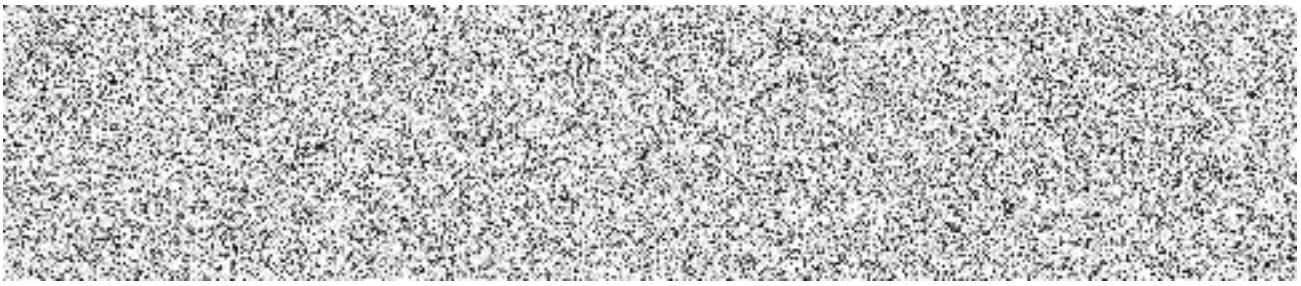
1.3.6 Spolupráce na veřejných zakázkách

Spolupráce na veřejných zakázkách probíhá bez větších problémů. Vzhledem k velikosti ÚOOÚ se jedná o spolupráci s jednou osobou, která veřejné zakázky na úřadu zajišťuje.

1.4 Zhodnocení stavu spolupráce s orgány centrální koordinace ICT a eGovernmentu

1.4.1 Centrální koordinace řízení ICT státu

Centrální koordinace řízení ICT státu je z pohledu ÚOOÚ lehce problematická. Hlavním problémem je nemožnost škálování požadavků dle velikosti úřadu. Současné požadavky na kybernetickou bezpečnost a řízení architektury ICT jsou natolik rozsáhlé, že v praxi společně s provozem čerpají prakticky kompletní kapacitu IT odborníků na ÚOOÚ. Najít kapacity na rozvoj je v takovém stavu velmi nesnadné. Je nutné také připomenout, že kombinace pravidel ZoZVZ a nutnosti tvorby Formuláře OHA pro tvorbu větších informačních systémů znamená praktickou nezbytnost externích konzultací pro veškerý větší rozvoj, což je v podmínkách a rozpočtových možnostech ÚOOÚ také velmi nesnadné. Jakékoliv omezení povinností pro menší úřady by bylo výraznou pomocí. Na druhou stranu vítáme tlak na strategické řízení ICT a metodickou podporu při tvorbě IK ÚOOÚ.



1.4.2 Ekonomická koordinace

Ekonomická koordinace probíhá s odborem provozu a ekonomiky formou ročních finančních plánů. Zatím nejsou realizovány žádné projekty ze strukturálních fondů.

1.4.3 Koordinace realizace změn a dosahování přínosů

Realizace změn probíhá formou projektů, které jsou řízeny většinou ředitelem OIT za využití metodiky PRINCE2, případně její modifikované podoby. Řízení a evaluace projektů probíhá ve formě půlročních plánů a jejich vyhodnocování.

1.4.4 Řízení licencí

Řízení licencí probíhá ve spolupráci s představenými jednotlivých útvarů, kteří navrhují konkrétní osoby pro nakoupené licence, případně žádají o nové licence cestou interního Service Desku. OIT pravidelně vyhodnocuje využívání licencí a snaží se minimalizovat množství málo využívaných či vůbec nevyužívaných licencí.

1.4.5 Spolupráce na úrovni celého resortu

ÚOOÚ je samostatný úřad, spolupráce na úrovni resortu pro něj tedy není relevantní.

1.5 Přehled běžících a schválených projektů pro řízení ICT

1.5.1 Přehled projektů řízení ICT

Tabulka 17: Přehled projektů řízení ICT

Kód projektu	Název projektu	Předmět projektu	Fáze projektu	Odpovědný útvar	Termín zahájení	Termín dokončení
P1	Vega D2-G	Implementace systému Vega D2-G pro potřeby tvorby a práce s utajovanými dokumenty do výše režimu utajení „Důvěrné“ .	Běží	OIT	06/2022	11/2023
P5	Nový web ÚOOÚ	Implementace nového webu ÚOOÚ v souladu s Design systémem gov.cz .	Běží	TO/OIT	01/2021	06/2023
PZ1	Projekt na uvedení ICT do souladu s novou VoDŘISVS	Vytvoření plánu prací pro naplnění požadavků novely vyhlášky č. 529/2006 Sb., tento plán bude následně naplňován navazujícím projektem.	V přípravě	INF	Q3 2023	Q2 2024
PZ2	Vyhodnocení výhodnosti a náročnosti přechodu informačních systémů ÚOOÚ do cloudu	Vytvoření analýzy náročnosti a finanční výhodnosti přesunutí aplikací provozovaných na infrastruktuře ÚOOÚ do cloudové infrastruktury, včetně návrhu plánu případné migrace.	V přípravě	INF	Q3 2023	Q1 2024
PZ3	Maximalizace možností práce z domova	Vytvoření materiálu shrnujícího všechny prostředky, které mohou napomoci zaměstnancům ÚOOÚ pracovat ze svých domovů. Výstupem projektu bude návrh potřebných kroků a	V přípravě	INF	Q1 2024	Q4 2024

Kód projektu	Název projektu	Předmět projektu	Fáze projektu	Odpovědný útvar	Termín zahájení	Termín dokončení
		harmonogram jejich realizace.				
PZ4	Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ	Aktualizace dokumentace týkající se kybernetické bezpečnosti IS Provoz ÚOOÚ. Součástí projektu bude tvorba damých dokumentů, nakoupení potřebných technických prostředků a externích služeb pro složitější úlohy.	V přípravě	INF	Q3 2023	Q1 2024
PZ5	Obnovení HW IS ORG	Dlouhodobý projekt na obnovu HW IS ORG, kterému skončila podpora od výrobce.	V přípravě	OZI	Q3 2023	Q4 2028
PZ6	Obnovení HW IS ÚOOÚ	Dlouhodobý projekt, který bude realizován pouze v případě, že se ukáže, že cloudové řešení není pro ÚOOÚ buď finančně nebo technicky realizovatelné.	V přípravě	INF	zrušeno!	
PZ7	Vytvoření řešení pro správu a tvorbu formulářů	Vytvoření prostředí, ve kterém bude možné jednoduše vytvářet a spravovat formuláře. Součástí projektu bude návrh technického řešení.	V přípravě	INF	Q4 2023	
PZ8	Analýza přesunu provozu IS ORG na eGovernment Cloud	Výstupem projektu bude analýza hypotetického přesunu provozu IS ORG na cloudové řešení. Cílem je navrhnout konceptuální architekturu nového	V přípravě	OZI	Q3 2023	Q2 2024

Kód projektu	Název projektu	Předmět projektu	Fáze projektu	Odpovědný útvar	Termín zahájení	Termín dokončení
		řešení a identifikovat rizika, hrozby a příležitosti.				
PZ9	Nasazení nové technologie pro service desk	Projekt bude obsahovat analýzu potřebnosti nového service desku, plán jeho případného nasazení a směr rozvoje.	V přípravě	INF	Q1 2024	Q3 2024

1.6 Shrnutí potřeb ze stávajícího stavu

Základním nedostatkem řízení ICT v rámci ÚOOÚ je absence strategického dokumentu a jasně definované vize a cílů útvaru ICT. Vedle toho částečně chybí lépe zpracovaná a aktualizovaná dokumentace vyplývající z požadavků na kybernetickou bezpečnost pro interní IT. Velkou nutností je také přesnější definice procesu realizace změn a jeho ukotvení do interních aktů řízení ÚOOÚ. Zároveň chybí metodika řízení životního cyklu IS.

Naopak IS ORG je z pohledu řízení ICT v dobrém stavu - jak z pohledu řízení změn, tak z pohledu kybernetické bezpečnosti.

Velkou výzvou pro řízení ICT je poté interní soulad s věcnými útvary ohledně nakládání s osobními údaji a nalézání shody s dalšími útvary, kterého bude nutné docílit pro realizaci dalšího rozvoje.

2 Přehled motivací ÚOOÚ ke změnám řízení ICT

2.1 Přehled externích cílů, úkolů a vlivů

Zásadním externím faktorem pro všechny IT útvary v rámci veřejné správy je legislativa. V případě ÚOOÚ jsou zásadní pro provoz IT zejména zákony a vyhlášky týkající se kybernetické bezpečnosti a VoDŘISVS, jejíž novelizace od roku 2023 probíhá.

Vedle toho evidujeme i některé požadavky vedení na další provoz IT na ÚOOÚ. Jedná se primárně o maximalizaci možností práce z domova a optimalizace fungování podpory koncových uživatelů. Zároveň je nutné při všech rozvojových krocích dbát zvýšené opatrnosti vzhledem k nakládání s osobními údaji.

Velkou řadu cílů i pro ICT generuje IK ÚOOÚ. Ať už ve směru realizace výše zmíněných projektových záměrů či s ohledem na cíle a směřování v koncepci stanovené.

2.2 Přehled identifikovaných vnitřních motivací

Vnitřní motivací pro řízení ICT je snaha provozovat IT efektivně a spolehlivě za dodržování všech zákonů a vyhlášek, které na ICT mají dopad. Realita malého úřadu s nevelkými finančními prostředky a omezenými personálními kapacitami dovedla OIT k několika základním principům, kterými se bude v dalších 5 letech řídit a které budou rámovat naplňování externích i byznysových cílů.

1) Maximální využívání pilotního provozu a postupné nasazování nových technologií

Jednou z mála výhod malého úřadu je možnost o něco snáz nasazovat nové technologie. Tyto technologie se ale musí nasazovat s jasnou představou, co takové nasazení pro organizaci znamená. Ideální je vyzkoušet nástroj na omezeném počtu uživatelů, a až následně uvažovat o jeho nasazení. Takový pilotní provoz zpravidla trvá 1–3 měsíce a je ukončen vyhodnocením a návrhem dalšího postupu schvalovaným vedením ÚOOÚ.

2) Maximální využívání již nakoupeného SW a licencí (včetně licencí zdarma)

Je důležité zohledňovat všechny služby a aplikace, které organizace má dlouhodobě či historicky zasmluvněné. V průběhu let se často podrobná znalost i personálními změnami ztrácí a je tedy nutné ji pravidelně obnovovat a mít na paměti všechny součásti portfolia. Důležité je to nejvíce ve spolupráci s velkými korporátními partnery typu Microsoft jejichž licenční politika se často mění, a tím pádem se mění rozsah a možnosti využívaných aplikací. Vedle toho je výhodné sledovat trh a hledat možnosti využívání SW zdarma, minimálně v rámci pilotního provozu, a tím pádem snížit náklady na pilotní provozy.

3) Postupný ústup od provozování HW na ÚOOÚ

Pro úřady malé velikosti je provozování HW velmi nákladnou záležitostí, a je tak nutné přemýšlet o alternativních řešeních. Dlouhodobým cílem pro IT ÚOOÚ tak je omezovat využívání on-premise HW a přecházet na cloud. V rámci aplikací nutných pro provoz ÚOOÚ a v případě dokumentů a dat, která jsou jakýmkoliv způsobem citlivá (dle DLP Red a Amber Strict/Amber), je možné uvažovat o využití šifrování pro zajištění bezpečnosti těchto dat. V případě systému IS ORG je preferovanou variantou využití státního cloudu.

4) Velký důraz na strategické řízení a dlouhodobou udržitelnost

Vzhledem k systému fungování veřejné správy a náročnosti jejích administrativních procesů je nutné veškeré změny plánovat s dostatečným předstihem. Každou změnu pak hodnotit nejen z pohledu krátkodobých, například investičních nákladů, ale i z pohledu dlouhodobé udržitelnosti a náročnosti na správu takových systémů.

5) Využívání externích služeb za účelem rozšíření know-how organizace a outsourcingu expertních služeb

Vzhledem k velikosti ÚOOÚ není možné veškeré činnosti potřebné pro řízení ICT vykonávat interními zaměstnanci. Pro rozvoj bude nutné nejen získat nové zaměstnance schopné vytvářet návrhy koncepčních změn, ale také spolupracovat s partnery ze soukromého sektoru, kteří mají znalosti nejnovějších technologií a jsou schopni pomoci vybrané projekty realizovat.

ID	Zásada	Relevance a praktické dopady do OVM
Z1	Na prvním místě je klient	Zásada je v ÚOOÚ aplikována, v současné době se bude orientovat primárně na interní klienty. V této oblasti jsou zásadní zejména projektové záměry Z1, Z2, Z4, Z10. Externí klienti by pak měli postupně získat snazší přístup ke službám ÚOOÚ díky projektovým záměrům Z3 a Z8.
Z2	Standardy plánování a řízení ICT	Zavádění pokročilých metod řízení je v procesu, není zde ambice zavádět komplexní metodiky řízení služeb, je však nutné definovat zásadní procesy a metodickými materiály se inspirovat. Řízení a plánování ICT bude úzce propojeno s kybernetickou bezpečností. Tato zásada tak bude naplňována primárně projektovým záměrem PZ4 a provozním projektovým záměrem PZ1.
Z3	Strategické řízení pomocí IK OVS	Bude naplněno vznikem, aktualizací a řízením dle zpracované IK ÚOOÚ.
Z4	Řízení architektury	Procesy v oblasti architektury budou přesněji definovány v rámci PZ1. Vizí je vytvoření interního architektonického týmu.
Z5	Řízení požadavků a změn	Bude realizováno a definováno v rámci PZ1 a PZ4.
Z6	Řízení výkonnosti a kvality	Bude realizováno v rámci PZ1.
Z7	Řízení zodpovědnosti	Bude realizováno v rámci PZ1 a PZ4.

ID	Zásada	Relevance a praktické dopady do OVM
	za služby a systémy	
Z8	Řízení ICT služeb	Bude realizováno v rámci PZ1 a PZ4.
Z9	Udržení interních kompetencí	O nové pracovní pozice, které by naplnily potřeby ICT útvaru, bude trvale žádáno v rámci nových systemizačních návrhů.
Z10	Procesní řízení v ICT	Bude realizováno v rámci PZ1 a PZ4.
Z11	Řízení přínosů a hodnoty	Bude realizováno v rámci PZ1 a PZ4. Konkrétně již vytváříme jednoduché šablony vyhodnocení pilotního provozu a analýzy potřebnosti před započetím pilotního provozu. Všechny projekty ISVS musí (spolu s formulářem OHA) disponovat zpracovaným investičním záměrem typu „business case“ s jasně identifikovaným přínosem pro veřejnost a/nebo ÚOOÚ. Je třeba pracovat s metodikou finančních kalkulací na bázi indexu rentability/CBA (analýza přínosů a celkových nákladů) a TCO (celkových nákladů na vlastnictví ICT), včetně budování kompetence ekonomicky kalkulovat optimální efektivitu a výkonnost agendy (procesu) s různou úrovní poměru personálních nákladů na její výkon a nákladů na její IT podporu.
Z12	Řízení kapacit zdrojů	O nové pracovní pozice, které by naplnily potřeby ICT útvaru, bude trvale žádáno v rámci nových systemizačních návrhů.
Z13	Nezávislost návrhu, řízení a kontroly kvality	Bude realizováno v rámci PZ1 a PZ4. Obecně bude aplikováno ve formě vnitřních kontrol v rámci implementačního týmu.
Z14	Vztah informatiky a legislativy	Není relevantní.
Z15	Řízení financování ICT	Zásada se prolíná obecně všemi projekty a cíli IK ÚOOÚ. Obecně je cílem ÚOOÚ zefektivnit využívání finančních prostředků. Stejně tak bude pro interní účely ÚOOÚ vyhodnoceno, nakolik je schopen zvládnout projekty ze strukturálních fondů.
Z16	Využívání otevřeného software a standardů	Reálné jen za předpokladu získání nových pracovních míst pro IT odborníky.

ID	Zásada	Relevance a praktické dopady do OVM
Z17	Podpora vyváženého partnerství s dodavateli	Ošetřeno v rámci současných smluvních vztahů, pokud by se dělaly dodatky, bude na tuto zásadu brán zřetel.

2.3 SWOT analýza

Silné stránky:

- Proklientský přístup v rámci podpory koncových uživatelů
- Personální obsazení zásadních pozic
- Profesionální vztahy s dodavateli a jejich flexibilita
- Základní možnost práce z domova

Příležitosti:

- Využít nutnost obnovy HW k přechodu na cloudové technologie
- Nahradit stávající legacy systémy novými moderními řešeními

Slabé stránky:

- Živelnost příjmu žádostí o změnu a podporu
- Nedostatek finančních prostředků
- Zastaralost IT infrastruktury (primárně ve vztahu k vnitřnímu IT)

Hrozby:

- Postupné vypadávání infrastruktury
- Velká závislost na jednotlivých zaměstnancích
- Vendor Lock

2.4 Shoda se zásadami řízení ICT z IK ČR

Bude realizováno v rámci PZ1.

2.5 Cíle zlepšování kvality řízení, rozvoje a provozu ICT služeb

Bude realizováno v rámci PZ1.

2.6 Cíle zlepšování v oblasti bezpečnosti

V roce 2023 proběhla analýza kybernetické bezpečnosti na ÚOOÚ v obou informačních systémech, které spadají pod zákon a vyhlášku o kybernetické bezpečnosti. Z analýzy vyplynuly následující skutečnosti a úkoly.

2.6.1 Identifikované nedostatky

Nízký stav dokumentace ICT činností ÚOOÚ a neaktuálnost bezpečnostní politiky IS ÚOOÚ. Není dle pravidel vytvářena dokumentace ke správě IT. Důvodem tohoto nevyhovujícího stavu je rozhodnutí bývalého vedení ÚOOÚ o ukončení outsourcingu bezpečnostních činností IS UOOU, které nebylo nahrazeno novou externí smlouvou nebo vnitřními zdroji ÚOOÚ.

Nejednoznačnost vymezení VIS ÚOOÚ - není jasné, které součásti IS ÚOOÚ jsou VIS dle zákona. Dle stávajícího stavu je rozpor mezi realitou správy IS ÚOOÚ, vnitřními předpisy a vyhláškou č. 317/2014, o významných informačních systémech a jejich určujících kritériích. Povinná osoba – předseda ÚOOÚ – musí na základě návrhu OIT a gestorů dat jednoznačně stanovit rozsah VIS úřadu.

Pro řízení ISMS musí být vytvořen systém jednotně stanovených postupů a bezpečnostních politik, a to cestou outsourcingu nebo posílením lidských kapacit OIT. Stávající bezpečnostní politika není v souladu s požadovaným rozsahem dle VoKB. Zde musí ÚOOÚ rozhodnout, zda systém dokumentace bezpečnostních politik zajistí cestou outsourcingu nebo cestou vlastních lidských zdrojů, kterými však OIT nedisponuje.

ÚOOÚ nemá vytvořenu aktuální metodiku pro hodnocení rizik IS ÚOOÚ, bez níž nelze správně provést analýzu rizik.

2.6.2 Identifikované úkoly

Organizačně doplnit VKB o popis rolí v oblasti kybernetické bezpečnosti a rozšířit je o architekta kybernetické bezpečnosti.

Aktualizovat stávající směrnice č. 8,10 a 12 z roku 2019, neboť plně neodpovídají současným požadavkům na zajištění KB v ÚOOÚ.

Vytvořit registr aktiv ve spolupráci s garanty aktiv a pověřencem pro ochranu osobních údajů, kdy registr aktiv je základním dokumentem ochrany kybernetické bezpečnosti v ÚOOÚ. V rámci registru aktiv stanovit Traffic Light Protocol (TLP), tj. stanovit bezpečnostní úroveň aktiv ÚOOÚ, pomocí doporučeného postupu NÚKIB. Následně provést analýzu rizik a stanovit způsob ochrany předmětných

aktiv ÚOOÚ v rámci IS ÚOOÚ, zejména správně zařadit aktiva spadající pod ustanovení vyhlášky č. 317/2018 Sb., o významných informačních systémech a jejich určujících kritériích.

Popsat a vytvořit systém bezpečnostních pravidel pro správu mobilních a technických zařízení, na kterých dochází vzdáleným přístupem k nakládání s daty ÚOOÚ, a to i u zařízení, která nejsou ve správě ÚOOÚ.

Posoudit dopad užívání cloudu společnosti Microsoft na aktiva ÚOOÚ z hlediska ochrany osobních údajů.

Vytvořit či aktualizovat bezpečnostní politiku IS ÚOOÚ v tomto rozsahu:

- Politika systému řízení bezpečnosti informací
- Politika organizační bezpečnosti
- Politika řízení dodavatelů
- Politika klasifikace aktiv
- Politika bezpečnosti lidských zdrojů
- Politika řízení provozu a komunikací
- Politika řízení přístupu
- Politika bezpečného chování uživatelů
- Politika zálohování a obnovy
- Politika bezpečného předávání a výměny informací
- Politika řízení technických zranitelností
- Politika bezpečného používání mobilních zařízení
- Politika licencování software a informací
- Politika dlouhodobého ukládání a archivace informací
- Politika ochrany osobních údajů
- Politika fyzické bezpečnosti
- Politika bezpečnosti sítě
- Politika ochrany před škodlivým kódem
- Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
- Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Politika bezpečného používání kryptografické ochrany
- Politika zvládání krizových situací a obnovy dat

Tyto úkoly budou realizovány v rámci projektového záměru PZ4: Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ. V rámci tohoto projektu a dle rozhodnutí vedení ÚOOÚ by mělo dojít k rozhodnutí, zda a do jaké míry budou příslušné služby dodány externě.

2.7 Shrnutí a interpretace identifikovaných změn řízení ICT

Tabulka 18: Přehled identifikovaných záměrů

Kód a název záměru	Předmět záměru	Fáze záměru	Odpovědný útvar	Termín zahájení	Termín dokončení	DČ
PZ1 – Projekt na uvedení ICT do souladu s novou VoDŘISVS	Vytvoření plánu prací pro naplnění požadavků novely vyhlášky č. 529/2006 Sb., tento plán bude následně naplňován navazujícím projektem.	V přípravě	INF	Q3 2023	Q2 2024	Ne
PZ2 – Vyhodnocení výhodnosti a náročnosti přechodu informačních systémů ÚOOÚ do cloudu	Vytvoření analýzy náročnosti a finanční výhodnosti přesunutí aplikací provozovaných na infrastruktuře ÚOOÚ do cloudové infrastruktury, včetně návrhu plánu případné migrace.	V přípravě	INF	Q3 2023	Q1 2024	
PZ3 – Maximalizace možností práce z domova	Vytvoření materiálu shrnující všechny prostředky, které mohou napomoci zaměstnancům ÚOOÚ pracovat ze svých domovů. Výstupem projektu bude návrh potřebných kroků a harmonogram jejich realizace.	V přípravě	INF	Q1 2024	Q4 2024	
PZ4 – Zajištění kybernetické bezpečnosti	Aktualizace dokumentace týkající se kybernetické bezpečnosti IS Provoz	V přípravě	INF	Q3 2023	Q1 2024	Ano, projektový záměr je

Kód a název záměru	Předmět záměru	Fáze záměru	Odpovědný útvar	Termín zahájení	Termín dokončení	DČ
IS Provoz ÚOOÚ	ÚOOÚ. Součástí projektu bude tvorba příslušných dokumentů, nakoupení potřebných technických prostředků a externích služeb pro složitější úlohy.					v ArchiRepu DČ
PZ5 – Obnovení HW IS ORG	Dlouhodobý projekt na obnovu HW IS ORG, kterému skončila podpora od výrobce.	V přípravě	OZI	Q3 2023	Q4 2028	Ne
PZ6 – Obnovení HW IS ÚOOÚ	Dlouhodobý projekt, který bude realizován pouze v případě, že se ukáže, že cloudové řešení není pro ÚOOÚ buď finančně nebo technicky realizovatelné.	V přípravě	INF	Q1 2024	Q4 2024	Ne
PZ7 - Vytvoření řešení pro správu a tvorbu formulářů	Vytvoření prostředí, ve kterém bude možné jednoduše vytvářet a spravovat formuláře. Součástí projektu bude návrh technického řešení.	V přípravě	INF	Q4 2023		Ne
PZ8 - Analýza přesunu provozu IS ORG na eGovernment Cloud	Výstupem projektu bude analýza hypotetického přesunu provozu IS ORG na cloudové řešení. Cílem je navrhnout konceptuální architekturu nového řešení a identifikovat rizika, hrozby a příležitosti.	V přípravě	OZI	Q3 2023	Q2 2024	NE
PZ9 – Nasazení	Projekt bude obsahovat analýzu	V přípravě	INF	Q1 2024	Q3 2024	

Kód a název záměru	Předmět záměru	Fáze záměru	Odpovědný útvar	Termín zahájení	Termín dokončení	DČ
nové technologie pro Service Desk	potřebnosti nového Service Desku, plán jeho případného nasazení a směr rozvoje.					

3 Návrh cílového stavu řízení ICT ÚOOÚ

3.1 Návrh způsobu řízení životního cyklu IS

Změny v řízení životního cyklu IS budou dvojího typu:

1) Založené na legislativě

Cílem IK ÚOOÚ je důsledněji a komplexněji dodržovat ustanovení VoDŘISVS, v jejím současném i již novelizovaném znění. Konkrétně je v plánu některá ustanovení vyhlášky vtělit do interních aktů řízení ÚOOÚ. Zároveň i procesy, které jsou již řízeny dle VoDŘISVS, mít podložené přesnější dokumentací. Sama IK ÚOOÚ a na ní založené procesy by měly napomoci větší evidenci změn a koncepčnějšímu řízení životního cyklu IS.

2) Organizačního charakteru

Řídící struktura vytvořená pro potřeby implementace cílů IK ÚOOÚ bude fungovat i v jednotlivých částech životního cyklu informačního systému. Řídící struktura bude definována metodikou projektového řízení, která vznikne v rámci projektu Z3 – Zavedení projektového řízení pro ICT projekty. ŘV ITA bude informován nejen o postupu v projektech implementujících IK ÚOOÚ, ale zároveň bude orgánem zodpovědným za schvalování větších změn informačních systémů a ukončování jejich provozu. Konkrétní úkoly výboru budou přesněji definovány během první fáze implementace IK ÚOOÚ.

Životním cyklem IS na ÚOOÚ se bude hlouběji zabývat PZ1 – Projekt na uvedení ICT do souladu s novelou VoDŘISVS, který definuje, jak budeme chápat na ÚOOÚ jednotlivé fáze a konkrétně uvede, ve které části probíhá jaké schvalování.

Obecným cílem je výraznější zapojení vedení ÚOOÚ do rozvoje i provozu IS.

3.2 Návrh způsobu řízení celkových schopností ICT útvaru

Zásadní změnou v řízení ICT architektury je vznik ŘV ITA. Ten bude suplovat roli hlavního IT architekta ÚOOÚ. Ředitel OIT bude místopředsedou a tajemníkem tohoto řídícího výboru.

Zásadní změnou ve strategickém plánování je vůbec vznik IK ÚOOÚ a na ní navázané metodiky projektového řízení. Do budoucna bude veškerý rozvoj IT vycházející z IK ÚOOÚ řízen projektově s reportingem vedení ÚOOÚ. Procesy budou standardizované, reporting pravidelný a jednání jednotlivých projektových týmů a řídících orgánů budou doplněna zápisem. Všechny toto projekty budou plnit strategické cíle schválené informační koncepcí.

Řízení změn bude nově obsahovat 2 procesy, jeden se bude týkat změn zásadních a druhý změn méně zásadních. Řízení změn bude definováno jak na úrovni projektů, tak na úrovni informačních systémů. Větší změny z obou úrovní se pak budou scházet u ŘV ITA. Změny budou přesněji definovány v rámci projektu PZ4 – Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ, který obsahuje konkrétní dokument, který dané změny bud popisovat.

Řízení rozvoje bude výrazně ovlivněno výše popsaným přechodem na strategické plánování a působností ŘV ITA. Řízení provozu pak bude zásadně změněno na základě výstupů projektu PZ1 - Projekt na uvedení ICT do souladu s novou VoDŘISVS. Vzniknou jednoznačné standardy vedení dokumentace. Druhou velkou změnu by pak měl přinést projekt PZ9 – Nasazení nové technologie pro Service Desk. Jeho cílem je zpřehlednit a zjednodušit pro uživatele hlášení závad na HW či SW, případně

požadavky na nový. Zároveň přechod na nové technologie přinese možnost standardizace některých procesů a větší přehled o využívaných službách a potřebách podpory.

Řízení rizik a bezpečnosti bude v rámci interního IT kompletně změněno výstupy projektu PZ4 – Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ. Zároveň proběhne revize statutu VKB a jeho rozdělení na 2 nezávislé entity, jednu týkající se IS ORG a jednu týkající se interního IT. Důvodem je snaha ÚOOÚ nedávat dodavatelům informace o systémech, které neprovozují.

3.3 Návrh způsobu spolupráce s ostatními útvary ÚOOÚ

Způsob spolupráce s ostatními útvary ÚOOÚ bude opět významně souviset se založením ŘV ITA a zavedením projektového řízení. V ŘV ITA bude zasedat kompletní výkonné vedení ÚOOÚ nebo jimi zvolení zástupci. Ostatní útvary by touto formou měly být informovány o postupu v jednotlivých projektech. Zároveň bude možné, aby ředitelé některých odborů byli i řediteli projektů, které se úzce dotýkají jejich působnosti. Nutností je pak nominace věcných gestorů do všech projektů, které nemají za cíl rozvíjet čistě fungování a řízení OIT. Všechny projekty zabývající se věcnou agendou ÚOOÚ budou mít věcného gestora z útvaru, v jehož gesci daná agenda je. Tato osoba pak bude definovat věcné zadání projektů.

3.4 Návrh způsobu spolupráce s centrálními autoritami v oblasti ICT a eGovernmentu

V této oblasti nejsou plánované žádné významnější změny. Zástupce ÚOOÚ se účastní plenárních zasedání RVIS, stejně tak některých pracovních skupin (např. pro architekturu a řízení ICT, či pracovních skupin týkajících se implementace zákona č. 12/2020 Sb., o právu na digitální služby). Plánujeme prozkoumat možnosti spolupráce se Státní pokladnou Centrem sdílených služeb v oblasti kybernetické bezpečnosti a provozování aplikací v cloudu.

4 Plán realizace změn ve způsobech řízení ICT

4.1 Plán projektů řízení ICT

Tabulka 19: Přehled všech běžících i plánovaných projektů

Kód projektu	Název projektu	Předmět projektu	Odpovědný útvar	Termín zahájení	Termín dokončení
PZ1	Projekt na uvedení ICT do souladu s novou VoDŘISVS	Vytvoření plánu prací pro naplnění požadavků novely vyhlášky č. 529/2006 Sb. Tento plán bude následně naplňován navazujícím projektem.	INF	Q3 2023	Q2 2024
PZ2	Vyhodnocení výhodnosti a náročnosti přechodu informačních systémů ÚOOÚ do cloudu	Vytvoření analýzy náročnosti a finanční výhodnosti přesunutí aplikací provozovaných na infrastruktuře ÚOOÚ do cloudové infrastruktury, včetně návrhu plánu případné migrace.	INF	Q3 2023	Q1 2024
PZ3	Maximalizace možností práce z domova	Vytvoření materiálu shrnujícího všechny prostředky, které mohou napomoci zaměstnancům ÚOOÚ pracovat ze svých domovů. Výstupem projektu bude návrh potřebných kroků a harmonogram jejich realizace.	INF	Q1 2024	Q4 2024
PZ4	Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ	Aktualizace dokumentace týkající se kybernetické bezpečnosti IS Provoz ÚOOÚ. Součástí projektu bude tvorba příslušných dokumentů, nakoupení potřebných technických prostředků a externích služeb pro složitější úlohy.	INF	Q3 2023	Q1 2024

Kód projektu	Název projektu	Předmět projektu	Odpovědný útvar	Termín zahájení	Termín dokončení
PZ5	Obnovení HW IS ORG	Dlouhodobý projekt na obnovu HW IS ORG, kterému skončila podpora od výrobce.	OZI	Q3 2023	Q4 2028
PZ6	Obnovení HW IS ÚOOÚ	Dlouhodobý projekt, který bude realizován pouze v případě, že se ukáže, že cloudové řešení není pro ÚOOÚ buď finančně nebo technicky realizovatelné.	INF	Q1 2024	Q4 2028
PZ7	Vytvoření řešení pro správu a tvorbu formulářů	Vytvoření prostředí, ve kterém bude možné jednoduše vytvářet a spravovat formuláře. Součástí projektu bude návrh technického řešení.	INF	Q4 2023	Q4 2024
PZ8	Analýza přesunu provozu IS ORG na eGovernment Cloud	Výstupem projektu bude analýza hypotetického přesunu provozu IS ORG na cloudové řešení. Cílem je navrhnout konceptuální architekturu nového řešení a identifikovat rizika, hrozby a příležitosti.	OZI	Q3 2023	Q2 2024
PZ9	Nasazení nové technologie pro Service Desk	Projekt bude obsahovat analýzu potřebnosti nového Service Desku, plán jeho případného nasazení a směr rozvoje.	INF	Q1 2024	Q3 2024

4.2 Plán řízení kvality IS – Činnosti v oblasti řízení kvality

Plán řízení kvality bude definován v rámci projektu PZ1 - Projekt na uvedení ICT do souladu s novou VoDŘISVS.

4.3 Plán řízení bezpečnosti IS – Činnosti v oblasti řízení bezpečnosti

Bude dodefinováno v rámci projektu PZ4 - Zajištění kybernetické bezpečnosti IS Provoz ÚOOÚ. Bude se jednat primárně o aktualizaci dokumentace a nasazení nového Firewallu s novým Log managerem. Je v plánu prozkoumat cestu šifrování dat uložených v cloudu za využití klíčů vytvořených uvnitř vlastního HSM modulu v infrastruktuře ÚOOÚ.

4.4 Způsob financování projektů s dopadem do řízení ICT

Tabulka 20: Plán přímých investičních nákladů na projekty

Rok	Investiční výdaje (Kč)	Zdroje financování
2023		
2024	0	
2025	20 000 000 Kč	Státní rozpočet
2026	20 000 000 Kč	Státní rozpočet/evropské fondy
2027	10 000 000 Kč	Státní rozpočet
2028		

ČÁST C: ŘÍZENÍ DOKUMENTU IK ÚOOÚ A JEHO NAPLŇOVÁNÍ

1 NAPLŇOVÁNÍ IK ÚOOÚ

1.1 Vyhodnocování dodržování IK ÚOOÚ

Pro vyhodnocování dodržování IK ÚOOÚ bude sloužit ŘV ITA. Tento orgán bude zřízen schválením IK ÚOOÚ a bude složen ze zástupců všech nejdůležitějších věcných sekcí ÚOOÚ, manažera kybernetické bezpečnosti a části vedení ÚOOÚ. ŘV ITA bude dávat předsedovi ÚOOÚ doporučení pro přijetí jistých kroků a bude vrcholným orgánem pro řízení projektů naplňujících IK ÚOOÚ. Vedle toho bude orgán fungovat jako schvalovací útvar pro řízení větších změn v architektuře ÚOOÚ či v samotné Informační koncepci.

Členy ŘV ITA budou následující role v rámci ÚOOÚ: místopředsedové ÚOOÚ, případně jejich zástupci, ředitelka kanceláře předsedy ÚOOÚ, ředitel OIT, ředitel odboru legislativy a metodiky, ředitel OIT, manažer kybernetické bezpečnosti, pověřenec pro ochranu osobních údajů.

ŘV ITA funguje jako poradní orgán předsedy ÚOOÚ. V případě větších neshod rozhoduje předseda ÚOOÚ. Stejně tak předseda ÚOOÚ schvaluje všechny větší změny v IK ÚOOÚ.

1.1.1 Postupy při vyhodnocování dodržování IK ÚOOÚ

Vyhodnocování bude probíhat 2x ročně.

První vyhodnocení bude tzv. průběžné, jeho účelem bude reportovat vedení sekce kanceláře předsedy ÚOOÚ pokrok v řízení implementace IK ÚOOÚ. Zároveň bude vyhodnocován postup v naplňování cílů pro daný kalendářní rok a případné změny v plánovaných aktivitách pro druhé pololetí. Průběžné vyhodnocování naplňování IK ÚOOÚ bude probíhat vždy v červnu daného kalendářního roku.

Druhé a důležitější vyhodnocení bude tzv. závěrečné. V rámci tohoto vyhodnocení předloží gestor IK ÚOOÚ (ředitel OIT) prezentaci shrnující plnění cílů IK ÚOOÚ pro daný kalendářní rok a odprezentuje ji ŘV ITA. Zároveň dostane každý člen prostor pro návrh změn v IK ÚOOÚ na základě předloženého vyhodnocení.

1.1.2 Oblasti pro vyhodnocování IK ÚOOÚ

V rámci vyhodnocování IK ÚOOÚ bude ředitel OIT předkládat primárně následující témata:

- zda je kompletně a aktuálně zachycen veškerý obsah požadovaný vzorovou osnovou IK OVM publikovanou OHA a (připravovanou) VoDŘISVS,
- zda jsou informace v IK ÚOOÚ v souladu s aktuálním obsahem IK ČR a jejích následných dokumentů,
- zda jsou informace uvedené v IK ÚOOÚ použity srozumitelně a průkazně k rozhodování o identifikovaných potřebách a o jejich pokrytí plánovanými záměry,
- zda jsou informace v IK ÚOOÚ v souladu s centrálními evidencemi, zejména agend, ISVS, služeb, údajů a dalších, a zda jsou aktuální,

- zda jsou plánované záměry na projekty realizovány ve stanoveném čase a rozsahu,
- zda všechny projekty informatizace a digitální transformace realizované v rámci ÚOOÚ skutečně legitimně vyplývají z analýzy a syntézy v IK ÚOOÚ a jsou i ve shodě s evidencí záměrů Digitálního Česka,
- zda jsou z IK ÚOOÚ a z následných dokumentů IK ČR implementovány do interních aktů řízení ÚOOÚ a do jeho praxe všechny zásady, postupy a organizační opatření z oblasti řízení informatiky a jednotlivých ISVS,
- zda realizované záměry a přijatá opatření přinesla předpokládaný účinek,
- zda dříve zjištěné nedostatky byly odstraněny nebo se k jejich odstranění směřuje.

1.1.3 Pravidla pro vytváření zápisu z vyhodnocování IK ÚOOÚ

Z vyhodnocování bude vytvořen zápis. Za jeho vyhotovení odpovídá zaměstnanec ÚOOÚ, který řídí vyhodnocování.

1.1.3.1 Rozsah zápisu z vyhodnocování

Zápis z vyhodnocování bude identifikovat verzi IK ÚOOÚ, které se týká, a dále pak bude jednoznačně identifikován pořadovým číslem zápisu. Zápis bude obsahovat následující části:

- identifikační údaje zápisu (verze IK ÚOOÚ, datum počátku platnosti vyhodnocované IK ÚOOÚ, pořadové číslo zápisu);
- identifikace všech zaměstnanců, kteří vyhodnocení prováděli, a jejich role (jméno, resp. jména, příjmení, útvar nebo externí organizace, funkce);
- záznam o průběhu vyhodnocování ve formě prezentace;
- poznatky a závěry z vyhodnocování (soupis zjištěných nedostatků, kladná hodnocení);
- soupis přijatých opatření (návaznost na zjištěný nedostatek, obsah opatření, způsob realizace);
- schválení zápisu z vyhodnocení (kdo - jméno, resp. jména, příjmení, útvar nebo externí organizace, funkce a kdy zápis schválil).

1.1.3.2 Postup vyhotovení zápisu z vyhodnocování

K zápisu se po úvodních identifikačních údajích nejprve zapisuje záznam o průběhu vyhodnocení a poznatky a závěry z něj. Zápis schvaluje ŘV ITA. Schválený zápis se zpřístupní členům ŘV ITA a je předán k informaci předsedovi ÚOOÚ.

V dalším kroku ředitel OIT zajistí ve spolupráci s příslušnými odbornými útvary zpracování návrhu vhodných opatření, jejichž přijetí povede k odstranění zjištěných nedostatků, pokud byly nějaké nalezeny. Návrh spolu se schváleným zápisem bude předložen ke schválení ŘV ITA, a následně předsedovi ÚOOÚ. Opatření s vlivem na obsah IK ÚOOÚ se promítnou v nejbližší řádné aktualizaci koncepce. Harmonogram její aktualizace bude součástí referátníku před schválením.

1.2 Postupy při provádění změn IK ÚOOÚ

Provádění změn v IK ÚOOÚ bude probíhat pravidelně 1x ročně během aktualizace IK ÚOOÚ, vždy po vyhodnocení za daný kalendářní rok.

Jiné změny v průběhu roku budou možné jen na základě dobře odůvodněné výjimky a po schválení ŘV ITA a předsedou ÚOOÚ. Tento postup bude ale využíván pouze minimálně, jedním z hlavních účelů existence IK ÚOOÚ a předpokladem strategického řízení pomocí IK ÚOOÚ je zajistit kontinuitu a stabilitu rozvoje ICT ÚOOÚ. Není proto žádoucí, aby byly změny prováděny příliš často a mimo určené období změn.

Změny IK ÚOOÚ budou součástí kompletního řešení řízení změn v rámci ÚOOÚ.

1.2.1 Postup pro zajištění včasné změny IK ÚOOÚ

Pro zajištění včasné aktualizace IK ÚOOÚ bude prováděna její revize 1x ročně, a to tak, aby byla v souladu s aktuálními požadavky ÚOOÚ, platnými strategiemi a požadavky příslušných právních předpisů. V případě zjištění potřeby promítnutí těchto změn do IK ÚOOÚ bude vydána její nová verze.

Událostmi, které povedou k nutnosti aktualizace IK ÚOOÚ i mimo stanovenou periodu, jsou zejména:

- významná změna organizační struktury ÚOOÚ, při které dojde ke změnám odpovědností vztahujících se k IS,
- významná změna procesů, ve kterých je užíván IS,
- vznik nového záměru na pořízení nebo vytvoření nové části IS,
- dokončení části IS (uvedení části IS do produktivního provozu), jejíž pořízení nebo vytvoření bylo zahájeno v předcházejícím nebo stávajícím období,
- ukončení provozu části IS,
- významné změny v právních předpisech,
- nové podstatné požadavky na podporu výkonu veřejné správy ÚOOÚ službami jeho informačních systémů.

V této souvislosti musí vedoucí zaměstnanci všech organizačních jednotek, které užívají IS, jsou věcnými garanty nějaké části IS, respektive odpovídají za správu nějaké části IS, hlásit výše uvedené změny zaměstnanci odpovědnému za přípravu změn a tvorbu nových verzí IK ÚOOÚ. Tento zaměstnanec je též povinen sledovat další výše uvedené změny a jejich dopad na Informační koncepci.

1.2.2 Postup zápisu změny do dokumentu IK ÚOOÚ

Změny IK ÚOOÚ budou prováděny formou vydání nové verze. Jednotlivé verze budou číslovány dvěma čísly, oddělenými tečkou:

- hlavní číslo verze, které bude odlišovat verze s významnými změnami (například kompletně přepracované kapitoly, změny zásadních postupů a podobně);
- vedlejší číslo verze, které bude odlišovat drobnější změny (například doplnění nového informačního systému, změny v personální oblasti, drobná změna v postupech).

Každá verze bude obsahovat tabulku změn oproti verzi předchozí. V této tabulce budou pro každou změnu stručně uvedeny následující informace:

- popis provedené změny;
- odůvodnění změny;
- identifikace místa (příp. více míst) dokumentu (minimálně číslem kapitoly), kterého se změna dotkla.

1.2.3 Postup přípravy nové IK ÚOOÚ

Zaměstnanec odpovědný za naplnění IK ÚOOÚ společně se zaměstnancem odpovědným za aktualizaci IK ÚOOÚ připraví 6 měsíců před ukončením její pětileté platnosti podklady pro strategické rozhodnutí vedení odboru ICT ohledně přípravy nové IK ÚOOÚ. Tyto podklady budou obsahovat:

- vyhodnocení stávající IK ÚOOÚ a její účinnosti (míru naplnění cílů, záměrů a opatření) za dobu od jejího vzniku,
- vyhodnocení způsobu vzniku a údržby stávající IK ÚOOÚ a doporučení pro postup tvorby nové IK ÚOOÚ (vlastními silami nebo s využitím externího dodavatele apod.),
- další podklady dle uvážení.

2 ODPOVĚDNOSTI ZA UPLATŇOVÁNÍ IK ÚOOÚ

Stanovení principiálních odpovědností v oblasti dlouhodobého řízení informačních systémů je nedílnou součástí IK ÚOOÚ.

Tyto odpovědnosti musí být implementovány do praxe Organizačním řádem a dalšími interními akty řízení. To platí o to více, že některé potřebné útvary a v nich požadované kompetence nebyly zatím v organizační struktuře ustaveny a nemůže po nich být odpovědnost reálně požadována.

Odpovědnosti související s IK ÚOOÚ lze rozdělit do tří částí, a to na stanovení odpovědností za:

- úkony v životním cyklu tvorby a údržby IK ÚOOÚ,
- realizaci záměrů a opatření z IK ÚOOÚ,
- splnění zákonných povinností spojených s dlouhodobým řízením ISVS.

2.1 Odpovědnosti za životní cyklus dokumentu IK ÚOOÚ

Životní cyklus IK ÚOOÚ je charakterizován těmito hlavními procesy a odpovědnostmi.

Tabulka 21: Odpovědnosti za životní cyklus dokumentu IK ÚOOÚ

Proces	Náplň	Odpovědnost
Tvorba IK ÚOOÚ	zahrnuje počáteční naplnění obsahu IK ÚOOÚ v souladu s § 2 VoDŘISVS, a současně v souladu s Informační koncepcí ČR a jejími následnými dokumenty, zejména NAP a MŘICT. Dále zahrnuje tvorbu nové IK MV ČR po uplynutí doby platnosti nebo při radikální změně ministerstva.	Ředitel OIT ve spolupráci se členy ŘV ITA.
Schvalování IK ÚOOÚ	probíhá v souladu s § 6 VoDŘISVS, koncepci schvaluje ministr vnitra. Schvalování se provádí pro každou verzi IK ÚOOÚ.	ŘV ITA a předseda ÚOOÚ.
Realizace IK ÚOOÚ	Realizace naplánovaných záměrů projektovým způsobem a přijatých opatření liniovým způsobem řízení. Vzhledem k rozsahu jsou tyto klíčové odpovědnosti upraveny samostatnou kapitolou níže.	Ředitel OIT ve spolupráci se členy ŘV ITA.
Změna IK ÚOOÚ (též aktualizace IK ÚOOÚ)	Provádí se v závislosti na změnách strategické motivace Úřadu, na změnách skutečného stavu informačních systémů a v souladu s aktuálními požadavky správců ISVS, za účelem aktualizace záměrů a plánování zdrojů.	Ředitel OIT po schválení ŘV ITA nebo předsedy ÚOOÚ.
Vyhodnocování dodržování IK ÚOOÚ	V souladu s § 7 VoDŘISVS, vytváří zpětnou vazbu, která podporuje naplnění cílů definovaných v koncepci.	ŘV ITA.

2.2 Odpovědnost za realizaci IK ÚOOÚ

Odpovědnost za naplnění IK ÚOOÚ patří OIT. Dílčí odpovědnosti v rámci jednotlivých oblastí IK ÚOOÚ však náleží i dalším útvarům, které jsou uvedené v následující tabulce.

Tabulka 22: Odpovědnosti za realizaci IK ÚOOÚ

Oblast	Odpovědnost	Četnost
identifikace změněných potřeb na služby ISVS	Věcní gestoři ISVS	při každém požadavku na pořízení nového ISVS
aktualizace modelů architektury ÚOOÚ	OIT	průběžně
schvalování záměrů na pořízení nových ISVS a rozvoji stávajících ISVS	ŘV ITA	při každém požadavku na pořízení nového ISVS nebo rozvoj stávajícího ISVS
řízení kvality ISVS	OIT	průběžně
řízení bezpečnosti ISVS	MKB	průběžně
příprava Plánu rozvoje ISVS v IK ÚOOÚ	Věcní gestoři ISVS	průběžně
schválení Plánu rozvoje ISVS	ŘV ITA	v rámci procesu přípravy nové verze IK ÚOOÚ
zajištění provozu a údržby ISVS	OIT	průběžně, resp. při změně informačního systému
zadávání, koordinace a vyhodnocování poskytovaných služeb ISVS při jeho pořízení a změnách	OIT	při pořízení a změně informačního systému
řízení ukončování provozu ISVS	OIT	při ukončení činností části informačního systému
vytváření a údržba plánu financování ISVS	OIT	min. 1x ročně - probíhá v rámci procesu přípravy rozpočtu
schvalování plánu financování ISVS	OPE	min. 1x ročně - probíhá v rámci procesu přípravy rozpočtu

2.3 Splnění zákonných povinností

Odpovědnost za splnění komplexních zákonných povinností byla stanovena předsedovi ÚOOÚ. Vybrané dílčí odpovědnosti za splnění konkrétních zákonných povinností jsou uvedeny v následující tabulce.

Tabulka 23:Odpovědnosti za plnění zákonných povinností

Zákon	Oblast	Odpovědnost
zákon č. 365/2000 Sb., ve znění pozdějších	spolupracovat s ministerstvem při plnění jeho úkolů podle § 4	OIT

předpisů, § 5, odst. 2 písm. a)		
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5, odst. 2 písm. b)	předložit odboru Hlavního architekta eGovernmentu k vyjádření návrhy dokumentací programů obsahujících pořízení nebo technické zhodnocení tzv. určených informačních systémů veřejné správy	OIT
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5, odst. 2 písm. c)	předložit odboru Hlavního architekta eGovernmentu k posouzení provozní dokumentaci tzv. určených informačních systémů veřejné správy před zahájením poskytování služby informačního systému	OIT
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5, odst. 2 písm. d)	zajistit, aby vazby jimi spravovaného informačního systému veřejné správy nebo provozního informačního systému uvedeného v § 1 odst. 4 písm. a) až d) na informační systémy veřejné správy jiného správce byly uskutečňovány prostřednictvím referenčního rozhraní	OIT
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5, odst. 2 písm. e)	odstranit zjištěné nedostatky ve lhůtě stanovené ministerstvem	OIT
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5a, odst. 2)	vytvářet a vydávat informační koncepci orgánu veřejné správy, uplatňovat ji v praxi a vyhodnocovat její dodržování	OIT ve spolupráci s ŘV ITA
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5a, odst. 3)	vytvářet a vydávat provozní dokumentaci k jednotlivým informačním systémům veřejné správy	OIT
	uplatňovat provozní dokumentaci v praxi a vyhodnocovat její dodržování	OIT
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5a, odst. 4)	zajistit atestaci dlouhodobého řízení informačních systémů veřejné správy s výjimkou provozních informačních systémů	ŘV ITA
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5b	uplatňovat opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy	MKB
zákon č. 365/2000 Sb., ve znění pozdějších předpisů, § 5a	uvést informační koncepci Ministerstva vnitra do souladu s informační koncepcí České republiky podle § 5a odst. 1 zákona č. 365/2000 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, do 24 měsíců ode dne jejího schválení vládou	OIT

ČÁST D: Dodatky a přílohy IK ÚOOÚ

1. Dodatky

1.1. Základní pojmy a zkratky

Tabulka 24: Základní pojmy a zkratky

Pojem / Zkratka	Význam
ÚOOÚ	Úřad pro ochranu osobních údajů
IK ÚOOÚ	Informační koncepce ÚOOÚ
ŘV ITA	Řídící výbor pro IT architekturu ÚOOÚ
VKB	Výbor pro kybernetickou bezpečnost ÚOOÚ
KB	Kybernetická bezpečnost
eGovernment Cloud	Sdílené cloudové služby eGovernmentu
AIS	Agendový informační systém – ISVS, který slouží k výkonu agendy orgánu veřejné moci
ICT ÚOOÚ	Veškeré informační a komunikační technologie používané v rámci ÚOOÚ
IS ORG	Uzavřený a organizačně oddělený kritický informační systém, který jako součást systému základních registrů slouží jako převodník identifikátorů
IS ÚOOÚ	IS, který je aktuálně ohlášen v RPP, nicméně bude se ohlašovat IS Provoz ÚOOÚ
IS Provoz ÚOOÚ	IS zajišťující výkon provozních agend ÚOOÚ, který se bude nově ohlašovat do RPP (bude obsahovat účetní systém, HR systém, spisovou službu, e-mailového klienta)
ZIFO	Zdrojový identifikátor fyzické osoby
AIFO	Agendový identifikátor fyzické osoby
GDPR	Obecné nařízení o ochraně osobních údajů - viz Seznam literatury
VoDŘISVS	Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy
VoKB	Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

1.2. Seznam modelů, schémat, obrázků

1.3. Seznam tabulek

1.4. Seznam literatury

IK ÚOOÚ je v souladu a respektuje především následující dokumenty:

- nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27/04/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů - GDPR);
- 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 (eIDAS);
- směrnici Evropského parlamentu a Rady (EU) 2016/2102 ze dne 26. října 2016 o přístupnosti internetových stránek a mobilních aplikací subjektů veřejného sektoru;
- směrnici Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009, o právní ochraně počítačových programů;
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů;
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů;
- zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů;
- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ve znění pozdějších předpisů.
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů;
- zákon č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů;
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů;
- vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy;
- vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS;

- vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti);
- vyhlášku č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů;
- nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury;
- usnesení vlády České republiky č. 139/2018 k 5. aktualizaci Seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu;
- usnesení vlády České republiky ze dne 3. října 2018 č. 629;
- usnesení vlády České republiky ze dne 2. listopadu 2015 č. 889k dalšímu rozvoji informačních a komunikačních služeb veřejné správy ve znění pozdějších změn;
- usnesení vlády ČR ze dne 20. 06. 2001 č. 624, o Pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů;
- usnesení vlády České republiky ze dne 15. června 2020 č. 644, kterým se schvalují implementační plány a novely dokumentů Digitálního Česka.

IK ÚOOÚ je v souladu a respektuje především následující interní akty řízení:

- směrnice č. 13/2022, organizační řád;
- směrnice č. 12/2019, o informačních a komunikačních technologiích;
- směrnice č. 10/2019, o systému řízení bezpečnosti informací;
- směrnice č. 8/2019, o výboru pro řízení kybernetické bezpečnosti.