

Metodika Digital First – FULL

Přílohy A–E (kontrolní seznamy, šablony, slovník pojmů, legislativa a zdroje, přehled zkratk) jsou vydávány jako samostatné dokumenty k této metodice.

Metodika pro orgány veřejné moci

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Reg. č.: CZ.31.5.0/0.0/0.0/23_106/0008503

Obsah

1 Jak tuto metodiku používat.....	5
Vymezení digitální služby, působnost a závaznost metodiky.....	5
Co je digitální služba (podle ZoPDS)	5
Pro koho je metodika určena	5
Kdy je metodika doporučena a kdy se stává závaznou.....	5
Vazba na zákon č. 365/2000 Sb. a na procesy OHA	5
Konvence „MUSÍ“ a „NESMÍ“ v této metodice	6
Kam ukládat výstupy metodiky (sběrné místo)	6
Správa a publikace metodiky	6
1.1 Jaké rozhodnutí kapitola podporuje.....	6
1.2 Výstupy / důkazy.....	6
1.3 Hlavní obsah kapitoly.....	7
1.3.1 Jak s metodikou pracovat v každodenní praxi (pravidla používání)	7
1.3.2 Rozhraní "řízení digitální služby" a "řízení ICT projektu"	7
1.3.3 Kontrolní brány – minimální pravidla STOP/GO	7
1.3.4 Evidence pack – doporučená struktura (minimální standard)	8
1.3.5 Pravidla práce s dodavatelem (aby nevznikl „dodavatelský stát“).....	8
2 Co je digitální služba	9
2.1 Jaké rozhodnutí kapitola podporuje.....	9
2.2 Výstupy / důkazy.....	9
2.3 Hlavní obsah kapitoly.....	10
2.3.1 Praktická definice digitální služby	10
2.3.2 Jak správně vymezit hranici služby (end-to-end scope).....	10
2.3.3 Minimální obsah karty digitální služby (doporučené položky)	11
2.3.4 Minimální sada metrik služby (bez ohledu na velikost projektu).....	11
2.3.5 Vazba služby na Katalog služeb veřejné správy	12
2.3.6 Zasazení služby do životní situace nebo události.....	12
2.3.7 Kanálová neutralita a princip „only once“	12
2.3.8 Elektronické zastupování	12
2.3.9 AI asistenti a agenti v návrhu služby.....	12
3 Rozhodnutí před zahájením	12
3.1 Jaké rozhodnutí kapitola podporuje.....	12
3.2 Výstupy / důkazy.....	13
3.3 Hlavní obsah kapitoly.....	14
3.3.1 Rozhodovací mapa před zahájením (co musí být rozhodnuto a kým)	14
3.3.1 Pravidla „NESMÍ SE ZAČÍT“ (No-go pravidla)	14

4 Právo jako konstrukční prvek	15
4.1 Jaké rozhodnutí kapitola podporuje	15
4.2 Výstupy / důkazy	15
4.3 Hlavní obsah kapitoly	16
4.3.1 Postup: přeložení práva do návrhu služby (Legal-to-Design workflow)	16
4.3.2 Typy právních požadavků a jejich dopady (praktická mapa)	17
4.3.3 Checklist „právní no-go“ (kdy je povinné STOP)	17
4.3.4 Co by mělo být smluvně zajištěno kvůli právní obhajitelnosti	17
5 Proces a data	18
5.1 Jaké rozhodnutí kapitola podporuje	18
5.2 Výstupy / důkazy	18
5.3 Hlavní obsah kapitoly	19
5.3.1 Datová inventura a vlastnictví dat (minimální rozhodnutí)	19
5.3.2 Rozhodnutí o „pravdě“ (autoritě) a řešení konfliktů dat	20
5.3.3 Interoperabilita a integrace (koncept – minimum pro zadání)	20
5.3.4 Kvalita dat a validace (minimální standard pro provoz)	20
5.3.5 Migrace dat a přechod (cutover) – doporučené minimum, pokud se migruje	20
5.3.6 Dohledatelnost a důkazy (audit trail) – minimum pro obhajitelnost	21
6 UX, obsah a přístupnost	21
6.1 Jaké rozhodnutí kapitola podporuje	21
6.2 Výstupy / důkazy	22
6.3 Hlavní obsah kapitoly	23
6.3.1 Mapa uživatelské cesty (service journey) – doporučený standard	23
6.3.2 Přístupnost – doporučený standard a důkazy	23
7 Architektura, bezpečnost, provoz	24
7.1 Jaké rozhodnutí kapitola podporuje	24
7.2 Výstupy / důkazy	24
7.3 Hlavní obsah kapitoly	26
7.3.1 Architektura služby (L0) – doporučený obsah a rozhodnutí	26
7.3.2 Bezpečnostní baseline – doporučené minimum (bez ohledu na dodavatele)	26
7.3.3 Identity a řízení přístupů (IAM) – minimum pro veřejnou službu	26
8 Kontrolní brány a rozhodování	27
8.1 Jaké rozhodnutí kapitola podporuje	27
8.2 Výstupy / důkazy	27
8.3 Hlavní obsah kapitoly	28
8.3.1 Model bran Digital First	28
Souhlas statutárního zástupce před spuštěním služby (součást brány DF-3)	29

8.3.2 STOP trigger a pravidla pro „GO s podmínkami“	29
9 Go-live	30
9.1 Jaké rozhodnutí kapitola podporuje	30
9.2 Výstupy / důkazy	30
9.3 Hlavní obsah kapitoly	32
9.3.1 Strategie spuštění (rollout) – povinné volby	32
9.3.2 Go-live checklist – minimum před/po spuštění	32
9.3.3 Komunikace a připravenost kanálů (včetně přepážek)	32
9.3.4 Evidence go-live a dohledatelnost (audit)	33
10 Řízení služby po spuštění	33
10.1 Jaké rozhodnutí kapitola podporuje	33
10.2 Výstupy / důkazy	33
10.3 Hlavní obsah kapitoly	34
10.3.1 Řízení incidentů a problémů (incident/problem management)	34
10.3.2 Řízení změn po spuštění (change management)	35
10.3.4 Bezpečnost v provozu (security operations) – minimální standard	35
10.3.3 Řízení kvality služby (KPI/SLO) – minimální dashboard	36
10.3.4 Udržení přístupnosti po spuštění (kontinuální)	36
10.3.5 Řízení právních a policy změn po spuštění	36
10.3.6 Kontrola dodavatelské závislosti a znalostní udržitelnost	37
11 Nejčastější selhání digitalizace	37
11.1 Jaké rozhodnutí kapitola podporuje	37
11.2 Výstupy / důkazy	37
11.3 Hlavní obsah kapitoly	38
11.3.1 Katalog selhání (antipatterns) – signály, dopady, prevence	38
11.3.3 Včasné signály selhání (early warning) – co sledovat	40
11.3.4 Minimální zásahy (co udělat, když se selhání objeví)	40
11.3.5 Nejčastější „dokumentové“ a governance selhání (co by nemělo projít)	41
12 Přílohy metodického balíčku (A–E)	41
12.1 Doplnkové materiály – zahraniční praxe a příklady z ČR	41
12.1.1 Zahraniční praxe – co převzít a jak to použít	41
12.1.2 Mapovací tabulka (inspirace → konkrétní doplnění)	41
12.1.3 Příklad z praxe v ČR: eRecept (přenositelné principy)	42
12.2 Zdroje (zahraniční standardy – odkazy)	42
13 Vize rozvoje ZoPDS po 1. 2. 2027	43
13.1 Průřezová kontrolní matice ZoPDS / OHA / ISDŘ / AI	43

1 Jak tuto metodiku používat

Rychlý start pro čtenáře

První rozhodnutí: určete, zda řešíte digitální službu, změnu existující služby nebo pouze podpůrný ICT prvek. Pokud nejde prokazatelně o jednoduchou změnu s nízkým rizikem, použije se úplnější režim řízení.

Druhé rozhodnutí: založte evidenci služby a master index důkazů. Každý checklist, rozhodnutí, gate pack a příloha má mít odkaz na konkrétní důkaz a odpovědnou osobu.

Třetí rozhodnutí: ověřte vazbu na ZoPDS, Katalog služeb VS, OHA/ISVS procesy, data, kanály, elektronické zastupování a případné použití AI asistentů nebo agentů.

Pravidlo interpretace

Metodika je doporučující metodický rámec DIA. Výrazy jako „mělo by“, „doporučuje se“ nebo „standard“ popisují metodickou dobrou praxi. Závaznost vzniká pouze tam, kde ji stanoví právní předpis, interní akt řízení, podmínky financování, schvalovací proces OHA/ISVS, smlouva nebo rozhodnutí odpovědného gestora.

Pokud text používá silnější výraz typu „musí“ nebo „nesmí“, vykládá se podle kontextu: buď jako přímá právní povinnost, nebo jako podmínka dané kontrolní brány/metodického režimu. Právní povinnost musí být dohledatelná v příslušném právním nebo procesním titulu.

Vymezení digitální služby, působnost a závaznost metodiky

Co je digitální služba (podle ZoPDS)

Digitální službou se v této metodice rozumí digitální služba podle zákona č. 12/2020 Sb., o právu na digitální služby (ZoPDS). Jde o úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agentury, který je veden v katalogu služeb jako úkon v elektronické podobě; za digitální službu se považuje i úkon vykonávaný vůči uživateli služby kontaktním místem veřejné správy v rámci agentury.

Metodika se vztahuje k digitálním službám veřejné správy, nikoli obecně ke každému ICT projektu. ICT projekt je v této metodice chápán jako prostředek k vytvoření, změně nebo provozu digitální služby, nikoli jako samostatný cíl.

Digitální služba se v metodice vždy posuzuje ve vzájemné vazbě těchto prvků: agenda, v jejímž rámci je úkon vykonáván; konkrétní úkon (digitální úkon uživatele a navazující úkon OVM); katalogový záznam služby v Katalogu služeb veřejné správy; a obslužný kanál, jímž je služba poskytována. Tato vazba zajišťuje, že se nedigitalizuje izolovaný formulář, ale služba ukotvená v právním a evidenčním kontextu.

Pro koho je metodika určena

Metodika je určena orgánům veřejné moci, které připravují, realizují nebo provozují digitální službu, a jejich útvarům a dodavatelům podílejícím se na návrhu a provozu služby (gestor služby, vlastník služby, projektové řízení, architektura, bezpečnost, právní útvar, provoz).

Okruh adresátů (povinných subjektů) se pro konkrétní službu odvozuje z působnosti příslušného právního předpisu a z agend, do nichž služba spadá. Metodika netvrdí, že všechny subjekty veřejné správy spadají automaticky do stejného režimu.

Kdy je metodika doporučena a kdy se stává závaznou

Metodika je primárně doporučeným rámcem dobré praxe. Pro konkrétní službu se může stát závaznou na základě jednoho nebo více z následujících titulů:

Tam, kde metodika hovoří o závaznosti, je třeba vždy doplnit konkrétní právní nebo procesní základ. Metodika není obecně závazná bez uvedení takového základu.

Vazba na zákon č. 365/2000 Sb. a na procesy OHA

Metodika navazuje na zákon č. 365/2000 Sb., o informačních systémech veřejné správy, a na procesy posuzování ICT záměrů a vydávání stanovisek OHA. Výstupy metodiky (karty, kontrolní seznamy, rozhodnutí, evidence) mají sloužit jako podklad pro tyto procesy, nikoli jako paralelní dokumentace.

Před zahájením realizace se ICT záměr předkládá ke schválení v procesu OHA prostřednictvím příslušného formuláře / příslušného typu žádosti podle aktuálních pravidel OHA (archi.gov.cz). Před uvedením služby do provozu se ověřuje připravenost služby; metodika k tomu poskytuje strukturované podklady (viz kontrolní brány DF).

Kontrolní brány a požadavky metodiky jsou procesním (schvalovacím) mechanismem zajišťujícím obhajitelnost a kvalitu rozhodnutí; nejde o samoučelnou administrativu.

Konvence „MUSÍ“ a „NESMÍ“ v této metodice

Pojmy „MUSÍ“ a „NESMÍ“ označují metodický požadavek nebo pravidlo kontrolní brány v rámci této metodiky; samy o sobě neznamenají přímou právní povinnost. Tam, kde požadavek vyplývá přímo z právního předpisu, je u něj uveden konkrétní právní základ. V ostatních případech jde o doporučený standard, jehož závaznost se odvozuje podle titulů uvedených výše.

Kam ukládat výstupy metodiky (sběrné místo)

Výstupy metodiky nemají končit jako samostatné dokumenty bez dalšího využití. Vyplněné karty, kontrolní seznamy, rozhodnutí, evidence, datové inventury a další artefakty se ukládají do strukturovaného a verzovaného sběrného místa — preferovaně do ISDŘ, případně do jiného strukturovaného a verzovaného prostředí určeného OVM.

Výstupy mají být datově zpracovatelné, verzované, vyhodnotitelné, opakovaně použitelné a navázané na konkrétní službu, agendu, systém a obslužný kanál.

Je-li to relevantní, výstupy se propojují s Registrem práv a povinností (RPP), s Katalogem služeb veřejné správy a s ohlašování agend tak, aby evidence služby odpovídala jejímu právnímu a agendovému ukotvení.

Správa a publikace metodiky

Pouhé zveřejnění dokumentu a příloh na webu není cílovým stavem. Dokument má být publikačním výstupem ze strukturovaného, verzovaného a zpracovatelného obsahu.

Obsah metodiky lze spravovat v ISDŘ, ve wiki, v prostředí Archi.gov nebo v jiném vhodném strukturovaném prostředí tak, aby bylo možné metodiku aktualizovat, verzovat a opakovaně využívat její jednotlivé části.

1.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl nejpozději před schválením projektového záměru formálně rozhodnout a doložit, že:

- MĚLO BY je zřízen a průběžně udržován evidence pack (složka důkazů) a decision log (rozhodovací stopa),
- MĚLO BY jsou nastaveny kontrolní brány a pravidla STOP/GO (zastavení a pokračování),
- MĚLO BY je určena odpovědnost za digitální službu (řízení služby) a současně je řízení dodávky vedeno dle Metodiky řízení ICT projektů (řízení projektu).

1.2 Výstupy / důkazy

TABULKA 1 – Výstupy / důkazy

Název výstupu	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Kde se vede
Rozhodnutí o závazném použití metodiky Digital First	Záznam rozhodnutí, rozsah (na jakou službu), datum, schvalovatel	Nositel projektu / Řídící výbor projektu	Nejpozději při přípravě podkladů ke schválení projektového záměru	Repository projektu + spisová služba (pokud relevantní)
Plán aplikace metodiky (1–2 strany)	Seznam kontrolních bran, povinných artefaktů, harmonogram na úrovni fází, způsob správy rozhodnutí	Projektový manažer (PM)	Nejpozději před zahájením projektu (kick-off)	Repository projektu
Evidence pack – index	Index důkazů, odpovědné osoby za obsah, pravidla verzování, odkaz na umístění	PM (vedení) + přispěvatelé dle odpovědností	Nejpozději k první kontrolní braně	Repository projektu
Decision log (log rozhodnutí)	ID rozhodnutí, popis, varianty, kritéria, kdo rozhodl, datum, dopad, odkazy na důkazy	PM (správa), Nositel (schvaluje klíčová rozhodnutí)	Průběžně od prvního rozhodnutí	Repository projektu
Mapa "řízení služby vs. řízení projektu"	Rozhraní: co je řízení služby (odpovědnost po spuštění) a co je řízení projektu (dodávka změny)	Nositel + PM	Nejpozději před zahájením projektu	Repository projektu
Kalendář kontrolních bran a účastníků	Termíny, účastníci, vstupy/výstupy, pravidlo STOP/GO, vazba na Řídící výbor projektu	PM	Nejpozději po schválení projektového záměru a před detailním plánováním	Repository projektu

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Název výstupu	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Kde se vede
ČASTÁ CHYBA Evidence pack se „slíbí“, ale není nikde fyzicky založený (chybí index a jednotné místo). Ve chvíli auditu nebo incidentu se pak dohledává „v e-mailech“ nebo „u dodavatele“.				

1.3 Hlavní obsah kapitoly

1.3.1 Jak s metodikou pracovat v každodenní praxi (pravidla používání)

Checklist – základní pravidla (MUSÍ / NESMÍ / MĚLO BY):

- MĚLO BY existovat jeden „zdroj pravdy“ pro dokumenty projektu a služby (repository) a musí být známý všem účastníkům.
- MĚLO BY existovat decision log a musí se aktualizovat při každém rozhodnutí s dopadem na rozsah, termín, rozpočet, právo, bezpečnost, provoz nebo UX.
- MĚLO BY být jasné, který dokument je podklad pro rozhodnutí a který je pouze pracovní.
- MĚLO BY být zavedena kontrola verzí (minimálně: datum, autor, stav, schválil).
- NEMĚLO BY se schvalovat prezentace bez podkladových artefaktů v evidence packu.
- NEMĚLO BY se považovat dodávka dodavatele za důkaz splnění povinnosti úřadu (úřad vždy odpovídá za rozhodnutí a jejich obhajitelnost).
- MĚLO BY – se používat jednotné šablony a jednotná pojmenování dokumentů napříč projekty (auditní stopa a předatelnost).

TIP

Zaveďte pravidlo: „Žádné rozhodnutí bez odkazu na důkaz.“

V decision logu musí být u každého zásadního rozhodnutí minimálně jeden odkaz do evidence packu.

1.3.2 Rozhraní "řízení digitální služby" a "řízení ICT projektu"

Rozhraní je závazné: metodika Digital First řídí obsah a kvalitu digitální služby; Metodika řízení ICT projektů řídí dodání změny jako projekt (role, odpovědnosti, fáze, eskalace, akceptace).

TABULKA 2 – Rozhraní odpovědností

Oblast	Kdo řídí (logika)	Kde se formálně rozhoduje	Co by mělo vzniknout jako důkaz
Smysl služby, uživatelé, výsledky a metriky	Řízení digitální služby	Rozhodnutí Nositele / Řídícího výboru projektu v rámci schvalování klíčových podkladů	Decision log + definice cíle a metrik (v evidence packu)
Dodání řešení (čas / rozpočet / rozsah)	Řízení ICT projektu	Řídící výbor projektu, PM, eskalace dle tolerancí	Projektový plán / Plán řízení projektu + reporting
Rizika, eskalace, změnové řízení	Řízení ICT projektu	PM / Řídící výbor, eskalace při překročení tolerancí	Registr rizik + záznam eskalací a rozhodnutí
Provoz po spuštění, udržitelnost přínosů	Řízení digitální služby (navazuje na předání)	Předání do následné podpory a udržitelného rozvoje	Vlastník výstupů + předávací protokol + plán provozu

POZOR

V rámci projektu by nemělo vzniknout paralelní „řídící struktura služby“, která by obcházela Řídící výbor projektu nebo Projektovou komisi. Řízení služby je věcná odpovědnost za obsah a provoz, nikoliv nové projektové orgány.

1.3.3 Kontrolní brány – minimální pravidla STOP/GO

Kontrolní brána je formální bod, kdy se rozhoduje, zda je možné pokračovat do další části prací. Kontrolní brány by měly být navázány na rozhodovací orgány projektu (zejména Řídící výbor projektu).

Kontrolní brána	[NÁZEV BRÁNY]
Evidence pack – MĚLO BY	☐ Seznam dokumentů (minimální sada): ... ☐ Odkaz na evidence pack: ...
Rozhodnutí – MĚLO BY	STOP / GO Podmínky (pokud GO): ... Termíny pro splnění podmínek: ...
Role – MĚLO BY	Vlastník přípravy podkladů (typicky PM): ... Příspěvatelé dle odpovědností týmů: ...
Zápis – MĚLO BY obsahovat	Rozhodnutí (STOP/GO) Podmínky Termíny Odpovědné osoby Odkazy do evidence packu
NEMĚLO BY	Informativní status bez možnosti změnit plán/rozsah nebo práce zastavit.
MĚLO BY	Jasná vazba do plánování: nesplněné vstupní podmínky ⇒ standardní reakce je přeplánování.
ČASTÁ CHYBA Brána proběhne bez předem distribuovaných podkladů. Účastníci pak rozhodují bez možnosti ověřit důkazy.	

1.3.4 Evidence pack – doporučená struktura (minimální standard)

Master index důkazů

Evidence pack se vede přes centrální master index důkazů. Index propojuje checklisty, rozhodnutí, gate packy, přílohy, datové artefakty, právní posouzení a provozní dokumentaci do jedné dohledatelné struktury.

Minimální pole master indexu: ID důkazu, kapitola/metodický krok, checklistový bod, související rozhodnutí z decision logu, vlastník, odkaz na artefakt, stav, datum poslední aktualizace a vazba na příslušnou kontrolní bránu.

Pravidlo pro audit: bez odkazu na důkaz se bod považuje za nedoložený. Samotné zaškrtnutí checklistu bez odkazu na artefakt, vlastníka a stav nestačí.

Orgán veřejné moci by měl vést evidence pack jako strukturované úložiště důkazů. Minimální struktura složek by měla být:

- 00_Rozhodnutí_a_schválení (decision log, zápisy, schválení)
- 01_Definice_služby (definice, scope, metriky)
- 02_Právo_a_compliance (analýzy, stanoviska, výklady)
- 03_Procesy_a_data (mapy procesu, datové modely, evidenční vazby)
- 04_UX_obsah_přístupnost (výzkum, testy, výstupy přístupnosti)
- 05_Architektura_bezpečnost (architektura, klasifikace, bezpečnostní výstupy)
- 06_Provoz_a_podpora (provozní model, SLA/OLA, incidenty, monitoring)
- 07_Go-live_a_předání (go-live checklist, předávací protokoly, zvýšená podpora)

Minimální standard metadat pro každý dokument/důkaz v Evidence packu:

- Název dokumentu (co je obsahem) + ID/odkaz na službu/projekt.
- Verze a datum (kdy je dokument platný).
- Autor / vlastník (kdo odpovídá za obsah).
- Schválil (kdo dal go) + odkaz na rozhodnutí v Decision logu.
- Odkaz/umístění (repo/IS) – aby bylo dohledatelné při auditu.

DŮSLEDEK

Bez jednotné struktury evidence packu nelze projekt předat, auditovat ani opakovat v jiné službě.
V praxi to vede k ručnímu dohledávání, ztrátě znalostí a nárůstu závislosti na dodavateli.

1.3.5 Pravidla práce s dodavatelem (aby nevznikl „dodavatelský stát“)

Kontrolní pravidlo proti vendor lock-in

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Dodavatel může zajišťovat realizaci, ale vlastnictví služby, dat, rozhodnutí, dokumentace, rozhraní, provozních postupů a exit scénáře zůstává u OVM. Chybějící exit scénář nebo nedostupná dokumentace je významné riziko pro kontrolní bránu.

Checklist – minimální pravidla:

- MĚLO BY být stanoveno, které artefakty dodavatel povinně dodá jako podklady pro rozhodnutí (nejen jako výstupy implementace).
- MĚLO BY být stanoveno, které artefakty úřad vždy schvaluje a za které nese odpovědnost (zejména s právním, bezpečnostním a provozním dopadem).
- NEMĚLO BY být akceptace „díla“ zaměněna za akceptaci připravenosti služby k provozu (jsou to dvě různé věci).
- MĚLO BY – být zajištěno průběžné předávání znalostí (ne až na konci), aby předání do následné podpory bylo reálné.

2 Co je digitální služba

Účelem kapitoly je závazně vymezit, co se v praxi orgánů veřejné moci považuje za digitální službu, jak se digitální služba odlišuje od ICT systému/projektu a jak se určuje její hranice, uživatelé a cíle. Kapitola zajišťuje, že úřad řídí „službu“ (uživatelskou cestu a výsledky), nikoliv pouze „systém“ (technickou dodávku).

2.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zahájením detailních prací rozhodnout a doložit:

- MĚLO BY zda je iniciativa digitální službou, změnou existující digitální služby, nebo pouze podpůrným ICT projektem (bez přímé služby uživateli).
- MĚLO BY k jaké konkrétní službě (službám) se iniciativa vztahuje a jaký je očekávaný uživatelský výsledek (co se uživateli reálně zlepšilo).
- MĚLO BY hranici služby end-to-end: od spouštěcí situace (trigger) po doručení výsledku (včetně nedigitálních kroků, které ovlivňují zkušenost a lhůty).
- MĚLO BY kdo v organizaci nese věcnou odpovědnost za službu a kdo ponese odpovědnost za provoz a udržitelný rozvoj po spuštění (v návaznosti na vlastníka výstupů projektu).
- MĚLO BY minimální měření výsledku služby (metriky) a způsob, jak se data o službě budou získávat a vyhodnocovat.

POZOR

Digitální služba není synonymum ICT systému.

Za digitální službu se považuje uživatelská cesta a výsledek, který úřad uživateli poskytuje, bez ohledu na to, kolik systémů ji tvoří a zda část kroků probíhá nedigitálně.

2.2 Výstupy / důkazy

TABULKA 1 – Výstupy / důkazy pro vymezení digitální služby

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kde se vede
Karta digitální služby (Service card)	Název služby, poskytovatel, cíloví uživatelé, spouštěč, výsledek, kanály, základní proces, klíčové registry/data, klíčové závislosti, metriky, věcný vlastník	Nositel projektu ve spolupráci s věcným gestorem služby; správa v projektu: PM	Nejpozději před první kontrolní bránou v předprojektové fázi	Jasně vymezení „co je služba“ pro řízení rozsahu a rozhodování	Repository projektu (evidence pack)
Mapa hranice služby (End-to-end scope)	Začátek/konec služby, zahrnuté a vyloučené kroky, hranice odpovědnosti úřadu vs. externích subjektů, výjimky a alternativní scénáře	Věcný gestor služby; správa v projektu: PM	Nejpozději před zahájením analýz a návrhů řešení	Zabraňuje tomu, aby projekt řešil jen „UI“ a ignoroval zbytek služby	Repository projektu
Seznam uživatelských skupin a situací (User)	Minimálně 3–5 typických situací uživatele, včetně okrajových (výjimky), a jejich očekávání	Věcný gestor služby; zapojení: UX/obsah	Nejpozději před návrhem řešení a zadáním dodavateli	Podklad pro rozsah, obsah, přístupnost a	Repository projektu

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kde se vede
segments & scenarios)				provozní scénáře	
Základní metriky a měření služby (KPI/Metrics)	Definice metrik, zdroj dat, periodicita, odpovědnost, výchozí stav (pokud existuje)	Věcný vlastník služby; technické zajištění: projektový tým	Nejpozději před schválením projektového záměru / před vstupem do realizace	Podklad pro přínosy, udržitelnost a řízení po spuštění	Repository projektu + reportingové místo organizace
Vazba na katalog služeb / evidenci služeb (pokud existuje v organizaci)	Jednoznačný identifikátor služby, verze, datum změny, vazba na agendu / právní titul (v základní úrovni)	Věcný vlastník služby; správa: určený správce katalogu	Nejpozději před go-live	Zajišťuje dohledatelnost a řízení životního cyklu služby	Katalog služeb / vnitřní evidence
Rozhraní „služba vs. projekt“ (RACI/odpovědnosti)	Kdo rozhoduje o obsahu služby, kdo rozhoduje o dodávce, kdo schvaluje změny, kdo nese odpovědnost po spuštění	Nositel projektu + PM (v návaznosti na metodiku ICT projektů)	Nejpozději při zahájení projektu	Zabraňuje paralelním strukturám a sporům o odpovědnost	Repository projektu

Záznam o vymezení služby (vazba služba – agenda – úkon – katalogový záznam – obslužný kanál) se ukládá do sběrného místa (ISDR) podle kap. 1, strukturovaně a verzovaně, aby byl datově propojitelný s Katalogem služeb veřejné správy.

2.3 Hlavní obsah kapitoly

Digitální službou se podle zákona č. 12/2020 Sb. (ZoPDS) rozumí úkon vykonávaný orgánem veřejné moci vůči uživateli služby v rámci agendy, vedený v katalogu služeb a poskytovaný v elektronické podobě. Tato kapitola na uvedené vymezení navazuje a rozpracovává je do návrhu konkrétní služby; nepracuje s izolovaným ICT projektem, ale s digitální službou v tomto smyslu.

2.3.1 Praktická definice digitální služby

Digitální služba je taková služba orgánu veřejné moci, která splňuje současně:

- MĚLO BY mít identifikovatelného uživatele (občan, podnikatel, jiný OVM, interní pracovník v roli uživatele služby) a jeho spouštěcí situaci.
- MĚLO BY poskytovat uživateli konkrétní výsledek (rozhodnutí, potvrzení, zápis, vydání dokladu, provedení změny, informaci s právním dopadem apod.).
- MĚLO BY mít definované kanály a pravidla jejich kombinace (digitální kanál je primární, ale služba může mít i nedigitální kroky).
- MĚLO BY mít end-to-end proces, který je řízen jako jeden celek (i když je realizován více systémy a útvary).
- MĚLO BY mít určenou věcnou odpovědnost za kvalitu služby a odpovědnost za provozní rozhodnutí po spuštění.

Za digitální službu se naopak nemělo by považovat pouze:

- NEMĚLO BY samostatný ICT systém bez přímé uživatelské cesty (např. čistě interní technická infrastruktura).
- NEMĚLO BY jednotlivá technická komponenta (API, integrace, datová migrace) bez vymezení služby, kterou podporuje.
- NEMĚLO BY pouhá digitalizace dokumentu (PDF) bez možnosti dokončit záležitost end-to-end nebo bez jasného uživatelského výsledku.

2.3.2 Jak správně vymezit hranici služby (end-to-end scope)

Checklist – vymezení hranice služby:

- MĚLO BY být popsán spouštěcí okamžik: co uživatel řeší a proč (např. změna stavu, povinnost, žádost, oznámení).
- MĚLO BY být popsán konec služby: kdy je uživatel „hotový“ (výsledek doručen, změna provedena, povinnost splněna).
- MĚLO BY být uvedeny všechny kanály a jejich role (digitální, přepážka, pošta, datová schránka, telefon, zastoupení).

- MĚLO BY být popsány interní kroky, které ovlivňují lhůty a výsledek (předání, kontrola, posouzení, schválení, archivace).
- MĚLO BY být uvedeny klíčové výjimky a alternativní průchody (neúplné podání, opravy, odvolání, nedoložení, zástupce).
- MĚLO BY být popsány závislosti na registrech a externích subjektech (kdo dodává data, kdo je spotřebovává, kdo rozhoduje).
- NEMĚLO BY být hranice vymezena jen „tím, co dodá dodavatel“ (hranice je věcná, ne dodavatelská).

TIP

Vymezení hranice služby začínejte na papíře: 1) spouštěč, 2) výsledek, 3) kroky, 4) výjimky. Teprve potom rozhodujte o systému, integracích a UX.

2.3.3 Minimální obsah karty digitální služby (doporučené položky)

TABULKA 3 – Doporučená pole karty digitální služby (vyplnit vždy)

Položka	Povinnost	Jak to úřad reálně doloží	Typická chyba
Název služby a identifikátor	MĚLO BY	Název + interní ID / ID v katalogu	Stejná služba má v různých projektech jiný název; ztrácí se kontinuita.
Uživatelé a situace (scénáře)	MĚLO BY	Seznam segmentů + 3–5 scénářů včetně výjimek	Scénáře chybí; řeší se jen „standardní“ uživatel.
Spouštěč a výsledek	MĚLO BY	Jednověté vyjádření spouštěče a výsledku + příklady výstupů	Výsledek je popsán jako „odeslání formuláře“ místo skutečného dokončení záležitosti.
End-to-end hranice	MĚLO BY	Mapa kroků + vymezení začátku a konce + zahrnuto/vyloučeno	Hranice je jen frontend; interní kroky se neřeší.
Kanály a pravidla kombinace	MĚLO BY	Seznam kanálů + kdy a proč se použijí + co je primární	Neřeší se přechody mezi kanály (např. digitál → přepážka).
Závislosti na datech a systémech	MĚLO BY	Seznam registrů/systémů + vlastníci + typ integrace (na úrovni „co potřebujeme“)	Závislosti se objeví až v realizaci → dodatky a skluz.
Metriky a měření	MĚLO BY	Definice metrik + zdroj dat + periodičita + odpovědnost	Metriky jsou „přání“ bez zdrojů dat a bez odpovědnosti.
Odpovědnost po spuštění	MĚLO BY	Určený věcný vlastník služby + vazba na vlastníka výstupů projektu a podporu	Po ukončení projektu není kdo rozhoduje o změnách a provozu.

2.3.4 Minimální sada metrik služby (bez ohledu na velikost projektu)

Orgán veřejné moci by měl definovat minimálně následující typy metrik a způsob jejich měření:

- MĚLO BY objem a dokončenost: počet zahájených a dokončených případů/podání; míra nedokončení (drop-off).
- MĚLO BY čas: doba od zahájení služby po výsledek (včetně čekání na uživatele, pokud je relevantní).
- MĚLO BY kvalita: chybovost (vrácení, opravy, neúplnost), počet kontaktů na podporu k jedné záležitosti.
- MĚLO BY dostupnost a stabilita: základní provozní metriky (výpadky, degradace), pokud je služba digitálně poskytována.
- MĚLO BY přístupnost a obsah: prokazatelné ověření splnění požadavků přístupnosti a srozumitelnosti pro klíčové scénáře (důkaz, ne deklarace).

POZOR

Metrika bez zdroje dat není metrika. U každé metriky by mělo být určeno: odkud data vezmeme, jak často je vyhodnotíme a kdo za to odpovídá.

2.3.5 Vazba služby na Katalog služeb veřejné správy

Je-li to pro danou službu relevantní, má být služba navázána na odpovídající záznam v Katalogu služeb veřejné správy. Katalog služeb VS se používá jako evidence služeb, úkonů a obsluhovaných kanálů.

V dokumentaci služby se proto vzájemně propojuje digitální služba, agenda, úkon, obslužný kanál a katalogový záznam. Metodika nepracuje s izolovaným ICT projektem, ale se službou evidovanou nebo evidovatelnou ve veřejnosprávním kontextu.

2.3.6 Zasazení služby do životní situace nebo události

Služba má být zasazena do životní situace nebo životní události klienta. Cílem není digitalizace izolovaného formuláře, ale návrh služby podle toho, co klient skutečně řeší.

Každá služba má mít vazbu na jednu nebo více životních událostí, pokud je to pro daný typ služby relevantní. Tato vazba pomáhá navrhnout službu end-to-end napříč úkony a kanály, nikoli jako jednotlivý úkon.

2.3.7 Kanálová neutralita a princip „only once“

Služba má být navrhována kanálově neutrálně. Nemá být navržena jen jako formulář, portál nebo aplikace; návrh má být nezávislý na konkrétním kanálu a má umožnit poskytování služby více kanály.

Klient nemá opakovaně dokládat údaje, které stát již má v jiných agendových informačních systémech (princip „only once“), a to bez ohledu na to, jakým kanálem službu využívá.

Budoucí návrh služby má počítat i s asistenty nebo agenty, kteří mohou klientovi pomoci službu vyřídit (viz též 2.5.10).

2.3.8 Elektronické zastupování

Služba má počítat nejen s klientem samotným, ale i se zmocněncem nebo jinou oprávněnou osobou. Elektronické zastupování je součástí návrhu budoucích digitálních služeb.

Elektronické zastupování se zohledňuje v popisu kanálů, oprávnění, autentizace a autorizace a v průchodu službou (kdo a v jaké roli službou prochází a na základě jakého oprávnění).

2.3.9 AI asistenti a agenti v návrhu služby

Návrh služby má počítat s tím, že službu nemusí v budoucnu vyřizovat přímo subjekt práva, ale také AI asistent nebo agent jednající na základě zmocnění nebo oprávnění. Návrh má umožnit, aby asistent nebo agent mohl za klienta načíst relevantní údaje, pokud k tomu existuje právní titul a odpovídající oprávnění.

Metodika počítá s budoucím vývojem směrem k AI asistentům a agentům, nikoli jen s formuláři, portály a aplikacemi. Konkrétní povinnosti vždy závisejí na typu AI systému, na roli správce nebo poskytovatele služby a na použitém právním režimu; metodika nestanovuje plošné povinnosti.

Posouzení dopadů na základní práva (FRIA) a povinnosti podle nařízení (EU) 2024/1689 (AI Act) se uplatní podle konkrétního použití AI v dané službě (zejména podle rizikové kategorie systému a role subjektu), nikoli automaticky pro každou digitální službu.

3 Rozhodnutí před zahájením

3.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zahájením realizace (nejpozději před vyhlášením/výběrem dodavatele na implementaci) rozhodnout a doložit:

- MĚLO BY vymezení digitální služby a její hranice end-to-end (co přesně je předmětem změny a co ne).
- MĚLO BY cílový uživatelský výsledek a minimální metriky (jak poznáme, že služba funguje a zlepšila se).
- MĚLO BY právní proveditelnost: zda lze službu provozovat v cílovém režimu bez změny práva, nebo jaké změny jsou nezbytné a kdo je zajistí.
- MĚLO BY procesní a datovou proveditelnost: jak bude úřad rozhodovat, z jakých dat/registrů čerpá a kdo je vlastníkem zdrojových dat.
- MĚLO BY architektonické a bezpečnostní mantinely: klasifikaci dopadů, požadovanou úroveň ochrany a klíčové integrace.

- MĚLO BY provozní model: kdo službu vlastní po spuštění, jak bude zajištěna podpora, monitoring, incident management a udržitelný rozvoj.
- MĚLO BY dodavatelský a smluvní přístup: co bude předmětem zakázky, jaká jsou akceptační kritéria, jak se bude přebírat a jak se zabrání vendor lock-inu.
- MĚLO BY způsob řízení změn, rizik a tolerancí (kdy a jak se eskaluje, kdo může zastavit práce).
- NEMĚLO BY začít implementace bez kompletního rozhodovacího balíčku (Start pack) definovaného v této kapitole.

3.2 Výstupy / důkazy

TABULKA 1 – Start pack (povinné důkazy před zahájením realizace)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)
Karta digitální služby (Service card)	Název, uživatelé, spouštěč, výsledek, kanály, hranice, klíčová data/registry, metriky, věcný vlastník	Nositel projektu + věcný gestor služby; správa: PM	Před schválením zahájení realizace	Definuje, co se skutečně realizuje a proč	Předprojektová brána – rozhodnutí o zahájení realizace
Mapa end-to-end hranice služby	Zahrnuto/vyloučeno, výjimky, interní kroky, závislosti, předání mezi útvary	Věcný gestor služby; správa: PM	Před zadáním implementace	Zabraňuje tomu, aby se řešil jen frontend	Před zadáním implementace / před zahájením vývoje
Rozhodovací memorandum „Start realizace“	Shrnutí rozhodnutí, varianty a důvody, dopady na rozsah/čas/rozpočet, seznam podmínek, rozhodl	Nositel projektu; formální schválení: Řídicí výbor projektu	Bezprostředně před zahájením realizace	Jasná odpovědnost a auditní stopa	Rozhodnutí Řídicího výboru projektu
Právní proveditelnost (minimální právní stanovisko)	Právní titul/agenda, povinnosti, lhůty, omezení, potřeba legislativní změny (ANO/NE) + plán zajištění	Gestor práva / právní útvar; vlastníkem je úřad	Před zahájením realizace a před výběrem technického řešení s právním dopadem	Zabraňuje realizaci neprovozovatelné služby	Předprojektová brána
Procesní a datová proveditelnost (L0/L1)	Mapa procesu (min. L0), rozhodovací body, vstupy/výstupy, datové zdroje, vlastníci dat, kvalita a dostupnost	Věcný gestor služby + datoví vlastníci; koordinace: PM	Před zadáním implementace	Zajišťuje reálnou proveditelnost a předchází dodatkům	Brána před realizací
UX a přístupnost – minimální plán a kritéria	Klíčové scénáře, obsahové zásady, přístupnostní kritéria pro převzetí, plán testování s uživateli	Věcný gestor služby + UX/obsah; koordinace: PM	Před zadáním implementace	Umožní převzít službu podle jasných kritérií	Brána před realizací a brána před převzetím
Bezpečnostní a provozní rámec (minimální)	Klasifikace dopadů, požadavky na ochranu, základní provozní scénáře, monitoring, incidenty, role podpory, přístupová politika	Bezpečnostní role/útvary + provoz; koordinace: PM	Před zahájením realizace	Zabraňuje „provozu na poslední chvíli“	Brána před realizací
Dodavatelská a smluvní strategie (implementace)	Co se soutěží, jak se přebírá, akceptační kritéria, evidence povinností dodavatele, podmínky předání znalostí, práva k výstupům	PM + nákup/veřejné zakázky; schvaluje Řídicí výbor projektu dle pravidel	Před zahájením zadávacího řízení / před podpisem	Zabraňuje smlouvám bez převzetí a bez provozních záruk	Brána před zahájením realizace
Počáteční registr rizik a tolerancí	Top rizika, vlastníci, mitigace, eskalační pravidla, tolerance času/rozpočtu/rozsahu	PM; schvaluje Řídicí výbor projektu	Před zahájením realizace	Řízení podle tolerancí, ne podle „pocitu“	Rozhodnutí Řídicího výboru projektu

Předprojektová rozhodnutí a podklady pro ICT záměr se ukládají do sběrného místa (ISDR) tak, aby byly dohledatelné a opakovaně použitelné jako podklad pro proces OHA.

3.3 Hlavní obsah kapitoly

- MĚLO BY existovat právní stanovisko potvrzující proveditelnost cílového režimu (nebo formálně schválený plán legislativních kroků s odpovědností a termíny).

3.3.1 Rozhodovací mapa před zahájením (co musí být rozhodnuto a kým)

TABULKA 2 – Rozhodovací oblasti a minimální otázky

Oblast	Minimální otázka, na kterou musí být odpověď	Varianty (typicky)	Kdo rozhoduje (v rámci řízení projektu)	Důkaz (artefakt)	Co se stane, když chybí
Vymezení služby	Co je přesně služba a kde začíná/končí?	Jeden end-to-end proces / sada dílčích služeb / pouze podpurný projekt	Nositel + Řídící výbor projektu (na návrh věcného gestora)	Karta služby + mapa hranice + Decision log	Rozsah se rozpadá a realizace se řídí dodavatelem.
Právo a compliance	Je cílový režim legální a provozovatelný?	Bez změny práva / s legislativní změnou / nelze provozovat	Nositel + Řídící výbor projektu (podklad právního útvaru)	Právní stanovisko + seznam povinností	Právní stopka před spuštěním nebo provoz mimo zákon.
Proces a data	Kdo rozhoduje v procesu a z jakých dat?	Využití registrů / vlastní evidence / kombinace / sdílení s jiným OVM	Nositel + Řídící výbor projektu (podklad věcného gestora a datových vlastníků)	Procesní mapa + datová mapa + potvrzení vlastníků	Změny a integrace se objeví až v realizaci → dodatky.
UX, obsah, přístupnost	Jaké scénáře musí fungovat a podle čeho službu převezmeme?	Minimální scénáře + výjimky / postupné rozšiřování v iteracích	Řídící výbor projektu (akceptační kritéria); zpracování: věcný gestor + UX/obsah	Akceptační kritéria + plán testování	Nelze převzít; vzniká spor „splnili jsme / nesplnili“.
Architektura a bezpečnost	Jaké jsou mantinely a povinnosti ochrany?	Centrální platformy / vlastní řešení / integrace / refaktor stávajícího	Řídící výbor projektu (na základě architektury a bezpečnosti)	Bezpečnostní rámec + architektonické rozhodnutí	Bezpečnostní stopka nebo nákladné předělovky.
Provoz a podpora	Kdo službu provozuje a jak se bude řešit incident?	Interní provoz / externí / hybrid + jasné rozhraní	Nositel + Řídící výbor projektu	Provozní koncept + předávací model	Služba je spuštěna bez podpory; incidenty eskalují mimo řízení.
Dodavatelský přístup	Co přesně soutěžíme a jak přebíráme?	Implementace na klíč / postupné dodávky / integrátor + dílčí dodávky	Řídící výbor projektu dle pravidel organizace	Soutěžní dokumentace + akceptační kritéria + pravidla změn	Dodatkování a vendor lock-in.

POZOR

Rozhodnutí před zahájením by měla být rozhodnutelná: pokud není dohoda s datovými vlastníky nebo s provozem, nejde zahájit realizaci a projekt se musí vrátit do přípravy.

3.3.1 Pravidla „NEMÍ SE ZAČÍT“ (No-go pravidla)

Následující situace znamenají, že realizace by neměla být zahájena, dokud nejsou odstraněny:

- NEMĚLO BY chybět věcný vlastník služby nebo dohoda o odpovědnosti po spuštění (včetně podpory).
- NEMĚLO BY existovat nevyřešený spor o hranici služby nebo o povinné scénáře (včetně výjimek).
- NEMĚLO BY chybět právní stanovisko nebo je-li závěr „nelze provozovat“ bez schváleného plánu změny práva.
- NEMĚLO BY být neznámý nebo nepotvrzený vlastník klíčových dat/registrů, na kterých služba závisí.
- NEMĚLO BY být zadání/smlouva bez akceptačních kritérií a bez pravidel změnového řízení.

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- NEMĚLO BY být nejasné, kdo bude službu provozovat a jak se bude řešit incident (včetně kontaktů a odpovědností).

Součástí rozhodnutí před zahájením je předložení ICT záměru ke schválení v procesu OHA (posouzení ICT záměru a vydání stanoviska OHA, archi.gov.cz). Schválení ICT záměru je vstupní podmínkou pro zahájení realizace; výstupy této kapitoly slouží jako podklad pro toto posouzení, nikoli jako paralelní dokumentace.

U změn stávajících informačních systémů veřejné správy (ISVS) se postupuje podle aktuálních pravidel OHA pro ICT záměry. Cílovým směřováním je posuzovat změny primárně na úrovni digitálních služeb (obdoba „kolaudace“ služby) – viz kap. 9 a vize v kap. 13.

4 Právo jako konstrukční prvek

Účelem kapitoly je zajistit, aby právo nebylo pouze „kontrola na konci“, ale aby bylo používáno jako konstrukční prvek digitální služby: tj. aby právní povinnosti, lhůty, oprávnění, důkazní standardy, doručování, zastupování, poplatky, archivace a ochrana údajů byly přeloženy do konkrétních požadavků na službu, proces, data, UX a provoz. Kapitola zajišťuje, že úřad nevstoupí do realizace bez doložené právní proveditelnosti cílového režimu a bez rozhodnutí o legislativních krocích, pokud jsou nutné.

4.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zahájením realizace rozhodnout a doložit zejména:

- MĚLO BY jaký je právní titul poskytování služby (agenda / právní předpis / oprávnění úřadu) a jaký je právní účinek digitálního úkonu (co se právně stane).
- MĚLO BY jak se prokazuje identita a oprávnění jednající osoby (identifikace, autentizace, zastoupení, role) a jak se vede důkazní stopa.
- MĚLO BY jak se řeší doručování, lhůty a právní fikce (včetně alternativních kanálů a výjimek).
- MĚLO BY jaké údaje se zpracovávají a na jakém právním základě (včetně minimalizace, účelu, doby uchování, předávání a zveřejnění).
- MĚLO BY jaké dokumenty/výstupy jsou úřední záznamy a jak se archivují (spisová služba, skartační režim, auditní stopa).
- MĚLO BY jaké právní požadavky se promítají do akceptačních kritérií (právní účinek úkonu, doručení, validita podpisu, vedení spisu, evidence)
- NEMĚLO BY zahájit realizaci, pokud právní posouzení identifikuje nepřeklenutelnou překážku cílového režimu nebo chybí rozhodnutí o její nápravě.

POZOR

Právo se v digitální službě „implementuje“. Pokud není právní účinek úkonu a důkazní stopa navržena předem, nelze službu bezpečně převzít do provozu a nelze ji obhájit v řízení (např. při sporu, odvolání, kontrole).

4.2 Výstupy / důkazy

TABULKA 1 – Legal pack (povinné právní důkazy pro digitální službu)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Právní inventura služby (Legal inventory)	Seznam relevantních právních předpisů, povinností a právních účinků; role a oprávnění; lhůty; poplatky; doručování; opravné prostředky	Právní útvar / gestor práva; vlastníkem je úřad	V předprojektových fázích, před schválením projektového záměru	Základní „mapa práva“ pro návrh služby a rozsah	Schvalování projektového záměru	Evidence pack – Právo a compliance
Rozhodnutí o právní proveditelnosti cílového režimu	Závěr: lze / lze s podmínkami / nelze; identifikované překážky; podmínky a rizika; schválil	Nositel projektu (rozhodnutí), podklad: právní útvar	Nejpozději před zahájením realizace (Start realizace)	STOP/GO rozhodnutí pro zahájení realizace	Rozhodnutí Řídicího výboru projektu	Decision log + zápis

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Plán legislativních kroků (pokud relevantní)	Co se mění, důvod, odpovědný gestor, termíny, závislosti, dopady na projekt, rizika a mitigace	Nositel projektu + gestor legislativy; koordinace: PM	Před zahájením realizace, pokud je potřeba změna práva	Zajištění, že projekt nevyvíjí neprovozovatelný režim	Schválení projektového záměru / Start realizace	Evidence pack – Právo a compliance + registr rizik
Matrice právních povinností → požadavky (Legal traceability)	Každá povinnost má: popis, dopad na proces/UX/data/provoz, požadavek, test/ověření, odpovědnost	Právní útvar + věcný gestor; správa: PM	Před zadáním implementace; u změn průběžně	Zabraňuje „právu v PDF“ bez implementace	Brána před realizací a před převzetím	Evidence pack – Právo + Testy/akceptace
Rozhodnutí o identitě, oprávnění a zastoupení	Jak se ověřuje identita; jak se ověřuje oprávnění (role); jak se řeší zastoupení; logování; výjimky	Věcný gestor + bezpečnost + právní útvar; schvaluje Řídicí výbor projektu	Před návrhem detailního řešení a před implementací přihlášení/rolí	Zajišťuje právní platnost úkonů a obranu proti zneužití	Brána před realizací	Evidence pack – Právo + Bezpečnost + UX
Režim doručování a lhůt (včetně fikcí)	Kanály, pravidla doručení, okamžiky účinku, výjimky, evidence o doručení, návazné úkony	Právní útvar + věcný gestor; koordinace: PM	Před návrhem komunikace a UX; před implementací notifikací	Zajišťuje právní účinnost komunikace	Brána před realizací a před go-live	Evidence pack – Právo + Provoz
DPIA / posouzení ochrany osobních údajů (je-li vyžadováno)	Rozsah, rizika, opatření, zbytkové riziko, schválení, návaznost na bezpečnostní opatření	Pověřenec/odpovědný útvar ochrany údajů; spolupráce: bezpečnost + projekt	Před zahájením realizace v relevantních případech	Prokazuje řízení rizik zpracování	Brána před realizací / před go-live (dle povahy)	Evidence pack – Právo a compliance + Bezpečnost
Pravidla uchování a evidence (spisová služba, auditní stopa)	Co je dokument/úřední záznam, kde vzniká, jak se ukládá, doba uchování, skartace, přístupová práva, audit	Spisová služba/archiv + věcný gestor + právní; koordinace: PM	Před implementací a před převzetím	Zajišťuje dohledatelnost a zákonnou evidenci	Brána před převzetím a go-live	Evidence pack – Provoz + Právo
Texty pro uživatele s právním významem (notices)	Poučení, prohlášení, souhlasy (pouze pokud jsou legální), informace o zpracování údajů, podmínky, práva uživatele	Věcný gestor + právní + obsah/UX	Před testováním a před go-live	Zajišťuje srozumitelnost a právní účinek informací	Brána před go-live	Evidence pack – UX/obsah + Právo

TIP

Legal pack by měl být řízen jako „živý“: každá legislativní nebo výkladová změna se promítne do traceability matice a do Decision logu (co se změnilo, dopad, rozhodnutí).

Právní analýza, evidence titulů zpracování a případné posouzení (vč. FRIA) se ukládají do sběrného místa (ISDŘ) jako verzovaný a datově zpracovatelný výstup.

4.3 Hlavní obsah kapitoly

4.3.1 Postup: přeložení práva do návrhu služby (Legal-to-Design workflow)

Postup je doporučeným minimem a zahrnuje zejména následující kroky:

- MĚLO BY vzniknout právní inventura (povinnosti, účinky, lhůty, doručování, role, opravné prostředky).
- MĚLO BY každá právní povinnost být přiřazena ke konkrétnímu kroku end-to-end procesu (kde se uplatní).
- MĚLO BY z právních povinností vzniknout implementační požadavek (na UX, data, logování, provoz) a ověřovací scénář (test).
- MĚLO BY existovat rozhodnutí, zda a jak se řeší výjimky (neúplné podání, zastoupení, odmítnutí, doplnění).
- MĚLO BY být stanoveno, co je „právně relevantní důkaz“ (logy, časové razítko, doručení, podpis, vazba na spis).

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- MĚLO BY – být proveden minimálně jeden společný workshop: právní + věcný gestor + UX/obsah + bezpečnost + provoz (z důvodu provázanosti).

POZOR

„Právně relevantní důkaz“ není screenshot. Úřad by měl být schopen doložit: kdo jednal, kdy, s jakým oprávněním, co bylo podáno/doručeno, jaký nastal účinek a kde je to uloženo ve spisu/evidenci.

4.3.2 Typy právních požadavků a jejich dopady (praktická mapa)

TABULKA 2 – Typy právních požadavků → co to znamená pro službu

Typ právního požadavku	Typický dopad na proces	Typický dopad na data a evidenci	Typický dopad na UX/obsah	Typický dopad na provoz
Právní účinek úkonu (zahájení, změna, rozhodnutí)	Definice okamžiku účinku; navazující kroky a lhůty	Evidence o úkonu, čas, identita, obsah, vazba na spis	Srozumitelné potvrzení, poučení, stav řízení	Auditní stopa, export důkazů, incidenty se stopou
Doručování a fikce	Kanály doručení, pravidla doručení, opakování, výjimky	Důkaz o doručení, časové značky, identifikace adresáta	Texty o doručení, upozornění, stav doručení	Monitoring doručování, opakování, eskalace
Zastoupení a oprávnění	Role, delegace, kontrola oprávnění před úkonem	Evidence oprávnění, vazby na registr/zdroj, log přístupu	Výběr role, informace o oprávnění, odmítnutí s důvodem	Správa rolí, revize oprávnění, incidenty zneužití
Lhůty a procesní úkony (doplnění, odvolání)	Běh lhůt, přerušení, doplnění, rozhodnutí o odmítnutí	Evidence lhůt, stavů, úkonů a rozhodnutí	Zobrazení termínů, poučení, výzvy k doplnění	SLA/OLA na vyřízení, eskalace kapacit
Poplatky a platby (pokud relevantní)	Vznik povinnosti, vrácení, výjimky, potvrzení	Evidence platby, vazba na případ, doklad	Jasně informace, potvrzení, stav platby	Napojení na ekonomiku, reconciliation, výpadky
Ochrana údajů (účel, minimalizace, uchování)	Zpracování jen nezbytných údajů, sdílení a přístup	Katalog údajů, doby uchování, přístupové politiky	Informování uživatele, práva subjektu údajů (pokud relevantní)	Řízení přístupů, logování, reakce na incidenty
Spisová služba a archivace	Zařazení do spisu, úřední záznamy, uzavírání spisu	Ukládání dokumentů, metadata, skartace	Uživatelé se neprezentují interní evidenční detaily; jen relevantní potvrzení	Exporty, integrace se spisovou službou, audit

4.3.3 Checklist „právní no-go“ (kdy je povinné STOP)

Následující situace znamenají STOP, dokud nejsou odstraněny nebo formálně rozhodnuty s mitigací:

- NEMĚLO BY chybět vyjasnění právního účinku digitálního úkonu (není jasné, co se právně děje).
- NEMĚLO BY být nevyřešeno doručování a okamžik účinku (není důkaz o doručení nebo není jasná fikce).
- NEMĚLO BY být nevyřešeno zastoupení/opravení jednatelů osoby, pokud je pro agendu běžné.
- NEMĚLO BY být plánováno hlavní zpracování osobních údajů na základě „souhlasu“, pokud pro veřejnou moc není vhodný a není právně zdůvodněn.
- NEMĚLO BY být nevyřešena evidence a vazba na spis (není jasné, kde bude dokument a kdo ho dohledá).
- NEMĚLO BY být identifikována nutná legislativní změna bez schváleného plánu a bez dopadu na harmonogram projektu.

4.3.4 Co by mělo být smluvně zajištěno kvůli právní obhajitelnosti

Checklist – povinné smluvní body (bez ohledu na typ dodavatele):

- MĚLO BY být povinnost dodavatele dodat a udržovat dokumentaci k právně relevantním funkcím (doručení, podpis, logování, export důkazů).
- MĚLO BY být povinnost dodavatele umožnit export právně relevantních důkazů (logy, auditní záznamy, dokumenty) v definovaném formátu.
- MĚLO BY být povinnost dodavatele dodržet akceptační kritéria včetně právních scénářů (zastoupení, výjimky, lhůty).
- MĚLO BY být povinnost řešit změny práva/výkladu jako řízené změny (dopad, plán, cena, termín, rozhodnutí).

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- NEMĚLO BY být právně kritické části služby neověřitelné (bez testu, bez logu, bez důkazu).

ČASTÁ CHYBA

Úřad koupí „funkcionalitu“ bez definice důkazů a auditní stopy. Pak má obrazovku, ale nemá obhajitelný úkon.

Je-li ve službě využit AI asistent nebo agent, je nutné se právně vypořádat s tím, že úkon za uživatele nečiní přímo subjekt práva, ale asistent nebo agent jednající na základě zmocnění či jiného oprávnění (vazba na elektronické zastupování). V právní analýze se vymezí titul jednání, rozsah oprávnění a odpovědnost.

Podle typu a role AI systému se posoudí povinnosti podle nařízení (EU) 2024/1689 (AI Act) a potřeba posouzení dopadů na základní práva (FRIA). Tyto povinnosti se uplatní podle konkrétního použití AI v dané službě, nikoli plošně pro každou službu.

5 Proces a data

5.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zahájením realizace (nejpozději před zadáním implementace) rozhodnout a doložit:

- MĚLO BY end-to-end proces služby včetně výjimek a návratových stavů (nejde jen o „happy path“).
- MĚLO BY kde vzniká rozhodnutí (úkon úřadu) a kde vzniká důkaz o úkonu (záznamy, dokumenty, logy, vazba na spis/evidenci).
- MĚLO BY jaká data jsou potřeba pro každý krok procesu, odkud pocházejí, kdo je vlastníkem a za jakých podmínek jsou dostupná.
- MĚLO BY která data jsou referenční (autorita), která jsou odvozená a která jsou pouze dočasná (pracovní).
- MĚLO BY integrace a interoperabilitu: jaké systémy/registry se dotýkají služby a jaké rozhraní se použije (na úrovni rozhodnutí, ne detailního technického návrhu).
- MĚLO BY pravidla kvality dat (minimální standard) a postup při nekvalitních/konfliktních datech (včetně dopadu na UX a provoz).
- MĚLO BY pokud se migrují data: zda je migrace nutná, jaký je rozsah, odpovědnosti, kritéria úspěchu a plán ověření.
- NEMĚLO BY zahájit realizaci, pokud nejsou potvrzeni vlastníci klíčových datových zdrojů a není rozhodnuto, jak se získají data pro kritické scénáře.

POZOR

„Proces“ není BPMN diagram pro archiv. Proces by měl být použitelný pro zadání, testování a provoz: musí obsahovat výjimky, lhůty, odpovědnosti a datové zdroje.

„Data“ nejsou „tabulky v databázi“. Data jsou evidenční fakta a dokumenty, které musí být dohledatelné a obhajitelné.

5.2 Výstupy / důkazy

TABULKA 1 – Process & Data pack (povinné důkazy)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Mapa end-to-end procesu (L0)	Kroky od spouštěče po výsledek, hlavní větve, odpovědnosti (útvary/role), vstupy/výstupy, kanály	Věcný gestor služby; koordinace: PM	Před zadáním implementace	Základ pro rozsah, testy, provozní scénáře	Brána před realizací	Evidence pack – Procesy a data
Detailní proces pro kritické scénáře (L1)	Pro každý kritický scénář: kroky, výjimky, lhůty, rozhodovací body, požadované dokumenty/údaje	Věcný gestor + dotčené útvary; koordinace: PM	Před návrhem detailního řešení a testů	Podklad pro akceptační kritéria a testování	Brána před realizací a brána před převzetím	Evidence pack – Procesy a data

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Datová inventura (Data inventory)	Seznam datových prvků a dokumentů, zdroj (registr/systém), vlastník, právní titul přístupu, kvalita, frekvence aktualizace	Datový vlastníci + věcný gestor; koordinace: PM	Před zadáním integrací a před realizací	Zabraňuje překvapení v integracích a v kvalitě dat	Brána před realizací	Evidence pack – Procesy a data
Rozhodnutí o referenčních datech (Authority)	Co je autoritní zdroj pro klíčové údaje; pravidla při konfliktu; kdo rozhoduje o opravě	Nositel (podporuje) + věcný gestor + datový vlastníci	Před realizací a před nastavením validací	Zabraňuje sporům o „pravdu“ a chybným rozhodnutím	Brána před realizací	Evidence pack – Procesy a data + Decision log
Koncept integrací (Integration concept – L0)	Seznam integrací: kdo s kým, proč, jaký typ rozhraní (API/ISDS/ruční), režim (online/batch), kritičnost	Architektura + věcný gestor; koordinace: PM	Před zadáním implementace	Podklad pro zadání, plánování a rizika	Brána před realizací	Evidence pack – Procesy a data + Architektura
Pravidla kvality dat a validací (Data quality rules)	Minimální standardy (povinné/volitelné, formáty, rozsahy, konzistence), reakce na nekvalitu, odpovědnost	Věcný gestor + datový vlastníci; UX (dopad na uživatele)	Před implementací formulářů/validací	Zabraňuje provozu na nekvalitních datech	Brána před převzetím	Evidence pack – Procesy a data + UX/obsah
Plán migrace a ověření (pokud relevantní)	Rozsah migrace, mapování, kritéria úspěchu, ověřovací postup, rollback, odpovědnosti	Architektura/technické role v projektu; schvaluje Řídicí výbor projektu dle pravidel	Před realizací migrace a před převzetím	Snižuje riziko ztráty dat a incidentu po go-live	Brána před převzetím a go-live	Evidence pack – Procesy a data + Řízení projektu
Důkaz provozní dohledatelnosti (audit trail)	Co se loguje, kde, jak se dohledá konkrétní případ; vazba na spis/evidenci; export	Provoz + bezpečnost + věcný gestor; koordinace: PM	Před go-live	Obhajitelnost, kontroly, incidenty, stížnosti	Brána před go-live	Evidence pack – Provoz + Bezpečnost + Procesy a data

TIP
Udržujte proces a data v přímé vazbě na kritické scénáře z kapitoly „Co je digitální služba“ a na akceptační kritéria. Proces bez testu a data bez vlastníka nejsou použitelné důkazy.

Datová inventura, mapy procesů a toků a evidence sdílených údajů se ukládají do sběrného místa (ISDR), aby byly opakovaně použitelné a datově vyhodnotitelné.

5.3 Hlavní obsah kapitoly

5.3.1 Datová inventura a vlastnictví dat (minimální rozhodnutí)

Data ownership se eviduje jako rozhodovací artefakt: datová entita, zdroj, vlastník, právní titul, kvalita dat, sdílení, zápis, přístupová oprávnění a odpovědnost za opravu chyb.

TABULKA 2 – Šablona datové inventury (minimální pole pro klíčové datové prvky)

Datový prvek / dokument	Kde se používá (krok procesu)	Zdroj (registr/systém/uživatel)	Vlastník zdroje (OVM/útvár)	Autorita (ANO/NE)	Právní titul přístupu / sdílení	Kvalita a známá rizika	Fallback (když data nejsou)
-------------------------	-------------------------------	---------------------------------	-----------------------------	-------------------	---------------------------------	------------------------	-----------------------------

TIP

U každého klíčového datového prvku uveďte fallback: co se stane, když údaj není dostupný, je konfliktní nebo zastaralý. Fallback by měl mít dopad na proces i UX (co uvidí uživatel a co udělá úřad).

5.3.2 Rozhodnutí o „pravdě“ (autoritě) a řešení konfliktů dat

Checklist – pravidla autority dat by měla být stanovena pro klíčové údaje:

- MĚLO BY být určeno, který zdroj je autoritní (registr/systém) a kdy se použije.
- MĚLO BY být určeno, co se stane při konfliktu (které údaje mají přednost, kdo rozhodne a jak se provede oprava).
- MĚLO BY být určeno, kdo může údaj opravit (v jakém systému) a jak se oprava promítne do služby.
- MĚLO BY být určeno, jak se konflikt projeví uživateli (transparentní informace + další krok).
- NEMĚLO BY se rozhodování o konfliktu přenést na uživatele bez právního a procesního zdůvodnění

ČASTÁ CHYBA

Služba zobrazí konflikt dat a žádá uživatele „vyberte správnou hodnotu“. Bez procesního pravidla je to neobhajitelné a často vede k nesprávným údajům a sporům.

5.3.3 Interoperabilita a integrace (koncept – minimum pro zadání)

TABULKA 3 – Koncept integrací (L0) – minimum pro rozhodnutí a zadání

Integrace	Účel v procesu	Zdroj → cíl	Režim (online/batch/ručně)	Kritičnost (kritická/nekritická)	Vlastník rozhraní	Fallback / degradace
-----------	----------------	-------------	----------------------------	----------------------------------	-------------------	----------------------

Checklist – integrace by měla mít před startem realizace rozhodnutí:

- MĚLO BY účel (k čemu slouží v konkrétním kroku procesu) a dopad při výpadku.
- MĚLO BY vlastníka rozhraní a potvrzenou součinnost (kontaktní bod, okna, SLA/OLA pokud relevantní).
- MĚLO BY degradační režim: co se stane, když integrace nefunguje (uživatel, úřad, lhůty).
- NEMĚLO BY být kritické scénáře závislé na integraci bez fallbacku a bez rozhodnutí o dopadu na lhůty a provoz.

POZOR

Interoperabilita je řízené riziko. Kritická integrace bez potvrzeného vlastníka a bez fallbacku je důvodem pro STOP na bráně před realizací.

5.3.4 Kvalita dat a validace (minimální standard pro provoz)

Checklist – pravidla kvality dat by měla obsahovat minimálně:

- MĚLO BY pravidla úplnosti (co je povinné), formátu (např. datum, identifikátory) a konzistence (např. vazby mezi údaji).
- MĚLO BY pravidla pro historizaci a časovou platnost (kdy je údaj „aktuální“).
- MĚLO BY pravidla pro manuální doplnění/opravu (kdo, kde, kdy) a jak se změna eviduje.
- MĚLO BY pravidla pro práci s chybami: uživatelská chyba vs. chyba zdroje vs. technická chyba.
- MĚLO BY dopad na UX: jak uživatel dostane srozumitelnou informaci a jaký je další krok.
- NEMĚLO BY být validace nastaveny tak, že blokují službu kvůli známé nekvalitě zdroje bez alternativního postupu.

TIP

Když zdroj dat občas vrací nekonzistenci, řešení není „validaci vypnout“. Řešení je: řízený fallback + evidence + proces opravy.

5.3.5 Migrace dat a přechod (cutover) – doporučené minimum, pokud se migruje

Checklist – pokud je součástí změny migrace, mělo by být splněno:

- MĚLO BY být rozhodnuto, co se migruje (rozsah), co se nemigruje a proč.
- MĚLO BY být definována mapování (zdroj → cíl) a pravidla pro duplicity a konflikty.

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- MĚLO BY být definována kritéria úspěchu migrace (měřitelná) a ověřovací postup (sampling + plný kontrolní průchod pro kritické položky).
- MĚLO BY být definován rollback / návratový postup a kdo rozhoduje o spuštění/vrácení.
- MĚLO BY být rozhodnuta dočasná paralelní evidence (pokud je nutná) a jak dlouho potrvá.

ČASTÁ CHYBA

Migrace se nechá „na konec“ a řeší se jako technický sprint. Následně se zjistí chybějící vazby na případy, dokumenty nebo historii.

5.3.6 Dohledatelnost a důkazy (audit trail) – minimum pro obhajitelnost

Checklist – služba by měla umožnit dohledat alespoň:

- MĚLO BY identifikaci případu (jednoznačný identifikátor) a jeho stav v čase.
- MĚLO BY kdo jednal (uživatel/úředník/systém), kdy a s jakým oprávněním (odkaz na mechanismus identity/role).
- MĚLO BY co bylo podáno nebo přijato (obsah, dokumenty) a jak bylo doručeno/potvrzeno.
- MĚLO BY jaké rozhodnutí bylo učiněno a na základě jakých dat (minimálně odkazy na zdroje/údaje).
- MĚLO BY kde je dokumentace případu vedena (vazba na evidenci/spis) a jak se exportuje pro kontrolu.

POZOR

Audit trail je provozní požadavek. Pokud neexistuje dohledatelnost, nelze službu bezpečně provozovat ani obhájit.

Při návrhu procesů a dat se uplatňuje princip „only once“: klient nemá opakovaně dokládat údaje, které stát již má v jiných agendových informačních systémech. V datové inventuře se proto identifikují údaje dostupné z jiných AIS a navrhnou se jejich sdílení namísto opětovného vyžádání od klienta, a to bez ohledu na využitý obslužný kanál.

6 UX, obsah a přístupnost

Účelem kapitoly je zajistit, aby digitální služba byla navržena tak, že ji uživatel reálně dokončí (včetně výjimek), porozumí tomu, co se děje a co bude následovat, a aby byla prokazatelně přístupná. Kapitola stanoví minimální doporučené rozhodnutí a důkazy pro UX návrh, obsah a přístupnost tak, aby mohly být použity jako závazné vstupy do zadání, akceptace a go-live, a aby úřad udržel kontrolu nad službou i po spuštění (změny textů, scénářů, formulářů). Kapitola je navržena pro praxi veřejné správy: kombinace kanálů, povinnost vysvětlovat právní účinky, časté výjimky, a nutnost obhájit rozhodnutí i v případě stížnosti nebo kontroly.

6.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zadáním implementace a před převzetím rozhodnout a doložit:

- MĚLO BY které uživatelské scénáře jsou závazné pro převzetí (kritické scénáře) a které výjimky musí být obslouženy digitálně, včetně návratových stavů.
- MĚLO BY jaké jsou akceptační podmínky UX, obsahu a přístupnosti (Definition of Done pro službu, nikoliv jen pro UI prvky).
- MĚLO BY jaké texty mají právní význam (poučení, prohlášení, informace o zpracování údajů, rozhodné informace pro lhůty) a kdo je schvaluje.
- MĚLO BY jak je řešena komunikace se službou: potvrzení, stavové obrazovky, notifikace, chyby a kontakt/eskalace (uživatelsky i provozně).
- MĚLO BY na jakých datech se ve službě rozhoduje a jak se to projevuje v UX (co uživateli předvyplňujeme, co ověřujeme, co požadujeme).
- MĚLO BY minimální standard přístupnosti: co se testuje, jakými metodami, na jakých scénářích, a jak se dokládá splnění.
- NEMĚLO BY předat dodavateli implementaci UI bez schválené informační architektury/flow pro kritické scénáře a bez schválených akceptačních kritérií.

POZOR

UX/obsah/přístupnost nejsou estetika. Jsou to převzatelná a auditovatelná kritéria služby.

Pokud úřad nemá akceptační kritéria a důkazy, nemá reálně možnost službu převzít nebo odmítnout a vzniká vendor lock-in.

6.2 Výstupy / důkazy

TABULKA 1 – UX/Obsah/Přístupnost pack (povinné důkazy pro FULL)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede (evidence pack)
Seznam kritických scénářů a výjimek	Pro každý scénář: spouštěč, kroky, výsledek, výjimky, potvrzení/stavy, data a dokumenty, akceptační podmínky	Věcný gestor služby; koordinace: Projektový manažer	Před zadáním implementace; průběžně aktualizovat při změnách	Praktické vymezení toho, co je „služba“ a co se testuje	Brána před realizací; brána před převzetím	UX/obsah/přístupnost + Řízení projektu
Mapa uživatelské cesty (service journey)	End-to-end cesta včetně kanálových přechodů, stavů, notifikací, podpory a „co se děje v úřadu“	Věcný gestor + UX/obsah	Před uzavřením rozsahu a zadáním implementace	Zabraňuje „jen formuláři“; dává podklad pro provoz	Brána před realizací	UX/obsah/přístupnost
Informační architektura + flow (IA/flow)	Seznam obrazovek a kroků, navigace, návratové cesty, stavové obrazovky, chybové stavy	UX/obsah + věcný gestor; koordinace: PM	Před implementací UI	Základ pro zadání, testy a akceptaci	Brána před realizací	UX/obsah/přístupnost
Wireframy / prototyp pro kritické scénáře	Minimálně: rozložení, hierarchie, formuláře, potvrzení, chyby, stavy, notifikace; varianty pro výjimky	UX; schvaluje věcný gestor	Před implementací UI; před začátkem vývoje klíčových obrazovek	Redukce změn v realizaci; podklad pro testování	Brána před realizací	UX/obsah/přístupnost
Content pack (schválené texty)	Názvy kroků, instrukce, popisky, chybové hlásky, potvrzení, notifikace, poučení a právně významné informace; verze a schválení	Věcný gestor + obsah; právní schvaluje právně významné texty	Návrhová verze před testováním; schválená verze před go-live	Jeden zdroj pravdy pro texty; přejímka a provozní změny	Brána před převzetím; brána před go-live	UX/obsah/přístupnost + Právo
Katalog chyb a stavů (Error & State catalogue)	Seznam chybových stavů a stavových informací: spouštěč, text, další krok, logování, dopad na proces a lhůty	UX/obsah + věcný gestor; provoz pro eskalace	Před testováním a před převzetím	Zajišťuje, že výjimky nejsou řešeny ručně mimo systém	Brána před převzetím	UX/obsah/přístupnost + Provoz
Plán a protokoly uživatelského testování	Metoda, vzorek, scénáře, zjištění, nápravná opatření, rozhodnutí o zbytkových problémech	UX + věcný gestor; koordinace: PM	Minimálně jednou před převzetím; u zásadních změn opakovat	Důkaz použitelnosti pro kritické scénáře	Brána před převzetím	UX/obsah/přístupnost + Decision log
Přístupnostní plán a důkaz splnění	Požadavky, metody testů (klávesnice, asistivní)	UX/obsah (požadavky) + dodavatel	Plán před realizací; důkaz před převzetím a go-live	Prokazuje splnění přístupnosti a eliminuje	Brána před převzetím; brána před go-live	UX/obsah/přístupnost

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede (evidence pack)
	technologie, automatizované), výstupy, nápravy, zbytková rizika	(implementace) + úřad (ověření)		právní/komunikační riziko		
Návrh informací pro podporu a zpětnou vazbu	Kontakty, kanály, SLA očekávání, formulář pro hlášení problému, postup eskalace	Provoz + věcný gestor; koordinace: PM	Před go-live	Zajišťuje, že uživatel má jasnou cestu při problému	Brána před go-live	Provoz + UX/obsah/přístupnost
TIP Vedení evidence: každý artefakt má vlastníka, verzi, datum schválení a vazbu na Decision log (co bylo rozhodnuto a proč). Bez řízení verzí vzniká v zadání a akceptaci konflikt „co platí“.						

Výstupy návrhu UX, obsahu a přístupnosti se ukládají do sběrného místa (ISDŘ) jako verzované artefakty navázané na konkrétní službu.

6.3 Hlavní obsah kapitoly

6.3.1 Mapa uživatelské cesty (service journey) – doporučený standard

Checklist – mapa uživatelské cesty by měla obsahovat:

- MĚLO BY spouštěč služby (proč uživatel přichází) a očekávaný výsledek v uživatelských slovech.
- MĚLO BY kroky uživatele, kroky úřadu (backstage) a mezistavy (čekání, doplnění, odmítnutí).
- MĚLO BY kanálové přechody (web/mobil/přepážka/telefon/datová schránka) a co se v přechodu ztrácí/nesmí ztratit.
- MĚLO BY informování uživatele: potvrzení, stav, notifikace a kde je „jeden zdroj pravdy“ o stavu.
- MĚLO BY místa, kde vznikají důkazy (podání, doručení, rozhodnutí) a jak je uživatel informován.
- MĚLO BY kontaktní bod a postup při problému (podpora) pro kritické kroky.

6.3.2 Přístupnost – doporučený standard a důkazy

Checklist – přístupnost by měla být řešena jako součást návrhu, implementace i akceptace:

- MĚLO BY být definován rozsah přístupnosti: které kanály a části služby se posuzují (web, mobil, dokumenty, vložené prvky).
- MĚLO BY být provedeno testování na kritických scénářích: klávesnice, fokus, formuláře, stavové zprávy, kontrast a struktura.
- MĚLO BY být proveden alespoň jeden scénářový spot-check s asistivní technologií (např. čtečka obrazovky) na klíčových obrazovkách.
- MĚLO BY být opraveny zjištěné chyby, nebo musí existovat rozhodnutí o zbytkových odchylkách (s dopadem a plánem nápravy) v Decision logu.
- MĚLO BY být zajištěna přístupnost dokumentů poskytovaných službou (pokud služba generuje nebo vyžaduje dokumenty).
- NEMĚLO BY být přístupnost posouzena pouze automatizovaným nástrojem bez scénářového a klávesnicového testu.

TABULKA 6 – Matice testů přístupnosti (minimum)

Test	Co se ověřuje	Na čem (scénáře/stránky)	Kdo provádí	Důkaz (co se ukládá)	Akceptační pravidlo
Klávesnicový průchod	Ovládání bez myši, fokus, pořadí, pasti	Všechny kritické scénáře	Úřad + dodavatel	Protokol + seznam vad + nápravy	Bez vad blokujících průchod scénářem
Formuláře a chyby	Popisky, asociace chyb k polím, srozumitelnost, rekapitulace	Formuláře v kritických scénářích	Úřad + dodavatel	Protokol + screenshoty/odkazy + opravy	Chyby musí být opravitelné sdělené

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Test	Co se ověřuje	Na čem (scénáře/stránky)	Kdo provádí	Důkaz (co se ukládá)	Akceptační pravidlo
Kontrast a čitelnost	Čitelnost textu, informace ne pouze barvou	Klíčové obrazovky a komponenty	Dodavatel; kontrola: úřad	Výstup kontroly + nápravy	Bez vad znemožňujících čitelnost
Struktura a názvy prvků	Nadpisy, landmarky, názvy tlačítek a odkazů	Klíčové obrazovky	Dodavatel; kontrola: úřad	Výstup + nápravy	Ovládací prvky jsou jednoznačně identifikované
Stavové zprávy	Potvrzení odeslání, změny stavu, live regiony	Odeslání a stavové obrazovky	Úřad + dodavatel	Protokol + nápravy	Uživatel je informován i bez vizuálních signálů
Spot-check s asistivní technologií	Průchod scénářem se čtečkou obrazovky (min. 1–2 scénáře)	Nejdůležitější scénáře	Úřad (ověření)	Krátký protokol + zjištění + nápravy	Bez vad blokujících dokončení scénáře

POZOR

Přístupnost se prokazuje důkazem: protokoly testů, seznam vad, rozhodnutí o zbytkových odchylkách a jejich plán. Bez toho nelze přístupnost obhájit ani řídit.

7 Architektura, bezpečnost, provoz

7.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před zahájením realizace a před go-live rozhodnout a doložit zejména:

- MĚLO BY základní architektonické vymezení služby (kontext, hranice, hlavní komponenty, integrace, datové toky).
- MĚLO BY bezpečnostní klasifikaci služby a dat (dopad na opatření, audit, logging, přístupová práva).
- MĚLO BY model identity a řízení přístupů (uživatelé, role, zastoupení; administrace; revize oprávnění).
- MĚLO BY minimální bezpečnostní opatření (řízení zranitelností, šifrování, segmentace, zálohování, hardening, logování).
- MĚLO BY provozní model: kdo službu provozuje, jaké jsou SLA/OLA, jak se řeší incidenty, změny a dostupnost.
- MĚLO BY monitoring a observabilitu (co měříme, jak detekujeme incident, kdo reaguje) a postup při výpadku integrací (degradace).
- MĚLO BY předávací a přejímací podmínky do provozu (důkazy bezpečnosti a provozuschopnosti).
- NEMĚLO BY jít do go-live bez schváleného provozního modelu, bez ověřeného zálohování/obnovy a bez schopnosti dohledat incidenty a právně relevantní události.

POZOR

Architektura není výkres pro dodavatele. Architektura je rozhodnutí o hranicích a odpovědnostech: co je součástí služby, na čem služba závisí a kdo nese rizika.

Bez provozního modelu a bezpečnostních důkazů je go-live neobhájitelný a vzniká provozní i právní dluh.

7.2 Výstupy / důkazy

TABULKA – Architecture/Security/Operations pack (povinné důkazy)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede (evidence pack)
Architektonický kontext a hranice služby (LO)	Kontext (systémy/registry/aktéři), hranice služby, hlavní	Architektura; spolupráce: věcný gestor, bezpečnost,	Před zadáním realizace (před zahájením implementace)	Podklad pro zadání, rizika, odpovědnosti, náklady na provoz	Brána před realizací	Architektura + Řízení projektu

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede (evidence pack)
	komponenty, integrace, datové toky (L0)	provoz; koordinace: PM				
Bezpečnostní klasifikace služby a dat	Klasifikace (citlivost, dopady), požadavky na opatření, logování, uchování, audit	Bezpečnost (CISO/odpovědný útvar) + věcný gestor; PM koordinuje	Před návrhem bezpečnostních opatření a před realizací	Základ pro rozsah opatření a ověření	Brána před realizací	Bezpečnost + Právo a compliance
Model identity a přístupů (IAM)	Role, oprávnění, administrace, zastoupení, revize oprávnění, logování přístupů	Bezpečnost + věcný gestor; architektura; provoz	Před implementací přihlášení/rolí	Zabraňuje zneužití a sporům o oprávnění	Brána před realizací	Bezpečnost + UX/obsah
Bezpečnostní požadavky a opatření (security baseline)	Šifrování, hardening, segmentace, správa tajemství, zranitelnosti, patching, logging, WAF/ochrany (dle prostředí)	Bezpečnost + architektura; dodavatel implementuje; úřad ověřuje	Před realizací; průběžně	Podklad pro implementaci a akceptaci bezpečnosti	Brána před převzetím; brána před go-live	Bezpečnost + Architektura
Plán testování bezpečnosti a výsledky (minimální)	Typy testů (zranitelnosti, konfigurace, penetrační test dle rizika), nálezy, nápravy, rozhodnutí o zbytkových rizicích	Bezpečnost; dodavatel poskytuje součinnost; PM koordinuje	Plán před testy; výsledky před převzetím/go-live	Důkaz bezpečnosti pro převzetí	Brána před převzetím; brána před go-live	Bezpečnost + Decision log
Provozní model služby (Operating model)	Provozní role a odpovědnosti, SLA/OLA, incident management, změny, release, údržba, okna, eskalace	Provozní útvar; věcný gestor; PM koordinuje	Před go-live (pracovní) a schválený před go-live	Zajišťuje provozuschopnost a kontinuitu	Brána před go-live	Provoz + Řízení služby
Monitoring a alerting (observabilita)	Co se měří (dostupnost, výkon, chybovost, integrace), prahy, alarmy, kdo reaguje, runbook	Provoz + bezpečnost; dodavatel implementuje dle zadání	Před go-live	Detekce incidentů a degradací	Brána před go-live	Provoz + Bezpečnost
Plán zálohování a obnovy (Backup & Restore)	Co se zálohuje, frekvence, RPO/RTO, test obnovy, odpovědnosti	Provoz + architektura; dodavatel dle prostředí	Před go-live; test obnovy před go-live	Kontinuita a prevence ztráty dat	Brána před go-live	Provoz + Bezpečnost
Degradační režimy (výpadek integrací)	Pro kritické integrace: co se stane při výpadku, jaký je fallback, informace uživateli, dopad na lhůty	Architektura + provoz + věcný gestor; UX/obsah pro komunikaci	Před go-live (a před testováním)	Zabraňuje chaosu při výpadcích a sporům	Brána před go-live	Provoz + Procesy a data + UX/obsah
Předávací protokol do provozu (handover)	Seznam předaných artefaktů, přístupy, dokumentace, runbooky, kontakty, školení, backlog známých problémů	PM + provoz; dodavatel poskytuje; věcný gestor potvrzuje	Před go-live	Formální převzetí a odpovědnost	Brána go-live	Řízení projektu + Provoz

TIP

Ověření obnovy (restore) by mělo být provedeno jako reálný test. „Máme zálohy“ bez testu obnovy není důkaz.

Architektonické a bezpečnostní výstupy včetně nefunkčních požadavků (NFR) se ukládají do sběrného místa (ISDR) strukturovaně a verzovaně.

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

7.3 Hlavní obsah kapitoly

7.3.1 Architektura služby (L0) – doporučený obsah a rozhodnutí

Checklist – architektonické vymezení by mělo obsahovat:

- MĚLO BY kontext: aktéři (uživatel, úředník, systémy/registry), hranice služby a dotčené externí služby.
- MĚLO BY hlavní komponenty (front-end, back-end, integrační vrstva, evidence/spisové vazby) a jejich odpovědnosti.
- MĚLO BY datové toky: odkud kam se přenáší klíčová data, kde se ukládají a kde vzniká důkaz/auditní stopa.
- MĚLO BY integrace: seznam a kritičnost; odkazy na degradační režimy.
- MĚLO BY provozní vymezení: kdo co provozuje (úřad vs dodavatel), kde běží prostředí, kdo má přístup.
- NEMĚLO BY být architektura neurčitá v hranicích odpovědnosti (kdo nese riziko a kdo řeší incident).

TABULKA 2 – Architektonické rozhodnutí (decision list) – minimum

Rozhodnutí	Varianty	Zvolená varianta + odůvodnění	Dopady (bezpečnost, provoz, náklady)	Schválil / datum
Hranice služby (co je součástí)	A) pouze portál/formulář, B) portál + procesní back-end, C) end-to-end včetně spisové vazby			
Režim integrací	A) online, B) batch, C) kombinace, D) ruční fallback			
Umístění a provoz prostředí	A) interní infrastruktura, B) cloud dle pravidel, C) externí hosting s odpovědností dodavatele			
Evidence a auditní stopa	A) jen v aplikaci, B) aplikace + centrální log, C) aplikace + spis/evidence + centrální log			

POZOR

Architektonická rozhodnutí musí být zaznamenána v Decision logu a použita v zadání. Pokud nejsou závazná, dodavatel dodá vlastní řešení, které nemusí být provozovatelné v podmínkách úřadu.

7.3.2 Bezpečnostní baseline – doporučené minimum (bez ohledu na dodavatele)

Checklist – bezpečnostní opatření by měla zahrnout minimálně:

- MĚLO BY řízení identity a přístupů (IAM): autentizace, autorizace, správa rolí, revize oprávnění, audit přístupů.
- MĚLO BY logování a auditní stopu: bezpečnostní události, administrace, přístupy k citlivým datům, integrace, chyby.
- MĚLO BY šifrování dat v přenosu a dle klasifikace i v úložišti; správa klíčů/tajemství.
- MĚLO BY hardening a bezpečnou konfiguraci prostředí (minimální služby, aktualizace, segmentace, ochrany).
- MĚLO BY řízení zranitelnosti: pravidelné skeny, evidence nálezů, nápravy a rozhodnutí o zbytkovém riziku.
- MĚLO BY bezpečné zacházení s dokumenty a přílohami (typy, antivirová kontrola, limity, ukládání).
- MĚLO BY ochranu proti zneužití (rate limiting, ochrana formulářů, detekce anomálií) dle rizika.
- NEMĚLO BY být přístup do produkce sdílený, neauditovaný nebo bez revize oprávnění.

ČÁSTÁ CHYBA

Logování se implementuje, ale nikdo ho nečte a neexistuje postup reakce. Log bez runbooku je jen úložiště dat.

7.3.3 Identity a řízení přístupů (IAM) – minimum pro veřejnou službu

Checklist – IAM by měl řešit:

- MĚLO BY uživatelskou identitu a oprávnění (včetně zastoupení, pokud je relevantní pro agendu).
- MĚLO BY administrátorské účty a jejich ochranu (oddělené účty, MFA, audit).
- MĚLO BY životní cyklus oprávnění: přidělení, změna, odebrání, periodická revize.
- MĚLO BY princip nejmenších oprávnění a oddělení rolí (minimálně pro kritické operace).

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- MĚLO BY logování přístupů k citlivým údajům a administrátorských akcí.

TABULKA 3 – Matice rolí a oprávnění (minimum)

Role	Co může dělat	Na jakých datech	Kritické akce (vyžadují audit)	Kdo přiděluje/odebírá	Revize (jak často)
POZOR Role a oprávnění jsou provozní schopnost. Pokud chybí revize a audit, vzniká bezpečnostní incident „na časové ose“.					

Z pohledu architektury a bezpečnosti se počítá i s přístupem AI asistentů a agentů ke službě (např. prostřednictvím rozhraní/API), s autentizací a autorizací jednatelů asistenta nebo agenta na základě zmocnění a s evidencí, kdo a v jaké roli úkon provedl. Nefunkční a bezpečnostní požadavky se navrhuji tak, aby tento způsob vyřízení služby umožnily a zároveň ošetřily jeho rizika.

8 Kontrolní brány a rozhodování

Účelem kapitoly je nastavit závazný systém kontrolních bran (STOP/GO) a rozhodování tak, aby digitální služba nevstoupila do realizace ani do provozu bez splnění minimálních podmínek práva, procesu a dat, UX/přístupnosti, architektury/bepečnosti a provozu. Kapitola definuje, jaké rozhodnutí se v jednotlivých branách přijímá, jaké důkazy musí existovat, jak se řídí výjimky a jak se eskalují sporná rozhodnutí v rámci řízení ICT projektu. Kapitola je kompatibilní s Metodikou řízení ICT projektů: brány jsou nadstavbou rozhodovacích „gate“ v projektu, nikoliv paralelním procesem.

8.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl zavést a používat minimálně tyto rozhodovací brány Digital First (DF):

- MĚLO BY DF-1: Brána před zahájením realizace – rozhodnutí, že zadání je úplné a služba je realizovatelná bez neobhájitelných rizik.
- MĚLO BY DF-2: Brána před převzetím – rozhodnutí, že služba je převzatelná a splňuje minimální důkazy (testy, bezpečnost, přístupnost, dohledatelnost).
- MĚLO BY DF-3: Brána go-live – rozhodnutí, že službu lze spustit do produkce bez kritických otevřených vad a s provozním modelem.
- MĚLO BY DF-4: Brána po stabilizaci – rozhodnutí o ukončení zvýšené podpory a přechodu do standardního řízení služby.
- NEMĚLO BY proběhnout go-live bez formálního rozhodnutí DF-3 a bez kompletního Evidence packu pro brány DF-1 až DF-3.
- MĚLO BY – být stanoveno, kdy je rozhodnutí vráceno k přepracování (STOP), a kdy je povolena podmíněná akceptace (GO s podmínkami).

POZOR

Brána není prezentace. Brána je formální rozhodnutí založené na důkazech. Pokud brána není schopna odůvodnit GO/STOP, nejde o bránu, ale o informativní schůzku.

8.2 Výstupy / důkazy

TABULKA 1 – Doporučené důkazy pro řízení bran a rozhodování (Evidence & Decision pack)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Decision log (záznam rozhodnutí)	Datum, rozhodnutí, varianty, odůvodnění, vstupní artefakty, akceptovaná rizika, schválil	Projektový manažer; schvalují rozhodovací orgány dle Metodiky řízení ICT projektů	Od DF-1 průběžně; uzavřený před DF-3	Auditovatelnost a řízení změn	DF-1 až DF-4	Řízení projektu – Decision log

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Gate checklisty (DF-1 až DF-4)	Seznam povinných bodů (by měl/by neměl/MĚLO BY), stav splnění, odkaz na důkazy	PM + věcný gestor; validuje dotčený útvar (právní/bezpečnost/provoz/UX)	Před každou branou	Standardizace rozhodnutí, zabránění selektivnímu „vynechávání“	DF-1 až DF-4	Řízení projektu – Gate pack
Evidence pack index (rejstřík důkazů)	Seznam všech povinných artefaktů s verzí a umístěním; vazba na kapitoly 1–6	PM	Před DF-1 (verze 1); aktualizace před DF-2 a DF-3	Zajišťuje, že důkazy jsou dohledatelné	DF-1 až DF-3	Evidence pack – rejstřík
Registr rizik a rozhodnutí o riziku	Rizika, hodnocení, opatření, vlastník, termíny; záznam akceptace rizika a kdo ji schválil	PM; vlastníci rizik dle projektu	Před DF-1; aktualizace před DF-2, DF- 3	Řízení tolerancí a eskalace	DF-1 až DF-3	Řízení projektu – rizika
Seznam otevřených vad a dluhů (open issues / known limitations)	Seznam vad, závažnost, dopad, workaround, termín nápravy, rozhodnutí o akceptaci	PM + dodavatel; schvaluje dle pravidel projektu	Před DF-2 a DF-3; uzavřený před DF-4	Podmíněná akceptace a kontrola dluhů	DF-2 až DF-4	Řízení projektu – issues
Go-live readiness report	Souhrn splnění DF-3, otevřené vady, provozní připravenost, komunikační plán, rollback, kontakty	PM + provoz; přispívají bezpečnost, UX, architektura, právní	Před DF-3	Jednotný podklad pro GO/STOP	DF-3	Řízení projektu + Provoz

TIP

Evidence pack musí být založen tak, aby přežil personální změny. Dokumenty a protokoly by se neměly držet „u lidí“ v e-mailu; musí být v evidenci projektu se stabilním odkazem.

Rozhodnutí kontrolních bran a jejich důkazy se evidují ve sběrném místě (ISDŘ) tak, aby byla rozhodnutí dohledatelná a auditovatelná.

8.3 Hlavní obsah kapitoly

8.3.1 Model bran Digital First

Standard gate packu

Každá kontrolní brána má mít jednotný gate pack: rozhodnutí, odkaz na master index důkazů, relevantní checklisty, decision log, rizika, otevřené podmínky, vlastníka uzavření a termín další kontroly.

Decision log se nepoužívá izolovaně. Každé rozhodnutí, které ovlivňuje rozsah, právo, data, bezpečnost, UX, dodavatele, provoz nebo termín, se naváže na příslušný checklistový bod a kontrolní bránu.

TABULKA 2 – Přehled bran a minimálních rozhodnutí

Brána	Kdy (typicky)	Rozhodnutí (co podporuje)	Minimální důkazy (souhrn)	Výsledek	Možné varianty	Stop trigger (typické)	Poznámka k řízení
DF-1: Před zahájení	Před zadáním implementace / před	Zadání je úplné a testovatelné; klíčová	Service definice + právní konstrukce + proces/data + UX/obsah/přístupnost +	STOP/GO	GO / GO s podmínkami / STOP	Chybí vlastníci dat/integrací; neuzavřená právní	GO s podmínkami jen s

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Brána	Kdy (typicky)	Rozhodnutí (co podporuje)	Minimální důkazy (souhrn)	Výsledek	Možné varianty	Stop trigger (typické)	Poznámka k řízení
m realizace	zahájením vývoje	rozhodnutí kapitol 1–6 jsou uzavřena	architektura/bezpečnost/provoz (min. LO)			konstrukce; nejsou akceptační kritéria; chybí arch. hranice	termínem a vlastníkem
DF-2: Před převzetím	Před akceptací a předávkou do provozu	Služba je převzatelná: testy, přístupnost, bezpečnost, dohledatelnost, provozní připravenost	Protokoly testů (funkční, scénářové) + přístupnost + bezpečnostní testy + monitoring/runbooky + evidence	STOP/GO	GO / GO s omezením / STOP	Kritické vady; chybí důkaz přístupnosti; bezpečnostní kritické nálezy; není test obnovy	GO s omezením = omezení funkce s jasnou komunikací
DF-3: Go-live	Bezprostředně před spuštěním do produkce	Lze bezpečně spustit: provozní model je aktivní, rollback je připraven, komunikace je hotová	Go-live readiness report + go-live checklist + rollback plan + kontakty + stav integrací	GO/STOP	GO / STOP	Neexistuje rollback; monitoring není v provozu; nejasné odpovědnosti; neuzavřené kritické dluhy	Rozhodnutí musí být zaznamenáno v Decision logu
DF-4: Po stabilizaci	Po domluvené době zvýšené podpory	Zvýšená podpora končí; přechod do standardního řízení služby; dluhy jsou řízené	Stabilizační report + incidenty a nápravy + předání backlogu + aktualizace runbooků	GO/STOP	GO / STOP (pokračovat ve zvýšené podpoře)	Opakované incidenty; chybí nápravy; monitoring/alerting nefunkční; backlog bez vlastníka	Vazba na kapitolu 9 (řízení služby)

POZOR

„GO s omezením“ je přípustné pouze tehdy, pokud omezení: (1) je jasně definované, (2) je komunikované uživateli a interně, (3) má workaround a (4) má termín odstranění. Jinak je to skrytý STOP.

Souhlas statutárního zástupce před spuštěním služby (součást brány DF-3)

Součástí go-live brány (DF-3) je souhlas statutárního zástupce orgánu veřejné moci nebo jím pověřené odpovědné osoby se spuštěním služby do provozu.

Nejde nutně o osobní testování každého detailu služby statutárem. Odpovědná osoba svým souhlasem potvrzuje, že služba byla ověřena z pohledu klienta, provozu, bezpečnosti, přístupnosti, právního rámce a návazných procesů, a to na základě doložených výstupů (Evidence pack bran DF-1 až DF-3).

8.3.2 STOP trigger a pravidla pro „GO s podmínkami“

TABULKA 3 – Typické STOP trigger (nekompromisní)

Oblast	STOP trigger (příklad)	Dopad	Kde se řeší (v řízení projektu)
Právo	Neuzavřená právní konstrukce; nejasné právní účinky; chybí schválení právně významných textů	Neobhajitelná služba, stížnosti, rušení rozhodnutí	Eskalace dle Metodiky řízení ICT projektů; rozhodnutí orgánu projektu
Proces a data	Chybí vlastník klíčového datového zdroje/integrace; neexistuje fallback pro kritické scénáře	Neprovozovatelnost, ruční obcházení, skluz	Změnové řízení projektu + risk/issue management
UX a přístupnost	Kritický scénář nelze dokončit; chybí důkaz přístupnosti pro kritické scénáře	Nedokončení podání, diskriminace, reputační riziko	Akceptační řízení projektu; nápravný plán

Oblast	STOP trigger (příklad)	Dopad	Kde se řeší (v řízení projektu)
Bezpečnost	Kritické bezpečnostní nálezy bez opravy/akceptace rizika; neauditované přístupy do produkce	Incident, únik dat, sankce, ztráta důvěry	Bezpečnostní řízení + rozhodnutí dle pravidel úřadu
Provoz	Neexistuje test obnovy; chybí monitoring/alerting; nejsou runbooky a kontakty	Neřízený provoz, dlouhé výpadky, chaos při incidentech	Provozní připravenost – STOP do go-live

Checklist – pravidla pro „GO s podmínkami“:

- MĚLO BY být jasně definována podmínka (co přesně bude splněno) a její důkaz (co se doloží).
- MĚLO BY být určen vlastník podmínky a termín splnění (nejpozději k další bráně / před určeným milníkem).
- MĚLO BY být popsán dopad, pokud podmínka nebude splněna (automatický STOP, omezení služby, eskalace).
- MĚLO BY být rozhodnutí zapsáno v Decision logu a být dohledatelné, kdo podmínku schválil.
- NEMĚLO BY jít o podmínku v oblasti STOP triggerů (právo, kritické scénáře, přístupnost, kritické bezpečnostní nálezy, test obnovy).

TIP

U podmíněné akceptace vždy uveďte, zda jde o: (1) odloženou nápravu, (2) omezení funkce, nebo (3) dočasný workaround. Každý typ má jiný dopad na provoz a komunikaci.

Kontrolní brány metodiky se vážou na proces OHA: schválení ICT záměru a vydané stanovisko OHA jsou podmínkou pro průchod příslušnou bránou a brána před spuštěním (DF-3) navazuje na ověření připravenosti služby k provozu. Důkazy shromážděné pro brány jsou zároveň podkladem pro posouzení OHA.

9 Go-live

9.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl před spuštěním rozhodnout a doložit zejména:

- MĚLO BY zda služba je připravena ke spuštění (DF-3: GO/STOP) na základě důkazů, nikoliv pouze prohlášení.
- MĚLO BY jaký je způsob spuštění (např. postupné spuštění, omezené spuštění, plné spuštění) a jak se komunikuje uživatelům.
- MĚLO BY cutover plán: co se kdy nasazuje/migruje/aktivuje, kdo to provádí, jak se ověřuje úspěch a kdo schvaluje další krok.
- MĚLO BY rollback plán: kdy a jak se vrací zpět, co to znamená pro data, jak se komunikuje a kdo rozhoduje.
- MĚLO BY provozní režim prvních týdnů (zvýšená podpora/hypercare): kdo je dostupný, jak se sbírá zpětná vazba a jak se nasazují opravy.
- MĚLO BY způsob prokazování a uchování důkazů o spuštění (logy, konfigurace, protokoly, schválení, verze).
- NEMĚLO BY spustit službu bez aktivního monitoringu/alertingu, bez funkčních kontaktních a eskalačních cest a bez ověřeného rollbacku.

POZOR

Go-live není jen „nasazení verze“. Go-live je převzetí rizika do provozu. Pokud nejsou připraveny provozní schopnosti, dojde k eskalaci incidentů hned v prvních dnech.

9.2 Výstupy / důkazy

TABULKA 1 – Go-live pack (povinné důkazy pro DF-3)

Výstup / důkaz	Minimální obsah	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)		Kde se vede (evidence pack)
Go-live readiness report	Souhrn připravenosti: splnění DF-2,	Projektový manažer + provoz;	Před DF-3	Jednotný podklad pro rozhodnutí	DF-3	Řízení projektu + Provoz

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)		Kde se vede (evidence pack)
	otevřené vady, provozní model aktivní, integrace, rizika, doporučení GO/STOP	příspěvky: věcný gestor, bezpečnost, architektura, UX, právní				
Cutover plán (nasazení + aktivace)	Časová osa kroků, odpovědnosti, kontrolní body, kritéria úspěchu, plán komunikace a omezení, evidence provedení	PM + dodavatel + provoz; schvaluje provoz a věcný gestor	Před DF-3; finální verze před spuštěním	Řízené provedení a dohledatelnost	DF-3	Provoz + Řízení projektu
Rollback plán	Spouštěče rollbacku, kroky návratu, dopad na data a uživatele, časová okna, rozhodovací pravomoc, komunikace	PM + provoz + dodavatel; bezpečnost dle dopadů	Před DF-3; ověřený postup (min. tabletop nebo test) před spuštěním	Zabránění dlouhým výpadkům a improvizaci	DF-3	Provoz + Bezpečnost
Go-live checklist (protokol)	Seznam povinných bodů před/po spuštění, včetně evidence provedení, podpis/odsouhlasení	PM + provoz	Vyplněný v den go-live	Prokazuje, co se skutečně stalo	DF-3	Evidence pack – Go-live
Plán zvýšené podpory (hypercare)	Doba trvání, dostupnost rolí, metriky, denní rytmus, incident postupy, rychlé opravy, komunikační kanály	Provoz + PM; věcný gestor	Před go-live	Stabilizace a řízení očekávání	DF-3; DF-4	Provoz + Řízení služby
Komunikační plán go-live	Cílové skupiny, zprávy, kanály, termíny, odpovědnosti; texty ve službě a mimo službu	Věcný gestor + obsah/UX; PM koordinuje	Před go-live	Minimalizace dotazů a chyb uživatelů	DF-3	UX/obsah + Provoz
Provozní nastavení monitoringu/alertingu	Aktivní monitoring, alarmy, kontakty, runbooky, korelační ID a dohledatelnost; ověření funkcí	Provoz + bezpečnost; dodavatel poskytuje součinnost	Před go-live a aktivní při go-live	Detekce problémů v reálném čase	DF-3	Provoz + Bezpečnost
Záznam o „release“ a konfiguraci produkce	Verze, commit/release ID, konfigurace, parametry, aktivované feature toggles, seznam změn	Dodavatel + provoz; PM eviduje	Při go-live; aktualizace při hotfixech	Audit a dohledatelnost	DF-3	Evidence pack – release
Předávka přístupů a provozních kontaktů	Seznam účtů, přístupů, klíčů dle pravidel, kontakty L1/L2/L3, escrow/uložení tajemství dle interních pravidel	Provoz + bezpečnost; dodavatel poskytuje	Před go-live	Zajištění reakce na incidenty	DF-3	Provoz + Bezpečnost
TIP						

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)		Kde se vede (evidence pack)
----------------	-----------------	-----------------------	-------------------------	-----------------------	--	-----------------------------

V rámci go-live packu udržujte „jeden zdroj pravdy“: index artefaktů, verze, datum schválení a vazbu na Decision log.

Výstupy a důkazy připravenosti k provozu se ukládají do sběrného místa (ISDŘ) a slouží jako podklad pro ověření připravenosti služby (kolaudaci) i pro proces OHA.

9.3 Hlavní obsah kapitoly

9.3.1 Strategie spuštění (rollout) – povinné volby

Checklist – orgán veřejné moci by měl zvolit a zdůvodnit strategii spuštění:

- MĚLO BY zvolit režim: plné spuštění / postupné spuštění / omezené spuštění (např. vybraná skupina, omezený čas, omezené funkce).
- MĚLO BY uvést, jak se režim projeví v komunikaci (texty ve službě, na webu, na přepážce, podpora).
- MĚLO BY uvést, jak se řeší souběh kanálů (digitál + papír/přepážka) a jak se zabrání duplicitám a sporům.
- MĚLO BY uvést, jak se bude rozhodovat o rozšíření (přechod z omezeného na plné) – na základě jakých metrik a incidentů.
- NEMĚLO BY být omezené spuštění bez jasných pravidel, koho se týká a jak se to kontroluje.

TABULKA 2 – Volba režimu spuštění (šablona)

Režim spuštění	Pro koho/na co se vztahuje	Omezení (funkce/čas/region)	Kritéria rozšíření/ukončení	Rizika a mitigace	Schválil / datum
POZOR Postupné spuštění nesmí znamenat „test v produkci“ bez podpory. Musí mít stejné požadavky na evidence, monitoring a bezpečnost jako plné spuštění.					

9.3.2 Go-live checklist – minimum před/po spuštění

Checklist – body před spuštěním (by měl):

- MĚLO BY být schválen GO (DF-3) a zapsán v Decision logu (včetně seznamu otevřených vad).
- MĚLO BY být ověřena dostupnost kritických integrací a funkčnost degračních režimů (alespoň smoke).
- MĚLO BY být aktivní monitoring a alerting; kontakty L1/L2/L3 jsou dostupné.
- MĚLO BY být připraven komunikační obsah: stavové hlášení ve službě, web, instrukce pro přepážky a podporu.
- MĚLO BY být připraven rollback postup a rozhodovací režim (kdo a jak rychle).
- MĚLO BY být uzamčená verze release (release ID) a evidována konfigurace (včetně feature toggles).

Checklist – body po spuštění (by mělo):

- MĚLO BY proběhnout ověření kritických scénářů v produkci (smoke test) a záznam výsledku.
- MĚLO BY proběhnout ověření logování a dohledatelnosti (korelační ID; dohledání testovacího případu).
- MĚLO BY proběhnout ověření notifikací a stavových obrazovek (pokud jsou součástí služby).
- MĚLO BY běžet monitoring a být vyhodnoceny první metriky (dostupnost, chybovost, výkon).
- MĚLO BY být založen režim hypercare (denní rytmus, evidence incidentů, triage).

9.3.3 Komunikace a připravenost kanálů (včetně přepážek)

Checklist – komunikační a kanálová připravenost by měla zahrnout:

- MĚLO BY instrukce pro uživatele: co služba umožňuje, co potřebují připravit, jaké jsou kroky a jak sledovat stav.
- MĚLO BY instrukce pro přepážky a podporu: jak uživatele navést, jak ověřit stav případu, jak eskalovat incident.
- MĚLO BY texty pro výpadek a degradaci (stavová stránka / hlášení ve službě) – schválené a připravené k aktivaci.
- MĚLO BY kontaktní bod pro hlášení problému (uživatelský) a interní kanál pro eskalace.
- NEMĚLO BY být komunikační sdělení v rozporu s reálným stavem služby nebo s právně významnými informacemi.

TABULKA 7 – Komunikační plán (šablona)

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Cílová skupina	Zpráva (co sdělit)	Kanál	Kdy	Vlastník	Příloha / text	Poznámka
TIP Přepážky a call centrum musí mít krátký „script“: 5 vět, co říct a kam uživatele poslat. Bez toho se digitální služba znehodnotí v prvních dnech.						

9.3.4 Evidence go-live a dohledatelnost (audit)

Auditní pravidlo go-live

Go-live rozhodnutí se opírá o master index důkazů. Pokud není dohledatelný důkaz o splnění podmínky, podmínka se považuje za otevřenou a musí mít vlastníka, termín a rozhodnutí, zda brání spuštění.

Checklist – pro dohledatelnost go-live by mělo být uloženo:

- MĚLO BY rozhodnutí DF-3 (GO/STOP) v Decision logu + seznam otevřených vad a akceptací.
- MĚLO BY go-live protokol (vyplněný) včetně času, kdo co potvrdil a odkazy na důkazy.
- MĚLO BY release ID/verze a konfigurace produkce (včetně aktivovaných feature toggles).
- MĚLO BY logy a monitoring pro první dny: schopnost dohledat incidenty a konkrétní případy.
- MĚLO BY záznam o aktivaci komunikačních textů (pokud byly použity degradační hlášky).
- NEMĚLO BY být důkazní stopa pouze v e-mailu; musí být v Evidence packu.

POZOR

Ve veřejné správě musí být dohledatelné: co bylo spuštěno, kdo to schválil, kdy, s jakými omezeními a proč. Bez evidence nelze obhájit postup při stížnosti, kontrole ani incidentu.

Před uvedením služby do provozu se ověřuje připravenost služby (obdoba „kolaudace“) ve vazbě na proces OHA a na bránu DF-3, včetně souhlasu statutárního zástupce (viz kap. 8). Cílovým směřováním je posuzovat připravenost na úrovni digitální služby, nikoli pouze jako změnu ISVS (viz vize v kap. 13).

10 Řízení služby po spuštění

Účelem kapitoly je zajistit, aby digitální služba byla po spuštění řízena jako živá služba: se stabilním vlastníkem, provozní odpovědností, řízením změn, incidentů a bezpečnosti, pravidelným vyhodnocováním kvality (včetně přístupnosti), a s kontrolou provozního dluhu. Kapitola stanoví minimální governance a rytmus řízení služby v prostředí veřejné správy, kde dochází ke změnám legislativy, datových zdrojů, integrací a organizačních kompetencí.

10.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl po go-live rozhodnout a doložit zejména:

- MĚLO BY kdo je věcný vlastník služby (business owner) a kdo je provozní vlastník (service/operations owner) – bez zavádění nových rolí mimo rámec řízení ICT projektů a řízení služby.
- MĚLO BY jaký je provozní režim (SLA/OLA, incident management, eskalace) a jak se udržuje provozní dokumentace (runbooky).
- MĚLO BY jak se řídí změny po spuštění (prioritizace, schvalování, release, evidence) a jak se rozhoduje o rozšiřování služby.
- MĚLO BY jak se řídí bezpečnost a zranitelnosti (pravidelné kontroly, patching, revize oprávnění, audit logů).
- MĚLO BY jak se vyhodnocuje kvalita služby: dostupnost, výkon, dokončenost kritických scénářů, podpora, a přístupnost.
- MĚLO BY jak se řídí právní změny a dopady na procesy a data (legislativa jako konstrukční prvek i po spuštění).
- NEMĚLO BY být služba „ponechána dodavateli“ bez dohledatelné odpovědnosti úřadu za rozhodnutí, změny a provozní rizika.

POZOR

V provozu se neřeší, kdo co měl udělat v projektu. V provozu se řeší incident, dopad na uživatele a odpovědnost za rozhodnutí. Proto musí být governance služby nastavena a evidována.

10.2 Výstupy / důkazy

TABULKA 1 – Minimální Service Management pack (povinné důkazy po spuštění)

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod	Kde se vede
Service charter (základní popis služby)	Účel služby, kritické scénáře, okruh uživatelů, kanály, hranice služby, hlavní integrace, kontakty	Věcný vlastník služby + provoz; správa v evidenci služby	Do ukončení hypercare; aktualizace při změnách	Jednotný „zdroj pravdy“ pro řízení služby	DF-4 / pravidelná kontrola	Evidence služby
Provozní dokumentace (runbooky)	Incident postupy, degradace integrací, restart/obnova, kontakty, eskalace, okna údržby	Provozní vlastník; technická část dle prostředí	Před DF-4; průběžně	Reakce na incidenty a snížení MTTR	Měsíčně/po incidentech	Provozní evidence
Katalog změn / backlog (change backlog)	Požadavky, vady, priority, dopady, schválení, termíny, vlastníci	Věcný vlastník + PM/řízení změn dle režimu organizace	Od go-live; průběžně	Kontrola rozsahu a priorit	Týdenně/měsíčně	Řízení služby
Release plán a evidence release	Frekvence release, verze, obsah změn, testování, rollback, schválení	Provoz + dodavatel; schvaluje vlastník služby	Od stabilizace; průběžně	Zabránění „ad hoc“ změnám	Před každým releasem	Provoz + Evidence release
Incident registry + post-mortem	Incidenty, dopady, doby, nápravná opatření, post-mortem pro významné incidenty	Provoz	Od go-live; průběžně	Řízení dostupnosti a poučení	Týdenně/měsíčně	Provozní evidence
Bezpečnostní režim po spuštění	Plán patching/aktualizací, zranitelnosti, revize oprávnění, audit logů, evidence nálezů a náprav	Bezpečnost + provoz	Od go-live; průběžně	Kontrola kyber rizik	Měsíčně/kvartálně	Bezpečnostní evidence
KPI/SLO dashboard (minimální)	Dostupnost, chybovost, výkon, integrace, dokončenost kritických scénářů, podpora	Provoz + vlastník služby	Od DF-4; průběžně	Řízení kvality a priorit	Měsíčně	Monitoring/Reporting
Pravidelný review přístupnosti	Výsledky kontrol přístupnosti po změnách, evidence vad a náprav, opakovaná validace kritických scénářů	Vlastník služby + UX/obsah; dodavatel poskytuje nápravy	Po významných změnách; minimálně periodicky	Zajištění kontinuální přístupnosti	Po release / kvartálně	UX/obsah evidence
Evidence právních změn a dopadů	Záznam změny, dopad na proces, data, texty, UX, termíny, schválení	Věcný vlastník + právní; PM/řízení změn koordinuje	Průběžně	Zajištění souladu a auditovatelnosti	Při změně legislativy	Právo + Decision log změn
TIP Service charter a Evidence služby musí být čitelné i pro nového člověka. Pokud službu nelze převzít při personální změně, governance není dostatečná.						

Výstupy provozního řízení (service review, metriky, backlog, technický dluh) se evidují ve sběrném místě (ISDR), aby byly datově vyhodnotitelné v čase.

10.3 Hlavní obsah kapitoly

10.3.1 Řízení incidentů a problémů (incident/problem management)

Checklist – řízení incidentů by mělo zajistit:

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

- MĚLO BY jednotnou evidenci incidentů (ID, čas, dopad, stav, vlastník, rozhodnutí).
- MĚLO BY klasifikaci incidentů (závažnost) a cílové časy reakce/obnovy dle provozního režimu.
- MĚLO BY komunikační režim při incidentech (uživatelé, přepážky, interně).
- MĚLO BY post-mortem pro významné incidenty: příčina, poučení, opatření, termíny a vlastníci.
- MĚLO BY napojení na backlog a release – incidenty se nesmí ztrácet v e-mailech.
- NEMĚLO BY být incident uzavřen bez rozhodnutí o nápravě nebo akceptaci zbytkového rizika.

TABULKA 3 – Incident registry (šablona)

Incident ID	Datum/čas	Závažnost	Dopad (uživatel/proces/právo)	Detekce (monitoring/hlášení)	Stav	Vlastník	Nápravné opatření / release
TIP U významných incidentů vždy zaznamenejte: kdy byly aktivovány degradační režimy, kdy byla spuštěna komunikace a kdo rozhodl.							

10.3.2 Řízení změn po spuštění (change management)

Checklist – změnové řízení by mělo zajistit:

- MĚLO BY jeden backlog pro požadavky a vady s prioritou, dopadem a vlastníkem.
- MĚLO BY pravidla schvalování změn (kdo schvaluje funkční změnu, kdo schvaluje bezpečnostní dopady, kdo schvaluje komunikaci).
- MĚLO BY evidenci release: co se nasadilo, kdy, kdo schválil, jak bylo ověřeno, jaký byl rollback.
- MĚLO BY řízení konfigurace a přístupů (IAM) jako součást změnového řízení.
- MĚLO BY kontrolu dopadů na: právo, procesy, data, UX/přístupnost, bezpečnost, provoz.
- NEMĚLO BY být nasazena změna do produkce bez evidence a bez možnosti dohledání důkazů o testování.

TABULKA 4 – Záznam změny (šablona)

Change ID	Popis změny	Dopad (právo/proces/data/UX/bezp./provoz)	Priorita	Schválení (kdo)	Testy / důkazy	Release / datum	Rollback
ČASTÁ CHYBA Bez změnového řízení se do produkce dostanou „rychlé opravy“, které rozbíjí přístupnost nebo auditní stopu.							

10.5.4 Bezpečnost v provozu (security operations) – minimální standard

Checklist – bezpečnostní režim po spuštění by mělo zahrnout:

- MĚLO BY pravidelné patchování a aktualizace (plán + evidence) pro všechny komponenty v rozsahu služby.
- MĚLO BY řízení zranitelností: skeny, evidence nálezů, náprav a rozhodnutí o zbytkových rizicích.
- MĚLO BY revize oprávnění (IAM) v definované periodě a při personálních změnách; evidence revize.
- MĚLO BY pravidelný audit logů a detekci anomálií dle rizika služby.
- MĚLO BY správu tajemství/klíčů dle pravidel; omezení přístupů do produkce; audit administrátorských akcí.
- MĚLO BY cvičení incidentů: alespoň tabletop pro bezpečnostní incident a výpadek kritické integrace (periodicky).
- NEMĚLO BY být kritická zranitelnost „odložena“ bez formálního rozhodnutí a termínu nápravy.

TABULKA 5 – Bezpečnostní režim (šablona)

Aktivita	Frekvence	Vstup	Výstup (důkaz)	Vlastník	Eskalace	Poznámka
Patching/aktualizace						
Sken zranitelností						
Revize oprávnění						
Audit logů / anomálie						
POZOR Bezpečnostní opatření v provozu jsou „proces“: pokud není evidence, nelze prokázat, že byla opatření provedena.						

10.3.3 Řízení kvality služby (KPI/SLO) – minimální dashboard

Checklist – minimální řízení kvality by mělo zahrnout:

- MĚLO BY sledovat dostupnost a chybovost kritických scénářů (ne jen uptime).
- MĚLO BY sledovat výkon (odezva) pro klíčové kroky a integrace; vyhodnocovat trendy.
- MĚLO BY sledovat dokončenost kritických scénářů (drop-off) a důvody selhání (včetně validací).
- MĚLO BY sledovat zatížení podpory (objem, typy dotazů) a používat ho pro prioritizaci.
- MĚLO BY mít definované prahy pro eskalaci a rozhodnutí o omezení/rollbacku funkce při degradaci.
- NEMĚLO BY být metriky jen sbírané; musí být rozhodovací (navázané na backlog a opatření).

TABULKA 6 – Minimální KPI/SLO dashboard (šablona)

Oblast	Metrika	Cíl/SLO	Aktuální stav	Trend	Rozhodnutí (opatření)	Vlastník
Kritické scénáře	Úspěšnost dokončení kritického scénáře					
Dostupnost	Dostupnost syntetických testů kritických scénářů					
Integrace	Chybovost kritických integrací / fallbacky					
Výkon	95. percentil odezvy pro klíčové kroky					
Podpora	Počet kontaktů na podporu / top důvody					

TIP

Pro veřejnou službu je často nejdůležitější metrika: „kolik lidí dokončilo kritický scénář bez zásahu úřadu“.

10.3.4 Udržení přístupnosti po spuštění (kontinuální)

Checklist – přístupnost po spuštění by měla být řízena takto:

- MĚLO BY být přístupnost součástí akceptace každé významné změny (release) – minimálně na kritických scénářích.
- MĚLO BY existovat evidence vad přístupnosti a jejich náprav v backlogu (ne odděleně).
- MĚLO BY být u změn, které mění UI/flow, provedena kontrola klávesnice a screen reader scénářů (dle pravidel organizace).
- MĚLO BY být periodický review přístupnosti i bez změn (minimálně dle interního režimu), aby se zachytil degradující stav.
- NEMĚLO BY být přístupnost řešena až na základě stížnosti – to znamená, že kontrolní mechanismus selhal.

POZOR

Přístupnost se nejčastěji rozbije drobnými UI změnami nebo změnou validací. Proto musí být přístupnost v change procesu.

10.3.5 Řízení právních a policy změn po spuštění

Checklist – právní změny by měly být řízeny jako změny služby:

- MĚLO BY existovat evidence právních změn a jejich dopadů (na proces, data, texty, rozhodnutí, integrace).
- MĚLO BY být rozhodnuto, zda změna vyžaduje úpravu služby, změnu provozních pravidel nebo pouze obsahovou změnu.
- MĚLO BY být změna promítnuta do právně významných textů a komunikace (včetně verzování).
- MĚLO BY být změna evidována v Decision logu změn a napojena na release/operativní opatření.
- NEMĚLO BY být právní změna „zapracována bez evidence“ – hrozí neobhajitelnost postupu.

TABULKA 7 – Evidence právní změny (šablona)

ID změny	Popis změny (právní/policy)	Dopad na proces	Dopad na data/integrace	Dopad na texty/UX	Rozhodnutí + termín	Schválil / datum
ČÁSTÁ CHYBA Změna legislativy se řeší pouze metodickým pokynem. Pokud služba zůstane v původním flow, vzniká rozpor a uživatel je penalizován.						

10.3.6 Kontrola dodavatelské závislosti a znalostní udržitelnost

Checklist – úřad by měl zajistit:

- MĚLO BY dohledatelnost konfigurace, verzí, přístupů a dokumentace nezávisle na konkrétním dodavateli.
- MĚLO BY předávání znalostí: pravidelné předávky, aktualizace dokumentace, přenos odpovědnosti.
- MĚLO BY smluvně a procesně ošetřené reakční doby a podporu (včetně bezpečnostních incidentů).
- MĚLO BY minimální schopnost úřadu ověřit změnu a rozhodnout o prioritě (ne jen přijímat návrhy dodavatele).
- NEMĚLO BY být jediný člověk/dodavatel, který „ví, jak to běží“ – to je provozní a bezpečnostní riziko.

TABULKA 8 – Knowledge transfer a vendor control (šablona)

Oblast	Co musí být předáno	Frekvence aktualizace	Kdo vlastní	Důkaz	Riziko, když chybí
Konfigurace a prostředí					
Runbooky a provozní postupy					
Release a změny					
Integrace a degrační režimy					
DŮSLEDEK Pokud úřad nekontroluje znalosti a konfiguraci, vzniká vendor lock-in a služba je neřiditelná při změně dodavatele nebo lidí.					

11 Nejčastější selhání digitalizace

11.1 Jaké rozhodnutí kapitola podporuje

Orgán veřejné moci by měl rozhodnout a doložit, že:

- MĚLO BY používá jednotný katalog selhání a kontroluje ho v branách DF (minimálně DF-1 až DF-3).
- MĚLO BY má definované STOP triggery a eskalační cestu: kdy se rozhodnutí vrací (STOP) a kdo rozhoduje o výjimce (pokud je přípustná).
- MĚLO BY vede evidenci zjištěných selhání, jejich nápravy a rozhodnutí o zbytkovém riziku (Decision log + Risk/Issue registry).
- MĚLO BY vyžaduje důkazy (artefakty) k prevenci selhání – neakceptuje deklarace bez evidence.
- NESMÍ – spustit službu (go-live), pokud existuje selhání typu „hard stop“ uvedené v této kapitole bez nápravy nebo bez formálního rozhodnutí o akceptaci (pokud je přípustné).

11.2 Výstupy / důkazy

TABULKA 1 – Doporučené důkazy pro práci se selháními (Anti-failure pack)

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
Katalog selhání (tato kapitola) jako checklist	Seznam selhání, hard stop/soft stop, signály, požadované důkazy, odkazy	PM + věcný gestor; útvary přispívají dle tématu	Před DF-1; aktualizace před DF-2 a DF-3	Jednotný standard kontroly	DF-1 až DF-3	Gate pack / Evidence pack

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Výstup / důkaz	Minimální obsah	Kdo odpovídá za existenci	Kdy by mělo existovat	Použití (k čemu slouží)	Kontrolní bod (brána)	Kde se vede
	na relevantní kapitoly metodiky					
Evidence pack index (rejstřík důkazů)	Odkazy na artefakty pro prevenci selhání (právo, proces/data, UX/přístupnost, bezpečnost, provoz)	PM	Před DF-1; aktualizace průběžně	Dohledatelnost a audit	DF-1 až DF-3	Evidence pack
Decision log (rozhodnutí + výjimky)	GO/STOP, podmínky, akceptace rizika, odůvodnění, vlastníci a termíny	PM; schvaluje governance projektu	Od DF-1 průběžně; uzavřený před DF-3	Obhajitelnost rozhodnutí	DF-1 až DF-4	Řízení projektu – Decision log
Risk/Issue registry (selhání jako rizika a issues)	Záznam selhání, dopad, vlastníci, nápravný plán, termín, eskalace	PM + vlastníci dle oblasti	Od DF-1 průběžně	Řízení tolerancí a eskalace	DF-1 až DF-3	Řízení projektu – rizika/issues
Post-mortem a lessons learned (po incidentech a významných odchylkách)	Příčina, rozhodnutí, opatření, termíny, změny v checklistech a standardech	Provoz (incidenty) / PM (projektové odchylky)	Po významných incidentech / po DF-4	Zabránění opakování selhání	DF-4 / řízení služby	Provozní evidence + Řízení služby

TIP

Selhání by se mělo zapisovat jako rizika/issues s vlastníkem a termínem. „VÍ se o tom“ bez evidence znamená, že se to nestane prioritou a problém se vrátí v provozu.

Zjištěná selhání a nápravná opatření se evidují ve sběrném místě (ISDŘ) tak, aby byla data o selháních vyhodnotitelná napříč službami.

11.3 Hlavní obsah kapitoly

11.3.1 Katalog selhání (antipatterns) – signály, dopady, prevence

TABULKA 2 – Katalog selhání (používat jako kontrolní seznam v DF branách)

ID	Selhání (vzor)	Hard stop?	Typické signály	Dopad	Minimální prevence (kontrola)	Požadovaný důkaz	Kdy se odhaluje	Vazba na kapitolu
F-01	Nejasná hranice služby a kritické scénáře	ANO	Rozsah se mění; „to se dořeší“; různé definice u útvarů/dodavatele	Skluz, dodatky, neobhajitelné rozhodnutí o rozsahu	Definice služby + seznam kritických scénářů + co není součástí	Service definice (kap. 1–2) + akceptační kritéria (kap. 5)	DF-1	1,2,5,7
F-02	Právo řešení až po vývoji	ANO	Právní útvar není v Decision logu; texty nejsou schválené; chybí verzování	Neplatné postupy, stížnosti, rušení rozhodnutí	Právní konstrukce + schválení právně významných informací	Právní konstrukce, seznam právně významných textů (kap. 3)	DF-1, DF-3	3,7,8
F-03	Proces existuje jen „na papíře“, ne v provozu	ANO	Nejsou výjimky; není napojení na evidenci/spis; ruční obcházení	Chaos v provozu, ztráta důkazů, růst papíru	Proces L0/L1 + výjimky + odpovědnosti + evidence	Mapa procesu + výjimky + evidence (kap. 4)	DF-1, DF-2	4,7

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

ID	Selhání (vzor)	Hard stop?	Typické signály	Dopad	Minimální prevence (kontrola)	Požadovaný důkaz	Kdy se odhaluje	Vazba na kapitolu
F-04	Data bez vlastníka a autority (data ownership)	ANO	Spory o „správná data“; integrace bez odpovědného útvaru; nejasné zdroje pravdy	Nekonzistence, chyby, právní spory	Datová inventura + vlastníci + pravidla oprav	Datová inventura + pravidla oprav (kap. 4)	DF-1	4,7
F-05	Integrace bez degradačních režimů	ANO	„Když registr nejede, tak to nejede“; fallback není definován; výpadky paralyzují službu	Výpadky, improvizace mimo evidence, dotazy/stížnosti	Pro kritické integrace fallback a texty pro uživatele	Šablona degradačních režimů + runbook (kap. 6,8)	DF-3	6,8
F-06	UX jako estetika, ne jako dokončení kritického scénáře	ANO	Vysoké drop-off; nejasné texty; uživatel neví, co dělat; chybí IA/flow	Nedokončení podání, přepážka přebírá práci	IA/flow + texty + testy kritických scénářů	IA/flow + protokoly testů (kap. 5)	DF-2	5,7
F-07	Přístupnost řešená až po stížnosti	ANO	Neexistuje důkaz přístupnosti; „dodělá se“; po releasu se zhoršuje	Diskriminace, reputace, právní riziko	Přístupnostní plán + ověřování kritických scénářů	Protokoly přístupnosti + backlog vad (kap. 5,9)	DF-2, po release	5,9
F-08	Bezpečnost deklarativní bez důkazů	ANO	Chybí výsledky testů; neexistuje evidence náprav; sdílené účty	Incident, únik dat, sankce	Security baseline + testy + rozhodnutí o zbytkovém riziku	Bezpečnostní protokoly + decision o riziku (kap. 6,7)	DF-2, DF-3	6,7
F-09	Logy existují, ale nejsou použitelné	ANO	Nelze dohledat konkrétní případ; chybí korelace; logy bez runbooku	Neobhajitelnost, dlouhé incidenty	Logování + korelační ID + postup reakce	Monitoring & logging požadavky + runbook (kap. 6)	DF-3	6,8
F-10	Provoz přizvaný na konci (předávka = „kód“)	ANO	Chybí runbook, přístupy, monitoring; test obnovy není; provoz odmítá převzetí	Neřízený provoz, dlouhé výpadky	Operating model + handover pack + restore test	Provozní model + předávací protokol (kap. 6,8)	DF-2, DF-3	6,8,7
F-11	Go-live bez rollbacku a hypercare	ANO	Neexistuje cutover/rollback; žádná zvýšená podpora; incidenty bez triage	Chaos, reputační škoda, návrat k papíru	Cutover + rollback + hypercare režim	Go-live pack (kap. 8)	DF-3	8,7
F-12	Změny po spuštění ad hoc, bez evidence	ANO	Hotfix bez schválení; nejasné verze; nárůst vad; „nevíme, co je v produkci“	Neauditovatelný stav, dluh, bezpečnostní riziko	Change backlog + release evidence + governance služby	Change log + release evidence (kap. 9)	Po DF-4	9
F-13	Dodavatelská závislost a ztráta znalostí	ANO	Znalost drží jednotlivci; dokumentace chybí; úřad neumí rozhodovat	Vendor lock-in, neschopnost změny	Evidence konfigurace, know-how předávky, kontrola přístupů	Knowledge transfer evidence (kap. 9)	DF-4 a provoz	9

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

ID	Selhání (vzor)	Hard stop?	Typické signály	Dopad	Minimální prevence (kontrola)	Požadovaný důkaz	Kdy se odhaluje	Vazba na kapitolu
F-14	Metriky nejsou rozhodovací (sbírá se, ale neřídí)	NE (soft stop)	Dashboard bez akce; backlog neroste podle dopadu; rozhoduje „kdo křičí“	Zhoršující se kvalita, nárůst dotazů	KPI/SLO navázané na rozhodnutí a backlog	Service review report (kap. 9)	Po DF-4	9

POZOR

Hard stop znamená: bez nápravy nelze pokračovat do další brány. Soft stop znamená: lze pokračovat pouze s formální podmínkou (vlastník, termín, důkaz) a s řízeným rizikem.

11.3.3 Včasné signály selhání (early warning) – co sledovat

Checklist – včasné signály, které MĚLY BY vyvolat eskalaci nebo STOP:

- MĚLO BY – přibývání změn rozsahu bez aktualizace kritických scénářů a bez dopadové analýzy (F-01).
- MĚLO BY – vznik nových „právních výjimek“ bez rozhodnutí v Decision logu (F-02).
- MĚLO BY – nejasné odpovědnosti za integrace nebo odmítání poskytnout rozhraní (F-04, F-05).
- MĚLO BY – přesun řešení problémů do e-mailu/telefonu bez evidence v issues (F-03, F-12).
- MĚLO BY – odkládání přístupnosti, testů obnovy, monitoringu na „později“ (F-07, F-10).
- MĚLO BY – časté hotfixe bez release evidence a bez změnového řízení (F-12).
- MĚLO BY – závislost na jednotlivci (dodavatel/úředník), který jediný „ví jak“ (F-13).

DŮSLEDEK

Ignorování včasných signálů vede k tomu, že se selhání projeví až při DF-3 nebo v provozu, kdy je oprava nejdražší.

11.3.4 Minimální zásahy (co udělat, když se selhání objeví)

TABULKA 3 – Rychlá nápravná opatření (minimální)

Selhání	Okamžitá rozhodnutí	Minimální náprava (co doplnit)	Kdo zajišťuje (útvary)	Důkaz	Do kdy	Eskalace
F-01 Nejasný rozsah	STOP do DF-1 / změnové řízení	Uzavřít kritické scénáře + akceptační kritéria + co není součástí	Věcný gestor + PM + UX	Aktualizovaný seznam scénářů + Decision log	Před zahájením realizace	Governance projektu
F-02 Neuzavřené právo	STOP do DF-1	Schválit právní konstrukci a právně významné texty + verzování	Právní + věcný gestor	Schválení + seznam textů + verze	Před DF-1	Governance projektu
F-05 Bez fallbacku integrací	STOP do DF-3	Doplnit degradační režimy + runbook + texty pro uživatele	Architektura + provoz + UX/obsah	Tabulka degradačních režimů + runbook	Před DF-3	Governance projektu
F-10 Provozní nepřipravenost	STOP do DF-2/DF-3	Doplnit monitoring, runbooky, přístupy, restore test a předávku	Provoz + bezpečnost + dodavatel	Předávací protokol + protokol obnovy	Před DF-3	Řídící orgán projektu
F-12 Ad hoc změny v provozu	Zastavit ad hoc nasazování	Zavést change backlog + release evidence + pravidla schvalování	Vlastník služby + provoz	Change log + release evidence	Do 2 týdnů od zjištění	Vedoucí provozu / governance služby

POZOR

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Selhání	Okamžité rozhodnutí	Minimální náprava (co doplnit)	Kdo zajišťuje (útvary)	Důkaz	Do kdy	Eskalace
Rychlá náprava nesmí být „rychlý patch“ bez evidence. Náprava musí posílit kontrolní mechanismus (důkaz + pravidlo), jinak se selhání vrátí.						

11.3.5 Nejčastější „dokumentové“ a governance selhání (co by nemělo projít)

Checklist – následující stavy by neměly být akceptovány jako důkazy:

- NEMĚLO BY „Seznam požadavků“ bez akceptačních kritérií a bez kritických scénářů (F-01, F-06).
- NEMĚLO BY právní stanovisko bez navázání na konkrétní texty ve službě a bez verzování (F-02).
- NEMĚLO BY procesní diagram bez výjimek a bez vymezení odpovědností a evidence (F-03).
- NEMĚLO BY bezpečnostní prohlášení bez výsledků testů a bez evidence náprav (F-08).
- NEMĚLO BY „máme zálohy“ bez testu obnovy (F-10).
- NEMĚLO BY „monitoring je nastaven“ bez alertingu, vlastníků a runbooku (F-09).
- NEMĚLO BY GO s podmínkami bez vlastníka, termínu a důkazu (kap. 7).

ČASTÁ CHYBA

Za „důkaz“ se považuje dokument vytvořený dodavatelem bez schválení a bez vazby na rozhodnutí a provozní dopady.

12 Přílohy metodického balíčku (A–E)

Přílohy jsou součástí metodického balíčku Digital First a jsou vydávány jako samostatné dokumenty. Při odkazování uvádějte vždy označení přílohy (A–E) a název dokumentu. Použití příloh se doporučuje evidovat v rozhodovací evidenci (např. Decision log / evidence pack), pokud je to relevantní pro auditovatelnost.

- Příloha A – Kontrolní seznamy Digital First (A1...): kontrolní otázky a minimální důkazy.
- Příloha B – Šablony a formuláře: vyplnitelné šablony pro evidenci rozhodnutí, rolí a řízení změn.
- Příloha C – Slovník pojmů: sjednocení terminologie napříč týmy a dokumenty.
- Příloha D – Legislativa a zdroje: orientační přehled právních a metodických zdrojů (doporučeno ověřovat aktuálnost).
- Příloha E – Přehled zkratk: jednotné zkratky používané v metodice a přílohách.

12.1 Doplnkové materiály – zahraniční praxe a příklady z ČR

12.1.1 Zahraniční praxe – co převzít a jak to použít

Zahraniční standardy fungují zejména díky tomu, že kombinují: (1) jasná kritéria, (2) panelové brány/assessment, (3) povinné důkazy, (4) rytmus měření po spuštění. Tyto prvky jsou přenositelné i do české praxe.

12.1.2 Mapovací tabulka (inspirace → konkrétní doplnění)

Země / praxe	Podstata	Konkrétní prvek k převzetí	Kam vložit (metodika)	Poznámka
UK	Service Standard + service assessments	Service assessment panel s výstupem PASS/CONDITIONAL/FAIL a povinnými důkazy	FULL Kap. 7; LIGHT Kap. 7 (spouštěče)	Model bran a hodnocení
USA	Digital Services Playbook (13 plays)	Kontrolní otázky při zahájení a go-live (uživatelé, iterace, tým, měření)	FULL Kap. 2 a 8; LIGHT Kap. 2–6	Použitelné jako pre-mortem
Austrálie	Digital Service Standard	Checkpointy: inkluze, důvěra, monitoring služby	FULL Kap. 5/6/9; LIGHT Kap. 4/5/6	Silné na měření služby
Nový Zéland	Digital Service Design Standard	Princip „design pro celý životní cyklus služby“	FULL Kap. 0/9; LIGHT Kap. 6	Důraz na provoz a zlepšování

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb včetně jejich kapacitního plánování a komunikace informací klientům veřejné správy, financovaného Evropskou unií NextGeneration.

Země / praxe	Podstata	Konkrétní prvek k převzetí	Kam vložit (metodika)	Poznámka
Kanada	Digital Standards + Guideline on Service and Digital	Standards jako základ + důraz na důvěryhodnost, bezpečnost, otevřenost	FULL Kap. 6/9; LIGHT Kap. 5/6	Dobré pro governance po go-live
NHS (UK)	Sektorová adaptace Service Standardu	Společný standard + sektorové body (specifika domény)	Příloha (sektorové přílohy)	Vzor pro resortní dodatky
Ontario (Kanada)	Digital Service Standard + assessment	1stránkový „poster“ pro vedení + assessment proces	Úvod + FULL Kap. 7	Užitečné pro prosazení standardu
Dánsko	Digital-ready legislation	Checklist digital-ready prvků legislativy	FULL Kap. 3	Vhodné pro legislativní změny
Estonsko/EU	Once-only + bezpečná výměna dat	Once-only kontrolní otázky + zdůvodnění, proč se data sbírají znovu	FULL Kap. 4/6; LIGHT Kap. 1/4	Vždy s právním titulem a interoperabilitou

12.1.3 Příklad z praxe v ČR: eRecept (přenositelné principy)

Poučení pro Digital First není „kopírovat řešení“, ale převzít principy: jasné rozhodnutí o odpovědnosti, integrace jako dohoda (ne předpoklad), bezpečnost jako evidence a průběžné měření kvality po spuštění.

Co je přenositelné do jiných služeb:

- Jasná odpovědnost (vlastník služby) a jednotný provozní režim (kdo reaguje na incidenty, kdo měří kvalitu).
- Integrační disciplína: definované rozhraní, fallback, auditní stopa.
- Důvěra uživatelů: potvrzení, dohledatelnost stavu, srozumitelné informace.
- Průběžné zlepšování po spuštění (release discipline + health report).

12.2 Zdroje (zahraniční standardy – odkazy)

TABULKA 5 – Odkazové zdroje použité jako inspirace

Zdroj	URL	Využití v metodice
UK – Service Standard (GOV.UK)	https://www.gov.uk/service-manual/service-standard	Kritéria služby + inspirace pro panelové brány
UK – Service assessments (GOV.UK)	https://www.gov.uk/service-manual/service-assessments	Model assessment panelu
USA – Digital Services Playbook (USDS)	https://playbook.usds.gov/	Kontrolní otázky (13 plays) pro zahájení a go-live
Austrálie – Digital Service Standard (digital.gov.au)	https://www.digital.gov.au/policy/digital-experience/digital-service-standard	Checkpointy inkluze, měření a provozu
Nový Zéland – Digital Service Design Standard	https://www.digital.govt.nz/standards-and-guidance/digital-service-design-standard	Principy designu pro celý životní cyklus
Kanada – Digital Standards	https://www.canada.ca/en/government/system/digital-government/government-canada-digital-standards.html	Standards pro důvěryhodné služby
Kanada – Guideline on Service and Digital	https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html	Doporučení pro implementaci standardů

Zdroj	URL	Využití v metodice
NHS – NHS service standard	https://service-manual.nhs.uk/standards-and-technology/service-standard	Sektorová adaptace standardu
Ontario – Digital Service Standard	https://www.ontario.ca/page/digital-service-standard	13 bodů + inspirace pro interní „poster“
Dánsko – Guidance on digital-ready legislation	https://en.digst.dk/digital-transformation/digital-ready-legislation/guidances-and-tools/guidance-on-digital-ready-legislation/	Checklist pro digital-ready legislativu
Estonsko – X-Road (e-Estonia)	https://e-estonia.com/solutions/interoperability-services/x-road/	Příklad bezpečné výměny dat (princip)
X-Road (projekt)	https://x-road.global/	Referenční zdroj pro koncept datové výměny
EU – Once-Only Principle (TOOP/ISA²)	https://ec.europa.eu/isa2/isa2conf18/once-only-principle-project-toop_en	Princip once-only pro kontrolní otázky v datech

13 Vize rozvoje ZoPDS po 1. 2. 2027

Po nabytí účinnosti dalších částí ZoPDS k 1. 2. 2027 má rozvoj digitálních služeb směřovat od čistě formulářového a portálového pojetí digitalizace ke službám navrženým podle skutečných potřeb klienta. Tato metodika je k takovému rozvoji připravena; jeho směr shrnuje následující vize.

Cílový stav rozvoje ZoPDS po 1. 2. 2027 zahrnuje zejména:

Tyto prvky se promítají do návrhu, schvalování (procesy OHA) i provozu služeb a mají být podporovány strukturovanou, verzovanou a datově zpracovatelnou správou metodiky i jejích výstupů.

13.1 Průřezová kontrolní matice ZoPDS / OHA / ISDŘ / AI

Následující tabulka převádí průřezové principy metodiky do evidence. Slouží jako minimální kontrolní vrstva pro karty, checklisty, gate pack a master index důkazů.

Oblast	Co se ověřuje	Důkaz / tabulka	Gate	Vlastník
ZoPDS / Katalog služeb VS	Vymezit službu, úkon, agendu, katalogový záznam a životní událost.	Karta služby / katalog / Příloha B	DF-1	Věcný gestor
OHA / z. 365/2000 Sb.	Ověřit, zda záměr nebo změna spadá do příslušného procesu OHA / ISVS.	OHA posouzení / stanovisko / ISDŘ odkaz	DF-1 až DF-3	IT gestor / architekt
ISDŘ / evidence pack	Uložit výstupy metodiky jako datově zpracovatelný a verzovaný evidence pack.	Master index důkazů / ISDŘ	všechny brány	Vlastník služby
Only once / data	Určit údaje, které stát již má, jejich zdroje, právní titul a datového vlastníka.	Datová inventura / integrační mapa	DF-2	Datový vlastník
Elektronické zastupování	Ověřit scénáře zmocnění nebo jiné oprávněné osoby.	Matice oprávnění / test scénář	DF-2 až DF-3	Právník / věcný gestor
AI asistent / agent	Vyhodnotit relevance asistenta/agenta, oprávnění, rizikovitost a případné posouzení.	AI assessment / FRIA pokud relevantní	DF-2 až DF-3	Věcný gestor / DPO / bezpečnost
Go-live souhlas	Doložit připravenost služby a souhlas odpovědné osoby.	Go/No-Go zápis / souhlas	DF-3	Vlastník služby