Smlouva o dodávce software s prvky umělé inteligence včetně podpůrných komponent realizované v rámci projektu AIDAS

Číslo 2026/117 NAKIT

Česká republika – Ministerstvo vnitra

se sídlem	Nad Štolou 936/3, 170 34 Praha 7
kontaktní adresa	nám. Hrdinů 1634/3, 140 21 Praha
IČO:	00007064
DIČ:	CZ00007064
zastoupena:	PhDr. Danielem Doležalem, Ph.D., ředitelem odboru archivní správy a spisové služby
bankovní spojení	Česká národní banka, Praha 1 č.ú. 3605881/0710

(dále jen **„Objednatel“**)

a

Národní agentura pro komunikační a informační technologie, s. p.

se sídlem	Kodaňská 1441/46, Vršovice, 101 00 Praha 10
IČO:	04767543
DIČ:	CZ04767543
zastoupen:	[redacted] pověřeným ředitelem
zapsán v obchodním rejstříku	vedeném Městským soudem v Praze oddíl A vložka 77322
bankovní spojení	Československá obchodní banka, a.s. č.ú. 117404973/0300

(dále jen **„Dodavatel“**)

(dále jednotlivě jako „**Smluvní strana**“ nebo společně jako „**Smluvní strany**“)

uzavírají v souladu s ustanovením § 1746 odst. 2 a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**Autorský zákon**“), nařízením Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice

2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (dále jen „**AI Act**“), tuto smlouvu o dodávce software s prvky umělé inteligence včetně podpůrných komponent realizované v rámci projektu AIDAS (dále jen „**Smlouva**“).

1. Úvodní ustanovení

1.1 Objednatel prohlašuje, že splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Dodavatel prohlašuje, že:

a) je státním podnikem ve smyslu zákona č. 77/1997 Sb., o státním podniku, ve znění pozdějších předpisů;

b) splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

c) ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, a zavazuje se Objednatele bezodkladně informovat o všech skutečnostech hrozícího úpadku, případně o prohlášení úpadku jeho podniku.

1.3 Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, který je jim ve Smlouvě, včetně jejích příloh, připisován.

1.4 Pro vyloučení pochybností Smluvní strany uvádí, že ve všech případech, kdy Smlouva stanoví doby nebo lhůty, jsou tyto doby nebo lhůty stanoveny v kalendářních dnech, pokud není v případě konkrétní doby nebo lhůty výslovně uvedeno, že se jedná o dny pracovní.

2. Účel Smlouvy

2.1 Objednatel realizuje projekt s názvem „Digitalizace správy dokumentů a využívání umělé inteligence v Ministerstvu vnitra“ (dále jen „**Projekt**“) reg. č. CZ.31.3.0/0.0/0.0/25_165/0011697, jehož cílem je:

a) provedení komplexní analýzy elektronického systému spisové služby GINIS (dále jen „**eSSL Objednatele**“) a správy dokumentů u Objednatele;

b) vytvoření nástrojů umělé inteligence (dále též jako „**AI**“) plně integrovaných v eSSL Objednatele a využití těchto nástrojů AI pro rozbor a přidělování doručených dokumentů, rozpoznávání doručených dokumentů pro nepříslušnost a při vyřizování příslušných agend státního občanství a vyřizování návrhů na přijetí opatření proti nečinnosti;

c) plná integrace nástrojů AI pro eSSL Objednatele, která umožní automatizované rozřazování přijatých dokumentů příslušným útvarům;

d) vytvoření modelu AI, který vyhodnotí přijaté doručené dokumenty jako nepříslušné na základě obsahu textové vrstvy nebo uživatelské poznámky v evidenční kartě;

e) zřízení digitalizačních linek pro pracoviště centrální podatelny Objednatele v objektech Letná a Centrotex a datové napojení linek na eSSL Objednatele;

f) zřízení nástroje pro snímání předloh na nestabilních médiích na pracovištích správního archivu v Kamýku nad Vltavou a v ukládacích prostorech ve Svojšicích a datové napojení nástroje na úložiště Objednatele.

2.2 Realizací Projektu dojde k významnému zefektivnění a zrychlení činností podatelen Objednatele, tzn. zrychlí se oběh elektronických dokumentů, neboť nebude potřeba předávat listiny, a bude splněna povinnost vykonávat eSSL Objednatele v elektronické podobě i v oblasti příjmu dokumentů, která vyplývá ze zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, a souvisejících předpisů.

2.3 S ohledem na předpokládanou komplexnost a složitost Projektu a na skutečnost, že Objednatel nedisponuje dostatečnými personálními a odbornými kapacitami v oblasti ICT a AI governance je vhodné a účelné zajistit pro potřeby Projektu odborné poradenské, metodické, architektonické a governance služby související s přípravou, řízením a kontrolou zavádění nástrojů umělé inteligence v prostředí Objednatele. Pro vyloučení pochybností tato Smlouva sama nezakládá závazek Dodavatele dodat hardware.

2.4 Smluvní strany shodně prohlašují, že ke dni uzavření této Smlouvy jsou splněny podmínky vertikální spolupráce podle ustanovení § 11 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále „**ZZVZ**“), a to zejména že:

a) Objednatel ovládá Dodavatele obdobně jako svou vnitřní organizační jednotku,

b) v Dodavateli nemá majetkovou účast jiná osoba než stát, resp. veřejný zadavatel, v rozsahu vyžadovaném ustanovením § 11 ZZVZ, a

c) více než 80 % celkové činnosti Dodavatele je prováděno při plnění úkolů svěřených ovládajícím veřejným zadavatelem nebo ovládajícími veřejnými zadavateli nebo jimi ovládanými osobami.

Dodavatel na výzvu Objednatele bezodkladně doloží podklady prokazující splnění podmínek podle předchozí věty, zejména podklady k výpočtu podílu činností dle ustanovení § 13 ZZVZ.

3. Předmět Smlouvy

3.1 Předmětem Smlouvy je závazek Dodavatele provést pro Objednatele dílo spočívající v návrhu, vývoji, dodávce a implementaci softwarového řešení využívajícího prvky umělé inteligence pro zpracování dokumentů v rámci vybraných agend veřejné správy, a zajišťující třídění dokumentů mezi útvary Objednatele, rozpoznání nepříslušnosti, postoupení podání a zajištění agendy opatření proti nečinnosti, včetně všech souvisejících komponent, rozhraní, bezpečnostních opatření, dokumentace a akceptačních artefaktů (tj. veškerých dokumentů, výstupů, vstupního školení uživatelů a relevantních zaměstnanců Objednatele), to vše dle podrobné specifikace obsažené v Přílohách č. 2 až č.14 Smlouvy (dále jen „**Systém**“), přičemž součástí díla jsou:

a) Služby AI governance, spočívající v/ve:

i. realizaci služeb v oblasti AI governance pro řízení využívání umělé inteligence;
ii. podpoře zavádění nástrojů AI do prostředí Objednatele;
iii. metodické a architektonické podpoře integrace AI řešení s informačními systémy Objednatele;
iv. nastavení bezpečnostních mechanismů, řízení přístupů, auditních logů a zajištění souladu s právními a regulatorními požadavky na AI řešení;
v. návrhu principů řízení životního cyklu AI modelů z pohledu governance a řízení rizik;
vi. zpracování rámce AI governance zahrnujícího pravidla řízení AI, správu modelů a dat a principy dohledu nad využíváním AI v souladu s platnými právními a regulatorními požadavky na AI řešení;
vii. provedení vstupního školení koncových uživatelů a relevantních zaměstnanců Objednatele.

Služby AI governance, tedy zajištění systematického rámce pro řízení, dohled a bezpečné využívání nástrojů umělé inteligence v prostředí Objednatele, musí splňovat soulad s platnými právními a regulatorními požadavky, zejména s ohledem na AI Act, aby byla zajištěna transparentnost, auditovatelnost a odpovědnost při využívání AI.

b) Služby projektového řízení, spočívající v/ve:

i. implementaci nástrojů AI pro eSSL Objednatele, která umožní automatizované rozřazování přijatých dokumentů příslušným útvarům;
ii. digitalizaci procesů zpracování dokumentů na pracovištích centrální podatelny Objednatele;

iii. podpoře zpracování dokumentů ze specifických médií a jejich napojení na eSSL Objednatele.

Součásti díla uvedené pod písm. a) a b) tohoto odstavce Smlouvy budou dále označovány jako „**Související plnění**“.

Systém spolu se Souvisejícím plněním budou dále společně označovány jako „**Dílo**“ nebo „**Plnění**“.

3.2 Dodavatel se zavazuje poskytnout Plnění Objednateli řádně a včas, v rozsahu definovaném v tomto článku Smlouvy.

3.3 Objednatel se zavazuje zaplatit Dodavateli za řádně a včas provedené Dílo v souladu se všemi podmínkami Smlouvy sjednanou cenu.

3.4 Navrhované technické řešení představuje modulární software s využitím umělé inteligence, který je navržen pro provoz v hybridním prostředí kombinujícím on-premise infrastrukturu a cloudové prostředí.

3.5 Architektura řešení je koncipována tak, aby umožňovala oddělení aplikační logiky, AI funkcionality, datové vrstvy a integračních komponent, a tím podporovala škálovatelnost, bezpečnost a dlouhodobý rozvoj systému.

3.6 Smluvní strany pro vyloučení všech pochybností uvádí, že Systém poskytuje doporučení, návrhy a předvyplnění; žádné rozhodnutí ani krok s externím účinkem nesmí být však proveden bez potvrzení oprávněnou fyzickou osobou – pracovníkem Objednatele.

3.7 Předmětem této Smlouvy není dodávka hardwaru. Jakékoli jiné plnění než Plnění výslovně uvedené výše v odst. 3.1 tohoto článku Smlouvy není předmětem této Smlouvy a může být sjednáno pouze samostatnou smlouvou nebo dodatkem k této Smlouvě, bude-li takový postup přípustný podle právních předpisů, s předem schválenou specifikací předmětu, ceny a harmonogramu, přičemž Dodavatel není povinen toto Plnění poskytnout.

3.8 Veškeré Plnění podle této Smlouvy poskytuje Dodavatel vlastním jménem a na vlastní odpovědnost. Dodavatel poskytuje Plnění zčásti prostřednictvím vlastních kapacit a zčásti svým poddodavatelem; využití třetích osob je přípustné pouze bez vzniku samostatného nároku těchto osob vůči Objednateli. Dodavatel odpovídá za činnost třetích osob, jako by Plnění poskytoval sám.

4. Místo, termín a podmínky plnění

4.1 Místem plnění je Česká republika.

4.2 Dodavatel se zavazuje provést Dílo v následujících termínech:

a) do 14. 6. 2026 - předání Díla (včetně všech jeho součástí) do akceptačního řízení,

b) do 29. 6. 2026 – termín pro provedení Díla (včetně všech jeho součástí), tj. akceptace Díla.

Termíny uvedené v odst. 4.2 Smlouvy mohou být upraveny (prodlouženy) na základě skutečné doby potřebné k dokončení jednotlivých aktivit v rámci plnění.

4.3 Dodavatel se zavazuje provést Dílo za podmínek uvedených v této Smlouvě, ve sjednané specifikaci, jakosti, termínech, rozsahu a sjednaným způsobem. Plnění musí být poskytnuto bez jakýchkoliv vad, ať již faktických či právních, v souladu s veškerými právními předpisy a technickými požadavky.

4.4 Dodavatel se zavazuje provést Plnění v co nejlepším provedení a kvalitě odpovídající aktuálnímu stavu technologického vývoje a poznání v dané oblasti a kategorii produktů, jakož i požadavkům Objednatele vymezeným v Přílohách č. 2 až č. 14 Smlouvy.

4.5 Veškeré hmotné složky Plnění musí být nové, nepoužité, nepoškozené a zhotovené z kvalitního materiálu. Hmotné a nehmotné věci tvořící Plnění nesmí být zatíženy právními vadami, např. zástavním právem, či právem duševního vlastnictví. Veškeré složky Plnění musí být schopny podávat trvale standardní výkon v souladu s vlastnostmi a kvalitou stanovenou v Dokumentaci a této Smlouvě a plně vyhovovat účelu, pro který jsou jako součást Plnění dodávány.

4.6 Dodavatel se dále zaručuje Objednateli, že Systém zhotovený Dodavatelem dle této Smlouvy bude plně funkční a způsobilý pro použití k určenému účelu, pro užití v České republice, odpovídat sjednané specifikaci, bez faktických vad, a bude splňovat veškeré nároky a požadavky českého právního řádu a AI Act.

5. Akceptační řízení

5.1 Proces akceptace Díla je řízen touto Smlouvou a Přílohou č.11 Smlouvy – Akceptační plán Systému, která upravuje podrobnosti a požadavky na akceptaci a kategorizaci vad Systému. Další podrobnosti akceptačního řízení týkající se jednotlivých modulů Systému, jsou uvedeny též v Přílohách č. 2 až č. 9 a č. 12 až č. 14 Smlouvy. V případě rozporu mezi Akceptačním plánem Systému a tělem Smlouvy nebo některou z jejích dalších příloh se použije vždy přísnější nebo speciální pravidlo stanovené v příslušné části Smlouvy a jejích příloh. Akceptační plán Systému tuto Smlouvu konkretizuje a nesmí vyloučit použití výsledku „*Akceptováno s výhradou*“, jsou-li splněny podmínky stanovené touto Smlouvou.

5.2 Dílo se považuje za řádně a včas provedené, je-li v termínu pro provedení Díla Systém řádně a včas dokončen, předán a převzat, a Související plnění řádně a včas poskytnuta, resp. je-li v termínu pro provedení Díla oprávněnými osobami podepsán Akceptační protokol s výsledkem „*Akceptováno bez výhrad*“ nebo „*Akceptováno s výhradou*“ za podmínek stanovených touto Smlouvou, zejména její Přílohou č.11

Smlouvy – Akceptačním plánem Systému. Vzhledem k povaze Plnění a k nastavení akceptačního řízení se sjednává, že případné výhrady k Plnění se mohou vztahovat pouze na část Díla tvořenou Systémem.

5.3 Dodavatel předá Dílo Objednateli do akceptačního řízení v termínu do 14. 6. 2026 Ustanovení § 2590 odst. 2 Občanského zákoníku se nepoužije. Řízení o akceptaci předaného Díla je zahájeno dnem předání Díla a je ukončeno podpisem akceptačního protokolu oprávněnými osobami Smluvních stran (dále jen „**Akceptační protokol**“) s výsledkem „*Akceptováno bez výhrad*“ nebo „*Akceptováno s výhradou,* anebo v případě výsledku *„Neakceptováno“* pokračuje po odstranění vad opakovaným akceptačním řízením.

5.4 Objednatel potvrdí Akceptační protokol pouze v případě, že předávaný Systém splňuje podmínky a vlastnosti stanovené Smlouvou a jejími přílohami, zejména Přílohou č. 11 Smlouvy – Akceptačním plánem Systému.

Výsledek „***Akceptováno s výhradou***“ lze použít pouze tehdy, pokud:

- otevřené vady nebrání bezpečnému a provozně použitelnému užívání převzatého Systému, a současně
- se jedná o vady, které nebrání převzetí Systému, neznamenají nepřijatelný dopad na bezpečnost, právní soulad, klíčové funkce, provozní použitelnost ani kritické uživatelské scénáře a jejichž odstranění je možné jednoznačně naplánovat a kontrolovat, a současně
- zbývající otevřené vady nebrání převzetí Systému, jejich odstranění je možné jednoznačně naplánovat a kontrolovat a jejich ponechání dočasně nepředstavuje nepřijatelný dopad na bezpečnost, právní soulad, klíčové funkce ani provozní použitelnost, a současně
- všechny otevřené vady Systému jsou přesně popsány v Akceptačním protokolu a je pro ně stanoven závazný způsob a termín vypořádání.

Podrobnosti jsou uvedeny v Příloze č. 11 Smlouvy – Akceptační plán Systému.

5.5 V případě akceptace Díla prostřednictvím Akceptačního protokolu s výsledkem „*Akceptováno s výhradou*“ se má za to, že Dílo bylo převzato s neblokujícími otevřenými vadami za podmínek stanovených touto Smlouvou.

V případě akceptace Díla prostřednictvím Akceptačního protokolu s výrokem „*Akceptováno s výhradou"* je Dodavatel oprávněn fakturovat 100 % Ceny za Dílo, na jakou má v souladu s touto Smlouvou nárok. Objednatel však Dodavateli ve lhůtě splatnosti uhradí na základě faktury pouze 80 % Ceny (dále jen „**Zádržné**“).

Uplatnění Zádržného je Objednatel povinen Dodavateli písemně oznámit. Oznámené Zádržné je Objednatel oprávněn zadržet až do úplného odstranění všech vad a ověření jejich odstranění Objednatelem. O úplném odstranění všech vad a o ověření jejich odstranění Objednatelem bude mezi Smluvními stranami sepsán a podepsán zápis (dále jen „**Zápis**“).

Je-li Dílo akceptováno s výrokem „*Akceptováno s výhradou*“, budou jednotlivé vady Systému odstraněny ve lhůtách/ve lhůtě uvedených/é v Akceptačním protokolu, a to tak, aby byla splněna všechna akceptační kritéria.

5.6 V případě výroku „*Neakceptováno*“ se má za to, že Dodavatel neprovedl Dílo v souladu s touto Smlouvou, a po odstranění vad Systému bude Akceptační řízení opakováno. Ohledně opakování Akceptačního řízení platí přiměřeně ustanovení této Smlouvy o akceptaci. Nebudou-li vady Systému vytknuté Objednatelem v Akceptačním protokolu s výrokem „*Neakceptováno*“ odstraněny tak, aby byl Akceptační protokol s výrokem „*Akceptováno*“ nebo „*Akceptováno s výhradou*“ Objednatelem podepsán v termínu pro provedení Díla, je Dodavatel v prodlení s provedením Díla se všemi důsledky z toho vyplývajícími.

5.7 Podpisem Akceptačního protokolu s výrokem „*Akceptováno*“ nebo „*Akceptováno s výhradou*“ Objednatelem a Dodavatelem se má za to, že je splněn závazek Dodavatele provést Dílo a Dodavateli vzniká právo na zaplacení ceny za provedení Díla. Podpis dle předchozí věty je podmínkou pro vznik oprávnění Dodavatele vystavit daňový doklad (fakturu) za realizaci Díla podle Smlouvy.

V případě podpisu Akceptačního protokolu s výrokem „*Akceptováno s výhradou*“ je Objednatel oprávněn zadržet příslušnou část Ceny v rozsahu a za podmínek stanovených cenovými a platebními ustanoveními této Smlouvy (viz. odst. 7.1 článku 7. Smlouvy).

5.8 Akceptační protokol/Zápis bude vyhotoven ve dvou (2) vyhotoveních nebo elektronicky a podepsán oběma Smluvními stranami. V případě tištěného vyhotovení obdrží každá ze Smluvních stran po jednom (1) vyhotovení a v případě elektronického vyhotovení obdrží každá ze Smluvních stran podepsanou elektronickou verzi Akceptačního protokolu/Zápisu.

5.9 Dodavatel je povinen předat Objednateli Dílo včetně dalších případných dokumentů nezbytných pro řádné provedení předmětu plnění (dále jen **„Dokumentace“**). Nedílnou součástí Akceptačního protokolu budou následující informace a Dokumentace:

a) potvrzení Objednatele o provedení implementace softwarového řešení a školení;

b) veškerá dokumentace vztahující se k Systému, zejména veškeré návody (manuály) k použití, doklady a dokumenty, jež jsou obvyklé, nutné (právními předpisy vyžadované) či vhodné k převzetí a k využití Systému, uživatelská dokumentace, provozní dokumentace, všechny vrstvy architektury v rámci projektové a provozní dokumentace, provozně bezpečnostní dokumentace, administrátorská dokumentace atp. Veškeré návody (manuály) k použití, funkční specifikace, doklady a dokumenty budou v českém jazyce; součástí Dokumentace jsou také podklady pro interní předpis Objednatele týkající se užívání a bezpečnosti softwarového řešení;

c) aktuální verze zdrojových kódů včetně aktuálních verzí veškeré související dokumentace;

d) jakékoli další materiály vztahující se k Systému.

Implementace, školení a Dokumentace předaná současně jako součást Systému do akceptačního řízení podléhá rovněž akceptačnímu řízení. Neúplnost nebo nedostatky Dokumentace a dalších předávacích artefaktů samy o sobě nebrání výsledku *„Akceptováno s výhradou“*, pokud nebrání bezpečnému, právně souladnému a provozně použitelnému užívání Systému a pokud je jejich dopracování přesně popsáno v Akceptačním protokolu včetně závazného termínu.

5.10 V případě výskytu vad a nedodělků bránících řádnému užívání Systému Objednatelem v termínu předání a převzetí, tj. vad nad rámec umožňujících akceptaci s výhradou v souladu s podmínkami stanovenými touto Smlouvou, nebude Dílo převzato až do jejich odstranění. Pokud Objednatel Dílo nepřevezme, protože Systém obsahuje vady, je povinen specifikovat tyto vady v Akceptačním protokolu.

Smluvní strany se písemně záznamem do Akceptačního protokolu dohodnou, do kdy Dodavatel odstraní tyto vady Systému tak, aby byla splněna všechna kritéria funkčnosti a úplnosti Systému.

5.11 Dodavatel zajistí po dobu od protokolárního předání Díla Dodavatelem Objednateli do akceptačního řízení až do doby vystavení Akceptačního protokolu s výrokem *„Akceptováno“* (a v případě vytknutí vad k takovému Plnění Objednatelem v rámci akceptačního řízení s výsledkem *„Akceptováno s výhradou“* až do kompletního vypořádání identifikovaných vad Dodavatelem, tj. až do podpisu Zápisu ve smyslu čl. 5 odst. 5.5 Smlouvy) podepsaného oprávněnou osobou Objednatele.

5.12 V případě, že Objednatel bude požadovat v rámci akceptačního řízení výstup v podobě písemného dokumentu, bude tento výstup předán Dodavatelem Objednateli v českém jazyce, a to tak, že Dodavatel jej předá Objednateli spolu s příslušným Protokolem v listinné formě vytištěné a podepsané ve dvou (2) originálech nebo v elektronické formě ve formátu Microsoft Word nebo v případě obrazových výstupů ve formátu PDF

(Portable Document Format) nebo v běžně používaných grafických formátech (BMP, JPG, GIF) na fyzických či cloudových digitálních médiích.

5.13 Místem předání akceptačních dokumentů uvedených v tomto článku Smlouvy je kontaktní adresa Dodavatele uvedená v záhlaví této Smlouvy, pokud nebude Objednatelem stanoveno jinak.

5.14 K podpisu Akceptačního protokolu jsou oprávněny osoby uvedené v čl. 11. odst. 11.2 a 11.3 Smlouvy.

5.15 Náležitosti Akceptačního protokolu jsou uvedeny v Příloze č. 15 Smlouvy.

5.16 Akceptace Díla Objednatelem podle tohoto článku Smlouvy nevylučuje právo Objednatele vytknout vady Systému i později, a to (i) v případech stanovených právními předpisy (např. skryté vady); a (ii) pokud je vada vytknuta v době trvání sjednané záruční doby. Veškeré vady Systému (včetně veškerých nedostatků a nedodělků), resp. rozpor se Smlouvou, budou Dodavateli oznámeny kdykoliv po jejich zjištění Objednatelem. Vady Systému či jeho části budou Dodavatelem bezplatně odstraněny bez zbytečného odkladu po jejich doručení Dodavateli či ve lhůtě stanovené Smlouvou, a to za podmínek stanovených Smlouvou.

6. Cena

6.1 Celková cena za provedení Díla činí 9 854 267,00 Kč bez DPH. DPH ve výši 21 % činí 2 069 396,07 Kč. Celková cena činí 11 923 663,07 Kč včetně DPH (dále jen „**Cena**“). Specifikace ceny za Plnění je obsažena v Příloze č. 1 Smlouvy.

6.2 Náklady na poddodávky dodavatelů Dodavatele jsou zahrnuty v ceně dle odst. 6.1 tohoto článku Smlouvy a nejsou samostatnou položkou ceny ani samostatným předmětem plnění.

6.3 Celková cena Plnění je stanovena jako cena nejvýše přípustná a nepřekročitelná. Cena za poskytnutí Plnění zahrnuje zejména veškeré výlohy, výdaje a náklady vzniklé Dodavateli v souvislosti s poskytováním Plnění a vyhotovením a předáním Plnění podle této Smlouvy.

6.4 K Ceně bude připočítána DPH dle příslušných předpisů ve výši platné ke dni uskutečnění zdanitelného plnění.

7. Platební podmínky

7.1 Cena za provedení Díla bude Objednatelem uhrazena na základě daňového dokladu (faktury) vystaveného Dodavatelem.

Daňový doklad (faktura) bude Dodavatelem vystaven po podpisu Akceptačního protokolu s výrokem „*Akceptováno*“ (bez výhrad) nebo „*Akceptováno s výhradou*“ (za podmínek uvedených v této Smlouvě a v jejích přílohách, zejména v Příloze č.11 Smlouvy – Akceptační plán Systému) oběma Smluvními stranami.

Nedílnou součástí daňového dokladu (faktury) bude kopie Akceptačního protokolu podepsaného oběma Smluvními stranami. Za den uskutečnění zdanitelného plnění se v tomto případě považuje den podpisu Akceptačního protokolu poslední Smluvní stranou.

V případě, že bude uplatněno Zádržné, bude toto uhrazeno nejpozději do pěti (5) dnů po ověření odstranění všech vad Systému, resp. po podpisu Zápisu ve smyslu čl. 5 odst. 5.5 Smlouvy Objednatelem. Oznámení uplatnění Zádržného vylučuje prodlení Objednatele s úhradou dotčené části Ceny.

7.2 Daňový doklad (faktura) musí obsahovat evidenční číslo Smlouvy Objednatele a veškeré údaje vyžadované právními předpisy, zejména ustanovením § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále „**Zákon o DPH**“), zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a ustanovením § 435 Občanského zákoníku. Dodavatel je povinen připojit k daňovému dokladu (faktuře) kopii Akceptačního protokolu podepsaného Objednatelem. Daňový doklad (faktura) bude dále obsahovat text, kterým se identifikuje podpořený Projekt: „Digitalizace správy dokumentů a využívání umělé inteligence v Ministerstvu vnitra“, reg. č.: CZ.31.3.0/0.0/0.0/25_165/0011697. Na daňovém dokladu (faktuře), např. v poznámce, musí být uvedeno „Národní plán obnovy“.

7.3 Splatnost řádně vystaveného daňového dokladu (faktury) činí 30 dnů ode dne jeho doručení Objednateli. Daňový doklad (faktura) bude doručen datovou zprávou prostřednictvím datové schránky.

7.4 Nebude-li daňový doklad (faktura) obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena nebo DPH, je Objednatel oprávněn daňový doklad (fakturu) před uplynutím lhůty splatnosti bez uhrazení vrátit Dodavateli k provedení opravy s vyznačením důvodu vrácení. V takovém případě vrácením daňového dokladu (faktury) pozbývá platnosti lhůta splatnosti a Objednatel není v prodlení se zaplacením daňového dokladu (faktury). Dodavatel provede opravu vystavením nového daňového dokladu (faktury). Nová lhůta splatnosti v délce 30 dnů začne běžet ode dne doručení nového daňového dokladu (faktury) Objednateli.

7.5 Daňový doklad (faktura) se považuje za uhrazený dnem připsání příslušné částky na účet Dodavatele. Všechny částky poukazované v korunách českých vzájemně Smluvními stranami na základě Smlouvy musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů druhé Smluvní strany spojených s převodem na jejich účty.

7.6 Objednatel neposkytuje Dodavateli jakékoliv zálohy na cenu za Plnění.

7.7 Objednatel bude hradit přijatý daňový doklad (fakturu) pouze na bankovní účet Dodavatele uvedený ve Smlouvě, který musí být zveřejněn správcem daně způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 96 odst. 2 Zákona o DPH. V případě, že Dodavatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po zveřejnění bankovního účtu Dodavatele v registru plátců a identifikovaných osob Dodavatelem.

7.8 Dodavatel prohlašuje, že správce daně před uzavřením Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu ustanovení § 106a Zákona o DPH (dále „**Nespolehlivý plátce**"). V případě, že správce daně rozhodne o tom, že Dodavatel je Nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do 3 pracovních dnů od vydání takového rozhodnutí. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.

7.9 Dodavatel je povinen uchovávat dokumenty související s poskytováním Plnění dle této Smlouvy nejméně po dobu 10 let od konce účetního období, ve kterém došlo k zaplacení ceny za poskytnuté Plnění, případně k poslednímu zdanitelnému plnění dle této Smlouvy, a to zejména pro účely kontroly oprávněnými kontrolními orgány.

7.10 Dodavatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly. Dodavatel je povinen poskytnout Objednateli na vyžádání veškerou součinnost nezbytnou k řádnému plnění povinností Objednatele jako příjemce podpory z Národního plánu obnovy na realizaci Projektu a k řádnému plnění povinností kontrolované osoby při případné kontrole čerpání a použití prostředků z této podpory prováděné příslušnými kontrolními orgány.

8. Záruka za jakost Systému a záruční servis k Systému

8.1 Dodavatel odpovídá za to, že Systém bude fungovat v souladu s požadavky Objednatele uvedenými ve Smlouvě a poskytuje záruku za jakost Systému po záruční dobu dvaceti čtyř (24) měsíců ode dne akceptace Díla (tj. ode dne podpisu Akceptačního protokolu s výrokem „*Akceptováno*", v jehož rámci bylo potvrzeno převzetí Díla Objednatelem bez jakýchkoli vad Systému či jeho nedodělků nebo po podpisu Zápisu ve smyslu čl. 5 odst. 5.5 Smlouvy Objednatelem) (dále jen „**Záruka**").

8.2 Vady Systému, včetně jeho dalších zjištěných nedostatků, nedodělků či vad, které vzniknou nebo se projeví v záruční době, je Dodavatel povinen v rámci Záruky odstranit na své náklady a bezplatně.

8.3 Záruka se vztahuje na celý Systém a jeho součásti, včetně jeho příslušenství, a na funkčnost Systému. Záruční doba Záruky se prodlužuje o dobu, po kterou měl Systém vadu bránící jeho řádnému užívání Objednatelem.

8.4 Dodavatel se zavazuje poskytnout Objednateli záruku na hmotné nosiče plnění (je-li Systém poskytován na hmotných nosičích) v délce dvanáct (12) měsíců. Záruční doba počíná běžet dnem podpisu Akceptačního protokolu s výrokem „*Akceptováno*“ Objednatelem nebo po podpisu Zápisu ve smyslu čl. 5 odst. 5.5 Smlouvy Objednatelem.

8.5 Dodavatel je povinen poskytovat Objednateli po dobu trvání záruční doby podle odst. 8.1 Smlouvy záruční servis mající následující parametry:

- Vady/u Systému vzniklé nebo odhalené v záruční době bude Objednatel oznamovat Dodavateli bez zbytečného odkladu po jejich/jejím zjištění e-mailem kontaktní osobě Dodavatele uvedené v čl. 11. odst. 11.2. této Smlouvy. Jestliže bude vada oznámena telefonicky, musí být následně doručena a potvrzena písemně.
- Nahlášení vady Systému musí být Dodavatelem potvrzeno nejpozději následující pracovní den a současně zahájeno řešení odstranění vady.
- Úplná oprava nebo funkčně rovnocenné náhradní řešení odstranění vady Systému musí být provedeno nejpozději do dvaceti (20) dnů od nahlášení vady.

Pokud je Dodavatel v prodlení s odstraněním vady a vadu neodstraní ani do pěti (5) dní od dodatečné písemné výzvy Objednatele, je Objednatel oprávněn jednostranně změnit svůj nárok z vadného plnění na přiměřenou slevu z ceny ve výši dle právních předpisů nebo nechat vadu odstranit na náklady Dodavatele třetí osobou nebo vadu na náklady Dodavatele odstranit sám. Tímto není dotčen nárok Objednatele změnit právo z vadného plnění na odstoupení od této Smlouvy, představuje-li daná vada podstatné porušení Smlouvy, a/nebo na úhradu smluvní pokuty.

Právo na změnu nároku dle tohoto článku Smlouvy Objednatel uplatní písemným prohlášením doručeným Dodavateli.

8.6 Práva a povinnosti Smluvních stran uvedená v tomto článku Smlouvy trvají, za podmínek zde uvedených, i po ukončení této Smlouvy.

8.7 Smluvní strany se zavazují poskytnout si součinnost pro vypořádání a odstranění vad Systému dle tohoto článku Smlouvy.

8.8 Systém má vady, jestliže nebyl dodán v souladu s touto Smlouvou. Za vady se považují i vady v návodech (manuálech) k použití, dokladech a/nebo dokumentech. Za vady se dále považují i právní vady Systému.

8.9 Dodavatel v rámci odpovědnosti za vady Systému odpovídá za vady, které má Systém v okamžiku jeho převzetí Objednatelem, i když se vada stane zjevnou až po této době. Dodavatel odpovídá rovněž za jakoukoli vadu Systému, jež vznikne v době trvání Záruky. Záruční doba neběží po dobu, po kterou Objednatel nemůže Systém užívat pro vady, za které odpovídá Dodavatel.

8.10 Nároky z vad Systém se nedotýkají nároku Objednatele na náhradu újmy nebo nároku na smluvní pokutu.

8.11 Záruka se vztahuje na Systém ve stavu k okamžiku podpisu Akceptačního protokolu s výrokem *Akceptováno* nebo k okamžiku podpisu Zápisu Objednatelem. Vznikne-li vada Systému až následně po provedení Díla v důsledku zásahu do Systému Objednatelem nebo třetí osobou, nebo v důsledku změn na externích systémech, Dodavatel za takovou vadu neodpovídá, záruka se na takovou vadu nevztahuje a Dodavatel není povinen vadu odstranit.

9. Vlastnické právo a práva duševního vlastnictví

Vlastnické právo

9.1 Vlastnické právo k případným hmotným složkám Plnění (zejména nosičům dat), a k ostatním materiálům se převádí na Objednatele okamžikem jejich převzetí.

Nebezpečí škody na hmotných složkách Plnění přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele (tj. okamžikem převzetí Objednatelem), pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Smluvních stran. Cena hmotných nosičů dat je již zahrnuta v ceně stanovené dle čl. 6. této Smlouvy.

Základní rozsah licence

9.2 Pokud při realizaci předmětu této Smlouvy vznikne plnění, které naplňuje znaky autorského díla ve smyslu Autorského zákona, poskytuje/postupuje Dodavatel Objednateli a Objednatel od Dodavatele získává oprávnění k výkonu práva užít dané autorské dílo všemi způsoby dle ustanovení § 12 Autorského zákona. Pro vyloučení pochybností se sjednává, že v rámci oprávnění k výkonu užít autorské dílo je Objednatel oprávněn autorské dílo dále rozvíjet podle svých potřeb. Dodavatel poskytuje tato práva v rozsahu nezbytném pro řádné užívání všech autorských děl, která budou vytvořena na základě této Smlouvy (dále jednotlivě jako „**Autorské dílo**“ a společně „**Autorská díla**“). Objednatel získává od Dodavatele uvedená práva k Autorským dílům, a to ke dni podpisu Akceptačního protokolu Objednatelem, v souladu s podmínkami dle čl. 5. této Smlouvy a jejími přílohami, zejména s Přílohou č. 2 až č. 14 Smlouvy, s výrokem „Akceptováno“ nebo „Akceptováno s výhradou“.

Práva k Autorským dílům jsou poskytována/postupována Dodavatelem Objednateli formou licenčního ujednání ve smyslu ustanovení § 2358 a násl. Občanského zákoníku majícího následující charakteristiky:

a) výhradní a neodvolatelná licence, k veškerým známým a zákonem povoleným způsobům užití jednotlivých Autorských děl a jejich případných dalších verzí, zejména k účelu, ke kterému byla taková Autorská díla Dodavatelem vytvořena v souladu se Smlouvou, a to v rozsahu minimálně nezbytném pro řádné užívání Autorského díla dle této Smlouvy,

b) licence neomezená územním (teritoriálním) a množstevním rozsahem a rovněž tak neomezená rozsahem užití, zejména neomezená počtem uživatelů či mírou využívání,

c) licence udělená na dobu určitou, a to na celou dobu trvání majetkových práv k předmětným Autorským dílům,

d) licence udělená s oprávněním Objednatele licenci zcela nebo z části, úplatně či bezúplatně, ve stejném nebo omezeném rozsahu poskytnout třetím osobám, a to formou poskytnutí podlicence podle ustanovení § 2363 Občanského zákoníku nebo toto právo na tyto třetí osoby postoupit podle ustanovení § 2364 Občanského zákoníku,

e) Objednatel není povinen uvádět na relevantních dokumentech autora Autorských děl; Dodavatel se zavazuje zajistit, že uvádění autora na relevantních dokumentech nebude po Objednateli požadováno,

f) licenci není možné Objednatelem vypovědět a na udělení těchto práv nemá vliv ani ukončení Smlouvy.

Objednatel není povinen poskytnutá práva (licenci) využít.

9.3 Dodavatel zároveň uděluje Objednateli souhlas k tomu, aby nejpozději ke dni akceptace Plnění dle této Smlouvy byl Objednatel oprávněn jednotlivá Autorská díla zveřejnit, upravovat, modifikovat, zpracovávat, překládat či měnit jejich název, a že je též oprávněn tato Autorská díla spojit s dílem jiným a zařadit je do díla souborného. Dodavatel prohlašuje, že disponuje veškerými souhlasy autorů ve smyslu tohoto odstavce Smlouvy. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel svěřil svá práva dle tohoto odstavce Smlouvy třetím osobám, které budou v budoucnu užívat Autorská díla vzniknuvší na základě této Smlouvy. Objednatel není povinen poskytnutá práva využít.

9.4 Dodavatel odpovídá za to, že je oprávněn udělit/postoupit Objednateli veškerá oprávnění k výsledkům plnění, včetně výsledků vytvořených třetími osobami. Je-li součástí plnění software, model, dataset, promptová knihovna, integrační vrstva, dokumentace nebo jiný výstup způsobilý právní ochrany, poskytuje/postupuje

Dodavatel Objednateli nejpozději ke dni akceptace Díla veškerá oprávnění potřebná k jeho neomezenému užití, úpravám, provozu, dalšímu rozvoji, bezpečnostnímu testování a předání v rámci státu a jím ovládaných subjektů. Dodavatel současně předá Objednateli úplnou technickou a provozní dokumentaci, a je-li to podle povahy plnění relevantní, i zdrojové kódy, konfigurační podklady, model cards, logiku rozhodování, popis tréninkových a validačních vstupů a auditní dokumentaci.

9.5 Vznikne-li v rámci Plnění dle této Smlouvy plnění naplňující znaky databáze dle Autorského zákona, poskytuje/převádí Dodavatel Objednateli k okamžiku podpisu Akceptačního protokolu zvláštní právo pořizovatele databáze, a to zejména právo databázi vytěžovat i zužitkovávat, a to jak celý její obsah, tak i její kvalitativně nebo kvantitativně podstatné části. Dodavatel dále poskytuje Objednateli právo udělit oprávnění k výkonu práva pořizovatele databáze jinému v rozsahu, jak je udělil Dodavatel Objednateli.

9.6 Smluvní strany dále výslovně prohlašují, že pokud při poskytování Plnění dle této Smlouvy vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Dodavatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena dle čl. 6. této Smlouvy je stanovena se zohledněním tohoto ustanovení a Dodavateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

9.7 Bude-li Autorské dílo nebo jeho část dílem zaměstnaneckým (dle ustanovení § 58 Autorského zákona) nebo dílem kolektivním (dle ustanovení § 59 Autorského zákona), je Dodavatel povinen vypořádat práva s autory takových děl (zejména opatřit potřebné souhlasy autorů a uhradit veškeré odměny autorům) tak, aby práva k takovému Autorskému dílu Objednateli mohl poskytnout v plném rozsahu dle tohoto článku Smlouvy a jejích příloh. Předáním Plnění či jeho části, které je Autorským dílem, Dodavatel poskytuje Objednateli potřebné licence a oprávnění k Autorskému dílu a zároveň tím stvrzuje, že veškerá práva s autory zaměstnaneckých či kolektivních děl řádně vypořádal a je oprávněn je poskytnout Objednateli.

9.8 Je-li část plnění dle této Smlouvy chráněna jiným způsobem, než jako Autorské dílo (ochrana jiných práv k duševnímu vlastnictví), uplatní se ustanovení tohoto článku Smlouvy analogicky tak, aby byl splněn účel této Smlouvy, tj. aby Objednatel obdržel dílo vč. všech jeho součástí vč. možnosti jej užívat, poskytovat k užívání, udržovat a rozvíjet, a to tak, aby tak mohl činit i samostatně nebo prostřednictvím třetí osoby. To se nevztahuje na začlenění proprietárních částí díla (např. knihoven), u nichž není možné taková práva zajistit, pokud s jejich začleněním Objednatel souhlasí.

Dodavatel je povinen k dosažení shora uvedeného účelu poskytnout rovněž související informace, zejm. zdrojové kódy, popisy databází, popisy architektury a jiné informace.

9.9 Licence ve smyslu odst. 9.2 až 9.8 tohoto článku Smlouvy se vztahuje ve stejném rozsahu na Autorská díla ve strojovém i zdrojovém kódu, jakož i k další Dokumentaci dle čl. 5 odst. 5.9 Smlouvy. Předchozí věta tohoto odstavce se vztahuje i na případné další verze Autorských děl vytvořených či upravených Dodavatelem na základě této Smlouvy a taktéž na související Dokumentaci.

9.10 Dodavatel prohlašuje, že udělení veškerých práv uvedených v odst. 9.2 až 9.9 tohoto článku Smlouvy nelze ze strany Dodavatele vypovědět a že na udělení těchto práv nemá vliv ani případné ukončení platnosti Smlouvy. V souvislosti s těmito ujednáními o licenční smlouvě ve smyslu tohoto čl. 9. Smlouvy Smluvní strany výslovně vylučují ustanovení § 2378, § 2379, § 2380, § 2381 a § 2382 Občanského zákoníku.

9.11 Dodavatel se zavazuje v případě, že se právo užití Autorského díla vztahuje k programům vytvořeným v programovacím jazyce, poskytnout Objednateli na jeho vyžádání strojové i zdrojové kódy takových programů vytvořených v programovacím jazyce, jakož i veškerou další Dokumentaci vztahující se k těmto zdrojovým kódům, to vše v plném rozsahu a aktuální verzi.

9.12 Dodavatel prohlašuje, že Autorská díla ani jejich části nemají žádné právní vady, že nejsou zatížena právy třetích osob týkajících se zejména vlastnického práva a práv duševního vlastnictví a že Dodavatel je zcela oprávněn disponovat bez jakéhokoliv omezení veškerými majetkovými právy k Autorským dílům a jejich částem a uzavřít s Objednatelem tuto Smlouvu na celý rozsah předmětu plnění. V případě, že se uvedené prohlášení Dodavatele nezakládá na pravdě, Dodavatel odpovídá Objednateli za vyplývající důsledky v plném rozsahu včetně odpovědnosti za skutečnou škodu a ušlý zisk. Uplatní-li třetí osoba své právo k Autorským dílům a/nebo jejich části, zavazuje se Dodavatel bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně oprávnění k výkonu práv užít Autorská díla Objednatelem, pokud jej k tomu Objednatel zmocní.

Možnost užití standardizovaného SW

9.13 Dodavatel se zavazuje zajistit k softwarovým produktům typu proprietárních SW, krabicových SW, komerčních SW či open source SW, které nejsou vyvíjeny na míru a jsou běžně distribuovány na trhu mnoha distributory, přičemž vzhledem k masovému užívání těchto SW nelze po Dodavateli spravedlivě požadovat, aby ovlivnil způsob sjednání licenčních podmínek požadovaných výrobcem SW a poskytl k takovýmto Autorským dílům a databázím licenci a související oprávnění ve smyslu předchozích odstavců tohoto čl. 9. Smlouvy (dále jen „**standardizované SW**“), minimálně takové formy licencí, které budou:

a) uděleny na dobu trvání majetkových práv,

b) nevýhradní,

c) přenositelné na třetí strany, tj. s právem Objednatele bez potřeby jakéhokoliv dalšího svolení Dodavatele a bez dalších nákladů, které by musel Objednatel nebo třetí strany vynaložit nad rámec Ceny uvedené v této Smlouvě (a to i v případě, že Objednatel nebo třetí strany mají již smluvně či jakkoli jinak zajištěná práva užívání licencí shodného výrobce či autora), udělit třetí osobě podlicenci k užití standardizovaného SW nebo svoje oprávnění k užití standardizovaného SW třetí osobě postoupit,

d) uděleny v územním rozsahu zahrnujícím celé území České republiky.

9.14 Pro vyloučení pochybností se stanoví, že v případě standardizovaného SW se může jednat jak o SW distribuovaný prostřednictvím hmotného nosiče, tak poskytnutí licence a SW prostřednictvím datové sítě, pro účel této Smlouvy se standardizovaným SW rozumí i proprietární knihovny třetích stran a jiný podobný SW, u kterého nelze po Dodavateli spravedlivě požadovat, aby ovlivnil způsob sjednání licenčních podmínek požadovaných výrobcem SW.

9.15 Dodavatel se zavazuje, že při provádění Plnění neporuší práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Dodavatel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku uplatnění práv třetích osob vůči Objednateli v souvislosti porušením povinnosti Poskytovatele dle tohoto odstavce Smlouvy.

9.16 Smluvní strany sjednávají, že veškerá finanční vyrovnání za poskytnutí Licence dle tohoto článku Smlouvy jsou zahrnuta v Ceně dle čl. 6. Smlouvy.

10. Další práva a povinnosti Smluvních stran

10.1 Dodavatel se zavazuje:

a) poskytovat Plnění řádně a včas v souladu s ujednáními obsaženými v této Smlouvě (včetně jejích příloh);

b) postupovat při poskytování Plnění s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy Objednatele a postupovat v souladu s interními předpisy souvisejícími s Plněním, pokud s nimi byl prokazatelně seznámen a jsou relevantní;

c) bez zbytečného odkladu oznámit Objednateli veškeré skutečnosti, které mohou mít vliv na povahu nebo na podmínky realizace Plnění;

d) informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách majících vliv na Plnění dle Smlouvy, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly Plnění ovlivnit;

e) použít veškeré podklady předané mu Objednatelem pouze pro účely Smlouvy a zabezpečit jejich řádné vrácení Objednateli, bude-li to objektivně možné vzhledem k jejich povaze a způsobu použití a v souladu s právními předpisy, s výjimkou informací a dokumentací uvedených v písm. f) a g) tohoto odstavce Smlouvy;

f) minimálně po dobu 10 let od účinnosti této Smlouvy poskytovat požadované informace a dokumentaci související s realizací předmětu Plnění zaměstnancům nebo zmocněncům pověřených orgánů (např. Ministerstva vnitra, Ministerstva financí, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci předmětu této Smlouvy a poskytnout jim při provádění kontroly součinnost;

g) uchovávat veškerou dokumentaci související s plněním předmětu této Smlouvy, včetně účetních dokladů, minimálně po dobu 10 let od účinnosti této Smlouvy. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji Dodavatel dodržet.

10.2 Poruší-li Dodavatel prokazatelně některou z výše uvedených povinností podle odst. 10.1 tohoto článku Smlouvy, nese odpovědnost za vady a za škodu, které v důsledku takového porušení povinnosti podle této Smlouvy Objednateli nebo třetím osobám vznikly.

10.3 Objednatel se zavazuje:

a) poskytovat Dodavateli úplné, pravdivé a včasné informace potřebné k řádné a včasné realizaci Plnění;

b) zabezpečit pro pracovníky Dodavatele přístup do určených objektů Objednatele za účelem řádného a včasného plnění Smlouvy;

c) zabezpečit účast pracovníků Objednatele či jím určených osob na pracovních schůzkách;

d) poskytnout Dodavateli veškeré informace relevantní pro poskytování Plnění podle této Smlouvy, zejména interní předpisy a pokyny, které jsou pro Dodavatele závazné, byl-li s nimi Dodavatel řádně prokazatelně seznámen;

e) poskytnout Dodavateli veškerou součinnost potřebnou k řádnému a včasnému poskytnutí Plnění.

10.4 Poruší-li Objednatel prokazatelně některou z výše uvedených povinností podle odst. 10.3 tohoto článku Smlouvy, nese odpovědnost za vady a za škodu, které v důsledku takového porušení povinnosti podle této Smlouvy Dodavateli nebo třetím osobám vznikly.

11. Oprávněné osoby Smluvních stran

11.1 Uzavřít Smlouvu, uzavírat dodatky ke Smlouvě a ukončovat Smlouvu prostřednictvím dohody nebo odstoupením od Smlouvy mohou výhradně oprávnění zástupci Smluvních stran. Za oprávněné zástupce Smluvních stran se považují pro účely této Smlouvy osoby, které mohou podle obecných právních předpisů jednat samostatně nebo společně s další osobou za Smluvní stranu (typicky ředitel příslušného útvaru nebo Projektu na straně Objednatele nebo ředitelé příslušných útvarů na straně Dodavatele).

11.2 Dodavatel dále určuje oprávněnou osobu pro účely Smlouvy. Oprávněná osoba vystupuje jako zástupce Dodavatele v případech právního jednání souvisejícího se Smlouvou s výjimkou případů stanovených v odst. 11.1 tohoto článku Smlouvy. Oprávněná osoba je zejména oprávněna podávat a přijímat informace o průběhu Plnění, vést s Objednatelem jednání obchodního charakteru, jednat v rámci akceptačního řízení, zejména podepsat Akceptační protokol/Zápis za Dodavatele.

Dodavatel určuje pro účely Smlouvy tyto oprávněné osoby:

- 
-

11.3 Objednatel dále určuje oprávněnou osobu pro účely Smlouvy. Oprávněná osoba vystupuje jako zástupce Objednatele v případech právního jednání souvisejícího se Smlouvou s výjimkou případů stanovených v odst. 11.1 Smlouvy. Oprávněná osoba je zejména oprávněna podávat a přijímat informace o průběhu Plnění, vést s Dodavatelem jednání obchodního charakteru a jednat v rámci akceptačního řízení, zejména podepsat Akceptační protokol/Zápis za Objednatele.

Objednatel určuje pro účely Smlouvy tuto oprávněnou osobu:

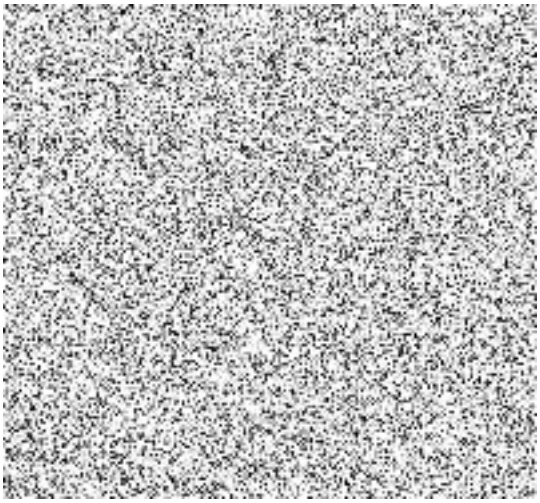
- PhDr. Daniel Doležal, Ph.D., tel: 974 847 602, 


11.4 Každá ze Smluvních stran dále určuje kontaktní osobu pro účely Smlouvy. Kontaktní osoba je určena zejména ke komunikaci mezi Smluvními stranami, pro řešení každodenních otázek spojených s poskytováním Plnění. Kontaktní osoba není oprávněna k právnímu jednání vyhrazenému oprávněnému zástupci podle odst. 11.1 tohoto článku Smlouvy nebo oprávněné osobě podle odst. 11.2 a 11.3 tohoto článku Smlouvy.

Smluvní strany určují pro účely Smlouvy následující kontaktní osoby:

a) Za Objednatele:

b) Za Dodavatele:



11.5 Každá ze Smluvních stran má právo změnit jí určenou oprávněnou osobu nebo kontaktní osobu, musí však o každé změně vyrozumět písemně (např. e-mailem) druhou Smluvní stranu. Změna oprávněné osoby nebo kontaktní osoby je vůči druhé Smluvní straně účinná okamžikem, kdy o ní byla písemně vyrozuměna. V souvislosti se změnou oprávněné nebo kontaktní osoby podle odst. 11.5 tohoto článku Smlouvy není nutné k této Smlouvě uzavírat dodatek.

12. Povinnost mlčenlivosti a zpracování osobních údajů

Povinnost mlčenlivosti

12.1 Smluvní strany se zavazují zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této Smlouvy získají od druhé Smluvní strany, o druhé Smluvní straně či jejich zaměstnancích a spolupracovnících, a nesmí je zpřístupnit bez písemného souhlasu druhé Smluvní strany žádné třetí osobě, využít pro sebe či pro jinou osobu, ani je použít v rozporu s účelem této Smlouvy, ledaže se jedná:

a) informace, které jsou veřejně přístupné; nebo

b) případ, kdy je zpřístupnění informace vyžadováno zákonem či závazným rozhodnutím oprávněného orgánu.

12.2 Smluvní strany jsou povinny zavázat povinností mlčenlivosti podle odst. 12.1 tohoto článku Smlouvy všechny osoby, které se budou podílet na poskytování Plnění podle této Smlouvy.

12.3 Povinnost mlčenlivosti trvá i po skončení účinnosti této Smlouvy.

Zpracování osobních údajů

12.4 V rámci řádného poskytování Plnění podle této Smlouvy je vyžadováno zpracování osobních údajů zaměstnanců Objednatele a Dodavatele. Osobní údaje budou zpracovávány v následujícím rozsahu:

- jméno a příjmení, titul;
- telefonní číslo;
- e-mailová adresa.

12.5 Zpracování osobních údajů je definováno příslušnou právní úpravou, přičemž se jedná zejména o jejich shromažďování, ukládání na nosiče informací, používání, třídění nebo kombinování, blokování a likvidaci s využitím manuálních a automatizovaných prostředků v rozsahu nezbytném pro zajištění řádného poskytování Plnění podle této Smlouvy. Pokud při plnění této Smlouvy dojde ke zpracování osobních údajů nad rámec kontaktních údajů smluvních stran, zejména v rámci analýzy, testování, validace nebo dokumentace řešení, uzavřou Smluvní strany před zahájením takového plnění samostatné ujednání o zpracování osobních údajů, které vymezí role stran, kategorie údajů, účely, dobu zpracování a bezpečnostní opatření.

12.6 Osobní údaje budou zpracovávány po dobu poskytování Plnění dle této Smlouvy. Ukončením této Smlouvy nezanikají povinnosti Smluvních stran týkající se bezpečnosti a ochrany osobních údajů až do okamžiku jejich protokolární úplné likvidace či protokolárního předání jinému zpracovateli.

13. Odpovědnost za škodu a pojištění

13.1 Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu podle platných právních předpisů a Smlouvy.

13.2 Žádná ze Smluvních stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že jí ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli. Překážka vzniklá ze škůdcových vnitřních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce podle Smlouvy povinen překonat, ho však povinnosti k náhradě škody nezprostí.

Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálního úsilí k jejich odvrácení a překonání.

13.3 Škoda se hradí v penězích nebo, je-li to možné nebo účelné, uvedením do předešlého stavu podle volby poškozené Smluvní strany v konkrétním případě.

13.4 Dodavatel se zavazuje, že bude mít po celou dobu účinnosti Smlouvy sjednánu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění minimálně ve výši 100 000 000 Kč. Dodavatel je povinen předat kopii pojistného certifikátu (pojistné smlouvy) Objednateli bezodkladně po podpisu Smlouvy oběma Smluvními stranami, a dále kdykoliv na vyžádání Objednatele, a to bez zbytečného odkladu, nejpozději však do 5 pracovních dnů od doručení písemné žádosti Objednatele.

13.5 Dodavatel je povinen k náhradě škody bez ohledu na to, zda je škoda kryta pojištěním. Škoda může být, byť částečně, uhrazena pojišťovnou dle sjednaného pojištění odpovědnosti za škodu.

14. Sankční ujednání

14.1 Smluvní strany se dohodly na smluvních pokutách podle následujících odstavců tohoto článku Smlouvy.

14.2 V případě prodlení Dodavatele s provedením Díla v termínu podle čl. 4 odst. 4.2 písm. b) Smlouvy je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 2 000 Kč, a to za každý i započatý kalendářní den prodlení.

14.3 Poruší-li Dodavatel jakoukoli svou další povinnost podle čl. 7. odst. 7.9, čl. 9. a čl. 13. odst. 13.4 této Smlouvy, zavazuje se Objednateli uhradit smluvní pokutu ve výši 100 000 Kč za každé jednotlivé porušení povinnosti.

14.4 V každém jednotlivém případě porušení povinnosti mlčenlivosti podle čl. 12 této Smlouvy je oprávněná Smluvní strana oprávněna požadovat od Smluvní strany, která povinnost porušila, zaplacení smluvní pokuty ve výši 50 000 Kč.

14.5 Pro jeden případ porušení povinností stanovených Smlouvou nelze kumulativně uplatnit více smluvních pokut.

14.6 Zaplacením smluvní pokuty není jakkoli dotčen nárok oprávněné Smluvní strany na náhradu škody ve výši přesahující výši smluvní pokuty. Zaplacením smluvní pokuty není dotčeno splnění povinnosti, která je prostřednictvím smluvní pokuty zajištěna.

14.7 V případě prodlení kterékoli Smluvní strany se zaplacením peněžité částky vzniká oprávněné Smluvní straně nárok na úrok z prodlení v zákonné výši počítaný z dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen její nárok na náhradu vzniklé škody.

14.8 Vyúčtování smluvní pokuty/úroků z prodlení – penalizační faktura – musí být druhé Smluvní straně zasláno datovou zprávou prostřednictvím datové schránky. Smluvní pokuta/úroky z prodlení jsou splatné ve lhůtě 30 dnů ode dne doručení penalizační faktury povinné Smluvní straně. Úhrada smluvní pokuty/úroků z prodlení se provádí bankovním převodem na účet oprávněné Smluvní strany uvedený v penalizační faktuře. Částka se považuje za zaplacenou okamžikem jejího připsání ve prospěch účtu oprávněné Smluvní strany.

14.9 Obě Smluvní strany se zavazují před uplatněním nároku na smluvní pokutu nebo úrok z prodlení vyzvat druhou Smluvní stranu k podání vysvětlení porušení smluvní povinnosti.

15. Spolupráce a vzájemná komunikace

15.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění Smlouvy.

15.2 Smluvní strany jsou povinny plnit své závazky vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a k prodlení splatnosti jednotlivých peněžních závazků.

15.3 Veškerá komunikace mezi Smluvními stranami bude probíhat primárně prostřednictvím kontaktních osob určených v čl. 11 odst. 11.4 této Smlouvy, v odůvodněných případech prostřednictvím oprávněných osob určených v čl. 11 odst. 11.2 a 11.3 této Smlouvy nebo oprávněných zástupců Smluvních stran.

15.4 Veškerá oznámení, tj. jakákoliv komunikace na základě Smlouvy, bude probíhat v souladu s tímto čl. 15 Smlouvy. Jakékoli oznámení, žádost či jiné sdělení, které má být učiněno nebo dáno Smluvní straně podle Smlouvy, bude učiněno nebo dáno písemně. Kromě jiných způsobů komunikace dohodnutých mezi Smluvními stranami (viz odst. 15.3 tohoto článku Smlouvy) se za účinné považují osobní doručování, doručování doporučenou poštou, kurýrní službou, datovou schránkou či elektronickou poštou, a to na adresy Smluvních stran uvedené v záhlaví Smlouvy nebo na takové adresy, které si Smluvní strany vzájemně písemně oznámí.

15.5 Oznámení správně adresovaná se považují za doručená:

a) dnem, o kterém tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, je-li oznámení zasíláno prostřednictvím datové zprávy do datové schránky ve smyslu tohoto zákona; nebo

b) dnem fyzického předání oznámení, je-li oznámení zasíláno prostřednictvím kurýra nebo doručováno osobně; nebo

c) dnem doručení potvrzeným na doručence, je-li oznámení zasíláno doporučenou poštou; nebo

d) dnem, kdy bude, v případě, že doručení výše uvedeným způsobem nebude z jakéhokoli důvodu možné, oznámení odesláno doporučenou poštou na adresu Smluvní strany, avšak k jeho převzetí z jakéhokoli důvodu nedojde, a to ani ve lhůtě 3 pracovních dnů od jeho uložení na příslušné pobočce pošty.

16. Doba trvání Smlouvy a možnosti jejího ukončení

16.1 Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění Smlouvy v registru smluv zajistí Objednatel.

16.2 Smlouva je uzavřena na dobu určitou, a to na dobu vyplývající z čl. 4 odst. 4.2 Smlouvy, nebo do splnění všech závazků z této Smlouvy, podle toho, která ze skutečností nastane dříve.

16.3 Uplynutím doby, na kterou je Smlouva uzavřena dle odst. 16.2 tohoto článku Smlouvy, nejsou dotčena práva a povinnosti, která mají podle zákona nebo Smlouvy trvat i po jejím ukončení.

16.4 Smlouva může být ukončena:

a) písemnou dohodou Smluvních stran; nebo
b) odstoupením od Smlouvy kteroukoliv ze Smluvních stran za podmínek uvedených v tomto článku Smlouvy.

16.5 Objednatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Dodavatelem, přičemž za podstatné porušení Smlouvy se bude považovat:

a) porušení povinnosti mlčenlivosti dle čl. 12. Smlouvy;
b) opakované (tj. nejméně 3x) prodlení Dodavatele s poskytnutím Plnění v termínu stanoveném touto Smlouvou v délce přesahující 30 dnů; nebo
c) další případy, o kterých tak stanoví výslovně Smlouva.

16.6 Dodavatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, přičemž za podstatné porušení Smlouvy se bude považovat zejména:

a) porušení povinnosti mlčenlivosti dle čl. 12. Smlouvy;
b) prodlení Objednatele s úhradou ceny za Plnění delší než 60 dnů, pokud Objednatel nezjedná nápravu ani do 30 dnů od doručení písemného oznámení Dodavatele o takovém prodlení se žádostí o jeho nápravu; nebo
c) opakované (tj. nejméně 3x) porušení povinnosti Objednatele uvedené v čl. 10. odst. 10.3 Smlouvy, které Objednatel neodstraní ani v dodatečné lhůtě stanovené v písemné výzvě Dodavatele, která nesmí být kratší než 30 dnů.

16.7 Smluvní strany se dále dohodly, že odstoupení od Smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně.

16.8 Ukončením účinnosti Smlouvy nejsou dotčena práva a povinnosti založená touto Smlouvou, která mají podle zákona, Smlouvy nebo na základě své povahy trvat i po jejím skončení, zejména ustanovení Smlouvy o odpovědnosti za škodu, o povinnosti mlčenlivosti, o právech duševního vlastnictví a o sankcích.

17. Závěrečná ustanovení

17.1 Smluvní strany podpisem Smlouvy sjednávají, že pokud Smlouva nestanoví jinak, závazky Smlouvou založené budou vykládány výhradně podle obsahu této Smlouvy, bez přihlédnutí k jakékoli skutečnosti, která nastala a/nebo byla sdělena jednou Smluvní stranou druhé Smluvní straně před uzavřením Smlouvy.

17.2 Smlouva představuje úplnou dohodu Smluvních stran o předmětu Smlouvy a všech náležitostech, které Smluvní strany měly a chtěly ve Smlouvě ujednat a které považují za důležité pro závaznost Smlouvy. Žádný projev Smluvních stran učiněný po uzavření Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními Smlouvy a nezakládá žádný závazek žádné ze Smluvních stran.

17.3 Smlouvu je možné měnit a doplňovat pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků Smlouvy, podepsaných oprávněnými zástupci obou Smluvních stran.

17.4 Smlouva se řídí českým právním řádem. Práva a povinnosti Smluvních stran, které nejsou přímo upraveny touto Smlouvou, se řídí zejména příslušnými ustanoveními Občanského zákoníku.

17.5 Všechny spory Smluvních stran vzniklé z této Smlouvy nebo v souvislosti s ní budou řešeny před příslušnými obecnými soudy České republiky.

17.6 Pokud kterékoli ustanovení této Smlouvy nebo jeho část je nebo se stane neplatným či nevynutitelným, nebude mít tato neplatnost či nevynutitelnost vliv na platnost či vynutitelnost ostatních ustanovení této Smlouvy nebo jejích částí, pokud nevyplývá přímo z obsahu této Smlouvy, že toto ustanovení nebo jeho část nelze oddělit od dalšího obsahu. V takovém případě se obě Smluvní strany zavazují neúčinné a neplatné ustanovení nahradit novým ustanovením, které je svým účelem a významem co nejbližší ustanovení této Smlouvy, jež má být nahrazeno.

17.7 Smlouva je uzavřena elektronicky a je podepsána elektronickými podpisy.

17.8 Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1: Struktura ceny Plnění
Příloha č. 2: Technická specifikace nástroje Třídění dokumentů mezi útvary
Příloha č. 3: Technická specifikace nástroje Třídění dokumentů nepříslušnost
Příloha č. 4: Technická specifikace nástroje Opatření proti nečinnosti
Příloha č. 5: Technická specifikace Pseudonymizační nástroj
Příloha č. 6: Technická specifikace komponenty „Bridge/API“
Příloha č. 7: Technická specifikace AI Responder
Příloha č. 8: Diagram architektury modulů
Příloha č. 9: Vývojový diagram pro Třídění dokumentů
Příloha č. 10: Exit plán
Příloha č. 11: Akceptační plán Systému
Příloha č.12: Diagram Nepříslušnost
Příloha č. 13: Diagram Třídění dokumentů mezi útvary
Příloha č. 14: Technická specifikace implementace
Příloha č. 15: Vzor Akceptačního protokolu

17.9 Smluvní strany shodně prohlašují, že si Smlouvu před jejím podpisem přečetly a že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.

Za Objednatele:	Za Dodavatele:
V Praze dne *dle elektronického podpisu*	V Praze dne *dle elektronického podpisu*
PhDr. Daniel Doležal, Ph.D.	Digitálně podepsal Datum: 2026.05.28 17:38:57 +02'00'
……. *ředitel odboru archivní správy a spisové služby*	……. *pověřený ředitel*

Elektronický podpis: 3.6.2026
Certifikát autora podpisu:
Jméno: PhDr. Daniel Doležal Ph.D.
Vydal: NCA SubCA1/RSA 10/2023
Platnost do: 22.9.2028 10:16 +02:00

Příloha č.1: Struktura ceny Plnění

1. Aktivity NAKIT – projektové řízení

Role	Cena/ČH bez DPH	Hodin	Celkem bez DPH	DPH 21 %	Celkem vč. DPH
Projektový manažer senior	2 321,00 Kč	585	1 357 785,00 Kč	285 134,85 Kč	1 642 919,85 Kč
Projektový manažer	1 624,00 Kč	510	828 240,00 Kč	173 930,40 Kč	1 002 170,40 Kč
AI architekt senior	2 306,00 Kč	630	1 452 780,00 Kč	305 083,80 Kč	1 757 863,80 Kč
Analytik senior	1 779,00 Kč	573	1 019 367,00 Kč	214 067,07 Kč	1 233 434,07 Kč
Specialista legislativy senior	1 755,00 Kč	40	70 200,00 Kč	14 742,00 Kč	84 942,00 Kč
Specialista nákupu senior	1 406,00 Kč	40	56 240,00 Kč	11 810,40 Kč	68 050,40 Kč
Produktový manažer senior	1 742,00 Kč	85	148 070,00 Kč	31 094,70 Kč	179 164,70 Kč
Architekt kybernetické bezpečnosti	2 036,00 Kč	300	610 800,00 Kč	128 268,00 Kč	739 068,00 Kč
Bezpečnostní manažer senior	1 557,00 Kč	90	140 130,00 Kč	29 427,30 Kč	169 557,30 Kč
Celkem projekt. řízení			**5 683 612,00 Kč**	**1 193 558,52 Kč**	**6 877 170,52 Kč**

2. Aktivity NAKIT – AI Governance

Role	Cena/ČH bez DPH	Hodin	Celkem bez DPH	DPH 21 %	Celkem vč. DPH
Projektový manažer senior	2 321,00 Kč	85	197 285,00 Kč	41 429,85 Kč	238 714,85 Kč
Architekt senior	2 306,00 Kč	90	207 540,00 Kč	43 583,40 Kč	251 123,40 Kč
Specialista legislativy senior	1 755,00 Kč	55	96 525,00 Kč	20 270,25 Kč	116 795,25 Kč
Analytik senior	1 779,00 Kč	55	97 845,00 Kč	20 547,45 Kč	118 392,45 Kč
Bezpečnostní manažer senior	1 557,00 Kč	60	93 420,00 Kč	19 618,20 Kč	113 038,20 Kč
Projektový manažer	1 624,00 Kč	85	138 040,00 Kč	28 988,40 Kč	167 028,40 Kč
Celkem – AI Governance			**830 655,00 Kč**	**174 437,55 Kč**	**1 005 092,55 Kč**

3. Externí náklady

Položka	Celkem bez DPH	DPH 21 %	Celkem vč. DPH
AI use cases	3 340 000,00 Kč	701 400,00 Kč	4 041 400,00 Kč
Celkem – Externí	**3 340 000,00 Kč**	**701 400,00 Kč**	**4 041 400,00Kč**

4. Souhrnná cenová tabulka

Položka	Celkem bez DPH	DPH 21 %	Celkem vč. DPH
Aktivity NAKIT	6 514 267,00 Kč	1 367 996,07 Kč	7 882 263,07 Kč
Externí dodávka	3 340 000,00 Kč	701 400,00 Kč	4 041 400,00 Kč
Celkem	**9 854 267,00 Kč**	**2 069 396,07 Kč**	**11 923 663,07 Kč**

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	B6D09A317667B215C86A9D6316D76E6455BF8C27D78ACFDB847DB79C4080DD4F
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 2 – Technická specifikace nástroje Třídění dokumentů mezi útvary

Obsah

1. Účel a rozsah

1.1 Tento dokument definuje požadavky na schopnost automatizovaného a poloautomatizovaného třídění příchozích dokumentů do organizačních útvarů Koncového zákazníka Objednatele, včetně podpory dávkového zpracování, ručních oprav, auditovatelnosti, metrik kvality a provozních standardů.

1.2 Cílem je snížit manuální zátěž, zvýšit rychlost doručení a zajistit prokazatelnou kvalitu i bezpečnost.

1.3 Modul pro Třídění dokumentů mezi útvary Objednatele je navržen tak, aby mohl být dodán a provozován jako samostatná služba s jasně definovanými rozhraními, nezávisle na dodavateli jiných komponent.

2. Definice a zkratky

2.1 Taxonomie útvarů: řízený referenční seznam útvarů a jejich rolí v rámci Objednatele (zdroj pravdy v Master Data).

2.2 Abstain/NEURČITO: stav, kdy systém nedosahuje stanoveného minimálního konfidenčního prahu a vyžaduje lidský přezkum.

2.3 Golden set: reprezentativní a anotovaný vzorek dokumentů pro měření kvality a regresní testy.

2.4 Correlation-ID: end-to-end korelační identifikátor pro trasování.

3. Předpoklady a vazby

3.1 Třídění probíhá výhradně nad pseudonymizovanými vstupy. Respektuje centrální katalog rozhraní, bezpečnostní politiku egress, pravidla logování bez PII a procesy akceptačních testů.

3.2 Změna taxonomie útvarů je řízená, verzovaná a vyžaduje přezkoušení kvality.

4. Role

4.1 Tato kapitola popisuje role, které se na procesu vyhodnocení třídění dokumentů, návrhu cílového útvaru Koncového zákazníka Objednatele a případného vrácení podání podílejí. Z role vyplývají typické činnosti uživatelů v rámci modulu třídění mezi útvary Koncového zákazníka Objednatele, jejich oprávnění a odpovědnost za jednotlivé kroky procesu.

4.2 Jednotlivé role jsou:

a) Superadmin: provádí opravy, schvaluje změny tříd, mapování a výjimky. Ověřuje úplnost, správnost a dohledatelnost procesů a záznamů. Spravuje integrační parametry, fronty, limity a přístupy.
b) Pracovník podatelny: iniciuje požadavek, který je skrze API/Bridge odeslán do modulu pro třídění dokumentů. Tento požadavek může být buď pro přiřazení útvaru pro zvolené podání, nebo pro odeslání zpětné vazby u chybných návrhů přiřazení. Kontroluje návrh zařazení.
c) Záruční servis, řeší vady v rámci záruky.

5. Nefunkční požadavky (NFR)

5.1 Interaktivní odezva UI bez AI do 300 ms p95.

5.2 Klasifikace 1 MB textu do 1500 ms p95.

5.3 Plná auditovatelnost včetně Correlation-ID.

5.4 RBAC/MFA, žádná nepseudonymizovaná PII v logu.

5.5 Sledování metrik: přesnost, pokrytí, podíl manuálních zásahů, latence, chybovost, náklady na 1000 dokumentů.

5.6 Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

6. Hlavní uživatelské scénáře (user stories s kritérii)

6.1 Tato kapitola popisuje typické situace, které uživatelé modulu pro rozřazení mezi útvary Koncového zákazníka Objednatele řeší, ve formě uživatelských scénářů s akceptačními kritérii. Slouží jako most mezi požadavky Objednatele a implementací Dodavatele, protože ukazuje, jak má systém v konkrétních případech fungovat. User stories jsou zároveň podkladem pro akceptační testy a ověřování splnění požadavků.

6.2 US-POD-01 Automatické přiřazení:

a) Jako pracovník podatelny Objednatele požaduji, aby modul po iniciování požadavku pro přiřazení útvaru (skrze Bridge/API) navrhl cílový útvar, abych minimalizoval ruční třídění.

b) Akceptační kritéria:

i. Given validní podání, When iniciuji požadavek, Then systém navrhne útvar s konfidenčním skóre ≥ 0,80 a stručným vysvětlením.

ii. Given skóre < 0,70, When iniciuji požadavek, Then systém vrátí NEURČITO a zařadí do fronty přezkumu.

iii. Given dokument nepřísluší žádnému útvaru, When iniciuji požadavek, Then systém vrátí „nepříslušný“ a doporučí předání na věcně příslušný orgán.

6.3 US-POD-03 Manuální oprava a učení z feedbacku:

a) Jako superadmin požaduji opravit chybné přiřazení přímo v modulu, aby se modul postupně zlepšoval.

b) Akceptační kritéria:

i. Given chybně přiřazený dokument, When zvolím jiný útvar a uložím, Then změna se zapíše do auditu a vstoupí do datové sady určené pro retrénink modelů.

ii. Given opakovaná chyba u stejné třídy, When se chybovost zvýší nad limit, Then je automaticky navržen retrénink.

6.4 US-POD-04 Inicializace požadavku skrze API/Bridge

a) Jako pracovník podatelny požaduji mít možnost iniciovat požadavek, který je systémem odeslán prostřednictvím API/Bridge do modulu pro třídění dokumentů. Tento požadavek může být buď pro přiřazení útvaru pro zvolené podání, nebo pro odeslání zpětné vazby u chybných návrhů přiřazení.

b) Akceptační kritéria:

i. Given je iniciován proces pracovníkem podatelny, When systém zahájí zpracování, Then systém vytvoří platný požadavek obsahující všechna povinná data.

ii. Given existuje platný požadavek, When je požadavek odesílán, Then systém odešle požadavek prostřednictvím definovaného API do cílového modulu.

iii. Given je požadavek odeslán, When systém obdrží odpověď nebo chybu z API, Then systém výsledek zaznamená a nastaví odpovídající stav požadavku (úspěch / chyba).

6.5 US-KUR-01 Změna taxonomie:

a) Jako superadmin požaduji schvalovat změny tříd, abych zachoval konzistenci třídění.

b) Akceptační kritéria:

i. Given návrh změny, When jej schválím, Then se verze taxonomie navýší a spustí se validační testy nad golden setem.

ii. Given kritická změna, When je publikována, Then se zablokuje nasazení, dokud nový model nedosáhne cílových metrik.

6.6 US-AUD-01 Auditovatelnost:

a) Jako superadmin požaduji dohledat, kdo a proč dokument přiřadil, abych ověřil soulad.

b) Akceptační kritéria:

i. Given ID dokumentu, When provedu dotaz, Then získám historii návrhů, opravy, skóre, důvody a Correlation-ID.

7. Negativní a hraniční scénáře

7.1 Poškozené soubory, neznámé formáty, extrémně krátké či dlouhé texty, vícejazyčné dokumenty, skeny s nízkou kvalitou. Pro každý typ je definováno deterministické chování, včetně návrhu manuálního postupu.

8. Kvalitativní metriky

8.1 Vedle „úspěšnosti“ se měří precision, recall a F1-score po třídách, macro/micro průměry a coverage (podíl predikcí bez abstain).

8.2 Cíle: macro-F1 ≥ 0,93, coverage ≥ 90 % při zachování přesnosti.

8.3 Metriky se reportují měsíčně; pokles pod práh vyvolá nápravný plán.

9. Akceptační testy a golden set

9.1 Dodavatel předloží golden set s reprezentativním pokrytím tříd, formátů a jazyků.

9.2 Akceptace probíhá nad dohodnutými metrikami a scénáři. Součástí je i stínový provoz a A/B nasazení s možností rychlého návratu verze.

10. Předávací artefakty

10.1 Konfigurační a provozní dokumentace, runbooky a DR playbooky, dashboardy a alerty, export přístupových politik, výchozí nastavení limitů a šablony reportů.

10.2 Dodavatel Bridge/API předloží závaznou specifikaci eSSL ↔ Bridge s detailní definicí payloadů, kódů chyb, validačních pravidel a pořadovosti událostí (OpenAPI/AsyncAPI + JSON Schema). Součástí je kontraktní test-pack, který musí projít jak implementace Bridge/API, tak adaptér eSSL. Změna kontraktu je řízena verzováním a nelze ji nasadit bez úspěšného průchodu integračními testy.

10.3 Dodavatel musí předložit exit plán pro případ ukončení provozu nebo změny dodavatele, včetně exportu dat, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v Příloze č. 9 Exit plán.

11. Definition of Done

11.1 Implementováno, otestováno (funkčně, integračně, výkonově), nastaven monitoring s prahy, předány artefakty z kapitoly 10, aktualizován katalog rozhraní a záznam o verzi.

12. User stories

12.1 Kapitola 12 slouží výhradně jako informativní příklad. Závazné jsou pouze požadavky a akceptační kritéria definovaná v kapitolách 5–11; odesílání mimo resort vyžaduje datový kontrakt cílových orgánů a důkaz doručení. Vynucení těchto podmínek probíhá přes Bridge/API (řízení rozhraní a bezpečný egress).

12.2 Jednotlivé user stories:

a) Příjem, spárování, návrh přiřazení

Pracovník podatelny iniciuje požadavek pro přiřazení útvaru pro vybrané podání (listinné skeny z výstupní složky skeneru s krátkou časovou prodlevou nebo elektronická podání z datové schránky/e-mailu), který je odeslán skrze Bridge/API do modulu. Modul dokument spáruje podle jednoznačného identifikátoru (štítek/QR/čárový kód) s kartou v eSSL. Modul navrhne přiřazení ke konkrétnímu útvaru na základě obsahové klasifikace (adresace, klíčová slova, jazykové rysy) a přes Bridge/API odešle zpět do výchozího systému stručné vysvětlení („reason code“). Kvalitativní prahy jsou konfigurovatelné per třída; pokud skóre klesne pod NEURČITO, dokument jde do fronty přezkumu. Je-li k dispozici vytěžování metadat, použije se k předvyplnění polí karty (jinak manuálně).

b) Kontroly před zpracováním

Před zpracováním požadavku na přiřazení modul provede kontrolu čitelnosti a ověření, zda dokument a jeho přílohy odpovídají seznamu povolených formátů. U elektronických podání (DS/e-mail) se dále ověřuje elektronický podpis/časové razítko a validita kontejneru ISDS (ZFO) včetně integrity a metadat obálky. Paralelně proběhne bezpečnostní kontrola (AV/DLP); podezřelé soubory jsou přesunuty do karantény. Nevyhovující podání je vráceno vždy s uvedením důvodu a záznamem v auditu. Vyhovující podání je dále zpracováno a modul vygeneruje návrh přiřazení. Konfidenční prahy per třída a stav NEURČITO se uplatňují

i v tomto kroku; jejich hodnoty se řídí metrikami kvality (kap. 8) a akceptačním rámcem (kap. 9–11).

c) **Historie**
Superadmin může sledovat historii (filtry dle období).

d) **Zpětná vazba v eSSL**
Pracovník podatelny zadá zpětnou vazbu na špatně zařazený dokument iniciováním požadavku, který je odeslán skrze API/Bridge do modulu. Modul ji převezme do učení/modelových korekcí.

e) **Parametry třídění (AI/Třídění)**
Superadmin (AI/Třídění) může nastavovat a upravovat parametry třídění (např. prahy, výjimky), nikoli administraci eSSL.

f) **Audit výkonu AI (AI/Třídění)**
Superadmin (AI/Třídění) má přístup k historii rozhodnutí AI a může auditovat výkon klasifikace (mimo administraci eSSL).

g) **Statistiky úspěšnosti**
Superadmin (AI/Třídění) může zobrazit statistiky úspěšnosti automatického třídění a podílu manuálních zásahů.

h) **Export dat**
Superadmin (AI/Třídění) může exportovat data o třídění pro další analýzu.

i) **RBAC/MFA (AI/Třídění)**
Superadmin (AI/Třídění) může spravovat uživatelské účty a oprávnění v rámci komponent třídění/AI (RBAC/MFA); správa účtů v eSSL zůstává mimo rozsah.

j) **Dávky – stav, chyby, duplicity**
Jako pracovník podatelny chci iniciovat dávku dokumentů pro zpracování, abych zrychlil zpracování. Superadmin může zobrazit stav zpracování dávky (úspěšně zařazeno / čeká na zásah / odesláno), včetně seznamu vadných položek s důvodem a detekce duplicit (s vazbou na původní záznam).

k) **Seznam neautomaticky zařazených dokumentů**
Superadmin může zobrazit seznam neautomaticky zařazených dokumentů (vyhodnocených jako NEURČITO).

l) **Opětovné zpracování (re-process)**
Pracovník podatelny může zadat opětovné zpracování (re-process) iniciováním požadavku, který je odeslán skrze API/Bridge do modulu.

m) **Auditní stopa a transakční protokoly**

Systém automaticky eviduje všechny kroky zpracování (auditní stopa, transakční protokoly); superadmin může dohledat korelace (Correlation-ID). To je odlišné od uživatelské historie v písm. c).

n) Integrační parametry a allow-list (AI/Třídění)

Superadmin (AI/Třídění) může nastavit integrační parametry pro napojení na spisové služby Objednatele a externí orgány (endpointy/formáty) a spravovat allow-list destinací na úrovni Bridge/API v souladu s governance; nejde o administraci eSSL.

o) Reason code

Superadmin může zobrazit důvod přiřazení u jednotlivých podání (vysvětlení/„reason code“). V případě iniciování požadavku pracovníkem podatelny prostřednictvím API/Bridge, modul po zpracování požadavku vrátí důvod přiřazení (vysvětlení/„reason code“) prostřednictvím API/Bridge zpět volajícímu systému.

p) Úrovně automatizace

Superadmin (AI/Třídění) může nastavit úrovně automatizace (plně automatické, s potvrzením, testovací).

q) Reporty o zpracování

Modul umožňuje superadminovi zobrazit a stáhnout reporty o zpracování za zvolené období (např. počty automaticky zařazených, ručně upravených, NEURČITO a chybně zařazených dokumentů, včetně podílů a trendů). Definice kvalitativních metrik třídění (např. macro-F1, coverage, prahy per-třída, pravidla NEURČITO) jsou převzaté z kapitoly 8, zatímco provozní SLO/SLA (např. dostupnost, chybovost a latence p95/p99 měřená na hraně služby, integrita doručenek a egressu) jsou převzaté z kapitoly 13.2. Reporty tyto metriky jen zobrazují a agregují, jejich výpočetní definice a metodika měření se v kapitole 12. nedefinují.

r) Výjimky

Superadmin (AI/Třídění) může spravovat seznam výjimek se záznamem změn a RBAC.

s) Historie feedbacku

Superadmin (AI/Třídění) může zobrazit historii zpětné vazby k dokumentům a její využití pro učení modelu a řízení kvality.

t) Stavová hlášení

Modul poskytuje průběžná stavová hlášení o zpracování dokumentu prostřednictvím Bridge/API, včetně informace o zahájení zpracování, jednotlivých krocích, dokončení nebo chybovém stavu.

13. Požadavky na kvalitu, bezpečnost, akceptaci

13.1 Akceptační a předávací řízení:

a) Akceptační řízení ověřuje splnění funkčních, nefunkčních a bezpečnostních požadavků na základě předem definovaných scénářů, metrik a prahových hodnot.

b) Dodavatel předá akceptační balíček obsahující testovací scénáře, datové sady, protokoly a měřicí skripty. Testovací scénáře musí být Objednatelem schváleny před zahájením testování.

c) Akceptace probíhá z pohledu Objednatele na hraně služby a zahrnuje kontrolu dashboardů, alertů a provozních runbooků.

d) Neúspěšné testy jsou zdokumentovány včetně nápravných opatření a termínů opakování.

13.2 Verzování, kompatibilita a deprekační politika:

a) Verze rozhraní a artefaktů se řídí schématem major.minor.patch.

b) Zpětná kompatibilita je povinná v rámci minor/patch verzí.

c) Pokud odstranění vady (v rámci záručního servisu) vyžaduje změnu, která není zpětně kompatibilní, je Dodavatel povinen na tuto skutečnost předem upozornit a dohodnout se s Objednatelem/Koncovým zákazníkem na postupu a termínu přechodu.

d) Veškeré kontrakty rozhraní (OpenAPI/AsyncAPI, schémata zpráv) jsou verzované a publikované v katalogu rozhraní.

13.3 Bezpečnost a suverenita dat:

a) Požadavky na kybernetickou bezpečnost jsou uvedené v Příloze č. 14 Smlouvy.

13.4 FinOps, kvóty a ochranné mechanismy:

a) Služba publikuje metriky využití pro účely showback/chargeback a kapacitního plánování.

b) Jsou definovány kvóty a limity na uživatele (počet požadavků, objem dat, paralelizace), včetně ochranných mechanismů proti degradaci kvality (rate-limit, circuit-breaker).

c) Překročení limitů generuje auditní záznam a notifikaci.

d) Reporty obsahují náklady na jednotku zpracování, predikci trendu a doporučení optimalizace.

13.5 AI governance a post-market monitoring:

a) Je-li součástí řešení model umělé inteligence nebo statistický model, dodavatel vede modelovou dokumentaci (model card), verzuje modely i datasety, zajišťuje sledování kvality v čase, detekci datového i konceptuálního driftu a bezpečné nasazování (stínový provoz, A/B testy, možnost rychlého návratu verze).

b) Řešení je klasifikováno dle relevantní regulace AI a je vedena vyžadovaná technická dokumentace.

c) Objednatel provede posouzení dopadů na ochranu osobních údajů; dodavatel poskytne podklady a součinnost.

d) Pokud řešení AI neobsahuje, kapitola je označena jako neaplikovatelná.

13.6 Předávací artefakty a provozní dokumentace:

a) Dodavatel předá kompletní balík:
   i. provozní a konfigurační dokumentaci,
   ii. runbooky a DR playbooky,
   iii. monitorovací dashboardy s alerty a prahovými hodnotami,
   iv. export přístupových politik,
   v. výchozí nastavení limitů,
   vi. testovací balíčky (funkční, integrační, výkonové, chaos) a protokoly o provedených akceptačních testech.

b) Součástí je aktualizace katalogu rozhraní, evidence verzí dodaných artefaktů a seznam známých omezení s plánem nápravy.

13.8 Integrátor a Go/No-Go brány:

a) Dodavatel nominuje hlavního integrátora odpovědného za E2E integraci a uvedení do provozu.

b) Nasazení probíhá přes Go/No-Go brány:

   i. kontraktní testy všech rozhraní,
   ii. E2E výkonnost,
   iii. E2E DR test,
   iv. E2E bezpečnost (DLP gating).

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	987411CACE0B1339F8734AF00457C183B98F10D867BE3F015883447CA2FD3A37
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 3 – Technická specifikace nástroje Třídění dokumentů nepříslušnost

Obsah

Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

1. Účel a rozsah

1.1 Tento dokument definuje požadavky na modul nepříslušnosti, tedy schopnost systému automaticky a poloautomaticky rozpoznat, že příchozí podání nepatří do působnosti Koncového zákazníka Objednatele (Ministerstva vnitra, dále jen „MV“, a jím spravované agendy), a dále:

a) navrhnout věcně příslušný orgán nebo adresáta,
b) zajistit auditovatelnost, měření kvality, provozní standardy a bezpečnost.

1.2 Modul řeší jak přímé rozpoznání nepříslušnosti (podání zjevně adresované jinému orgánu), tak situace, kdy se ani po jednom nebo více pokusech nepodaří podání věcně přiřadit do působnosti MV.

1.3 Rozsah zahrnuje:

a) algoritmickou a případně AI klasifikaci nepříslušnosti (text, metadata, adresace),
b) návrh věcně příslušného orgánu z taxonomie orgánů,
c) workflow pro postoupení podání včetně generování průvodních dokumentů,
d) integrační požadavky na spisovou službu (eSSL) a komunikační rozhraní,
e) uživatelské scénáře pracovníků podatelny, administrátorů a auditorů,
f) metriky kvality, akceptační kritéria a provozní SLO/SLA.

1.4 Modul nepříslušnosti je navržen tak, aby mohl být dodán a provozován jako samostatná služba s jasně definovanými rozhraními, nezávisle na dodavateli jiných komponent (například modulu pro třídění dokumentů mezi útvary).

2. Definice a zkratky

2.1 Tato kapitola sjednocuje terminologii, která je v dokumentu používána, aby nevznikaly nejasnosti při výkladu požadavků. Uvádí srozumitelné definice klíčových pojmů (například příslušné a nepříslušné podání, taxonomie orgánů, NEURČITO, golden set) a používané zkratky technické i procesní povahy. Cílem je zajistit jednoznačný výklad pro Objednatele, Koncového zákazníka Objednatele, Dodavatele i kontrolní a auditní orgány.

2.2 Pro účely této technické specifikace platí:

a) Příslušné podání – podání, které podle právních předpisů a interního vymezení agend spadá do věcné příslušnosti orgánu, pro nějž je modul provozován.

b) Nepříslušné podání – podání, které do věcné působnosti orgánu nespadá a má být postoupeno věcně příslušnému orgánu nebo vráceno odesílateli s uvedením důvodu.

c) Taxonomie orgánů – řízený a verzovaný seznam orgánů veřejné moci a případně dalších adresátů, s jejich identifikátory, kontaktními kanály a pravidly pro přiřazení podání.

d) NEURČITO (abstain) – stav, kdy klasifikační komponenta nedosáhne minimální úrovně jistoty a vyžaduje ruční přezkum.

e) Golden set – reprezentativní a anotovaná sada podání používaná pro měření kvality, regresní testy a trénink nebo ladění modelů nepříslušnosti.

f) Correlation-ID – jedinečný identifikátor použitý pro end-to-end sledování jedné transakce nebo životního cyklu podání napříč všemi komponentami.

g) Bridge/API – integrační vrstva, která zprostředkovává komunikaci mezi modulem nepříslušnosti a spisovou službou.

h) eSSL – elektronická spisová služba zajišťující evidenci podání, spisů, doručenek a související dokumentace.

i) DLP (Data Loss Prevention) – kontrolní mechanizmy bránící únikům dat při přenosu podání a souvisejících dokumentů mimo prostředí Koncového zákazníka Objednatele.

j) Re-process – opětovné zpracování již založeného podání, například po změně taxonomie orgánů, po opravě modelu nebo po ruční korekci.

3. Předpoklady a vazby

3.1 Tato kapitola popisuje vnější podmínky, za nichž může modul nepříslušnosti správně fungovat, a systémy, na které se funkčně nebo technicky váže. Uvádí, jaká data a služby musí být k dispozici (spisová služba, taxonomie orgánů, Bridge/API) a jaké bezpečnostní a organizační předpoklady musí být splněny. Zároveň stanovuje, jaké části řešení jsou mimo rozsah této technické specifikace a jsou považovány za okolní prostředí.

3.2 Pseudonymizace vstupů:

a) Dokumenty a metadata vstupující do modulu jsou pseudonymizované v rozsahu stanoveném DPIA a bezpečnostní politikou.
b) V logech, metrikách a trasování se nesmí vyskytovat nechráněné identifikátory subjektů údajů ani obsah dokumentů.

3.3 Vazba na spisovou službu (eSSL):

a) Každé podání má v eSSL jednoznačnou evidenční stopu.
b) Modul nepříslušnosti pracuje s referencí na záznam v eSSL (ID podání, ID spisu) a s odkazem na uložený obsah.

3.4 Vazba na modul příjmu podání:

a) Před vstupem do modulu nepříslušnosti proběhne technická kontrola formátu a čitelnosti, kontrola povinných náležitostí a případná kontrola duplicity.
b) Modul nepříslušnosti řeší pouze věcnou příslušnost, nikoliv formální bezvadnost podání.

3.5 Vazba na taxonomii orgánů:

a) Modul má přístup k aktuální verzi taxonomie orgánů včetně mapování agend na orgány a kontaktní kanály.
b) Změny taxonomie jsou verzované a aktivace nové verze může vyžadovat re-process vybraných podání.

3.6 Samostatnost dodávky

a) Modul nepříslušnosti musí být navržen tak, aby byl případně oddělitelný, tedy aby jej mohl dodat i jiný dodavatel než Dodavatel ostatních modulů, za předpokladu dodržení zde popsaných rozhraní a datových struktur.

4. Role

4.1 Tato kapitola popisuje role, které se na procesu vyhodnocení nepříslušnosti, návrhu cílového orgánu, postoupení a případného vrácení podání podílejí. Z role vyplývají typické činnosti uživatelů v rámci modulu nepříslušnosti, jejich oprávnění a odpovědnost za jednotlivé kroky procesu.

4.2.1 Jednotlivé role jsou:

a) Pracovník podatelny: iniciuje požadavek, který je skrze API/Bridge odeslán do modulu pro třídění dokumentů. Tento požadavek může být buď pro zpracování požadavku pro vyhodnocení příslušnosti pro zvolený dokument nebo pro odeslání zpětné vazby u chybných návrhů přiřazení. Kontroluje návrh zařazení.

b) Superadmin modulu nepříslušnosti:

i. spravuje konfigurační parametry klasifikace (prahy jistoty, pravidla NEURČITO, výjimky), konfiguruje integrační parametry (endpointy, formáty, politiky egressu), spravuje uživatelské účty a role v rámci modulu (RBAC, MFA), řeší incidenty druhé úrovně ve spolupráci s provozem,

ii. spravuje seznam orgánů a jejich agend, spravuje seznam orgánů a jejich agend, spolupracuje na anotaci golden setu z hlediska věcné příslušnosti,

iii. ověřuje úplnost a správnost záznamů o nepříslušnosti a postoupení, kontroluje soulad se správními předpisy a interními směrnicemi, využívá auditní stopu a reporty.

c) Provoz (L1–L3 technická podpora):

i. monitoruje dostupnost, latence, chybovost a kapacity,
ii. řeší technické incidenty, výpadky, problémy s integrací,
iii. koordinuje nápravná opatření.

5. Nefunkční požadavky (NFR)

5.1 Tato kapitola stanovuje požadavky na vlastnosti modulu, které se netýkají samotné funkcionality, ale kvality jeho provozu. Definuje zejména požadavky na výkon, odezvu, dostupnost, spolehlivost, bezpečnost, auditovatelnost a observabilitu modulu nepříslušnosti. Tyto parametry určují, za jakých podmínek je řešení považováno za prakticky použitelné v produkčním prostředí. Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

5.2.1 Mezi tyto požadavky patří:

a) Výkon a latence:

i. interaktivní uživatelské akce (zobrazení návrhu nepříslušnosti, náhled návrhů cílových orgánů) mají odezvu do 300 ms p95 bez nového běhu klasifikace.
ii. Klasifikace nepříslušnosti pro jedno podání s textem do 1 MB a standardními přílohami musí být dokončena do 1500 ms p95.
iii. Dávkové zpracování 1000 podání musí proběhnout v čase definovaném v akceptačních testech s možností horizontálního škálování.

b) Dostupnost a spolehlivost:

i. Dostupnost služby modulu nepříslušnosti je minimálně 99,95 procenta času za měsíc, bez započtení plánovaných výluk a vyšší moci.
ii. Integrita doručování při egressu (poměr úspěšně spárovaných doručenek nebo protokolů k pokusům o odeslání) je minimálně 99,9 procenta.
iii. V případě výpadku externího orgánu se uplatňuje retry politika a fronta dead-letter.

c) Bezpečnost:

i. Modul používá RBAC a tam, kde to dává smysl, i vícestupňové ověřování pro administrátorské funkce.
ii. Logy a metriky nesmí obsahovat obsah dokumentů ani nechráněné osobní údaje.
iii. Všechny přenosy mimo prostředí Koncového zákazníka Objednatele probíhají šifrovaně přes Bridge/API a prochází kontrolami AV a DLP.

iv. Průvodní dokumenty a usnesení jsou podepisovány prostřednictvím spisové služby nebo HSM, nikoliv přímo modulem pro nepříslušnost.

d) Auditovatelnost a observabilita

i. Každý krok procesu nepříslušnosti je logován s Correlation-ID, časem, výsledkem a identifikací uživatele, pokud jde o interaktivní akci.
ii. Jsou dostupné technické metriky (latence, chybovost, průchodnost, stav front) a metriky kvality klasifikace nepříslušnosti podle kapitoly 8.
iii. Dashboardy a alerty umožňují průběžné sledování stavu služby.

6. Hlavní uživatelské scénáře (user stories s kritérii)

6.1 Tato kapitola popisuje typické situace, které uživatelé modulu nepříslušnosti řeší, ve formě uživatelských scénářů s akceptačními kritérii. Slouží jako most mezi požadavky Objednatele a implementací dodavatele, protože ukazuje, jak má systém v konkrétních případech fungovat. User stories jsou zároveň podkladem pro akceptační testy a ověřování splnění požadavků.

6.2 US-NEP-01 Automatické rozpoznání nepříslušnosti

a) Jako pracovník podatelny chci, aby modul pro Nepříslušnost po iniciování požadavku (odeslán skrze Bridge/API) navrhl, zda je podání příslušné či nepříslušné vůči orgánu, pro nějž je služba provozována, abych minimalizoval ruční posuzování.

b) Akceptační kritéria:

i. Jasně nepříslušné podání s adresací na jiný orgán je označeno jako nepříslušné a systém navrhne cílový orgán s konfidenčním skóre nad nastaveným prahem.
ii. Podání s nízkou jistotou klasifikace je označeno stavem NEURČITO a zařazeno do fronty k ručnímu rozhodnutí.

6.3 US-NEP-02 Inicializace požadavku skrze API/Bridge

a) Jako pracovník podatelny chci mít možnost iniciovat požadavek, který je systémem odeslán prostřednictvím API/Bridge do modulu pro nepříslušnost. Tento požadavek může být buď pro vyhodnocení příslušnosti podání vůči orgánu, pro nějž je služba provozována, nebo pro odeslání zpětné vazby u chybných návrhů přiřazení.

b) Akceptační kritéria:

i. Given je iniciován proces pracovníkem podatelny, When systém zahájí zpracování, Then systém vytvoří platný požadavek obsahující všechna povinná data.
ii. Given existuje platný požadavek, When je požadavek odesílán, Then systém odešle požadavek prostřednictvím definovaného API do cílového modulu.
iii. Given je požadavek odeslán, When systém obdrží odpověď nebo chybu z API, Then systém výsledek zaznamená a nastaví odpovídající stav požadavku (úspěch / chyba).

6.4 US-NEP-03 Návrh cílového orgánu

a) Jako pracovník podatelny požaduji, aby modul pro Nepříslušnost podání po iniciování požadavku (odeslán skrze Bridge/API) navrhnul jeden nebo více věcně příslušných orgánů, abych mohl podání efektivně postoupit.
b) Akceptační kritéria:
   i. Pro každé nepříslušné podání systém zobrazí seznam navrhovaných orgánů seřazený podle konfidenčního skóre a stručné vysvětlení doporučení.
   ii. Pokud nelze cílový orgán určit, systém navrhne vrácení odesílateli nebo manuální výběr cílového orgánu.

6.5 US-NEP-05 Manuální korekce a učení z feedbacku

a) Jako pracovník podatelny požaduji, aby moje opravy chybně vyhodnocené nepříslušnosti byly využity k učení systému, aby se kvalita časem zlepšovala.

b) Akceptační kritéria:
   i. Při změně stavu podání nebo cílového orgánu se změna uloží do auditu a zároveň do datové sady určené pro retrénink modelů.

7. Negativní a hraniční scénáře

7.1 Tato kapitola se zaměřuje na situace, kdy se vstupy nebo okolnosti vymykají běžnému provozu, a popisuje, jak se v těchto případech má modul deterministicky chovat. Zahrnuje technicky vadná podání, nejasné nebo vícejazyčné texty, duplicity, opakovaná neúspěšná postoupení a výpadky integračních systémů. Cílem je, aby ani v těchto hraničních případech nedocházelo ke ztrátě podání nebo nekontrolovanému chování.

7.2 Modul nepříslušnosti musí definovat deterministické chování pro tyto situace:

a) Technicky vadná podání (poškozené soubory, nečitelné skeny, nepodporované formáty) – podání je označeno jako technicky vadné, zařazeno do zvláštní fronty a pracovník podatelny obdrží návod k nápravě.
b) Vícejazyčné a směsné dokumenty – klasifikace probíhá s indikací jazyka, v případě nejistoty stav NEURČITO.
c) Extrémně krátké nebo dlouhé texty – zohlednění v prahových hodnotách a případné dělení dlouhých textů na části, ale s výsledkem na úrovni celého podání.
d) Opakovaná neúspěšná přiřazení – po opakovaném selhání postoupení systém navrhne jiný orgán, vždy s notifikací.
e) Nedostupnost externích systémů – modul přechází do degradačního režimu s frontováním požadavků, retry a DLQ bez ztráty podání.

8. Kvalitativní metriky

8.1 Tato kapitola definuje metriky, podle kterých se hodnotí kvalita klasifikace nepříslušnosti a návrhu cílového orgánu. Popisuje zejména precision, recall, F1-score, úspěšnost Top 1/Top 3 návrhů, podíl NEURČITO a míru ručních zásahů. Přesné vymezení metrik je podkladem pro nastavení cílů kvality a pro objektivní vyhodnocování chování systému v čase.

8.2 Metriky kvality se vztahují k přesnosti rozpoznání nepříslušnosti a návrhu cílového orgánu:

a) Precision nepříslušnosti – podíl správně označených nepříslušných podání mezi všemi, která systém označil jako nepříslušná.
b) Recall nepříslušnosti – podíl správně zachycených nepříslušných podání mezi všemi skutečně nepříslušnými podáními v golden setu.
c) F1-score nepříslušnosti – harmonický průměr precision a recall pro třídu nepříslušné.
d) Úspěšnost návrhu cílového orgánu – podíl případů, kdy byl v návrzích obsažen skutečně příslušný orgán (Top 1, Top 3).
e) Podíl NEURČITO – procento podání v tomto stavu, indikující vhodnost nastavení prahů.
f) Míra ručních zásahů – podíl podání, u nichž pracovník podatelny změnil návrh systému. Konkrétní cílové hodnoty budou upřesněny v kontraktu, například F1 nepříslušnosti minimálně 0,93, Top 1 pro cílový orgán minimálně 0,85 a Top 3 minimálně 0,95.

9. Akceptační testy a golden set

9.1 Tato kapitola popisuje principy akceptačního testování modulu nepříslušnosti a roli golden setu v tomto procesu. Uvádí, jaké typy scénářů a dat musí dodavatel pokrýt, jak se měří výsledky a jak se dokládá splnění stanovených metrik. Zároveň popisuje využití stínového provozu a regresních testů při změnách modelů nebo taxonomie orgánů.

9.2 Akceptace modulu nepříslušnosti probíhá nad golden setem a sadou akceptačních scénářů. Dodavatel musí dodat:

a) popis použitých modelů a pravidel,
b) výsledky měření metrik z kapitoly 8 na golden setu,
c) protokoly zátěžových a výpadkových testů,

9.3 Součástí akceptace je stínový provoz, kdy modul běží nad reálným provozem, ale jeho rozhodnutí nejsou závazná; výsledky jsou porovnávány s rozhodnutími pracovníků.

10. Předávací artefakty

10.1 Tato kapitola vyjmenovává dokumenty, konfigurace, testovací podklady a další artefakty, které musí dodavatel předat současně při dokončení dodávky modulu nepříslušnosti. Cílem je, aby Objednatel a provozní tým měli k dispozici plnou dokumentaci, specifikace rozhraní, provozní a konfigurační manuály, definice dashboardů a výsledky testů. Soubor artefaktů umožňuje modul dlouhodobě provozovat, rozvíjet a auditovat.

10.2 Dodavatel modulu nepříslušnosti předá minimálně:

a) Provozní dokumentaci popisující architekturu, provozní model, zálohování a obnovu.
b) Konfigurační dokumentaci se seznamem parametrů a doporučenými hodnotami.
c) Specifikaci rozhraní modulu nepříslušnosti včetně datových struktur, kódů chyb a sekvenčních diagramů workflow.
d) Testovací materiály, akceptační scénáře, skripty a výsledky testů.
e) Definici dashboardů a alertů pro monitoring včetně nastavení retenčních dob a přístupů.

10.3 Dodavatel musí předložit exit plán pro případ ukončení provozu nebo změny dodavatele, včetně exportu dat, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v příloze č. 9 Exit plán.

11. Definition of Done

11.1 Tato kapitola stanovuje souhrnná kritéria, při jejichž splnění je modul nepříslušnosti považován za dokončený a připravený k převzetí. Shrnuje požadavek na implementaci funkcionality, splnění nefunkčních požadavků, úspěšné akceptační testy, předání artefaktů i nastavení monitoringu a provozních procesů. Slouží jako jednoznačný referenční bod pro závěrečné převzetí dodávky po akceptačním řízení.

11.2 Modul nepříslušnosti je považován za dokončený, pokud:

a) jsou implementovány všechny funkční požadavky z kapitol 1., 3., 4., 6., 7. a 12.,
b) jsou splněny nefunkční požadavky podle kapitoly 5. a metriky kvality podle kapitoly 8. na dohodnuté úrovni,
c) byly úspěšně provedeny akceptační testy podle kapitoly 9.,
d) byl předán balík artefaktů podle kapitoly 10.,
e) je nastaven monitoring a alerting pro klíčové metriky,
f) proběhlo proškolení uživatelů a modul je integrován do provozního prostředí včetně eSSL a Bridge/API.

12. User stories

12.1 Tato kapitola rozšiřuje formální uživatelské scénáře o podrobnější, narativně popsané příklady průchodu modulu nepříslušnosti. Ilustruje tok podání od příjmu přes rozhodnutí o příslušnosti, návrh cílového orgánu, zpětnou vazbu až po eskalace a re-process. Slouží jako praktická pomůcka pro analýzu, návrh UI, testování i školení uživatelů, přičemž normativní požadavky zůstávají v ostatních kapitolách.

12.2 Jednotlivé user stories:

a) Rozhodnutí o příslušnosti a nepříslušnosti

Pracovník podatelny iniciuje požadavek pro vyhodnocení příslušnosti pro vybrané podání (listinné skény z výstupní složky skeneru s krátkou časovou prodlevou nebo elektronická podání z datové schránky/e-mailu), který je odeslán skrze Bridge/API do modulu. Modul dokument páruje podle jednoznačného identifikátoru (štítek/QR/čárový kód) s kartou v eSSL. Po převzetí vstupu modul nepříslušnosti provede předzpracování textu a metadat (normalizace, detekce jazyka, identifikace klíčových částí textu) a poté spustí klasifikaci z hlediska příslušnosti.

Typický průběh:

i. modul vyhodnotí, zda typicky agendové znaky podání odpovídají působnosti Koncového zákazníka Objednatele,

ii. pokud model dosáhne dostatečné jistoty pro příslušnost, označí podání jako příslušné a modul nepříslušnosti se nad ním dále neaplikuje,
iii. pokud model dosáhne dostatečné jistoty pro nepříslušnost, označí podání jako nepříslušné a pokračuje scénářem návrhu cílového orgánu,
iv. pokud je jistota pod nastaveným prahem, je podání označeno jako NEURČITO a zařazeno do fronty pro ruční rozhodnutí pracovníkem podatelny.

Rozhodnutí (příslušné, nepříslušné, NEURČITO) včetně konfidenčního skóre a základních důvodů klasifikace je uloženo do auditu a přes Bridge/API odeslán zpět do výchozího systému.

b) Návrh cílového orgánu a volba postupu

U podání, která byla označena jako nepříslušná, modul nepříslušnosti pracuje s taxonomií orgánů a dalšími referenčními údaji. Na základě obsahu podání, adresace a agendových indicií navrhne:

i. jednoho cílového orgánu s vysokou mírou jistoty; nebo
ii. seznam několika kandidátů seřazených podle pravděpodobnosti.

Systém poskytuje vyhodnocení zpracování prostřednictvím Bridge/API a obsahuje:

i. navržený cílový orgán (nebo více návrhů) s konfidenčním skóre,
ii. stručné vysvětlení doporučení (například „zmínka o dávkách hmotné nouze – orgán: Úřad práce“, „předmět: rozvod – orgán: soud“),
iii. návrh doporučeného postupu (postoupit, vrátit, eskalovat).

Pracovník podatelny může pomocí iniciace požadavku prostřednictvím Bridge/API:

i. návrh cílového orgánu potvrdit,
ii. zvolit jiný orgán z taxonomie.

Jeho rozhodnutí se ukládá do auditní stopy a slouží jako zpětná vazba pro další zlepšování modelu.

c) Postoupení nepříslušného podání včetně doručenek

Pokud pracovník podatelny potvrdí návrh cílového orgánu (u nepříslušných podání), modul nepříslušnosti provede:

i. vygenerování průvodního dokumentu podle šablony (obsahuje identifikaci podání, právní základ postoupení, stručný popis obsahu a důvod postoupení);

d) Vrácení podání odesílateli

Pokud nelze identifikovat věcně příslušný orgán nebo pokud tak stanoví interní metodika, může pracovník podatelny rozhodnout o vrácení podání odesílateli.

Pracovník podatelny iniciuje požadavek, který je do modulu odeslán skrze Bridge/API. Modul nepříslušnosti potom:

i. podle šablony vygeneruje dokument vysvětlující důvod vrácení podání (například nedostatek věcné příslušnosti a nemožnost určit jiný orgán).

ii. prostřednictvím Bridge/API odešle vygenerovaný dokument.

e) Zpětná vazba a opětovné zpracování (re-process)

Pracovník podatelny může kdykoli zjistit, že podání bylo chybně vyhodnoceno (například systém je označil jako nepříslušné, ale ve skutečnosti příslušné je, nebo naopak). V takovém případě může odeslat požadavek prostřednictvím Bridge/API do modulu o nepříslušnost a:

i. změnit stav podání (příslušné, nepříslušné, NEURČITO),
ii. změnit cílový orgán, pokud bylo vyhodnocené jako nepříslušné,
iii. požádat o re-process, tedy opětovné vyhodnocení podání aktuální verzí modelu a taxonomie orgánů.

Každá taková změna je zaznamenána v auditní stopě včetně původního a nového stavu, identifikace uživatele a času. Re-process může být spuštěn i hromadně superadminem, například po nasazení nové verze modelu nebo po rozsáhlé změně taxonomie orgánů. Modul musí umět re-process plánovat, frontovat a provádět tak, aby nenarušil běžný provoz.

f) Notifikace a přehled vadných přidělení

Modul nepříslušnosti musí poskytovat pracovníkům podatelny a superadminovi přehled o podáních, u nichž došlo k problémům nebo nestandardnímu průběhu zpracování. Typické situace:

i. opakované změny cílového orgánu během krátkého období (indikace nejasné agendy),
ii. vysoký počet manuálních zásahů u určitého typu podání.

Systém generuje notifikace podle konfigurovatelných prahů a rolí a tyto informace odešle skrze Bridge/API zpět do výchozího systému. Současně je k dispozici přehled vadných přidělení, kde je u každého případu možné:

i. zobrazit kompletní historii rozhodnutí,
ii. spustit re-process,
iii. upravit cílový orgán nebo zvolit vrácení,
iv. přidat poznámku pro audit nebo další zpracování.

g) Reporty a analýza trendů

Modul nepříslušnosti poskytuje reporty, které pomáhají řídit kvalitu a efektivitu procesu nepříslušnosti. Typické reporty zahrnují:

i. počty příslušných, nepříslušných a NEURČITO podání za období,
ii. rozdělení nepříslušných podání dle cílových orgánů,
iii. podíl automaticky postoupených podání versus ručně zpracovaných,
iv. míru ručních zásahů a změn návrhů systému,
v. výskyt vadných přidělení a opakovaných problémů (například často chybně navrhovaný orgán).

Reporty lze filtrovat podle období, typu podání, agendy nebo zdrojového kanálu. Výstupy se používají pro:

i. ladění prahů klasifikace a stavu NEURČITO,
ii. návrh změn v taxonomii orgánů,
iii. plánování kapacit podatelny,
iv. přípravu podkladů pro audit a kontrolní orgány.

h) Scénář změny taxonomie orgánů a dopad na stávající podání

Taxonomie orgánů se v čase mění, například v důsledku legislativních změn, reorganizací nebo přebírání agend mezi orgány. Modul nepříslušnosti musí tuto skutečnost zvládat řízeným způsobem. Typický scénář:

i. superadmin připraví novou verzi taxonomie (například vznik nového úřadu nebo přesun agendy z jednoho orgánu na druhý),
ii. nová verze je otestována na vzorku podání a v testovacím prostředí modulu nepříslušnosti,
iii. po schválení je nová verze nasazena do produkce s datem účinnosti,
iv. modul nepříslušnosti od tohoto data používá novou verzi taxonomie pro všechna nově přijatá podání,

Všechny změny taxonomie jsou verzované a auditované, včetně informací o tom, kdy a kým byly schváleny a nasazeny.

i) Nastavení rolí administrátorem (RBAC/MFA)

Superadmin má možnost spravovat uživatelské účty a oprávnění v rámci modulu nepříslušnosti. V rámci systému může:

i. zakládat nové uživatelské účty pro pracovníky podatelny, analytiky a další role,
ii. přiřazovat a měnit role uživatelů,

iii. nastavovat přístupová práva k jednotlivým funkcím systému (například možnost zadávat zpětnou vazbu, spouštět re-process, zobrazovat auditní stopu, exportovat data apod.),

iv. spravovat životní cyklus účtů (aktivace, deaktivace, reset hesla, audit změn oprávnění).

Správa uživatelských účtů a oprávnění v evidenčním systému eSSL zůstává mimo rozsah této funkcionality – superadmin má oprávnění pouze v rámci modulu nepříslušnosti.

j) Stavová hlášení

Modul poskytuje průběžná stavová hlášení o zpracování dokumentu prostřednictvím Bridge/API, včetně informace o zahájení zpracování, jednotlivých krocích, dokončení nebo chybovém stavu.

13. Požadavky na kvalitu, bezpečnost a akceptaci

13.1 Akceptační a předávací řízení:

a) Akceptační řízení ověřuje splnění funkčních požadavků, naplnění nefunkčních požadavků, dosažení metrik kvality na golden setu a nastavení monitoringu a provozních postupů.

b) Dodavatel předá akceptační scénáře, protokoly testů, konfiguraci dashboardů a alertů.

13.2 Bezpečnost:

a) Požadavky na kybernetickou bezpečnost jsou uvedené v Příloze č. 14 Smlouvy.

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	E444A3671D2D06A82E3D69CD95785345BE8FD6130DFEF482CCEDFA0B0664C462
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 4 – Technická specifikace nástroje Opatření proti nečinnosti

Obsah

1. Účel a rozsah

1.1 Tento dokument stanovuje požadavky na modul Opatření proti nečinnosti, jež je součástí systému využívajícího umělou inteligenci, včetně souvisejícího uživatelského rozhraní a integrační vrstvy, pro podporu procesu vyřizování návrhů na přijetí opatření proti nečinnosti správního orgánu na úseku pobytu cizinců na území České republiky. Cílem je zajistit efektivní, rychlé a zákonně konformní zpracování rostoucího počtu podání.

1.2 Rozsah řešení zahrnuje:

a) Modul využívající umělou inteligenci pro automatizaci vyhodnocení návrhů na opatření proti nečinnosti,
b) Uživatelské rozhraní sloužící k nahrání vstupních podkladů, iniciaci vyhodnocení, sledování stavu zpracování, zobrazení výsledků vyhodnocení a poskytování zpětné vazby uživatele,
c) Zajištění souladu s legislativními požadavky, zejména zákonem o pobytu cizinců a GDPR.

1.3 Mimo rozsah:

a) Proces podání návrhu občanem (předpokládá se, že návrh je již doručen),
b) Personální řízení a organizační změny mimo technické řešení.

1.4 Modul Opatření proti nečinnosti a Uživatelské rozhraní je navržen tak, aby mohl být dodán a provozován jako samostatná služba s jasně definovanými rozhraními, nezávisle na dalších modulech a případných dalších dodavatelích těchto jiných komponent.

2. Definice a zkratky

2.1 Pro účely tohoto dokumentu platí následující pojmy a zkratky:

a) Opatření proti nečinnosti (OPN): proces podle správního řádu, v jehož rámci nadřízený správní orgán vyhodnocuje, zda je podřízený orgán nečinný a zda je třeba uložit opatření (přikázat vydání rozhodnutí, převzít věc, stanovit lhůtu apod.).
b) Návrh OPN: podání žadatele (účastníka řízení), kterým se domáhá přijetí opatření proti nečinnosti.
c) Komise: Komise pro rozhodování ve věcech pobytu cizinců, jako orgán Koncového zákazníka Objednatele příslušný k projednání návrhů na opatření proti nečinnosti na úseku pobytu cizinců.

d) Modul OPN: samostatná funkční část systému Opatření proti nečinnosti, která podporuje proces vyřizování návrhů na opatření proti nečinnosti, včetně práce s podáními, lhůtami, podklady a rozhodnutími.

e) Spis: elektronický spis vedený ve spisové službě (eSSL) Kocového zákazníka Objednatele, obsahující veškeré dokumenty a metadata vztahující se k jednomu řízení o OPN.

f) Podání: jednotlivý dokument (návrh), který je vstupem do procesu OPN a je identifikován jednoznačným identifikátorem ve spisové službě.

g) AI komponenta: část řešení využívající metody umělé inteligence (např. strojové učení, NLP) pro klasifikaci podání, doporučení dalšího postupu, výpočet rizik nedodržení lhůt a návrhy textů rozhodnutí.

h) Golden set: reprezentativní sada historických případů, které jsou ručně anotovány experty a slouží k tréninku, ladění a akceptačnímu testování AI komponenty.

i) Lhůta: zákonná nebo interní časová hranice pro provedení určitého úkonu (např. vydání rozhodnutí).

j) Nečinnost: stav, kdy správní orgán v zákonné lhůtě nevydal rozhodnutí ani neučinil jiný úkon, který by byl podle práva dostačující.

3. Předpoklady a vazby

3.1 Řešení musí být realizováno v souladu s platnou legislativou, zejména zákonem o pobytu cizinců na území ČR, správním řádem, zákonem o archivnictví a spisové službě a předpisy v oblasti ochrany osobních údajů (GDPR).

3.2 Předpokládá se dostupnost elektronických podání a spisů v interním systému Komise (eSSL) skrze Bridge/API a existence historických dat o předchozích návrzích OPN, včetně výsledků rozhodnutí. Tato data budou v případě potřeby anonymizována nebo pseudonymizována v souladu s GDPR pro účely tréninku a testování AI komponenty.

3.3 Organizační nastavení je zajištěno Koncovým zákazníkem Objednatele. Modul OPN na toto nastavení navazuje, ale sám jej nemění. Správa uživatelských účtů a přístupových práv je v kompetenci provozovatele systému.

3.4 Technické prostředí musí umožňovat zabezpečený přístup k interním systémům Komise, zejména ke spisové službě. Musí být k dispozici výpočetní infrastruktura pro běh AI komponenty, a to v souladu s bezpečnostní politikou Objednatele, resp. Koncového zákazníka Objednatele (on-premise nebo cloud, dle rozhodnutí Objednatele nebo Kocového zákazníka Objednatele). Všechny vstupy pro AI komponentu, které obsahují osobní údaje, musí být zpracovávány v pseudonymizované podobě.

3.5 Řešení je procesně a technicky provázáno zejména:

a) se spisovou službou – předávání metadat skrze Bridge/API,
b) s výstupy interních agendových systémů – nahráním podkladů do uživatelského rozhraní a jejich evidování,
c) s infrastrukturními prvky autentizace a autorizace (např. IDM, LDAP, IAM) – řízení přístupů,
d) s auditním a logovacím systémem – ukládání auditních záznamů o činnosti uživatelů i AI komponenty.

3.6 Modul OPN je navržen jako samostatně nasaditelný a provozovatelný modul, který může být dodán i jiným dodavatelem, pokud dodrží zde uvedené požadavky na funkci, rozhraní a nefunkční parametry. Všechny vazby na okolní systémy musí být popsány rozhraními a datovými modely v rámci předávacích artefaktů.

4. Role

4.1 Tato kapitola popisuje role, které se na procesu Opatření proti nečinnosti podílejí. Z jednotlivých rolí vyplývají typické činnosti uživatelů v rámci modulu OPN, jejich oprávnění a odpovědnost za jednotlivé kroky procesu.

4.2 Role v systému jsou kombinovatelné. Uživatel má vždy jeden výsledný přístup do systému, který je odvozen z kombinace přiřazených rolí, nikoli samostatné přístupy pro jednotlivé role

4.3 Jednotlivé role jsou:

a) Referent komise: úředník odpovědný za zpracování konkrétního návrhu OPN. Pracuje zadává dotazy do modulu pro vyhodnocení návrhu pro opatření proti nečinnosti, kontroluje jejich úplnost, hodnotí doporučení AI, nahrává podklady pro vyhodnocení pomocí AI.
b) Administrátor systému: technický správce modulu OPN odpovědný za správu uživatelských oprávnění na aplikační úrovni a základní provozní nastavení.
c) Správce dat: role odpovědná za správu golden setu a dalších datových sad, dohled nad kvalitou dat.
d) Bezpečnostní administrátor / auditor: osoba s přístupem k auditním záznamům, která provádí náhodné či cílené kontroly souladu používání modulu OPN s bezpečnostními politikami, GDPR a interními standardy.

5. Nefunkční požadavky (NFR)

5.1 Tato kapitola definuje nefunkční požadavky na modul OPN z hlediska výkonu, dostupnosti, bezpečnosti, auditovatelnosti, použitelnosti a konfigurovatelnosti. Požadavky jsou závazné pro všechny dodavatele implementující tento modul. Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

5.2 Výkon a odezva:

a) 95 % běžných interakcí uživatele musí být zpracováno do 2 sekund.
b) 99 % běžných interakcí musí být zpracováno do 5 sekund.
c) Hromadné výpočty mohou běžet asynchronně; jejich výsledky musí být pro uživatele dostupné do 10 minut od spuštění.
d) Modul musí podporovat práci alespoň 50 současně přihlášených uživatelů bez znatelného zhoršení odezvy.

5.3 Dostupnost a odolnost:

a) Modul OPN musí být provozován s minimální měsíční dostupností 99,5 % v provozním okně definovaném Objednatelem.
b) Musí být zajištěna odolnost vůči výpadku integračních vazeb: při nedostupnosti spisové služby musí být uživatel srozumitelně informován a nesmí dojít ke ztrátě již zadaných dat.
c) Kritická data (spojení podání se spisem, nastavení lhůt, rozhodnutí) musí být zálohována dle politik Koncového zákazníka Objednatele a umožňovat obnovu na úroveň jednotlivého spisu.

5.4 Bezpečnost a ochrana osobních údajů:

a) Přístup do modulu OPN musí být řízen centralizovaným systémem identity a přístupových práv a podporovat RBAC podle rolí uvedených v kapitole 4.
b) Všechna komunikace mezi modulem OPN a okolními systémy musí být šifrována (např. TLS) a autentizována.
c) Osobní údaje musí být zpracovávány v rozsahu nezbytném pro plnění zákonných povinností Komise; AI komponenta pracuje s pseudonymizovanými daty, přičemž mapování pseudonymů je uloženo mimo AI komponentu.
d) Modul musí podporovat výkon práv subjektů údajů (např. dohledatelnost, výmaz nebo omezení zpracování tam, kde to právní předpisy umožňují).

5.5 Auditovatelnost a transparentnost:

a) Systém musí evidovat auditní záznamy o všech klíčových operacích, včetně přihlášení, změny stavu podání, úprav rozhodnutí, aplikace či odmítnutí AI doporučení a nastavení lhůt.
b) U každého doporučení AI musí být uchován záznam o vstupních datech, parametrech modelu a výsledku (včetně míry jistoty), aby bylo možné zpětně vysvětlit, jak k doporučení došlo.
c) Auditní záznamy musí být uloženy ve formě neměnitelného logu po dobu minimálně stanovenou interními předpisy Koncového zákazníka Objednatele.

5.6 Použitelnost a ergonomie:

a) Uživatelské rozhraní modulu OPN musí být přizpůsobeno práci referenta.
b) Všechny chyby a výjimky musí být prezentovány uživateli srozumitelným způsobem, který uvádí příčinu a doporučený postup nápravy.
c) Modul musí být responzivní v rámci cílových rozlišení používaných v prostředí Koncového zákazníka Objednatele. (typicky kancelářské monitory).

5.7 Konfigurovatelnost a rozšiřitelnost:

a) Modul musí umožňovat přidání nových typů řízení nebo změnu rozhodovacích pravidel formou konfiguračních souborů nebo administrátorského rozhraní.
b) AI komponenta musí být navržena tak, aby bylo možné nasazovat nové verze modelu formou standardizovaného releasu, včetně paralelního běhu staré a nové verze pro účely A/B testů.

6. Hlavní uživatelské scénáře (user stories s kritérii)

6.1 Tato kapitola strukturovaně popisuje hlavní funkční scénáře modulu OPN ve formě user stories a akceptačních kritérií. Scénáře jsou závazné z pohledu funkčnosti; detailnější popis chování je uveden v kapitole 7. (negativní a hraniční scénáře).

6.2 Scénář 1 – Zobrazení seznamu návrhů OPN:

a) Jako referent Komise chci v uživatelském rozhraní vidět seznam rozpracovaných návrhů OPN, abych je mohl efektivně zpracovávat a prioritizovat. Zároveň chci mít možnost přidání nového návrhu OPN a přiřazení příslušného identifikátoru podání z eSSL.
b) Akceptační kritéria:
   i. Po přihlášení a otevření modulu OPN se referentovi zobrazí seznam rozpracovaných návrhů OPN.

ii. Seznam obsahuje minimálně číslo spisu, identifikaci žadatele, datum podání, typ řízení, stav a informaci o zbývající lhůtě.
iii. Uživatel může seznam filtrovat (např. podle stavu, blížících se lhůt, typu podání) a řadit (např. podle data podání, priority).
iv. Načtení seznamu splňuje požadavky na odezvu dle kapitoly 5.

6.3 Scénář 2 – Ověření úplnosti podání:

a) Jako referent Komise požaduji rychle ověřit, zda podání obsahuje všechny povinné náležitosti, abych minimalizoval riziko chyb a potřebu opakovaného doplňování.
b) Akceptační kritéria:
   i. Systém automaticky zkontroluje přítomnost povinných údajů (identifikace žadatele, označení nečinného orgánu, označení řízení, popis tvrzené nečinnosti apod.).
   ii. Chybějící nebo nevalidní údaje jsou zobrazeny přehledně, s uvedením, proč jsou považovány za nedostatečné.
   iii. Všechny změny a rozhodnutí jsou zaznamenány v auditu.

6.4 Scénář 3 – Iniciace vyhodnocení AI:

a) Jako referent Komise chci iniciovat vyhodnocení návrhu OPN AI komponentou.
b) Akceptační kritéria:
   i. Zahájení vyhodnocení je iniciováno z uživatelského rozhraní přes Bridge/API.
   ii. Data jsou předána k pseudonymizaci před vstupem do AI komponenty. AI komponenta pracuje výhradně s pseudonymizovanými daty.
   iii. Systém vrátí potvrzení o zahájení zpracování.

6.5 Scénář 4 - Sledování stavu zpracování:

a) Jako referent Komise chci sledovat stav zpracování vyhodnocení návrh OPN AI komponentou, abych měl přehled o průběhu.
b) Akceptační kritéria
   i. Uživatelské rozhraní zobrazuje stav vracený systémem přes API.
   ii. Stav je aktualizován asynchronně.
   iii. Chybové nebo výjimečné stavy jsou jasně indikovány.

6.6 Scénář 5 – Zobrazení doporučení AI:

a) Jako referent Komise požaduji vidět doporučení AI komponentou, jak s návrhem naložit, abych získal podporu pro rychlejší a konzistentnější rozhodování.
b) Akceptační kritéria

i. Systém pro konkrétní podání zobrazí doporučení AI (např. „pravděpodobně nečinnost – doporučeno vyhovět“, „neprokázaná nečinnost – doporučeno nevyhovět“), včetně míry jistoty.
ii. AI doporučení je doplněno vysvětlením hlavních faktorů (např. délka trvání řízení, historie úkonů, typ rozhodované věci).
iii. Referent má možnost doporučení přijmout, upravit nebo odmítnout; jeho volba je zaznamenána v auditu.
iv. Nezobrazení doporučení z důvodu technické chyby je indikováno srozumitelnou hláškou, přičemž uživatel může v procesu pokračovat manuálně.

6.7 Scénář 6 – Úprava návrhu rozhodnutí:

a) Jako referent Komise chci mít možnost upravit návrh rozhodnutí vygenerovaný AI komponentou, abych zajistil jeho soulad s konkrétními okolnostmi případu a právním názorem Komise.
b) Akceptační kritéria:
   i. AI komponenta vygeneruje návrh textu rozhodnutí včetně výroku a odůvodnění.
   ii. Referent může editovat celý text, vkládat nebo odebírat odstavce a doplňovat vlastní odůvodnění.
   iii. Systém uchovává historii verzí návrhu rozhodnutí a umožňuje porovnat AI návrh s finální verzí.
   iv. Uložení finální verze je podmíněno kontrolou povinných náležitostí rozhodnutí (např. označení účastníků, právní základ, poučení).

6.8 Scénář 7 – Označení podání jako vyřízené:

a) Jako referent Komise chci po dokončení všech kroků označit podání jako vyřízené, aby byl proces správně ukončen.
b) Akceptační kritéria:
   i. Systém ověří splnění všech povinných kroků.
   ii. Uzavření je zaznamenáno v auditu.

6.9 Scénář 8 – Výběr vzoru rozhodnutí podle typu žádosti a stavu řízení:

a) Jako referent Komise chci při přípravě rozhodnutí vybrat vhodný vzor, aby byl text rozhodnutí konzistentní a v souladu s metodikou.
b) Akceptační kritéria:
   i. Systém nabízí sadu vzorů rozhodnutí, filtrovanou podle typu žádosti a stavu řízení (vyhovění, nevyhovění, částečné vyhovění apod.).

ii. Použitý vzor je evidován u spisu pro účely zpětné analýzy.

6.10 Scénář 9 – Vkládání dokumentů z různých zdrojů

a) Jako referent Komise chci přidávat do spisu dokumenty z různých systémů, abych měl podklady na jednom místě.
b) Akceptační kritéria:
   i. Systém podporuje vkládání dokumentů z CIS, Alberta, OAM a dalších definovaných systémů, včetně přímého přetažení souboru (uploadu).
   ii. U každého dokumentu je evidován zdroj, autor (pokud je znám), datum vložení a typ dokumentu.
   iii. Vkládání dokumentů respektuje oprávnění uživatele a je auditováno.

6.11 Scénář 10 – Manuální zásah v každém kroku

a) Jako referent Komise požaduji mít možnost v důležitých bodech procesu upravit automatické návrhy systému, aby konečné rozhodnutí odráželo odborný úsudek člověka.
b) Akceptační kritéria:
   i. Ve všech klíčových krocích má referent Komise možnost manuální úpravy.
   ii. Každá manuální úprava je evidována s identitou uživatele a časem změny.
   iii. Manuální zásah nesmí porušit základní datovou integritu.

7. Negativní a hraniční scénáře

7.1 Tato kapitola popisuje vybrané situace, které představují hraniční nebo chybové stavy procesu OPN. Pro každý scénář je uvedeno očekávané chování systému.

7.2 Systém detekuje chybějící povinné náležitosti a označí podání jako neúplné. referent Komise má možnost pokračovat s upozorněním, že rozhodnutí může být napadnutelné. V logu je uloženo, které náležitosti chyběly a jak referent Komise rozhodl.

7.3 Při přebírání dat z výstupů systémů CIS nebo Alberta systém zjistí nesoulad (např. odlišná identita účastníka, jiný stav řízení). Systém tuto situaci zvýrazní. V auditním záznamu je uloženo, která data byla nakonec použita.

7.4 Refere vyhodnotí AI doporučení jako zjevně nevhodné. Může jej odmítnout, upravit a označit důvod nesouhlasu (např. nová judikatura, zvláštní okolnosti případu). Tyto případy jsou sbírány do zvláštního datasetu pro ladění modelu.

8. Kvalitativní metriky

8.1 Kvalita fungování modulu OPN je posuzována pomocí následujících metrik. Konkrétní cílové hodnoty lze upřesnit v provozní smlouvě.

8.2 Metriky kvality AI doporučení:

a) Podíl případů z golden setu, ve kterých se návrh výsledku řízení AI shoduje s historickým rozhodnutím Komise (cílově např. ≥ 80 %).
b) Podíl případů, kdy referent převzal AI doporučení bez úpravy (měřeno v reálném provozu, sledováno trendově).
c) Podíl případů, kdy referent označil doporučení AI jako nevhodné a důvod tohoto nesouhlasu.

8.3 Metriky dodržování lhůt:

a) Podíl podání, u nichž Komise rozhodla v zákonné lhůtě (cílově ≥ 95 %).
b) Podíl podání, u nichž systém včas (např. min. 5 pracovních dní před uplynutím lhůty) vygeneroval upozornění.

8.4 Metriky použitelnosti:

a) Průměrný počet kliknutí/úkonů potřebných k dokončení standardního případu OPN (sledováno v pilotním provozu).
b) Počet incidentů klasifikovaných jako „chyba v ovládání“ za období (cílem je jejich pokles v čase).

8.5 Metriky kvality dat:

a) Podíl spisů s kompletně doplněnými klíčovými metadaty (typ řízení, nečinný orgán, datum doručení, výsledné rozhodnutí).
b) Podíl dokumentů ve spisu, u nichž je vyplněn zdroj a typ dokumentu.

9. Akceptační testy a golden set

9.1 Akceptace modulu OPN musí zahrnovat jak funkční testy, tak ověření výkonu a kvality AI komponenty pomocí golden setu.

9.2 Golden set:

a) Dodavatel ve spolupráci s Komisi připraví golden set minimálně 300 historických spisů OPN, které reprezentují běžné i hraniční situace (vyhovění, nevyhovění, různé typy nečinnosti, kombinace s jinými řízeními).

b) U každého případu bude k dispozici cílové rozhodnutí Komise, časový průběh řízení a informace o tom, zda došlo k marnému uplynutí lhůt.
c) Dataset bude rozdělen na část pro trénink/ladění a na nezávislý akceptační set.

9.3 Akceptační testy AI komponenty:

a) Na akceptační části golden setu bude měřena úspěšnost doporučení AI (shoda s historickým rozhodnutím) a další metriky dle kapitoly 8.
b) Minimální prahové hodnoty úspěšnosti budou stanoveny Objednatelem; nesplnění vede k nutnosti model upravit nebo modul vrátit do ladění.
c) Součástí akceptace je i manuální revize vybraných případů experty Komise, kteří posoudí srozumitelnost a přijatelnost doporučení AI.

9.4 Funkční a integrační testy:

a) Dodavatel připraví sadu testovacích scénářů pokrývajících kapitoly 6. a 7., včetně negativních a chybových stavů.
b) Pro každý scénář budou definována očekávaná výsledná data ve spisové službě, logech a v modulu OPN.
c) Testy musí být opakovatelné (automatizované, pokud je to možné) a jejich výsledky budou součástí předávacích artefaktů.

10. Předávací artefakty

10.1 Dodavatel je povinen při předání modulu OPN poskytnout minimálně následující dokumentaci a artefakty:

a) Technická dokumentace řešení – architektura modulu, popis interních komponent, datový model, přehled integračních rozhraní.
b) Konfigurační dokumentace – popis nastavení lhůt, číselníků, typů rozhodnutí, rolí a přístupových práv.
c) Dokumentace AI komponenty – popis použitých modelů, vstupních a výstupních dat, způsobu tréninku, použitých metrik a výsledků vyhodnocení na golden setu.
d) Provozní dokumentace – provozní manuál, postupy zálohování a obnovy, postup při incidentu, kontakty na odpovědné osoby.
e) Uživatelská dokumentace – návody pro referenty, schvalovatele, vedoucí a administrátory, včetně popisu hlavních obrazovek a běžných postupů.
f) Testovací dokumentace – scénáře a výsledky funkčních, integračních, výkonových a bezpečnostních testů.
g) Artefakty k golden setu – popis připraveného golden setu, statistiky kvality modelu, seznam známých omezení.

10.2 Dodavatel také musí předložit exit plán pro případ ukončení provozu nebo změny poskytovatele, včetně exportu dat, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v Příloze č. 9 Smlouvy (Exit plán).

11. Definition of Done

11.1 Tato kapitola stanovuje, kdy je implementace modulu OPN považována za dokončenou.

11.2 Modul OPN je „Done“, pokud jsou současně splněny následující podmínky:

a) Byly implementovány všechny funkce popsané v kapitole 6., včetně negativních scénářů dle kapitoly 7..
b) Modul splňuje nefunkční požadavky z kapitoly 5., což je doloženo výsledky výkonových a dostupnostních testů.
c) Byly úspěšně provedeny akceptační testy včetně vyhodnocení AI komponenty na golden setu podle kapitoly 9. a dosaženy dohodnuté prahové hodnoty metrik.
d) Všechny předávací artefakty uvedené v kapitole 10. byly předány, schváleny Objednatelem a uloženy v dohodnutém úložišti dokumentace.
e) Je nastaven monitoring modulu OPN (aplikační i infrastrukturní) v rozsahu umožňujícím sledovat dostupnost, výkon a klíčové metriky kvality, včetně definovaných prahů pro alerty.
f) Byl aktualizován katalog rozhraní a centrální evidence verzí systému tak, aby modul OPN byl řádně zařazen a dohledatelný.
g) Provedeno školení klíčových uživatelů (referenti, schvalovatelé, administrátoři) a předán plán školení pro ostatní uživatele.
h) V produkčním prostředí proběhla pilotní fáze na omezeném vzorku reálných podání, v jejímž rámci nebyly zjištěny kritické nedostatky bránící plnému nasazení.

12. User stories

12.1 Tato kapitola slouží výhradně jako informativní příklad. Závazné jsou pouze požadavky a akceptační kritéria definovaná v kapitolách 5. až 11.

12.2 Jednotlivé user stories:

a) Zobrazení seznamu návrhů pro zahájení zpracování

Referent Komise potřebuje mít k dispozici přehled všech návrhů na přijetí opatření proti nečinnosti, které modulu OPN předal k vyhodnocení. Tento seznam musí být dostupný prostřednictvím uživatelského rozhraní systému a obsahovat klíčové informace, jako je číslo spisu, datum podání, stav návrhu a základní identifikační

údaje žadatele. Funkce musí umožňovat řazení a filtrování podle různých kritérií (např. datum podání, priorita, stav), aby referent mohl rychle identifikovat podání s blížící se lhůtou. Zobrazení seznamu je výchozím bodem pro další kroky, jako je kontrola úplnosti podání, vyhodnocení doporučení AI a příprava rozhodnutí. Přístup k seznamu musí být zabezpečen autentizací a autorizací, aby byla zajištěna ochrana osobních údajů a dodržení legislativních požadavků.

b) Ověření úplnosti podání

Referent Komise potřebuje možnost rychle ověřit, zda podání obsahuje všechny povinné náležitosti stanovené zákonem a interními předpisy. Systém musí automaticky kontrolovat přítomnost klíčových údajů (např. identifikace žadatele, důvod návrhu, přílohy) a upozornit na chybějící nebo nevalidní informace. Funkce by měla umožnit manuální doplnění referentem Komise.

c) Zobrazení doporučení AI

Referent má možnost vidět doporučení AI komponenty, které na základě historických dat a rozhodovací logiky navrhne optimální postup. Doporučení musí být prezentováno transparentně, včetně vysvětlení hlavních faktorů, které vedly k návrhu. Funkce nesmí být závazná, tedy referent má vždy možnost doporučení odmítnout nebo upravit.

d) Úprava návrhu rozhodnutí

Po vygenerování návrhu rozhodnutí AI komponentou má referent Komise možnost tento návrh editovat. Funkce musí podporovat jednoduché úpravy textu, doplnění odůvodnění a vložení dalších informací. Systém uchovává historii změn pro auditní účely a umožňuje porovnání původního návrhu s finální verzí.

e) Kontrola duplicity podání

Referent má možnost ověřit, zda již nebylo stejné podání evidováno v modulu. Systém automaticky porovnává nové podání s existujícími záznamy podle klíčových údajů a v případě nalezení duplicity upozorní referenta, který může rozhodnout o dalším postupu.

f) Výběr vzoru rozhodnutí podle typu žádosti a stavu řízení

Na základě typu žádosti a aktuálního stavu řízení systém nabídne referentovi předem připravené vzory rozhodnutí. Referent může vybrat vhodný vzor, který může dále doplnit o specifické informace k danému případu.

g) Vkládání dokumentů z různých zdrojů

Referent má možnost vkládat do spisu dokumenty získané z agendových systémů nebo jiných relevantních zdrojů.

h) Manuální zásah v každém kroku

Ve všech klíčových krocích procesu má referent možnost provést manuální zásah, upravit automaticky získané údaje, doplnit poznámku, změnit rozhodnutí navržené AI komponentou.

13. Požadavky na kvalitu, bezpečnost, akceptaci

13.1 Tato kapitola shrnuje průřezové požadavky vztahující se ke kvalitě dodávky, bezpečnostním aspektům, procesu akceptace a provoznímu zajištění modulu OPN.

13.2 Kvalita dodávky:

a) Dodavatel je povinen dodržet standardy Koncového zákazníka Objednatele pro tvorbu dokumentace, testování a verzování.
b) Zdrojové kódy modulu OPN musí být uloženy ve verzovacím systému určeném Objednatelem a opatřeny komentáři umožňujícími jejich údržbu.
c) Změny v modulu OPN musí být prováděny řízeným změnovým řízením (change management) včetně schválení, plánování a dokumentace dopadů do okolních systémů.

13.3 Bezpečnost:

a) Požadavky na kybernetickou bezpečnost jsou uvedené v Příloze č. 14 Smlouvy.

13.4 Akceptace:

a) Proces akceptace je řízen akceptačním plánem, který definuje rozsah testů, metriky úspěšnosti a způsob předání výsledků.
b) Akceptace probíhá v prostředí odděleném od produkce; přechod do produkce je podmíněn formálním akceptačním protokolem.
c) V rámci akceptace musí být ověřeno, že modul OPN neohrožuje funkci stávajících systémů Komise (regresní testy integračních vazeb).

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	808177BAD505F74155F4CCDEEDABBE9A0C95844CDF86DD1DBAB523FA71C79D98
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 5 – Technická specifikace Pseudonymizační nástroj

Obsah

1. Účel a funkce

1.1 Objednatel poptává dodávku a implementaci Pseudonymizačního nástroje, který bude provozován v prostředí Koncového zákazníka Objednatele na jeho infrastruktuře.

1.2 Účelem nástroje je zajistit pseudonymizaci a depseudonymizaci dat pro účely jejich dalšího zpracování, zejména při předávání dat do AI nástroje prostřednictvím Bridge/API.

1.3 Pseudonymizační nástroj musí umožnit:

a) pseudonymizovat vstupní data na základě definovaných profilů a pravidel,
b) provádět depseudonymizaci, je-li to oprávněné a povolené,
c) uchovávat a spravovat mapy pseudonymů, klíče a další prostředky nutné k jednoznačnému, bezpečnému a auditovatelnému procesu.

1.4 Modul Pseudonymizační nástroj je navržen tak, aby mohl být dodán a provozován jako samostatná služba s jasně definovanými rozhraními, odděleně a nezávisle na případných dodavatelích jiných komponent.

2. Umístění a architektura

2.1 Pseudonymizační nástroj bude provozován výhradně v infrastruktuře Koncového zákazníka Objednatele.

2.2 Dodavatel se zavazuje, že nástroj nebude vyžadovat závislost na externích cloudových službách ani na prostředí třetích stran mimo kontrolu Koncového zákazníka Objednatele.

2.3 Komunikace s Pseudonymizační službou musí probíhat prostřednictvím definovaného rozhraní, které využívá Bridge/API.

2.4 Architektura musí být navržena podle principů „zero trust“, minimálních oprávnění a deklarativního řízení („as code“).

2.5 Veškeré integrační body musí být popsány v katalogu rozhraní a podléhat verzování.

3. Požadavky na funkčnost

3.1 Pseudonymizační služba musí podporovat různé typy dat, zejména:

a) strukturovaná data (databázové záznamy, tabulky, JSON/XML),
b) nestrukturovaná data (textové dokumenty, e-maily).

3.2 Pseudonymizace musí být konfigurovatelná pomocí profilů, které určují úroveň ochrany a typ pseudonymizace (deterministická/nedeterministická).

3.3 Pseudonymizace musí být deterministická tam, kde je to požadováno, a musí být možné ji auditovat.

3.4 Depseudonymizace musí být povolena pouze v případech, kdy existuje právní základ a oprávnění k jejímu provedení.

3.5 Pseudonymizační služba musí zajistit, že žádná data nebudou depseudonymizována bez odpovídajícího oprávnění a auditní stopy.

3.6 Modul musí umožnit správu životního cyklu pseudonymů a klíčů včetně rotace a expiračních politik.

3.7 Modul podporuje:

a) strukturovaná data (DB, CSV/JSON/XML),
b) nestrukturované texty (DOCX, PDF, e-mail),
c) obrazové/PDF skeny s integrovaným OCR (CZ/EN).

3.8 Detekce citlivých entit využívá kombinaci pravidel, slovníků a modelů NER; výstupem je masking map a aplikovaná transformace.

3.9 Podporované transformace:

a) tokenizace,
b) format-preserving encryption (FPE),
c) hash se solí,
d) masking a redakce.

3.10 Volba je řízena profilem; pro datová pole s validační logikou (rodná čísla, IČO) se požaduje FPE/format-preserving tokenizace.

3.11 Kvalita je vyhodnocována na golden setu Objednatele. Minimální požadavky:

a) precision ≥ 98 %,
b) recall ≥ 97 % pro definované entity osobních údajů,
c) maximální FN ≤ 1 % pro vyjmenované kritické entity.

3.12 Metriky jsou měsíčně reportovány; při nesplnění probíhá nápravný plán.

3.13 Seznam kritických entit PII (např. rodné číslo, číslo dokladu, adresa, podpis) je definován v souladu s platnou legislativou na ochranu osobních údajů, zejména nařízením GDPR (Nařízení Evropského parlamentu a Rady (EU) 2016/679). Při jakékoli detekci kritické entity v odchozím obsahu do dalších komponent volání zablokuje, incident se zaloguje a vyžádá se přezkum. DLP pravidla a prahy FN/FP se vyhodnocují měsíčně na reálném provozu.

3.14 Předávání dat mezi pseudonymizačním nástrojem a ostatními komponentami či systémy probíhá prostřednictvím Bridge/API.

4. Bezpečnost a ochrana dat

4.1 Pseudonymizační nástroj musí splňovat požadavky GDPR a souvisejících právních předpisů.

4.2 Mapy pseudonymů a klíče musí být uchovávány bezpečně, v šifrované podobě, a nesmí být přístupné neoprávněným osobám.

4.3 Veškeré secrety a šifrovací klíče musí být spravovány v centrálním trezoru s auditní stopou a pravidelnou rotací.

4.4 Pseudonymizační nástroj musí podporovat řízení přístupových práv na základě rolí a atributů, s podporou vícefaktorové autentizace.

4.5 Veškerá komunikace s ostatními komponentami musí probíhat šifrovaným a autentizovaným kanálem.

4.6 Nástroj musí obsahovat mechanismy pro detekci a prevenci neoprávněného přístupu a exfiltrace dat.

4.7 Oddělení rolí: Operátor pseudonymizace ≠ Správce klíčů ≠ Auditor.

4.8 Depseudonymizace je možná pouze v režimu „four-eyes“ (dvojí schválení) a je plně auditovaná; žádost i odůvodnění jsou uloženy.

4.9 Přístupové tokeny jsou krátkodobé; klíče jsou v HSM/KMS s rotací a envelope encryption.

5. Spolehlivost a provozní požadavky

5.1 Pseudonymizační nástroj musí být navržen jako vysoce dostupný a odolný proti výpadkům.

5.2 Dodavatel se zavazuje zajistit, aby nástroj byl horizontálně škálovatelný a schopen zpracovat předpokládané objemy dat v dohodnutých časech odezvy.

5.3 Nástroj musí podporovat paralelní zpracování více požadavků a být optimalizován pro provozní toky mezi zdrojovým systémem a AI nástrojem.

5.4 Musí být definovány fallback scénáře a plán obnovy v případě incidentu.

5.5 Mapy pseudonymů jsou šifrované, verzované, se časovou expirací. Retence a skartace se řídí spisovým a bezpečnostním řádem Koncového zákazníka Objednatele; exporty map jsou zakázány mimo definované úřední postupy.

5.6 Nástroj splňuje RTO ≤ 30 min a RPO ≤ 5 min. Konfigurace, klíče a auditní záznamy jsou replikovány do DR lokality; 2× ročně se provádí cvičení obnovy s protokolem. Nasazení do produkce je podmíněno úspěšným DR testem.

5.7 Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

6. Audit, observabilita a dohledatelnost

6.1 Pseudonymizační nástroj musí vytvářet auditní záznamy o každém provedení pseudonymizace a depseudonymizace, včetně identifikátoru požadavku, časového razítka, typu operace a identity žadatele.

6.2 Auditní záznamy nesmí obsahovat původní osobní údaje, ale musí umožnit zpětnou kontrolu a prokázání souladu.

6.3 Auditní logy musí být uchovávány v prostředí Koncového zákazníka Objednatele a chráněny proti neoprávněné změně.

6.4 Každý požadavek musí být opatřen korelačním identifikátorem pro end-to-end tracing napříč všemi komponentami.

6.5 Observabilita musí zahrnovat metriky výkonu, chybovosti, dostupnosti a kvality služby, včetně panelů a alertingu pro provozní a bezpečnostní role.

6.6 Nástroj provádí DLP kontrolu výstupů; auditní logy nesmí obsahovat původní PII. Telemetrie zahrnuje přehled transformací dle profilu, míru zásahů, FN/FP a anomálie (nečekané entity/kontexty).

7. Výkonnostní parametry a FinOps

7.1 Zpracování musí být optimalizováno tak, aby nenarušovalo provozní toky dat mezi zdrojovým systémem a AI nástrojem.

7.2 Musí být umožněno měření nákladů na provoz a reporting spotřeby (showback/chargeback) podle jednotlivých scénářů a útvarů.

7.3 Výkon:

a) latence pseudonymizace textu do 1 MB: p95 ≤ 400 ms; 10 MB: p95 ≤ 1200 ms,
b) dostupnost služby: ≥ 99,95 %,
c) dávkové zpracování: min. 50 dokumentů/s (referenční HW Objednatele).

8. Chybové stavy a odolnost

8.1 Pseudonymizační nástroj musí jednoznačně signalizovat chybové stavy (např. nevalidní vstupní data, nemožnost provést pseudonymizaci, neoprávněný požadavek na depseudonymizaci) a poskytovat informace potřebné pro diagnostiku.

8.2 Nástroj musí být odolný vůči výpadkům a obsahovat mechanismy pro opakování operací, automatické zotavení a řízení chyb (retry, time-out, failover).

8.3 Musí být pravidelně prováděny cvičení obnovy a testy odolnosti vůči incidentům.

9. Testování a validace

9.1 Dodavatel provede před uvedením nástroje do produkce funkční, integrační, bezpečnostní a zátěžové testy, včetně testů správnosti pseudonymizace a depseudonymizace podle vzorových datových sad.

9.2 Testovací data musí být pseudonymizovaná nebo syntetická, v souladu s požadavky na ochranu osobních údajů.

9.3 Výsledky testů musí být zdokumentovány a předány Objednateli ke schválení.

9.4 Dodavatel udržuje testy přesnosti, regrese a adverzární sady (např. skeny nízké kvality, ruční poznámky). Výsledky jsou součástí akceptace i kontinuálního provozu.

10. Odpovědnosti dodavatele a exit plán

10.1 Dodavatel odpovídá za správnou implementaci a provozuschopnost Pseudonymizačního nástroje v prostředí Koncového zákazníka Objednatele.

10.2 Dodavatel se zavazuje zajistit, že Pseudonymizační nástroj bude v souladu s požadavky této přílohy a že jeho provoz bude v souladu s právními předpisy o ochraně osobních údajů.

10.3 Dodavatel odpovídá objednateli za škody vzniklé v důsledku chybné pseudonymizace či neoprávněné depseudonymizace.

10.4 Dodavatel musí předložit exit plán pro případ ukončení smlouvy nebo změny dodavatele řešení, včetně exportu dat, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v příloze č. 9 Exit plán.

11. Požadavky na kvalitu, bezpečnost, akceptaci

11.1 Akceptační a předávací řízení:

a) Akceptační řízení ověřuje splnění funkčních, nefunkčních a bezpečnostních požadavků na základě předem definovaných scénářů, metrik a prahových hodnot.
b) Dodavatel předá akceptační balíček obsahující testovací scénáře, datové sady, protokoly a měřicí skripty.

c) Akceptace probíhá z pohledu Objednatele na hraně služby a zahrnuje kontrolu dashboardů, alertů a provozních runbooků.
d) Neúspěšné testy jsou zdokumentovány včetně nápravných opatření a termínů opakování.
e) Ukončení akceptace je možné pouze po splnění akceptačních kritérií a kompletním předání artefaktů.

11.3 Verzování, kompatibilita a deprekační politika:

a) Verze rozhraní a artefaktů se řídí schématem major.minor.patch.
b) Zpětná kompatibilita je povinná v rámci minor/patch verzí.
c) Pokud odstranění vady (v rámci záručního servisu) vyžaduje změnu, která není zpětně kompatibilní, je Dodavatel povinen na tuto skutečnost předem upozornit a dohodnout se s Objednatelem/Koncovým zákazníkem na postupu a termínu přechodu.
d) Veškeré kontrakty rozhraní (OpenAPI/AsyncAPI, schémata zpráv) jsou verzované a publikované v katalogu rozhraní.

11.4 Bezpečnost a suverenita dat:

a) Požadavky na kybernetickou bezpečnost jsou uvedeny v Příloze č. 14 Smlouvy.

11.5 FinOps, kvóty a ochranné mechanismy:

a) Nástroj publikuje metriky využití pro účely showback/chargeback a kapacitního plánování.
b) Jsou definovány kvóty a limity na uživatele (počet požadavků, objem dat, paralelizace), včetně ochranných mechanismů proti degradaci kvality (rate-limit, circuit-breaker).
c) Překročení limitů generuje auditní záznam a notifikaci.
d) Reporty obsahují náklady na jednotku zpracování, predikci trendu a doporučení optimalizace.

11.6 AI governance a post-market monitoring:

a) Je-li součástí řešení model umělé inteligence nebo statistický model, Dodavatel vede modelovou dokumentaci (model card), verzuje modely i datasety, zajišťuje sledování kvality v čase, detekci datového i konceptuálního driftu a bezpečné nasazování (stínový provoz, A/B testy, možnost rychlého návratu verze).
b) Řešení je klasifikováno dle relevantní regulace AI a je vedena vyžadovaná technická dokumentace.

c) Objednatel provede posouzení dopadů na ochranu osobních údajů; dodavatel poskytne podklady a součinnost.
d) Pokud řešení AI neobsahuje, kapitola je označena jako neaplikovatelná.

11.7 Předávací artefakty a provozní dokumentace:

a) Dodavatel předá kompletní balík:
   i. provozní a konfigurační dokumentaci,
   ii. runbooky a DR playbooky,
   iii. monitorovací dashboardy s aletry a prahovými hodnotami,
   iv. export přístupových politik,
   v. výchozí nastavení limitů,
   vi. testovací balíčky (funkční, integrační, výkonové, chaos) a protokoly o provedených akceptačních testech.
b) Součástí je aktualizace katalogu rozhraní, evidence verzí dodaných artefaktů a seznam známých omezení s plánem nápravy.

11.8 Integrátor a Go/No-Go brány:

a) Dodavatel nominuje hlavního integrátora odpovědného za E2E integraci a uvedení do provozu.
b) Nasazení probíhá přes Go/No-Go brány:
   i. kontraktní testy všech rozhraní,
   ii. E2E výkonnost,
   iii. E2E DR test,
   iv. E2E bezpečnost (DLP gating).

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	F5C08CE1D4F0993C53CCE499B5952DB432CF145BBD6F04E8A29C4FD8B19546AF
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 6 – Technická specifikace komponenty „Bridge/API“

Obsah

Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

1. Účel a funkce

1.1 Objednatel poptává dodávku a implementaci komponenty Bridge/API, která bude sloužit jako integrační vrstva mezi elektronickým systémem spisové služby (eSSL) Koncového zákazníka Objednatele, pseudonymizačním nástrojem a nástrojem umělé inteligence (AI Responder) a moduly využívající umělou inteligenci (Nástroj: Třídění mezi útvary, Nepříslušnost, Opatření proti nečinnosti).

1.2 Bridge/API bude zajišťovat:

a) převzetí vstupních dat ze zdrojového systému,

b) jejich předání pseudonymizačnímu nástroji,

c) doručení pseudonymizovaných dat do AI Responderu a modulů využívající umělou inteligenci,

d) převzetí výstupu z modulů využívající umělou inteligenci,

e) předání tohoto výstupu zpět pseudonymizačnímu nástroji k dalšímu zpracování,

f) doručení výsledku zpět do zdrojového systému.

1.3 Bridge/API musí být navrženo a implementováno tak, aby data, která nejsou pseudonymizovaná, neopustila prostředí Koncového zákazníka Objednatele.

1.4 Modul komponenty Bridge/API je navržen tak, aby mohl být dodán a provozován jako samostatný modul s jasně definovanými rozhraními, nezávisle na dodavateli jiných komponent.

2. Umístění a architektura

2.1 Komponenta Bridge/API bude provozována v infrastruktuře Koncového zákazníka Objednatele.

2.2 Bridge/API bude řídit tok dat mezi on-premise částmi (eSSL, pseudonymizačním systémem) a cloudovým AI Responderem a moduly využívající umělou inteligenci, přičemž bude zajišťovat bezpečné připojení a řízení komunikace.

2.3 Bridge/API musí podporovat provoz v synchronním i asynchronním režimu a zpracování jak jednotlivých požadavků, tak dávkových dat.

2.4 Architektura musí být navržena podle principů "zero trust", minimálních oprávnění a deklarativního řízení ("as code").

2.5 Veškeré integrační body musí být popsány v katalogu rozhraní a podléhat verzování.

2.6 Datové kontrakty a katalog rozhraní (závazné požadavky):

a) Bridge/API je řízena principem API-first.

b) Dodavatel předá a průběžně udržuje:

i. specifikaci OpenAPI 3.1 pro synchronní REST rozhraní,

ii. specifikaci AsyncAPI pro asynchronní události,
iii. verzovaná schémata zpráv (JSON/Avro dle potřeby),
iv. katalog chybových stavů s kódy a remediačními postupy,
v. kontraktní testy a validační sady.

c) Všechny artefakty jsou verzované (viz 8.5) a publikované v katalogu rozhraní Koncového zákazníka Objednatele. Katalog uvádí limity velikosti požadavků/odpovědí, rate-limit a požadavky na bezpečné použití (autentizace, autorizace, mTLS).

2.7 Dodavatel Bridge/API předloží závaznou specifikaci eSSL ↔ Bridge s detailní definicí payloadů, kódů chyb, validačních pravidel a pořadovosti událostí (OpenAPI/AsyncAPI + JSON Schema). Součástí je kontraktní test-pack, který musí projít jak implementace Bridge/API, tak adaptér eSSL. Změna kontraktu je řízena verzováním a nelze ji nasadit bez úspěšného průchodu integračními testy.

3. Bezpečnost a ochrana dat

3.1 Bridge/API musí být navrženo tak, aby do AI Responderu a modulů využívající umělou inteligenci byla vždy předávána pouze pseudonymizovaná data.

3.2 Veškerá komunikace mezi Bridge/API a ostatními komponentami musí probíhat prostřednictvím šifrovaného kanálu a s použitím bezpečných autentizačních mechanismů.

3.3 Bridge/API musí obsahovat mechanismy pro kontrolu a validaci, že nedochází k neautorizovanému přenosu dat mimo prostředí Koncového zákazníka Objednatele.

3.4 Veškeré secrety a šifrovací klíče musí být spravovány v centrálním trezoru s auditní stopou a pravidelnou rotací.

3.5 Přístupová práva musí být řízena na základě rolí a atributů, s podporou vícefaktorové autentizace.

4. Spolehlivost a provozní požadavky

4.1 Bridge/API musí podporovat idempotentní zpracování požadavků a zajistit, že každý požadavek bude identifikován a trasován.

4.2 Bridge/API musí být horizontálně škálovatelné a navrženo pro vysoce dostupný provoz.

4.3 Bridge/API musí zaznamenávat všechny významné události, chyby a stavové přechody, aby bylo možné zpracování vždy zpětně dohledat.

4.4 Komponenta musí být navržena pro provoz v režimu "failover" a obsahovat mechanismy pro automatické zotavení a opakování operací.

4.5 Každý požadavek nese Correlation-ID a Idempotency-Key. Bridge/API zajišťuje exactly-once zpracování vůči downstream službám, včetně deduplikace pozdních a opakovaných doručení. Dávkové zpracování podporuje transakční hranice „batch“ s možností partial commit, nevalidní položky jsou přesunuty do poison fronty s auditovaným důvodem.

5. Audit, observabilita a dohledatelnost

5.1 Bridge/API musí vytvářet auditní záznamy o průběhu zpracování, včetně identifikace požadavku, časových údajů a výsledného stavu.

5.2 Auditní záznamy musí být uchovávány v prostředí Koncového zákazníka Objednatele v podobě, která neumožňuje jejich neoprávněnou změnu.

5.3 Auditní logy nesmí obsahovat nepseudonymizovaná data.

5.4 Každý požadavek musí být opatřen korelačním identifikátorem pro end-to-end tracing napříč všemi komponentami.

5.5 Observabilita musí zahrnovat metriky výkonu, chybovosti, dostupnosti a kvality nástroje, včetně panelů a alertingu pro provozní a bezpečnostní role.

5.6 Nástroj publikuje telemetrii měřenou na hraně Bridge/API: latence (p50/p90/p95), propustnost, chybovost podle kódů, počet a příčiny retry, obsazenost a zpoždění front, egress objemy, využití kvót/limitů a základní business metriky (počet volání dle scénáře/útvaru). Všechny záznamy nesou Correlation-ID end-to-end. Součástí předání jsou předkonfigurované dashboardy, alerty s prahy.

6. Výkonnostní parametry a FinOps

6.1 Bridge/API musí umožňovat souběžné zpracování více požadavků.

6.2 Bridge/API musí umět zpracovávat požadavky s různými objemy dat a automaticky přepínat mezi synchronním a asynchronním režimem podle velikosti zpracovávaného vstupu.

6.3 Musí být umožněno měření nákladů na provoz a reporting spotřeby (showback/chargeback) podle jednotlivých scénářů a útvarů.

6.5 Výkonnostní požadavky:

a) Interaktivní požadavky bez RAG: p50 ≤ 300 ms, p95 ≤ 800 ms,
b) Požadavky s AI/RAG: p50 ≤ 1200 ms, p95 ≤ 2000 ms,
c) Dostupnost rozhraní: ≥ 99,95 % měsíčně,
d) Limity velikosti požadavku a rychlosti (rate-limit) jsou konfigurovatelné a musejí být uvedeny v katalogu rozhraní.

e) Time-outy a pořadovost: Defaultní time-out pro synchronní požadavky je 25 s, pro asynchronní potvrzení převzetí 5 s; při přepnutí do asynchronního režimu Bridge zajišťuje sekvenční identifikaci (Sequence-ID) a nezaručuje pořadí doručení; konzumenti musí zpracovat požadavky idempotentně dle 4.5.

f) Bridge/API emituje usage metriky pro showback/chargeback a kapacitní plánování. Jsou definovány kvóty a limity na konzumenta (počet požadavků za čas, objem dat, paralelismus) a ochranné mechanismy (rate-limit, circuit-breaker, back-pressure). Překročení limitů je auditováno a notifikováno.

g) Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

7. Chybové stavy a odolnost

7.1 Bridge/API musí jednoznačně signalizovat chybové stavy a poskytovat Koncovému zákazníkovi Objednatele informace potřebné pro diagnostiku.

7.2 Bridge/API musí být odolné proti výpadkům externích služeb a obsahovat mechanismy pro opakování operací a řízení chyb (retry, time-out, failover).

7.3 Musí být definovány fallback scénáře a plán obnovy v případě incidentu.

7.4 Při nedostupnosti downstreamu Bridge/API aplikuje exponenciální retry v definovaném časovém okně, trvale selhané požadavky ukládá do dead-letter s notifikací provozu a vrací deterministické chybové kódy s doporučením retry-after. Chybové stavy jsou popsány v katalogu chyb; runbooky obsahují postupy obnovy.

7.5 DLQ reprocessing SLA: L2 provoz zahájí reprocessing do 2 hodin od vzniku položky DLQ; položky starší 24 hodin mají prioritu P1.

8. Verzování, kompatibilita a onboarding konzumentů

8.1 Bridge/API musí být verzováno a Dodavatel se zavazuje zajistit zpětnou kompatibilitu mezi verzemi.

8.2 Při zavedení nové verze musí Dodavatel zajistit dostatečnou dobu pro migraci Koncového zákazníka Objednatele.

8.3 API musí být navrženo jako API-first, s jasným verzováním a katalogem rozhraní.

8.4 Onboarding konzumentů musí být řízený, s dokumentací a harmonogramem vyřazování starších verzí.

8.5 Verzování artefaktů a rozhraní se řídí schématem major.minor.patch. Pokud odstranění vady (v rámci záručního servisu) vyžaduje změnu, která není zpětně kompatibilní, je Dodavatel povinen na tuto skutečnost předem upozornit a dohodnout se s Objednatelem/Koncovým zákazníkem na postupu a termínu přechodu.

9. Testování a předání

9.1 Dodavatel se zavazuje provést před předáním Bridge/API funkční, integrační a zátěžové testy, včetně bezpečnostních a regresních scénářů.

9.2 Dodavatel předloží objednateli výsledky testů, které prokážou, že Bridge/API splňuje požadavky uvedené v této příloze.

9.3 Testovací data musí být pseudonymizovaná nebo syntetická, v souladu s požadavky na ochranu osobních údajů.

9.4 Pravidelně musí být prováděna cvičení obnovy a testy odolnosti vůči incidentům.

9.5 Dodavatel předá:

a) specifikace OpenAPI/AsyncAPI a schémata zpráv,
b) balíčky testů (funkční/integrační/zátěžové/chaos),
c) provozní runbooky a DR playbooky,
d) dashboardy a alerty s prahy,
e) export přístupových politik,
f) výchozí nastavení limitů a protokoly akceptačních scénářů.

9.6 Akceptace probíhá proti měřitelným SLO/SLA a předdefinovaným scénářům. Akceptace je možná pouze po úspěšném splnění všech akceptačních kritérií.

10. Odpovědnosti dodavatele a exit plán

10.1 Dodavatel odpovídá za správnou implementaci Bridge/API a jeho provozuschopnost v prostředí Koncového zákazníka Objednatele.

10.2 Dodavatel odpovídá za to, že Bridge/API bude správně komunikovat s pseudonymizačním nástrojem, AI Responderem a moduly využívající umělou inteligenci, jak jsou definovány v samostatných přílohách Smlouvy.

10.3 Dodavatel se zavazuje zajistit, aby Bridge/API splňovalo veškeré požadavky na bezpečnost, spolehlivost, auditovatelnost a výkon stanovené touto přílohou.

10.4 Dodavatel musí předložit exit plán pro případ ukončení provozu nebo změny poskytovatele, včetně exportu dat, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v Příloze č. 9 Smlouvy (Exit plán).

11. Egress politika a suverenita dat

11.1 Veškerá odchozí komunikace mimo prostředí Koncového zákazníka Objednatele je ve výchozím stavu zakázána.

11.2 Povolování egressu probíhá na základě řízeného allow-listu na síťové i aplikační vrstvě. Preferovány jsou privátní linky/peering.

11.3 Nepseudonymizovaná data nesmějí opustit prostředí Koncového zákazníka Objednatele.

11.4 Bridge/API vynucuje politiku suverenity dat na úrovni směrování požadavků, validace destinací a auditních záznamů. Logy a telemetrie neobsahují nepseudonymizované osobní údaje.

11.5 Klíče a secrety jsou spravovány v KMS/HSM s pravidelnou rotací a oddělením rolí.

11.6 Seznam kritických entit PII (např. rodné číslo, číslo dokladu, adresa, podpis) je definován v souladu s platnou legislativou na ochranu osobních údajů, zejména nařízením GDPR (Nařízení Evropského parlamentu a Rady (EU) 2016/679). Při jakékoli detekci kritické entity v odchozím obsahu do AI Responderu či modulů využívající umělou inteligenci, Bridge/API volání zablokuje, incident se zaloguje a vyžádá se přezkum. DLP pravidla a prahy FN/FP se vyhodnocují měsíčně na reálném provozu.

12. Disaster Recovery a business continuity

12.1 Pro služby třídy A je:

a) RTO: maximální doba pro obnovení plné funkčnosti služby po výpadku je 30 minut,
b) RPO: maximální přípustná ztráta dat je 5 minut.

12.2 Konfigurace, klíče a auditní záznamy jsou replikované do DR lokality; 2× ročně cvičení obnovy s protokolem.

12.3 Failover testy jsou součástí akceptačních zkoušek a pravidelného provozního režimu.

12.4 Plán kontinuity zahrnuje scénáře výpadku závislostí, degradovaný režim a postup obnovy.

13. Požadavky na kvalitu, bezpečnost, akceptaci a provoz

13.1 Akceptační a předávací řízení:

a) akceptace ověřuje splnění funkčních, nefunkčních a bezpečnostních požadavků na základě předem definovaných scénářů, metrik a prahových hodnot,
b) dodavatel předá akceptační balíček včetně testovacích scénářů, datových sad, protokolů a měřicích skriptů,
c) akceptace probíhá z pohledu Objednatele na hraně služby a zahrnuje kontrolu dashboardů, alertů a provozních runbooků,

d) neúspěšné testy jsou zdokumentovány včetně nápravných opatření a termínů opakování,
e) akceptace je možná pouze po splnění akceptačních kritérií a kompletním předání artefaktů.

13.2 Verzování, kompatibilita a deprekační politika:

a) verze rozhraní a artefaktů se řídí schématem major.minor.patch,
b) zpětná kompatibilita je povinná v rámci minor/patch verzí,
c) pokud odstranění vady (v rámci záručního servisu) vyžaduje změnu, která není zpětně kompatibilní, je Dodavatel povinen na tuto skutečnost předem upozornit a dohodnout se s Objednatelem/Koncovým zákazníkem na postupu a termínu přechodu,
d) tato subkapitola představuje jednotnou baseline; specifické požadavky Bridge/API jsou uvedeny v kapitole 8 této přílohy.

13.4 Bezpečnost a suverenita dat:

a) Požadavky na kybernetickou bezpečnost jsou uvedeny v Příloze č. 14 Smlouvy.

13.5 FinOps, kvóty a ochranné mechanismy:

a) nástroj publikuje metriky využití pro showback/chargeback a kapacitní plánování,
b) jsou definovány kvóty a limity na uživatele (objem požadavků, data, paralelizace) a ochranné mechanismy (rate-limit, circuit-breaker),
c) překročení limitů generuje auditní záznam a notifikaci,
d) reporty zahrnují náklady na jednotku zpracování, predikci trendu a doporučení optimalizace.

13.6 AI governance a post-market monitoring:

a) je-li součástí řešení model umělé inteligence nebo statistický model, Dodavatel vede modelovou dokumentaci (model card), verzuje modely i datasety, sleduje kvalitu v čase, detekuje datový/konceptuální drift a používá bezpečné postupy nasazování (stínový provoz, A/B testy, možnost rychlého návratu verze),
b) řešení je klasifikováno dle příslušné regulace AI a je vedena požadovaná technická dokumentace,
c) Objednatel provede DPIA. Dodavatel poskytne podklady a součinnost,
d) pokud Bridge/API AI neobsahuje, je tato kapitola označena jako neaplikovatelná.

13.7 Předávací artefakty a provozní dokumentace:

a) Dodavatel předá kompletní balík:

i. provozní a konfigurační dokumentaci,
ii. runbooky a DR playbooky,
iii. dashboardy s alerty a prahy,
iv. export přístupových politik, výchozí nastavení limitů,
v. testovací balíčky (funkční, integrační, výkonové, chaos),
vi. protokoly akceptačních testů.

b) Součástí je aktualizace katalogu rozhraní, evidence verzí dodaných artefaktů a seznam známých omezení s plánem nápravy.

13.8 Integrátor a Go/No-Go brány

a) nasazení probíhá přes Go/No-Go brány:
i. kontraktní testy všech rozhraní,
ii. E2E výkonnost,
iii. E2E DR test,
iv. E2E bezpečnost (DLP gating).

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	F7D25DBC1DCF9BE5162715AEC5D08045E903A1722C739784E9D86FC9045D0C99
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 7 – Technická specifikace AI Responder

Obsah

1. Účel a funkce

1.1 Objednatel poptává implementaci a provoz AI Responderu, který bude zpracovávat pseudonymizovaná data předaná komponentou Bridge/API a poskytovat výstupy na základě vyhodnocení modulů umělé inteligence dalším částem systému.

1.2 AI Responder musí umožňovat:

a) přehledné prezentování textových, strukturovaných nebo multimodálních odpovědí AI modulů,
b) podporu různých formátů výstupu,
c) umožnění zadávání vstupů,
d) reakce na uživatelské akce v reálném čase nebo asynchronně.

1.3 Modul AI Responder je navržen tak, aby mohl být dodán a provozován jako samostatný modul s jasně definovanými rozhraními, nezávisle na Dodavateli jiných komponent. Není to však vyžadováno, pokud rozsah nebo povaha zpracování nevyžaduje samostatnou transformaci dat. V takovém případě může být funkcionalita AI responderu realizována jako součást jiné komponenty systému, zejména Bridge/API.

2. Umístění a architektura

2.1 AI responder bude provozován v prostředí Koncového zákazníka Objednatele, v souladu s požadavky na suverenitu dat a bezpečnostními standardy.

2.2 Komunikace mezi AI Responderem a komponentou Bridge/API musí probíhat výhradně prostřednictvím šifrovaného a zabezpečeného kanálu.

2.3 AI Responder nesmí mít přístup k nepseudonymizovaným datům; všechna vstupní data budou předávána prostřednictvím Bridge/API a pseudonymizačního nástroje.

2.4 Architektura AI Responderu musí být navržena podle principů „zero trust“, minimálních oprávnění a deklarativního řízení („as code“).

2.5 Veškeré integrační body musí být popsány v katalogu rozhraní a podléhat verzování.

2.6 Suverenita, region, BYOK a zákaz využití dat k tréninku

2.7 AI služba je provozována výhradně v EU regionech, s BYOK/KMS klíči Koncového zákazníka Objednatele. Dodavatel garantuje, že žádná data, logy ani metriky nejsou použity k tréninku modelů třetích stran ani k profilaci mimo účely této smlouvy. Po ukončení smlouvy proběhne ověřitelná likvidace dat a artefaktů dle exit plánu.

3. Požadavky na funkčnost

3.1 AI Responder musí:

a) umožnit zadávání uživatelských dotazů prostřednictvím UI,
b) podporovat různé typy vstupů,

c) validovat uživatelský vstup před jeho odesláním AI modelu,
d) umožnit opakované odeslání nebo úpravu dotazu.

3.2 AI Responder musí umožnit komunikaci s ostatními komponentami a systémy prostřednictvím Bridge/API, jejich konfiguraci, výběr a výměnu bez nutnosti zásahu do prezentační vrstvy.

3.3 AI Responder musí umět přijímat odpovědi AI modelů, transformovat je do srozumitelné podoby a připravit je k prezentaci v uživatelském rozhraní.

3.4 AI Responder musí zobrazovat výsledky AI modelů přehledně, konzistentně a interaktivně, včetně podpory aktualizací v reálném čase a uchování historie výstupů. Zároveň musí umožňovat v případě chybného návrhu vytvořeného modulem využívající umělou inteligenci (viz. přílohy č. 1 - č. 3 Smlouvy) korekci uživatelem.

3.5 AI Responder musí uchovávat kontext a historii komunikace v rámci jedné relace a poskytovat tyto informace AI modelu pro zajištění konzistentních odpovědí.

3.6 AI Responder umožňuje definici uživatelských rolí a řídit přístup k funkcím a konfiguraci systému podle přidělených oprávnění.

3.7 AI Responder musí detekovat chybové stavy, poskytovat uživateli srozumitelnou zpětnou vazbu o průběhu zpracování a umožnit opakování neúspěšných akcí.

4. Výkonnostní parametry a FinOps

4.1 AI Responder musí být schopen zpracovat požadavky v dohodnutých časech odezvy, stanovených ve smlouvě o úrovni služeb (SLA).

4.2 Dostupnost služby AI Responder: ≥ 99,95 % měsíčně.

4.3 AI Responder musí podporovat horizontální škálování pro zpracování většího objemu požadavků v krátkém čase.

4.4 Musí být umožněno měření nákladů na provoz a reporting spotřeby (showback/chargeback) podle jednotlivých scénářů a útvarů.

4.5 Výkonnostní požadavky:

a) Interaktivní klasifikace do 1 MB textu: p50 ≤ 700 ms, p95 ≤ 1500 ms.
b) Dávkové zpracování: parametry škálování a cílová propustnost jsou součástí provozních profilů; služba musí horizontálně škálovat dle zátěže a respektovat kvóty/limity konzumentů.
c) Měření probíhá na hraně služby s využitím end-to-end Correlation-ID.

4.6 Tyto požadavky se neuplatní v případech, kdy jejich nesplnění bylo způsobeno výpadkem, omezením nebo nedostupností komponent, systémů nebo služeb třetích stran.

5. Bezpečnost a ochrana dat

5.1 Dodavatel se zavazuje, že AI Responder nebude uchovávat ani zpřístupňovat nepseudonymizovaná data.

5.2 Dodavatel zajistí, že data předaná AI modulům budou zpracovávána pouze k účelům definovaných v přílohách č. 1 - č. 3 Smlouvy, a to v souladu s GDPR a příslušnými právními předpisy.

5.3 AI Responder musí být chráněn proti neoprávněnému přístupu a kybernetickým hrozbám v rozsahu odpovídajícímu standardům pro cloudové služby zpracovávající osobní a důvěrná data.

5.4 Veškeré secrety a šifrovací klíče musí být spravovány v centrálním trezoru s auditní stopou a pravidelnou rotací.

5.5 Přístupová práva musí být řízena na základě rolí a atributů, s podporou vícefaktorové autentizace.

5.6 Nástroj musí obsahovat mechanismy pro detekci a prevenci neoprávněného přístupu a exfiltrace dat.

5.7 Modely, váhy, embeddingy a indexy jsou artefakty se SBOM a podpisy; jsou uloženy v registru artefaktů Koncového zákazníka Objednatele. Přístup je řízen RBAC/ABAC, klíče v KMS/HSM. Není povoleno využívat veřejná modelová rozhraní bez souhlasu Koncového zákazníka Objednatele.

5.8 AI služba je provozována výhradně v EU regionech, s BYOK/KMS klíči Koncového zákazníka Objednatele. Dodavatel garantuje, že žádná data, logy ani metriky nejsou použity k tréninku modelů třetích stran ani k profilaci mimo účely této Smlouvy. Po ukončení Smlouvy proběhne ověřitelná likvidace dat a artefaktů dle exit plánu.

6. Audit, observabilita a dohledatelnost

6.1 Dodavatel se zavazuje, že AI Responder bude uchovávat auditní záznamy o zpracování požadavků, a to minimálně v rozsahu: identifikátor požadavku, časové údaje, stav zpracování a výsledek klasifikace.

6.2 Auditní záznamy musí být na vyžádání zpřístupněny Objednateli a chráněny proti neoprávněné změně.

6.3 Auditní logy nesmí obsahovat nepseudonymizovaná data.

6.4 Každý požadavek musí být opatřen korelačním identifikátorem pro end-to-end tracing napříč všemi komponentami.

6.5 Observabilita musí zahrnovat metriky výkonu, chybovosti, dostupnosti a kvality služby, včetně panelů a alertingu pro provozní a bezpečnostní role.

6.6 Nástroj detekuje datový a konceptuální drift (posuny distribucí) a spouští varování/návrh retréninku. Metriky kvality jsou sledovány kontinuálně; pokles pod prahy aktivuje nápravná opatření.

7. Chybové stavy a odolnost

7.1 AI Responeder musí být schopen signalizovat situace, kdy není možné dokument jednoznačně zařadit, a vrátit odpovídající stavovou informaci.

7.2 V případě nedostupnosti AI modulů musí být komponenta Bridge/API schopna takovou situaci detekovat a oznámit Koncovému zákazníkovi Objednatele.

7.3 AI Responder musí být odolný vůči výpadkům a obsahovat mechanismy pro opakování operací, automatické zotavení a řízení chyb (retry, time-out, failover).

7.4 Musí být pravidelně prováděna cvičení obnovy a testy odolnosti vůči incidentům.

7.5 Služba splňuje RTO ≤ 30 min a RPO ≤ 5 min. Konfigurace, klíče a auditní záznamy jsou replikovány do DR lokality; 2× ročně se provádí cvičení obnovy s protokolem. Nasazení do produkce je podmíněno úspěšným DR testem.

7.6 Při vzniku chybového stavu musí systém rozlišovat mezi dočasnými a trvalými chybami, informovat uživatele srozumitelným způsobem bez zveřejnění technických detailů, zaznamenat událost do auditních a provozních logů a zabránit nekontrolovanému opakování operací.

8. Testování a validace

8.1 Dodavatel provede před uvedením AI Responderu do produkčního provozu testy funkčnosti, výkonnosti a bezpečnosti.

8.2 Výsledky testů musí být zdokumentovány a předány Objednateli ke schválení.

8.3 Testovací data musí být pseudonymizovaná nebo syntetická, v souladu s požadavky na ochranu osobních údajů.

9. Odpovědnosti dodavatele a exit plán

9.1 Dodavatel odpovídá za správnou funkčnost AI Responderu, jeho provozuschopnost v infrastruktuře Koncového zákazníka Objednatele a za dosažení stanovených parametrů úspěšnosti.

9.2 Dodavatel musí předložit exit plán pro případ ukončení provozu nebo změny poskytovatele, včetně exportu modelů, konfigurací a auditních záznamů. Specifikace exit plánu je definovaná v Příloze č. 9 Smlouvy (Exit plán).

10. Požadavky na kvalitu, bezpečnost, akceptaci a provoz

10.1 Akceptační a předávací řízení:

a) Akceptační řízení ověřuje splnění funkčních, nefunkčních a bezpečnostních požadavků na základě předem definovaných scénářů, metrik a prahových hodnot.
b) Dodavatel předá akceptační balíček obsahující testovací scénáře, datové sady, protokoly a měřicí skripty.
c) Akceptace probíhá z pohledu Objednatele na hraně služby a zahrnuje kontrolu dashboardů, alertů a provozních runbooků.
d) Neúspěšné testy jsou zdokumentovány včetně nápravných opatření a termínů opakování.
e) Předání do provozu je možné pouze po splnění akceptačních kritérií a kompletním předání artefaktů.

10.2 Verzování, kompatibilita a deprekační politika:

a) Verze rozhraní a artefaktů se řídí schématem major.minor.patch.
b) Zpětná kompatibilita je povinná v rámci minor/patch verzí.
c) Pokud odstranění vady (v rámci záručního servisu) vyžaduje změnu, která není zpětně kompatibilní, je Dodavatel povinen na tuto skutečnost předem upozornit a dohodnout se s Objednatelem/Koncovým zákazníkem na postupu a termínu přechodu.
d) Veškeré kontrakty rozhraní (OpenAPI/AsyncAPI, schémata zpráv) jsou verzované a publikované v katalogu rozhraní.

10.3 Bezpečnost a suverenita dat:

a) Požadavky na kybernetickou bezpečnost jsou uvedeny v Příloze č. 14 Smlouvy.

10.4 FinOps, kvóty a ochranné mechanismy:

a) Nástroj publikuje metriky využití pro účely showback/chargeback a kapacitního plánování.
b) Jsou definovány kvóty a limity na uživatele (počet požadavků, objem dat, paralelizace), včetně ochranných mechanismů proti degradaci kvality (rate-limit, circuit-breaker).
c) Překročení limitů generuje auditní záznam a notifikaci.
d) Reporty obsahují náklady na jednotku zpracování, predikci trendu a doporučení optimalizace.

10.5 AI governance a post-market monitoring:

a) Je-li součástí řešení model umělé inteligence nebo statistický model, Dodavatel vede modelovou dokumentaci (model card), verzuje modely i datasety, zajišťuje

sledování kvality v čase, detekci datového i konceptuálního driftu a bezpečné nasazování (stínový provoz, A/B testy, možnost rychlého návratu verze).

b) Řešení je klasifikováno dle relevantní regulace AI a je vedena vyžadovaná technická dokumentace.

c) Objednatel provede posouzení dopadů na ochranu osobních údajů; Dodavatel poskytne podklady a součinnost.

d) Pokud řešení AI neobsahuje, kapitola je označena jako neaplikovatelná.

10.6 Předávací artefakty a provozní dokumentace:

a) Dodavatel předá kompletní balík:
   i. provozní a konfigurační dokumentaci,
   ii. runbooky a DR playbooky,
   iii. monitorovací dashboardy s alerty a prahovými hodnotami,
   iv. export přístupových politik,
   v. výchozí nastavení limitů,
   vi. testovací balíčky (funkční, integrační, výkonové, chaos) a protokoly o provedených akceptačních testech.

b) Součástí je aktualizace katalogu rozhraní, evidence verzí dodaných artefaktů a seznam známých omezení s plánem nápravy.

10.7 Integrátor a Go/No-Go brány

a) Dodavatel nominuje hlavního integrátora odpovědného za E2E integraci a uvedení do provozu.

b) Nasazení probíhá přes Go/No-Go brány:
   i. kontraktní testy všech rozhraní,
   ii. E2E výkonnost,
   iii. E2E DR test,
   iv. E2E bezpečnost (DLP gating).

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	E9D93BC7644417906BBBB79B1483E3BFA3373AB44CD570F87DEE89C0230489E2
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

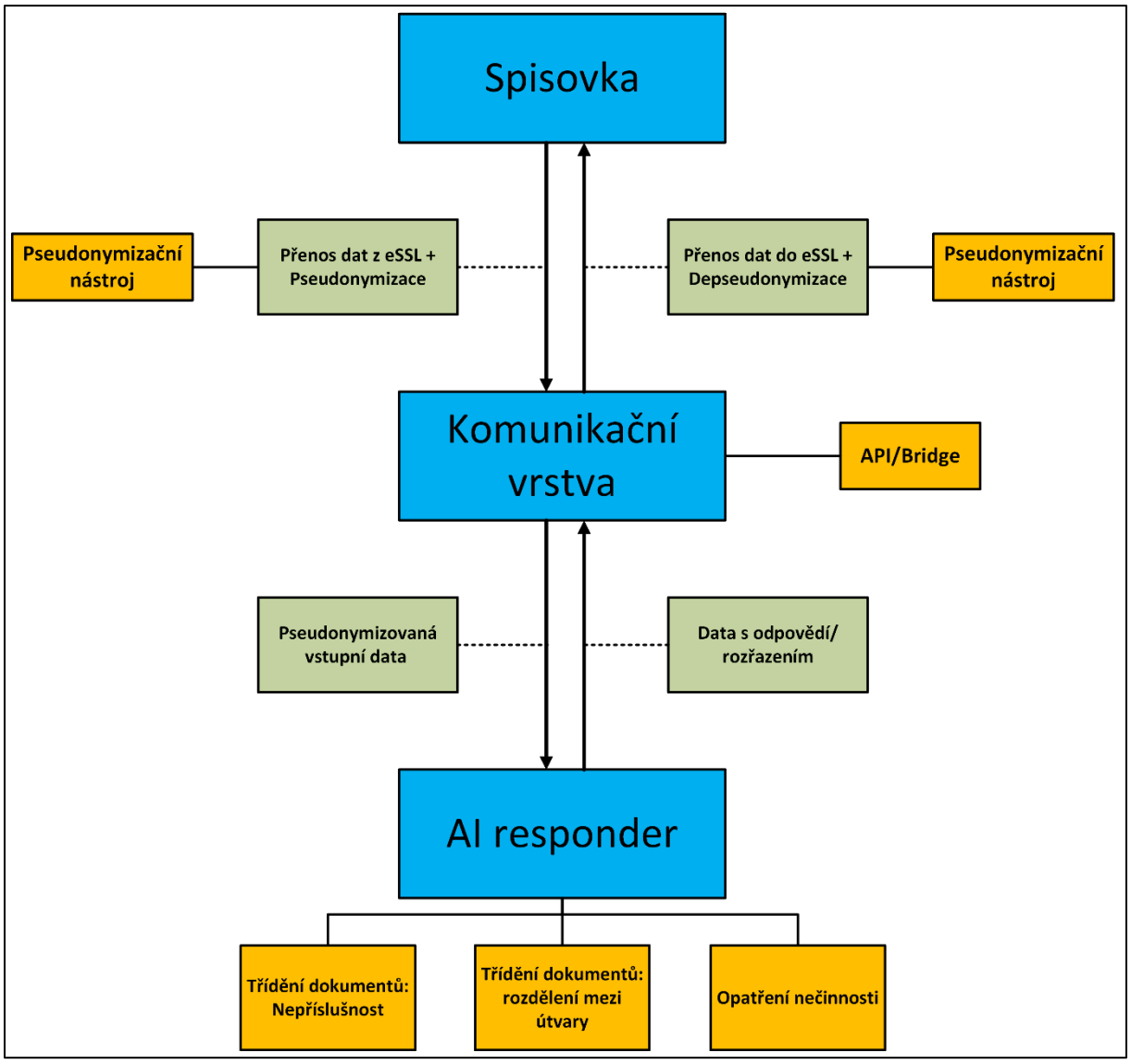
Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 8 – Diagram architektury modulů



Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	4992E8872C752483151A3BB632CB0B346B049C6901B38FE146476C837F8C45A7
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

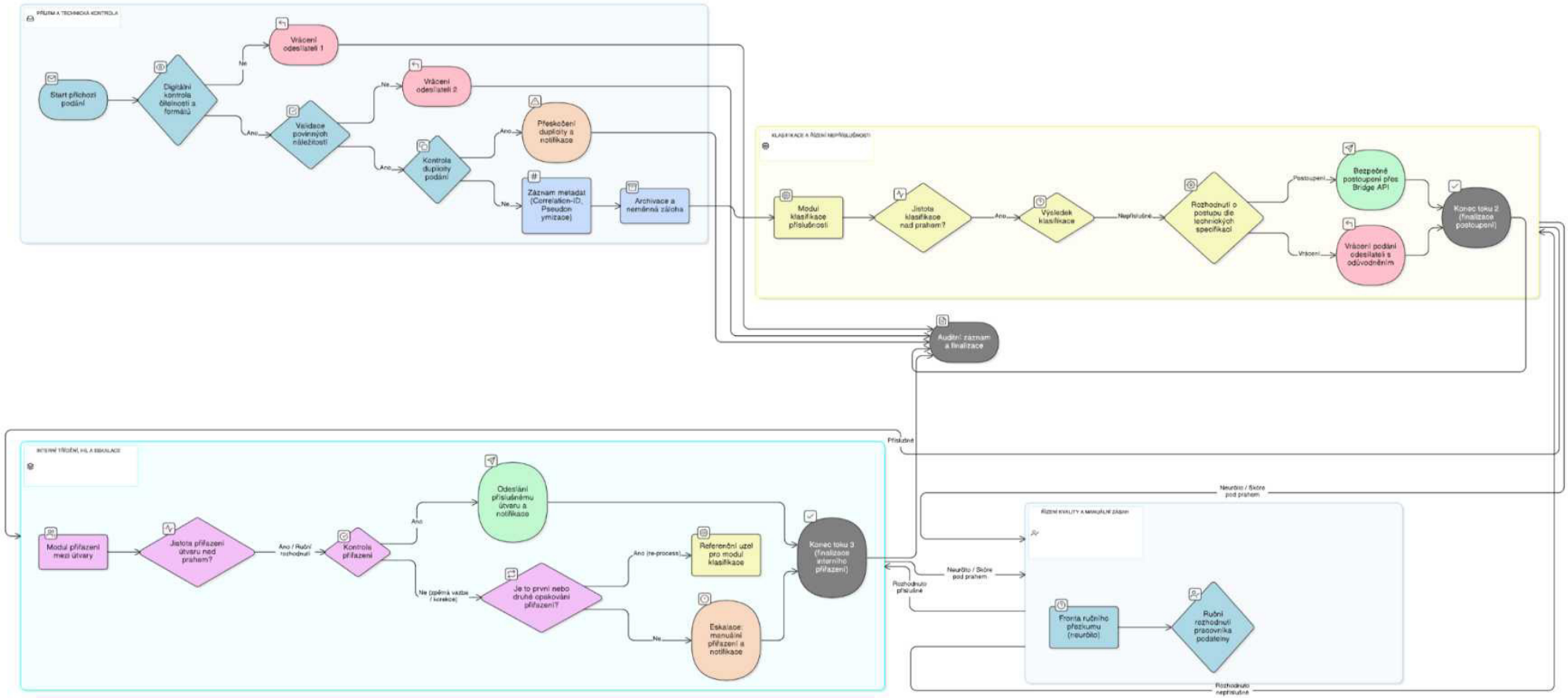
Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 9 – Vývojový diagram pro Třídění dokumentů



Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 – Vršovice **E:**

T: +420 234 066 500
info@nakit.cz

W: www.nakit.cz

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	369A2FCECEB105DC24DDE447C64D0C91087B5154DA5A65FEDFCA616B879A9B24
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 10 – Exit plán

Obsah

1. Účel a závaznost

1.1 Tento Exit plán stanovuje závazná pravidla, postupy, výstupy, role a technické požadavky pro ukončení součinnosti dodavatele po dodání a řádném předání Díla Koncovému zákazníkovi Objednatele nebo novému dodavateli. Cílem Exit plánu je zajistit, že po předání Díla je Koncový zákazník schopen Systém samostatně provozovat, rozvíjet a případně předat dalšímu dodavateli, bez závislosti na původním dodavateli. Exit plán definuje, co vše musí být součástí předání, aby byla zachována kontinuita provozu, bezpečnost a ochrana informací, auditovatelnost a aby byla minimalizována provozní, bezpečnostní a reputační rizika při případné změně dodavatele nebo provozního modelu.

1.2 Exit plán je samostatným dokumentem určeným jako příloha smlouvy. Dodavatel se zavazuje plnit Exit plán v plném rozsahu. Pokud se některé ustanovení tohoto Exit plánu odchyluje od ustanovení smlouvy, použije se smlouva; Exit plán však konkretizuje technický a procesní způsob plnění smluvních závazků.

2. Rozsah (co všechno Exit plán pokrývá)

2.1 Exit plán se vztahuje na celé dodávané řešení, zejména na:

a) aplikační vrstvu (frontend, backend, integrační vrstvy, API, integrační konektory),
b) datovou vrstvu (databáze, datové sklady, objektová úložiště, dokumenty, metadata, indexy),
c) infrastrukturu a runtime (kontejnerová platforma/Kubernetes, VM, síťové a bezpečnostní komponenty, storage),
d) provozní vrstvu (monitoring, alerting, log management, incident/problem/change procesy, runbooky),
e) bezpečnostní a compliance artefakty (hardening baseline, penetrační testy, evidence nálezů, auditní stopy),
f) AI komponenty (modelové verze, prompt šablony, guardrails, RAG knowledge base, embeddingy, eval sady, inference pipeline),
g) závislosti na třetích stranách (externí služby, licence, integrace, DNS, certifikáty, e-mailové a notifikační brány).

3. Spouštěcí události (Exit triggers) a typ exitu

3.1 Exit plán se aktivuje při ukončení smlouvy

3.2 Typ exitu se stanoví jako jeden z následujících:

a) předání díla „as-is“ (handover),
b) migrace do cílového prostředí,
c) ukončení služby bez náhrady (decommission).

4. Principy exitu

4.1 Exit je realizován tak, aby:

a) byl Systém předán ve funkčním a otestovaném stavu, připraveném k nasazení,
b) byla zajištěna přenositelnost dat a artefaktů ve standardních formátech,
c) byla zachována prokazatelnost (verze, konfigurace, změny, logy),
d) byly minimalizovány závislosti na Dodavateli a proprietárních mechanismech,
e) bylo zajištěno bezpečné předání, rotace tajemství a odebrání přístupů,
f) u AI bylo zajištěno přenositelné a ověřitelné chování (reprodukovatelnost v toleranci).

5. Řízení exitu (governance) a komunikace

5.1 Řídicí struktura – nejpozději do 5 pracovních dnů od aktivace Exit plánu strany ustanoví:

a) Exit Managera za dodavatele a za Objednatele,
b) technické vlastníky oblastí: aplikace, data, infrastruktura, bezpečnost, AI, integrace,
c) kontakty pro eskalace (operativa, bezpečnostní incidenty, management).

5.2 Komunikační režim – po dobu exitu platí:

a) předávací jednání (min. 1×, dle rozsahu předání),
b) jednotná evidence předávaných položek (předávací protokol, dostupný oběma stranám),
c) jednotný režim řízení změn (viz kapitola 8).

6. Časový rámec a fáze exitu (best practice harmonogram)

6.1 Exit probíhá ve fázích, jejichž standardní délky jsou následující (mohou být zkráceny při urgentním exitu, nikoliv však na úkor bezpečnosti a dokazatelnosti):

6.2 Fáze 0 – Průběžná připravenost („evergreen“):

a) Po celou dobu trvání Smlouvy Dodavatel udržuje aktuální provozní dokumentaci, IaC, exportní mechanismy a seznam komponent, aby Exit bylo možné provést bez neodůvodněných prodlev.

6.3 Fáze 1 – Zahájení a stabilizace (typicky 10 pracovních dnů):

a) formální aktivace Exit plánu a schválení cílového scénáře,
b) stabilizace prostředí, omezení změn, definice „baseline“ verzí,
c) detailní plán předání (milníky, odpovědnosti, termíny),
d) příprava exportů, přístupů a zajištění bezpečnostních předpokladů.

6.4 Fáze 2 – Předání artefaktů a znalostí (typicky 20 pracovních dnů):

a) předání výstupů dle kapitoly 7.,

b) znalostní transfer (workshopy, walkthrough runbooků, shadowing),
c) ověření nasaditelnosti v cílovém prostředí (zkušební nasazení),
d) ověření obnovy dat (restore test) a integrací.

6.5 Fáze 3 – Cut-over a stabilizace (typicky 10 pracovních dnů + hypercare):

a) řízené přepnutí provozu (cut-over) s rollback plánem,
b) stabilizace po přepnutí, uzavření otevřených incidentů,
c) odebrání přístupů původního dodavatele,
d) formální ukončení exitu podpisem Exit protokolu.

6.6 Hypercare (best practice):

a) Po cut-over se uplatní hypercare v délce 20 pracovních dnů (4 týdny), v režimu zvýšené součinnosti Dodavatele nebo dle dohody s novým dodavatelem. Hypercare zahrnuje prioritní řešení incidentů, dolaďování monitoringu a dokončení znalostního transferu.

7. Výstupy a předávané artefakty (minimální závazný obsah)

7.1 Dodavatel předá Objednateli nebo novému dodavateli modulů nebo upgradu modulů následující výstupy. Výstupy jsou předávány v elektronické podobě, ve strojově zpracovatelných formátech, a jsou jednoznačně verzované.

7.2 Datové výstupy:

a) export databází včetně schémat (např. dump + DDL),
b) export objektových úložišť (včetně metadat a vazeb),
c) export dokumentů a souvisejících metadat,
d) export integračních dat (konfigurační registry, mapování, transformace),
e) export auditních logů a bezpečnostních záznamů v dohodnuté retenci,
f) kontrolní report úplnosti exportu (počty záznamů, seznam entit, kontrolní součty).

7.3 Aplikační výstupy:

a) zdrojové kódy (repozitáře) a build instrukce,
b) CI/CD definice (pipeline konfigurace, deployment skripty),
c) releasové artefakty (balíčky) nebo image reference (tagy + digesty),
d) seznam komponent a jejich verzí (včetně runtime, knihoven),
e) dokumentace API a integračních kontraktů (OpenAPI/AsyncAPI, event schémata),
f) konfigurace aplikace včetně parametrů a feature flags.

7.4 Infrastruktura a provoz (IaC + Runbooks):

a) infrastruktura jako kód: manifesty, Helm charts, Terraform/Ansible,
b) síťová a bezpečnostní konfigurace relevantní pro provoz (bez předání tajemství v otevřené podobě),

c) runbooky pro provoz, incidenty, změny, release management,
d) dokumentace monitoringu a alertingu (co se měří, prahy, eskalace),p
e) ostupy obnovy a disaster recovery včetně pravidel RPO/RTO,
f) seznam externích závislostí (DNS, certifikáty, e-mail/SMS brány, licence, třetí strany).

7.5 Bezpečnostní a compliance výstupy:

a) hardening baseline a konfigurace bezpečnostních kontrol,
b) poslední penetrační testy a evidence nápravy (remediation),
c) evidence změn a schvalování v rozsahu nutném pro audit,
d) přehled rolí a oprávnění, RBAC/ABAC model, servisní účty a jejich účel,
e) bezpečnostní architektura a datové toky v rozsahu relevantním pro službu.

7.6 AI výstupy (přenositelnost AI chování):

a) identifikace modelových verzí používaných v produkci a testu,
b) prompt šablony, systémové instrukce, guardrails, bezpečnostní filtry,
c) RAG knowledge base: seznam zdrojů, indexy, embeddingy, konfigurace retrievalu,
d) golden set a eval metodika + poslední eval reporty,
e) popis inference pipeline, parametry, limity a provozní závislosti,
f) definice způsobu verifikace chování po migraci (exit evaluace).

8. Řízení změn během exitu (release freeze)

8.1 Od aktivace Exit plánu platí režim omezených změn:

a) běžné změny jsou pozastaveny; povoleny jsou pouze změny kritické pro bezpečnost nebo stabilitu,
b) každá změna musí být schválena Exit Managerem za Objednatele,
c) každá schválená změna musí být zaznamenána s dopadem na baseline (verze, konfigurace, data),
d) změny AI komponent (model version, prompt šablony, retrieval konfigurace) vyžadují navíc aktualizaci eval reportu.

9. Přístupy, tajemství a identity (security handover)

9.1 Dodavatel je povinen:

a) předat přehled všech identit, servisních účtů a integračních přístupů,
b) umožnit bezpečnou rotaci tajemství (API klíče, certifikáty, hesla, tokeny) nejpozději do 5 pracovních dnů před cut-over,
c) spolupracovat na převodu SSO a identity vazeb (IdP, OIDC/SAML, role mapping),
d) po Exit akceptaci odebrat veškeré své přístupy do 24 hodin,
e) doložit odebrání přístupů protokolem (rozsah, čas, odpovědná osoba),

f) zajistit, aby žádné tajemství nebylo předáno v otevřené podobě mimo dohodnutý bezpečný kanál a úložiště tajemství.

10. Migrace a cut-over (technická pravidla)

10.1 Cut-over plán obsahuje:

a) přesný časový plán přepnutí,
b) kroky pro „freeze“ dat (pokud relevantní),
c) synchronizaci a delta migraci,
d) ověření funkčnosti (smoke test) a ověření integrací,
e) ověření monitoringu a alertingu,
f) verifikaci výkonu v základní zátěži,
g) rollback plán a „go/no-go“ kritéria.

10.2 Rollback plán (best practice) - Rollback je povinnou součástí cut-over a je definován tak, aby:

a) bylo možné vrátit Systém do původního stavu bez ztráty integrity,
b) byla jasně definována hranice, kdy rollback již není bezpečný (např. po potvrzení finálního importu a otevření provozu),
c) byla stanovena odpovědnost a časový limit pro rozhodnutí o rollbacku.

11. Exit akceptace (kontrola úplnosti a funkčnosti předání)

11.1 Exit je dokončen až podpisem Exit protokolu po splnění Exit akceptace. Exit akceptace zahrnuje:

a) kontrolu úplnosti předaných artefaktů dle kapitoly 7 (checklist + kontrolní součty),
b) zkušební nasazení v cílovém prostředí nebo staging (je-li relevantní),
c) zkušební obnovu dat (restore test) a kontrolu integrity,
d) ověření všech klíčových integrací,
e) ověření monitoringu, logování, alertingu a incidentních postupů,
f) u AI provedení zkrácené exit evaluace golden setu a bezpečnostních scénářů k ověření, že chování se nezměnilo nad toleranci a nedošlo k regresi bezpečnostních opatření.

11.2 Výsledkem je Exit protokol podepsaný oprávněnými zástupci Objednatele nebo Koncového zákazníka Objednatele (určí Objednatel) a Dodavatele (a případně nového dodavatele).

12. Hypercare a součinnost po předání

12.1 Po cut-over běží hypercare po dobu 20 pracovních dnů. V hypercare Dodavatel zajišťuje zvýšenou součinnost:

a) prioritní řešení incidentů a problémů vzniklých přechodem,
b) podporu při dolaďování monitoringu, alertingu a výkonových prahů,
c) asistenci při dořešení integračních anomálií,
d) dokončení znalostního transferu,
e) podporu při vyhodnocení post-cut-over metrik a stabilizačních opatřeních.

13. Ukončení zpracování a výmaz dat (best practice bez mezer)

13.1 Výmaz primárních dat – Po podpisu Exit protokolu Dodavatel do 30 kalendářních dnů:

a) odstraní data Koncového zákazníka Objednatele a Objednatele ze svých produkčních systémů, které již nejsou nutné pro plnění smlouvy,
b) odstraní pracovní kopie dat používané pro podpůrné účely (test, troubleshooting), pokud nebyly výslovně schváleny k delšímu držení,
c) provede verifikaci výmazu a vyhotoví protokol o výmazu.

13.2 Výmaz dat ze záloh:

a) Dodavatel zajistí, že data Koncového zákazníka Objednatele a Objednatele budou z cyklu záloh odstraněna nejpozději do 90 kalendářních dnů od podpisu Exit protokolu (přirozeným vypršením retenční doby záloh nebo cíleným purge, pokud je technicky proveditelné a bezpečné). Dodavatel vyhotoví protokol potvrzující, že zálohy s daty Koncového zákazníka Objednatele a Objednatele již nejsou obnovitelné.

13.3 Retence nezbytných záznamů – Dodavatel je oprávněn uchovat pouze minimální rozsah záznamů nezbytný pro:

a) prokazatelnost plnění smlouvy a vypořádání případných reklamací nebo sporů,
b) splnění právních povinností (např. účetní nebo daňové doklady, pokud relevantní).

Best practice doba uchování takových minimálních záznamů je 12 měsíců od podpisu Exit protokolu, přičemž uchovávaný rozsah musí být minimalizovaný, přiměřený a zabezpečený. Po uplynutí této doby dodavatel provede výmaz a doloží jej protokolem.

13.4 Protokol o výmazu a odebrání přístupů:

a) Dodavatel předá Koncovému zákazníkovi Objednatele a Objednateli protokol o výmazu dat a protokol o odebrání přístupů nejpozději do 10 pracovních dnů po provedení výmazu a odebrání přístupů. Protokoly obsahují rozsah, čas, metodu, odpovědné osoby a potvrzení, že nedošlo k ponechání aktivních přístupů.

14. Scénáře exitu

14.1 Scénář A – Předání díla „as-is“ (handover):

a) Dodavatel předá prostředí a artefakty tak, aby Objednatel nebo nový dodavatel převzal provoz bez zásadní změny platformy. Součástí je kompletní provozní předání, předání IaC a zajištění rotace tajemství.

14.2 Scénář B – Migrace do cílového prostředí:

a) Dodavatel poskytne exporty a součinnost, nový dodavatel nebo Objednatel vytvoří cílové prostředí a provede import a nasazení. Cut-over proběhne řízeně, s rollbackem a verifikací metrik.

14.3 Scénář C – Ukončení bez náhrady (decommission):

a) Dodavatel předá data a auditní záznamy, provede vypnutí služby v dohodnutém termínu, odebere přístupy a provede prokazatelný výmaz dle kapitoly 13.

15. Přílohy (součást Exit plánu)

15.1 Součástí Exit plánu jsou následující přílohy:

a) Exit checklist (předání dat a artefaktů),
b) šablona Exit protokolu,
c) seznam systémových komponent a závislostí,
d) seznam integračních rozhraní a kontraktů,
e) šablona zkrácené AI exit evaluace (golden set + bezpečnostní scénáře).

Příloha A – Exit checklist (předání dat a artefaktů)

A.1 Identifikace exitu

Název služby/řešení:
Číslo smlouvy / objednávky:
Typ exitu: předání „as-is“ / migrace / decommission
Datum aktivace Exit plánu:
Plánovaný cut-over (datum/čas):
Exit Manager (Koncový zákazník Objednatele,):
Exit Manager (Dodavatel):
Kontakty pro eskalace (Koncový zákazník Objednatele, /Dodavatel):

A.2 Checklist předání (tabulka)

Oblast	Položka	Povinné (A/M/D)*	Forma předání	Stav (OK/NOK/NA)	Odkaz / Umístění	Poznámka
Řízení exitu	Plán exitu (milníky, harmonogram, RACI)	A/M/D	Dokument			
Řízení exitu	Evidence úkolů a rizik (backlog, risk log)	A/M/D	Export / odkaz			
Baseline	Seznam komponent a verzí (release/build, digesty)	A/M	Dokument / export			
Baseline	Konfigurační baseline prostředí (bez tajemství)	A/M	Export			
Data	Export DB včetně schémat (DDL + data)	A/M/D	Dump + DDL			
Data	Kontrolní report úplnosti exportu (počty, checksumy)	A/M/D	Report			
Data	Export objektového úložiště včetně metadat	A/M/D	Snapshot / export			
Data	Export dokumentů + metadata + vazby	A/M/D	Export			
Data	Export auditních a bezpečnostních logů (retence)	A/M/D	Export			
Aplikace	Zdrojové kódy (repo) + přístup / export	A/M	Repo/export			
Aplikace	Build instrukce + závislosti	A/M	Dokument			
Aplikace	CI/CD definice (pipeline, deploy skripty)	A/M	Repo/export			
Aplikace	Releasové balíčky / image reference (tag+digest)	A/M	Registry/export			
Aplikace	Dokumentace API a kontraktů (OpenAPI/AsyncAPI)	A/M	Dokument			
Infrastruktura	IaC (Terraform/Ansible/Helm/manifesty)	A/M	Repo/export			

Oblast	Položka	Povinné (A/M/D)*	Forma předání	Stav (OK/NOK/NA)	Odkaz / Umístění	Poznámka
Infrastruktura	Síťová topologie a pravidla (bezpečnostní zóny, FW)	A/M	Dokument			
Infrastruktura	Storage konfigurace + politiky (retence, snapshoty)	A/M	Dokument			
Provoz	Runbooky (incident, change, release, DR)	A/M	Dokument			
Provoz	Monitoring a alerting (co se měří, prahy, eskalace)	A/M	Dokument/export			
Provoz	DR plán (RPO/RTO, postupy obnovy)	A/M	Dokument			
Bezpečnost	Hardening baseline a konfigurace kontrol	A/M	Dokument			
Bezpečnost	Penetrační testy + remediation evidence	A/M	Report			
Bezpečnost	Seznam účtů, rolí, oprávnění (RBAC/ABAC)	A/M	Export			
Bezpečnost	Seznam servisních účtů a integrací	A/M	Export			
Bezpečnost	Plán rotace tajemství (secrets rotation)	A/M	Dokument			
Integrace	Seznam integrací + endpointy + certifikáty	A/M	Dokument/export			
Integrace	DNS záznamy, certifikáty, notifikační brány	A/M/D	Dokument			
AI	Model version (produkce/test), parametry inference	A/M	Dokument			
AI	Prompt šablony, systémové instrukce, guardrails	A/M	Repo/export			
AI	RAG KB: seznam zdrojů, indexy, embeddingy, konfigurace	A/M	Export			
AI	Golden set + eval metodika + poslední eval reporty	A/M	Dokument + data			
Exit akceptace	Zkušební nasazení v cílovém prostředí (evidence)	A/M	Protokol			
Exit akceptace	Restore test (evidence integrity)	A/M	Protokol			
Exit akceptace	Smoke test + ověření integrací	A/M	Protokol			
Exit akceptace	AI exit evaluace (zkrácená)	A/M	Report			
Ukončení	Protokol o odebrání přístupů (do 24 h po akceptaci)	A/M/D	Protokol			
Ukončení	Protokol o výmazu primárních dat (do 30 dnů)	A/M/D	Protokol			
Ukončení	Potvrzení vyřazení ze záloh / neobnovitelnosti (do 90 dnů)	A/M/D	Protokol			

* A/M/D = As-is handover / Migrace / Decommission

Příloha B – Šablona Exit protokolu (podpisový dokument)

B.1 Identifikace

Název služby/řešení:
Číslo smlouvy / objednávky:
Dodavatel:
Koncový zákazník Objednatele:
Typ exitu: předání „as-is“ / migrace / decommission
Datum aktivace Exit plánu:
Datum cut-over:
Datum zahájení hypercare:
Datum ukončení hypercare:

B.2 Předmět protokolu

Tento Exit protokol potvrzuje předání výstupů, provedení ověřovacích kroků a ukončení exitu dle Exit plánu. Protokol je závazným dokladem, že byly splněny podmínky Exit akceptace.

B.3 Přehled předaných výstupů

Odkaz na Exit checklist (Příloha A):
Umístění předaných artefaktů (repozitáře/úložiště):
Seznam klíčových exportů (data, logy, konfigurace):
Seznam klíčových aplikačních artefaktů (release/build, image digesty):
Seznam IaC artefaktů (repo/export):
AI artefakty (model version, prompt šablony, RAG export, golden set):

B.4 Ověření a testy

Zkušební nasazení v cílovém prostředí: PROVEDENO / NEPROVEDENO (odůvodnění)
Restore test a ověření integrity dat: PROVEDENO / NEPROVEDENO (odůvodnění)
Smoke test a ověření integrací: PROVEDENO / NEPROVEDENO (odůvodnění)
Ověření monitoringu a alertingu: PROVEDENO / NEPROVEDENO (odůvodnění)
AI exit evaluace (zkrácená): PROVEDENO / NEPROVEDENO (odůvodnění)

B.5 Výsledek Exit akceptace

Výsledek: AKCEPTOVÁNO / NEAKCEPTOVÁNO
Pokud NEAKCEPTOVÁNO: popis nedostatků a plán nápravy (včetně termínů)

B.6 Ukončení přístupů a zpracování

Plán rotace tajemství proveden: ANO / NE
Odebrání přístupů dodavatele: ANO / NE (datum/čas)
Protokol o odebrání přístupů přiložen: ANO / NE
Výmaz primárních dat zahájen: ANO / NE (datum)
Protokol o výmazu primárních dat bude předán do: (datum)

Potvrzení vyřazení dat ze záloh bude předáno do: (datum)

B.7 Podpisy

Za Koncového zákazníka Objednatele: jméno, funkce, podpis, datum
Za dodavatele: jméno, funkce, podpis, datum
Za nového dodavatele (je-li relevantní): jméno, funkce, podpis, datum

Příloha C – Seznam systémových komponent a závislostí (šablona)

C.1 Aplikační komponenty

Komponenta	Popis	Verze / build	Artefakt (repo/image)	Konfigurace (odkaz)	Vlastník

C.2 Datové komponenty

Komponenta	Typ	Verze	Umístění	Export metoda	Vlastník

C.3 Infrastruktura a runtime

Vrstva	Technologie	Verze	Konfigurace/IaC (odkaz)	Poznámka

C.4 Externí závislosti

Závislost	Účel	Typ (služba/licence)	Vlastník	Kritičnost	Poznámka

C.5 Bezpečnostní závislosti

Položka	Účel	Umístění / odkaz	Rotace / expirace	Vlastník

Příloha D – Seznam integračních rozhraní a kontraktů (šablona)

D.1 API rozhraní (synchronní)

Rozhraní	Směr	Protokol	Autentizace	Endpoint	Specifikace (odkaz)	SLA/limity

D.2 Eventy / asynchronní integrace

Rozhraní	Směr	Transport	Schéma	Téma/queue	Specifikace (odkaz)	Retence

D.3 Notifikace

Kanál	Účel	Poskytovatel	Konfigurace	Limity	Poznámka

D.4 DNS a certifikáty

Položka	Typ	Doména / CN	Expirace	Umístění	Vlastník

Příloha E – Šablona zkrácené AI exit evaluace (golden set + bezpečnostní scénáře)

E.1 Identifikace a baseline

Datum evaluace:
Prostředí: původní / cílové (uveď)
Model version:
Konfigurace inference (relevantní parametry):
Prompt šablony / systémové instrukce (verze/odkaz):
RAG konfigurace (retrieval parametry, zdroje, indexy – verze/odkaz):

E.2 Eval metodika

Popis golden setu (velikost, pokrytí, typy dotazů):
Způsob hodnocení (automatický/manuální, škála):
Role hodnotitelů a pravidla konzistence hodnocení:

E.3 Výsledky golden setu (souhrn)

Celkový počet případů:
PASS rate (celkem):
Grounding rate (pokud relevantní):
Nejčastější typy odchylek (stručně):

E.4 Bezpečnostní scénáře (prompt injection / exfiltrace / jailbreak)

Popis testovací sady:
Počet scénářů:
Počet kritických selhání:
Počet minor odchylek:
Popis případných selhání a mitigací:

E.5 Srovnání původní vs. cílové prostředí

Změna výsledků proti baseline (stručně):
Závěr: chování v toleranci / mimo toleranci
Doporučené kroky (pokud mimo toleranci):

E.6 Přílohy

Odkazy na detailní výsledky (logy, exporty odpovědí, skórování, evidence testů):

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	24CE15BB149F1FEDFFE16B3C2DCFCFEA4AB12DAEB1EC3857EDC59568FB811F41
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 11 – Akceptační plán Systému

Akceptační plán

Vývoj komplexního softwarového systému pro automatizované třídění příchozích dokumentů a vyřizování návrhů

Realizovaná v rámci projektu

AIDAS

(Digitalizace správy dokumentů a využívání umělé inteligence)

Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

1. Úvod

Tento dokument představuje akceptační plán pro dodávku komplexního softwarového systému pro automatizované třídění příchozích dokumentů a vyřizování návrhů s prvky umělé inteligence realizované v rámci projektu AIDAS (dále jen „Dílo“ nebo „Systém“ nebo „softwarové řešení“). Jeho cílem je definovat rozsah, přístup, odpovědnosti a kritéria akceptačního testování a předání a převzetí Díla, na jejichž základě bude ověřeno, že dodané řešení splňuje požadavky Objednatele a je připraveno k nasazení do produkčního prostředí u Koncového zákazníka Objednatele.

Akceptační testování se zaměřuje na ověření požadavků na Dílo definovaných v technických specifikacích modulů (Přílohy č. 1 – 6 Smlouvy) a dále v Příloze č. 13 Smlouvy, které stanoví požadavky dopadající na akceptaci dodávaného Díla a ověření:

- funkčních požadavků,
- nefunkčních vlastností systému, zejména výkonu, použitelnosti, spolehlivosti, kompatibility a možnosti odpojení nebo vypnutí všech modulů uvedených v Přílohách č.1 až č.6 Smlouvy bez narušení funkčnosti ostatních modulů systému.
- bezpečnostních požadavků na Dílo, včetně ochrany dat, řízení přístupů a odolnosti vůči běžným bezpečnostním hrozbám.

Tento akceptační plán slouží jako závazný podklad pro provedení akceptačních testů mezi Dodavatelem a Objednatelem a stanovuje podmínky, za kterých bude Dílo považováno za akceptované.

Akceptační plán vymezuje následující odpovědnosti související s akceptačním testováním:

- Dodavatel ve spolupráci s Objednatelem – odpovídá za provedení testování,
- Objednatel odpovídá za vyhodnocení výsledků testování,
- Objednatel – schvalovací autorita akceptace.

Veškeré odchylky, nalezené chyby a rizika identifikovaná během akceptačního testování budou zaznamenány a vyhodnoceny v souladu s postupy definovanými dále v tomto Akceptačním plánu .

1.1 Definice a zkratky

Níže uvedené pojmy a zkratky jsou pro účely tohoto Akceptačního plánu používány s následujícím významem:

- AI – umělá inteligence.
- LLM – jazykový model (Large Language Model) využívaný pro generování textu nebo analýzu obsahu.
- RAG – Retrieval-Augmented Generation; generování odpovědi s oporou o vyhledané zdroje/kontext.
- SLI – Service Level Indicator; měřitelný indikátor (např. latence p95).
- SLO – Service Level Objective; cílová hodnota SLI používaná pro akceptaci a provozní řízení.
- UAT – User Acceptance Testing; uživatelské akceptační testování.
- Golden set – referenční sada testovacích případů/vstupů s očekávanými výstupy pro opakovatelnou evaluaci.

- Neshoda/Vada – odchylka od požadovaného stavu zjištěná při akceptačním testování.
- Release/Build – konkrétní verze Díla identifikovaná číslem verze a/nebo build ID.
- Model version – jednoznačná verze modelu použitá při testování (včetně konfigurace, prompt šablon a parametrů).
- PII – osobní údaje nebo jiné identifikátory, které podléhají ochraně dle GDPR a interních pravidel správce údajů, zejména MV,
- SBOM - Bill of Materials - podrobný inventární seznam všech komponent, knihoven, modulů a závislostí, ze kterých se skládá softwarové řešení.

Hovoří-li se v této příloze o „neshodách“, rozumí se jimi „vady“, jak je tento pojem v souvislosti s akceptačním řízením používán v těle Smlouvy.

2. Průběh akceptačního testování

Akceptační testování je zahájeno po formálním potvrzení připravenosti dodaného softwarového řešení a testovacího prostředí Koncového zákazníka Objednatele. Zahájení akceptace je podmíněno dostupností všech vstupů definovaných v tomto Akceptačním plánu a v Přílohách č. 1 až č. 13 Smlouvy. Akceptační testování v prostředí Koncového zákazníka Objednatele musí být zahájeno nejpozději 15 kalendářních dnů před smluvním termínem dokončení plnění, není-li smluvními stranami písemně dohodnuto jinak.

Předpoklady a vstupní podmínky
Před zahájením akceptačního testování v prostředí Koncového zákazníka Objednatele musí být splněny minimální vstupní podmínky uvedené níže. Nesplnění jednotlivé podmínky samo o sobě automaticky nebrání zahájení akceptačního testování v prostředí Koncového zákazníka Objednatele. Objednatel posoudí povahu a dopad nesplněné podmínky a rozhodne, zda lze akceptační testování v jeho prostředí zahájit v omezeném rozsahu, zahájit s výhradou, nebo zda je nutné jeho zahájení odložit či testování dočasně pozastavit. Toto rozhodnutí musí být odůvodněno a zaznamenáno v readiness checklistu a akceptačním protokolu.

Doporučený způsob prokazování splnění readiness je vyplnění checklistu a jeho schválení zástupcem Objednatele a Dodavatele.

Oblast	Požadavek	Kritérium splnění	Ověření / důkaz	Odpovědnost
Prostředí	Testovací prostředí Objednatele odpovídá dohodnutému cílovému prostředí (verze, konfigurace, sítě).	Nasazena testovaná verze (release/build), dostupné integrační závislosti, stabilní konektivita.	Popis prostředí + export konfigurace + potvrzení dodavatele.	Dodavatel

Verzování	Jednoznačná identifikace Díla (release/build) a relevantních komponent.	Zaznamenáno build ID, verze aplikací, verzí knihoven, kontejnery / obrazy, model version, prompt šablony.	Release notes + (pokud je k dispozici) SBOM + seznam image / tagů.	Dodavatel
Přístupy	Zřízeny testovací účty a role dle požadovaných oprávnění.	Účty pro uživatele, administraci a audit; otestováno přihlášení a řízení přístupů dle rolí (RBAC).	Seznam účtů/rolí + potvrzení přístupu.	Koncový zákazník Objednatele – jeho součinnost Dodavateli zajistí Objednatel/ Dodavatel
Data	Dostupná testovací data a pravidla jejich použití (anonymizace / pseudonymizace).	Testovací data jsou legální, reprezentativní a neobsahují nepovolené PII nebo utajované informace.	Protokol o původu dat + popis anonymizace / pseudonymizace.	Objednatel
Logování a monitoring	Zapnuté logování a monitoring v rozsahu nutném pro vyhodnocení akceptace.	K dispozici auditní logy, aplikační logy, metriky výkonu (latence, chybovost) a korelační ID.	Ukázka logů/metrik + přístup do monitoringu.	Dodavatel
Bezpečnost	Dohodnutý rozsah bezpečnostních testů a pravidla pro vyhodnocení nálezů.	Jasná kritéria: bez kritických nálezů; pravidla pro vysoké/střední; postup pro výjimky.	Plán testů + protokol o provedení.	Dodavatel / Objednatel

2.1 Způsob provádění akceptačních testů – testovací scénáře

Akceptační testování je prováděno formou systematického prověřování softwarového řešení podle schválených testovacích scénářů. Dodavatel předloží návrh testovacích scénářů nejpozději 10 pracovních dnů před plánovaným zahájením akceptačního testování. Objednatel návrh scénářů do 5 pracovních dnů schválí nebo k němu uplatní připomínky. Akceptační testování může být zahájeno až

po písemném schválení testovacích scénářů Objednatelem, není-li Objednatelem výslovně rozhodnuto jinak. Testování je zaměřeno na ověření jednotlivých oblastí řešení a probíhá řízeným a opakovatelným způsobem.

Testovací scénáře definují zejména:

- provedení definovaných testovacích kroků,
- simulaci běžných i hraničních uživatelských situací,
- vyhodnocení chování systému vůči očekávaným výsledkům.

Výsledky jednotlivých testů jsou průběžně zaznamenávány.

2.2 Ověřované oblasti v rámci akceptačního testování

Rozsah a hloubka ověření jednotlivých oblastí v rámci akceptačního testování vychází z požadavků na softwarové řešení definovaných v Přílohách č.1 až č.6 Smlouvy. Akceptační testování zahrnuje ověřování následujících oblastí:

a) Funkční ověření

Ověřuje se, že softwarové řešení:

- poskytuje funkce definované v příslušné specifikaci Díla,
- reaguje korektně na standardní i nestandardní vstupy,
- vykazuje konzistentní chování napříč jednotlivými částmi systému.

b) Nefunkční ověření

Ověřují se zejména:

- základní výkonnostní charakteristiky,
- stabilita řešení při běžném používání,
- použitelnost a srozumitelnost ovládání,
- kompatibilita s definovaným prostředím.

c) Bezpečnostní ověření

Ověřuje se, že:

- přístup k systému odpovídá definovaným oprávněním,
- systém správně pracuje s uživatelskými rolemi,
- nedochází k neoprávněnému přístupu k datům nebo funkcím.

2.2.1 Akceptační kritéria a metriky (SLI/SLO)

Pro objektivní vyhodnocení akceptace jsou pro vybrané parametry stanoveny měřitelné indikátory (SLI) a cílové hodnoty (SLO). Konkrétní prahové hodnoty vychází primárně ze smluvní dokumentace a z technických specifikací (zejména Přílohy č. 1 – 6 Smlouvy). Pokud některá prahová hodnota není ve specifikacích uvedena, musí být před zahájením akceptace dohodnuta a zapsána do Akceptačního protokolu nebo do schválené změny dle kapitoly 6 tohoto Akceptačního plánu.

Měření musí být prováděno v dohodnutém testovacím prostředí při jednoznačně identifikované verzi dodávky (release/build) a při fixované konfiguraci relevantních komponent (včetně model version).

Oblast	SLI (metrika)	Metoda měření	SLO / akceptační práh	Důkazní artefakt
Výkon	Latence odezvy (p95 / p99)	Měření aplikační metrikou nebo APM v zátěžovém testu	800 ms (p95) / 2000 ms (p99)	Export metrik + report z testu
Výkon	Propustnost	Zátěžový test (počet požadavků/operací za čas)	20 req/s nebo 1 200 operací/min	Report z testu
Stabilita	Chybovost	Podíl neúspěšných požadavků / výjimek	max. 0,5 %	Logy + metriky
Použitelnost	Splnění UX/UAT kritérií	Kontrolní seznam + UAT scénáře	min. 95 % scénářů PASS	UAT protokol
Bezpečnost	Závažné nálezy	Penetrační testy / skeny dle plánu	0 kritických; pravidla pro high/medium dle kap. 3	Závěrečná zpráva z testů
AI kvalita	Věrnost vůči zdrojům (grounding) u RAG	Golden set + manuální/automatické skórování	min. 90 % odpovědí s prokazatelnou oporou ve zdrojích	Eval report + ukázky
AI kvalita	Bezpečnostní chování modelu	Testy prompt-injection / jailbreak / data-exfiltration scénáře	0 kritických selhání; max. 1 % minor odchylek	Report z AI bezpečnostních testů
Compliance	Ochrana PII	Kontrola výstupů a logů + testovací scénáře	Žádné neautorizované úniky PII; logy bez citlivých dat	Protokol kontroly + ukázky

2.3 Forma provádění akceptačního testování

Akceptační testování je prováděno kombinací následujících forem testování. Jednotlivé formy testování se vzájemně doplňují a společně zajišťují komplexní ověření dodaného softwarového řešení.

2.3.1 Uživatelské akceptační testování

Uživatelské akceptační testování je zaměřeno na ověření softwarového řešení z pohledu koncového uživatele. Testování je prováděno oprávněnými uživateli nebo zástupci Objednatele na základě předem definovaných scénářů odpovídajících reálnému používání systému.

Cílem uživatelského akceptačního testování je ověřit, že:

- systém podporuje očekávané pracovní postupy,
- funkce jsou srozumitelné a použitelné v praxi,
- chování systému odpovídá očekávání cílových uživatelů.

2.3.2 Testování dle uživatelských scénářů (User Stories)

Testování dle uživatelských scénářů vychází z uživatelských příběhů a akceptačních kritérií definovaných v technických specifikacích modulů (Přílohy č. 1 až č. 3 Smlouvy). Každá user story je ověřována z hlediska naplnění jejího zamýšleného cíle a očekávaného chování systému.

Testování je zaměřeno zejména na:

- ověření akceptačních podmínek user stories,
- správnou návaznost jednotlivých kroků scénáře,
- konzistentní chování systému napříč souvisejícími user stories.

Výsledky tohoto testování slouží jako podklad pro vyhodnocení splnění funkčních požadavků.

2.3.3 Automatizované testování

Automatizované testování je využíváno k ověření opakovatelných a technicky měřitelných aspektů softwarového řešení. Automatizované testy mohou být spouštěny samostatně nebo jako součást testovacího procesu.

Automatizované testování je zaměřeno zejména na:

- ověření klíčových funkčních toků,
- regresní testování po provedených úpravách,
- základní ověření stability řešení.

Výsledky automatizovaných testů jsou zaznamenávány a vyhodnocovány jako součást akceptačního procesu.

2.3.4 Bezpečnostní testování

Bezpečnostní testování je zaměřeno na ověření, že softwarové řešení splňuje definované bezpečnostní požadavky a je odolné vůči běžným bezpečnostním hrozbám. Rozsah bezpečnostního testování vychází z bezpečnostních požadavků a standardů definovaných v Přílohách č. 1 až č. 6 Smlouvy.

V rámci bezpečnostního testování je ověřováno zejména:

- řízení přístupů a oprávnění,
- ochrana dat a citlivých informací,

- odolnost vůči neoprávněnému přístupu a zneužití.

2.3.5 Systémové testování

Systémové testování je zaměřeno na ověření softwarového řešení jako celku v cílovém nebo dohodnutém prostředí Koncového zákazníka Objednatele (prostředí bude upřesněno Objednatelem. Testování ověřuje správnou spolupráci jednotlivých částí systému a jeho chování v běžných provozních scénářích.

Systémové testování zahrnuje zejména:

- ověření integrace jednotlivých komponent,
- chování systému při standardním provozu,
- základní ověření stability a dostupnosti.

2.3.6 Kombinace a návaznost testování

Jednotlivé formy testování mohou probíhat paralelně nebo postupně v závislosti na charakteru testovaného řešení. Výsledky všech forem testování jsou společně vyhodnoceny a tvoří podklad pro rozhodnutí o výsledku akceptačního testování.

2.3.7 AI-specifické testování (LLM/RAG)

AI-specifické testování doplňuje standardní formy testování o ověření typických rizik a vlastností řešení využívajícího modely umělé inteligence. Testování se provádí nad referenční sadou (golden set) a nad bezpečnostními testovacími scénáři.

V rámci AI-specifického testování se ověřuje zejména:

- reprodukovatelnost a stabilita výstupů při stejné konfiguraci (model version, prompt šablony, kontext),
- věrnost odpovědí vůči poskytnutým zdrojům (grounding) a schopnost uvést oporu ve zdrojích, pokud je to relevantní,
- správné odmítnutí odpovědi nebo bezpečné chování v situacích, kdy požadavek nelze splnit (např. chybí data, nevhodný dotaz),
- odolnost vůči prompt-injection, jailbreak, manipulativním vstupům a pokusům o exfiltraci dat,
- správné zacházení s citlivými informacemi (PII) ve vstupech, výstupech a v logování.

2.3.8 Výkonnostní a zátěžové testování

Výkonnostní a zátěžové testování ověřuje nefunkční parametry systému včetně chování při běžném i špičkovém zatížení. Součástí je měření latence, propustnosti, chybovosti a spotřeby prostředků včetně vyhodnocení percentilů (p95/p99), pokud je to relevantní.

Rozsah zátěže, délka testu, testované scénáře a akceptační prahy jsou stanoveny dle kapitoly 2.2.1 a dle technických specifikací Díla (Přílohy č. 1 až č. 6 Smlouvy).

Akceptační ověření propustnosti musí být provedeno jako scénářové zátěžové testování odpovídající očekávanému reálnému využití softwarového řešení. Scénář zátěže musí být předem schválen oběma stranami a musí obsahovat minimálně:

1. cílový počet souběžných uživatelů nebo paralelních klientů,
2. profil zátěže v čase (náběh, špička, ustálený stav) a délku trvání testu,
3. mix operací (např. podíl AI dotazů/RAG dotazů vůči standardním transakčním voláním),
4. datové předpoklady a reprezentativnost testovaných vstupů, a
5. způsob vyhodnocení metrik p95/p99 latence, chybovosti a propustnosti vůči akceptačním prahům dle kapitoly 2.2.1. Akceptačního plánu. Hodnota propustnosti uvedená v tabulce SLI/SLO představuje minimální akceptační baseline; v případě, že je ve smluvní nebo technické dokumentaci definován konkrétní očekávaný objem (např. špičkové zatížení, integrační dávky), má tento objem přednost a scénář zátěže musí tuto skutečnost reflektovat.

2.4 Evidence a vyhodnocování výsledků

Každý provedený test je vyhodnocen z hlediska splnění očekávaného výsledku. V případě zjištění odchylky je tato skutečnost zaznamenána včetně:

- popisu zjištěného stavu,
- identifikace dotčené části řešení,
- posouzení dopadu na akceptaci.

Evidence výsledků testování slouží jako podklad pro závěrečné vyhodnocení akceptačního testování.

Součástí evidence výsledků testování musí být rovněž identifikace testované verze dodávky (release/build), konfigurace prostředí a u AI komponent také model version a použitá konfigurace promptů/šablon. Bez těchto údajů nelze považovat výsledky testování za opakovatelné. Mezi tyto údaje patří:

- akceptační protokoly a checklisty (UAT, user stories, systémové testy),
- exporty metrik (latence, chybovost, dostupnost) a reporty ze zátěžových testů,
- logy a auditní záznamy související s testovanými scénáři (v rozsahu nezbytném pro dokazatelnost),
- závěrečné zprávy z bezpečnostních testů a vyhodnocení nálezů,
- AI eval report, je-li relevantní (výsledky golden setu, vyhodnocení bezpečnostních scénářů, ukázky výstupů).

2.5 Opakování testování

V případě, že jsou během akceptačního testování zjištěny vady, které brání úspěšné akceptaci softwarového řešení, je po jejich odstranění provedeno opakované testování v rozsahu odpovídajícím provedeným úpravám.

Cílem opakovaného testování je ověřit, že:

- zjištěné vady byly odstraněny,
- nedošlo k negativnímu ovlivnění ostatních částí řešení.

2.6 Ukončení akceptačního testování

Akceptační testování je ukončeno vyhodnocením celkových výsledků testování a jejich formálním zaznamenáním do Akceptačního protokolu. Výsledek akceptačního testování je stanoven podle pravidel tohoto akceptačního plánu; další podmínky akceptace upravuje čl. 3. Smlouvy.

Výsledkem akceptačního testování může být „akceptováno“, „akceptováno s výhradou“ nebo „neakceptováno“.

3. Řízení neshod a odchylek

Veškeré neshody a odchylky (tj. vady) zjištěné během akceptačního testování jsou evidovány. Každá neshoda je klasifikována podle závažnosti a dopadu na akceptaci řešení v souladu s pravidly definovanými v bodě 3.1 Akceptačního plánu a v Přílohách č.1 až č.6 Smlouvy. Postup řešení neshod a odchylek zjištěných v průběhu realizace plnění se řídí tímto Akceptačním plánem a změnovým řízením dle bodu 3.6 tohoto Akceptačního plánu.

V případě, že výsledky akceptačního testování vedou k výsledku „akceptováno s výhradou“ nebo „neakceptováno“, jsou zjištěné vady a odchylky popsány v akceptačním protokolu, a to včetně jejich dopadu, klasifikace a návrhu termínu jejich odstranění. Po odstranění vad je dodavatel oprávněn opětovně vyzvat k zahájení akceptačního testování.

3.1 Klasifikace závažnosti neshod

Pro účely akceptace se neshody klasifikují minimálně do níže uvedených úrovní. Pokud jsou v tomto Akceptačním plánu, v technických specifikacích modulů nebo v jiné části smluvní dokumentace definována přísnější pravidla, použije se přísnější požadavek.

Severity	Definice	Příklady	Dopad na akceptaci
S0 – Kritická	Zásadní porušení bezpečnosti, zákonných požadavků nebo nedostupnost klíčové funkce; vysoké riziko dopadu.	Únik citlivých dat, obejití autorizace, nefunkční kritická user story, nekontrolovaný přístup k administraci.	Automaticky vede k výsledku „neakceptováno“.
S1 – Vysoká	Významná funkční nebo nefunkční vada s dopadem na použití; existuje workaround jen omezeně.	Nestabilita, časté chyby při běžném toku, výkon pod prahy, chybná integrace.	Zpravidla vede k „neakceptováno“, pokud není výslovně schválena výjimka dle kap. 3.6. Akceptačního plánu
S2 – Střední	Vada bez zásadního dopadu na hlavní tok;	Dílčí odchylka UI, nekritický okrajový	Může být tolerováno dočasně, pokud je

	dostupný workaround; neohrožuje bezpečnost.	scénář, drobný výkonový problém v minor toku.	dohodnut termín odstranění a nedochází ke kumulaci rizik.
S3 – Nízká	Kosmetická nebo dokumentační vada bez dopadu na funkčnost a bezpečnost.	Typografie, textové popisy, drobné UX detaily.	Nemá vliv na výsledek akceptace; eviduje se k odstranění.

3.2 Pravidla pro výsledek akceptace

Výsledek akceptace je stanoven na základě splnění testovacích scénářů a na základě stavu otevřených neshod. Pokud je v jiné části smluvní dokumentace stanoven přísnější požadavek, použije se tento přísnější požadavek.

Pro účely tohoto plánu platí následující rozhodovací pravidla:

Výsledek „akceptováno bez výhrad“ je možný pouze tehdy, pokud nejsou evidovány žádné otevřené neshody S0 nebo S1 a současně nejsou evidovány otevřené neshody S2. Výjimka je přípustná pouze tehdy, pokud byla výslovně schválena Objednatelem dle kapitoly 3.6 Akceptačního plánu, je řádně odůvodněna a nemá dopad na bezpečnost, legislativní soulad ani kritické uživatelské scénáře.

Výsledek „akceptováno s výhradou“ je možný tehdy, pokud nejsou evidovány žádné otevřené neshody S0 nebo S1, všechny kritické scénáře jsou splněny, případné otevřené neshody S2 nebrání bezpečnému a provozně použitému užívání softwarového řešení, jsou přesně popsány v Akceptačním protokolu a je pro ně stanoven závazný způsob a termín vypořádání. Neshody S3 samy o sobě nebrání akceptaci Díla, pokud jejich souhrn nemá kumulativní dopad na bezpečnost, legislativní soulad, provozní použitelnost ani na kritické uživatelské scénáře; všechny neshody S3 však musí být evidovány a musí být pro ně stanoven způsob a termín vypořádání.

Výsledek „neakceptováno“ nastává v případě jakékoliv neshody S0, typicky také při existenci neodstraněných neshod S1 nebo při nesplnění akceptačních kritérií dle kapitoly 2.2.1. Akceptačního plánu nebo nesplnění kteréhokoliv kritického scénáře.

Kritické scénáře definované v testovací sadě (zejména scénáře pokrývající klíčové uživatelské toky a podstatné funkce všech modulů uvedené v Přílohách č. 1 až č. 6 Smlouvy) musí být splněny na 100 %. Nesplnění kteréhokoliv kritického scénáře automaticky vede k výsledku akceptace „neakceptováno“, a to bez ohledu na celkovou procentuální úspěšnost ostatních scénářů.

3.3 Stop podmínky a pozastavení akceptačního testování

Akceptační testování může být dočasně pozastaveno, pokud není možné zajistit objektivní provedení testů. Pozastavení je zaznamenáno v testovacím protokolu.

Typické stop podmínky zahrnují zejména:

- nestabilitu testovacího prostředí nebo nedostupnost klíčových závislostí (integrace, identity, síťové služby),
- výskyt kritické bezpečnostní vady (S0) nebo incidentu, který vyžaduje okamžitá opatření,
- zásadní změnu konfigurace nebo verze dodávky bez schváleného postupu dle kapitoly 3. 6. Akceptačního plánu (porušení baseline),
- nedostupnost testovacích dat nebo zjištění, že použitá data nesplňují pravidla ochrany informací.

3.4 Lhůty pro vyhodnocení neshod a komunikaci

Pro plynulý průběh akceptace se stanovují minimální lhůty pro triáž, návrh řešení a informování stran. Konkrétní lhůty lze dohodnout jinak v akceptačním protokolu.

Stanovené minimální lhůty jsou:

- triáž a přiřazení severity: do 2 pracovních dnů od nahlášení,
- návrh postupu řešení (fix / workaround / zamítnutí): do 3 pracovních dnů od triáže,
- poskytnutí opravy pro S0/S1: do 5 pracovních dnů od schválení řešení (nebo dle dohody),
- informování Objednatele o stavu řešení neshody: nejméně 1x za 2 dny, nebo při změně stavu.

3.5 Regresní testování po opravách

Po odstranění neshod Dodavatelem se provede opakované testování v rozsahu odpovídajícím provedeným změnám, včetně nezbytné regrese. Pokud změna zasahuje AI komponenty (model version, prompt šablony, retrieval logika), provede se znovu minimálně relevantní část AI-specifické evaluace (golden set a bezpečnostní scénáře).

3.6 Řízení změn

Zjistí-li se v průběhu akceptace potřeba změny testovaného softwarového řešení, testovacích scénářů, prostředí nebo termín plnění, posoudí se nejprve, zda jde o odstranění vady / issue, nebo o změnový požadavek (Request for Change).

Za issue se považuje odstranění vady, doplnění chybějícího artefaktu, korekce testovacího scénáře nebo jiné opatření, které nemění věcný rozsah požadavků na softwarové řešení; issue řeší Dodavatel bez změny akceptačních kritérií, pokud Objednatel nerozhodne jinak.

- Za Request for Change se považuje změna funkčního rozsahu, akceptačních kritérií, integračních předpokladů, datových vstupů, termín plnění nebo jiných parametrů, které mohou ovlivnit výsledek akceptace; RFC musí být před promítnutím do akceptace písemně schválen odpovědnými zástupci smluvních stran.
- Každá schválená změna musí být zaznamenána minimálně včetně popisu důvodu, dopadu na rozsah a termín plnění, , odpovědnosti za provedení a rozhodnutí, zda je nutné opakovat dotčené testy nebo regresi.

4. Výstupy akceptačního procesu

Výstupy akceptačního procesu slouží jako podklad pro rozhodnutí o přijetí nebo nepřijetí dodávaného softwarového řešení. Mezi hlavní výstupy patří zejména:

- záznam o průběhu akceptačního testování,
- přehled provedených testů a jejich výsledků,
- seznam zjištěných neshod a jejich stav,
- akceptační protokol.

Zásadním výstupem akceptačního procesu je Akceptační protokol podepsaný oprávněnými zástupci smluvních stran. Akceptační protokol obsahuje výsledek akceptačního řízení, kterým je zejména:

- akceptováno bez výhrad, nebo
- akceptováno s výhradou, včetně přesného popisu otevřených neshod, jejich dopadu, způsobu vypořádání a závazného termínu odstranění, nebo
- neakceptováno, včetně odůvodnění a popisu zjištěných neshod.

5. Ukončení akceptace

Akceptační proces je považován za ukončený vyhotovením Akceptačního protokolu s výsledkem „akceptováno“, „akceptováno s výhradou“ nebo „neakceptováno“ podle pravidel tohoto Akceptačního plánu a Smlouvy. V případě výsledku „akceptováno s výhradou“ se další postup řídí podmínkami uvedenými v Akceptačním protokolu a ve Smlouvě, zejména pokud jde o odstranění otevřených neshod, termíny jejich vypořádání a případné platební dopady (zejména Zádržné, smluvní pokuty). V případě výsledku „neakceptováno“ pokračuje akceptační proces odstraněním vad a následným opakováním akceptačního testování dle kapitoly 2.5. Akceptačního plánu.

V případě úspěšné akceptace (tj. v případě podpisu Akceptačního protokolu s výsledkem „akceptováno“ Objednatelem/v případě podpisu Zápisu stvrzujícího odstranění všech neshod vytknutých v rámci Akceptačního protokolu s výsledkem „akceptováno s výhradou“ Objednatelem) je softwarové řešení považováno za připravené k přechodu do další fáze životního cyklu, zejména k nasazení do produkčního prostředí.

6. Změny a výjimky v akceptačním procesu

Jakékoli změny v akceptačním procesu nebo výjimky z tohoto Akceptačního plánu musí být schváleny Smluvními stranami. Změny mohou zahrnovat úpravy rozsahu akceptace, termínu plnění nebo postupu testování.

Všechny schválené změny a výjimky jsou řádně zdokumentovány a uchovávány jako součást dodávané dokumentace. Tyto změny nesmí ohrozit dosažení cílů akceptačního procesu ani kvalitu výsledného dodávaného softwarového řešení.

Tento Akceptační plán nesmí být vykládán v rozporu se Smlouvou. Výsledek akceptace se primárně stanoví podle pravidel tohoto Akceptačního plánu; pokud však Smlouva nebo její přílohy stanoví přísnější nebo speciální požadavek, použije se tento přísnější nebo speciální požadavek.

7. Přílohy a šablony pro akceptační řízení

Následující šablony a matice slouží k jednotné evidenci a dokazatelnosti akceptačního řízení. Lze je převzít jako přílohy Akceptačního protokolu nebo jako samostatné dokumenty.

7.1 Matice RACI pro akceptační řízení

Matice RACI definuje role a odpovědnosti. R = Responsible (vykonává), A = Accountable (schvaluje/odpovídá), C = Consulted (konzultuje), I = Informed (informován).

Aktivita	Dodavatel	Objednatel	Bezpečnost/Compliance
Příprava testovacího prostředí a nasazení release/build	R	C	I
Zajištění testovacích dat a pravidel práce s daty	C	R/A	C
Vytvoření a schválení testovacích scénářů	R	A	C
Provedení UAT a user stories testů	C	R/A	I
Provedení automatizovaných a regresních testů	R	C	I
Provedení bezpečnostních testů a vyhodnocení nálezů	R	C	A
AI-specifická evaluace (golden set, safety scénáře)	R	C	C
Triage a klasifikace neshod (severity)	R	A	C
Opravy neshod a dodání fixu	R/A	I	I
Závěrečné rozhodnutí o výsledku akceptace a podpis protokolu	C	A	C

7.2 Šablona Akceptačního protokolu (minimální obsah)

Akceptační protokol musí minimálně obsahovat následující informace:

- Identifikace dodávky: název řešení, release/build ID, datum nasazení do testovacího prostředí.
- Identifikace prostředí: popis, konfigurace, integrační závislosti, případné omezení oproti produkci.
- AI komponenty: model version, konfigurace promptů/šablon, retrieval konfigurace (pokud je relevantní).
- Rozsah akceptace: seznam provedených testů (UAT, user stories, automatizované, bezpečnostní, systémové, AI-specifické).
- Souhrn výsledků: počet PASS/FAIL, splnění SLO/SLI dle kap. 2.2.1, přehled výkonových a bezpečnostních výsledků.
- Seznam neshod: ID, popis, severity, stav, odkaz na evidenci, kategorizace, rozhodnutí o dopadu na akceptaci.

- Výsledek akceptace: akceptováno bez výhrad / akceptováno s výhradou / neakceptováno + odůvodnění.
- Přílohy: reporty z testů, exporty metrik, bezpečnostní zprávy, AI eval report, readiness checklist.
- Podpisy oprávněných zástupců smluvních stran, datum a místo.

7.3 Šablona AI evaluačního reportu (je-li relevantní)

Pokud softwarové řešení obsahuje AI komponenty a v rámci akceptace se provádí AI specifické testování dle kapitoly 2.3.7 Akceptačního plánu, doloží Dodavatel AI evaluační report jako nutný požadavek na akceptaci Díla. Minimální doporučený obsah:

- Popis eval metodiky: golden set, způsob skórování, role hodnotitelů, verze nástrojů.
- Popis testovaných scénářů: typy dotazů, pokrytí funkcí, hraniční případy.
- Výsledky: agregované metriky, pass rate, identifikované failure-modes.
- Bezpečnostní scénáře: prompt-injection, jailbreak, exfiltrace, bezpečné odmítnutí.
- Ochrana dat: kontrola PII v odpovědích a logech, redakce, přístupová pravidla.
- Doporučení: mitigace, návrhy úprav promptů/retrievalu, potřeba doškolení uživatelů.

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	62F108C68FE24141F194FD1DD35F439180C17BC0858C6ECC46C7DBB6C6566C2A
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

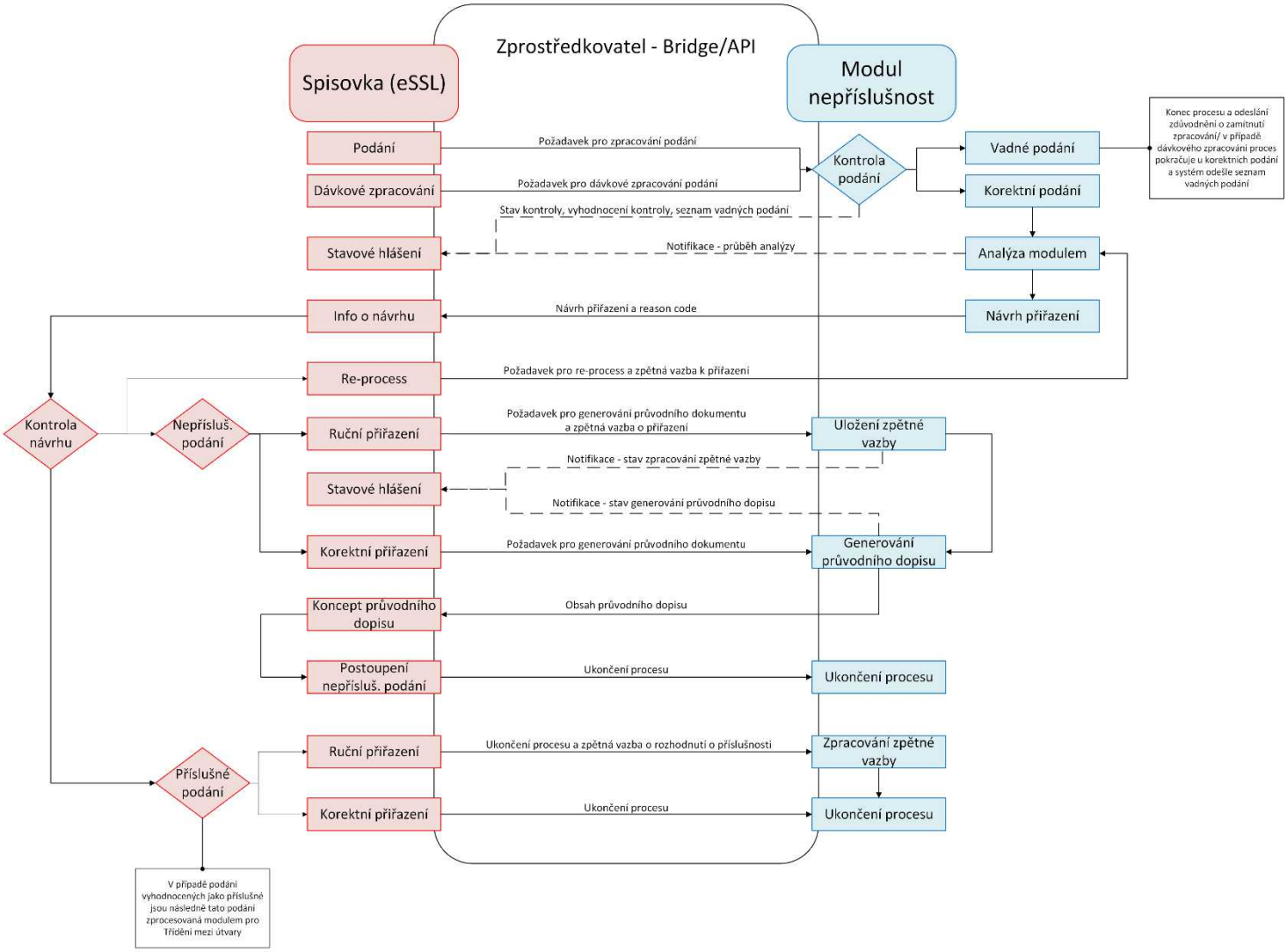
Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 12 – Diagram Nepříslušnost



Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	48CC5FC9BFB2E582B9E895D932049B086FBC4F7C72397E239C1D5E8DAA8C4000
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

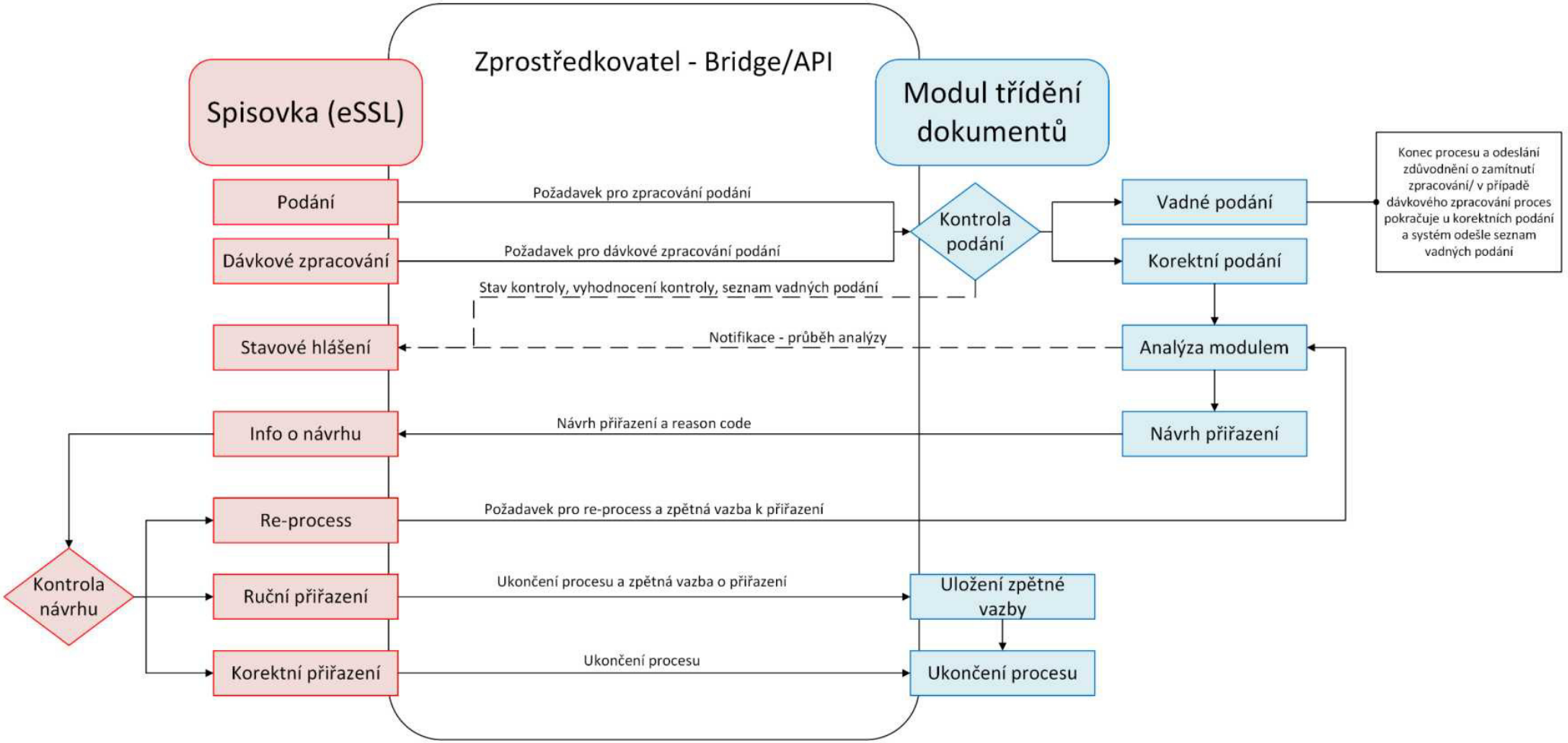
Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 13 – Diagram Třídění dokumentů mezi útvary



Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	9DA8A2748E8DF4FD437CAD3426F88917642BE6ED5EF498C6A5347C89A2D47EF8
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

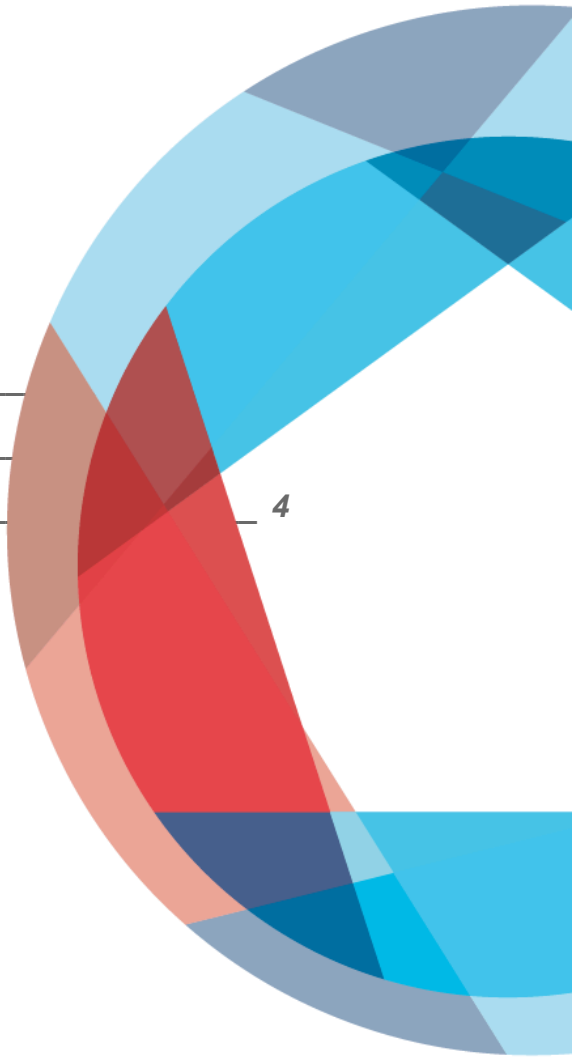
Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č.14 – Technické specifikace implementace

Obsah



Národní agentura pro komunikační a informační technologie, s. p.

A: Kodaňská 1441/46
101 00 Praha 10 - Vršovice

T: +420 234 066 500
E: info@nakit.cz

W: www.nakit.cz

1. Přesnost, spolehlivost systému

1.1. Dodavatel garantuje, že poptávané nástroje byly navrženy a vyvinuty podle zásad bezpečného vývoje již od návrhu (doporučení NÚKIB, OWASP a podobné). S ohledem na určený účel musí dosahovat odpovídající úrovně přesnosti, spolehlivosti a kybernetické bezpečnosti a měly by v těchto ohledech fungovat konzistentně po celou dobu své životnosti.

1.2. Dodavatel musí zajistit, aby byly poptávané nástroje co nejodolnější, pokud jde o chyby, poruchy nebo nesrovnalosti, které se mohou vyskytnout v daném nástroji nebo v prostředí, ve kterém tento nástroj funguje, zejména v důsledku jejich interakce s fyzickými osobami nebo jinými systémy. Poptávané nástroje musí být odolné proti pokusům neoprávněných třetích stran změnit jejich použití, chování, výstupy nebo výkonnost zneužitím zranitelných míst těchto systémů. Technická řešení umožňující řešení zranitelných míst specifických pro poptávané nástroje mohou zahrnovat tam, kde je to vhodné, opatření pro prevenci a detekci útoků, které se pokoušejí manipulovat se soubory trénovacích dat (tzv. data poisoning) nebo před trénovanými součástmi používanými v tréninku (tzv. model poisoning) a reakci, řešení a kontrolu těchto útoků, vstupů, jejichž cílem je přimět daný model k tomu, aby udělal chybu (tzv. matoucí vzory nebo vyhýbání se modelu), útoků na důvěrnost nebo chyb v modelech, které mohou vést ke škodlivým rozhodnutím.

1.3. Úroveň přesnosti a příslušné metriky popis spolehlivosti a kybernetické bezpečnosti dodavatel podrobně popíše v bezpečnostní dokumentaci.

2. Povinnosti dodavatele

Dodavatel se při poskytování plnění zavazuje plnit následující povinnosti:

2.1. jmenovat nejpozději do tří pracovních dnů po dni účinnosti Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této přílohy a související komunikace mezi smluvními stranami (dále také jen „Kontaktní osoba pro bezpečnost na straně Dodavatele“). Kontaktní osobu pro bezpečnost na straně Dodavatele sdělí písemně Objednateli v téže lhůtě;

2.2. zajistit, aby Kontaktní osoba pro bezpečnost na straně Dodavatele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění této Smlouvy za stranu Dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito bezpečnostními požadavky a bezpečnostní dokumentací správce systému poskytnutou v rámci VZ;

2.3. Informace uvedené v článku 2.1 a 2.2 budou uvedené v bezpečnostní dokumentaci. V případě změn provede Dodavatel změnu v bezpečnostní dokumentaci a tu neprodleně poskytne Objednateli;

2.4. v průběhu implementace poptávaných nástrojů zajistit rozhraní pro napojení na dohledová centra Objednatele a součinnost při zvládání kybernetických bezpečnostních událostí a incidentů;
2.5. dodavatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení. Tyto informace budou uvedené v bezpečnostní dokumentaci;
2.6. poptávané nástroje uplatňují principy minimálních oprávnění a řízeného egressu;
2.7. veškerá odchozí komunikace mimo prostředí objednatele je ve výchozím stavu zakázána a povoluje se pouze na základě řízeného seznamu povolených destinací.

3. Kryptografická ochrana

Za účelem ochrany aktiv Objednatele musí být implementována kryptografická ochrana již v cyklu vývoje poptávaných nástrojů tak, aby byly zabezpečeny minimálně následující oblasti:

a) AES-256 pro šifrování dat v klidu;
b) TLS 1.3 + mTLS pro šifrování dat při přenosu;
c) Ochrana modelů pomocí model encryption (secure enclaves, homomorfní šifrování) ;
d) Řízení přístupu založeném na kryptografii (certifikáty, HSM, klíče).
e) Pomocí vhodných kryptografických nástrojů zajistit ochranu trénovacích dat, ochranu modelů proti krádeži (model extraction), model promptů, ochranu inferenčních API.

3.1. Podrobný popis použitých kryptografických nástrojů bude uveden v bezpečnostní dokumentaci.

4. Bezpečnostní dokumentace

4.1. Bezpečnostní dokumentace obsahuje v závislosti na dotyčném poptávaném nástroji (tj. pro každý poptávaný nástroj zvlášť) alespoň tyto informace:
a) povahu údajů, které systém pravděpodobně zpracovává nebo má zpracovávat, a v případě osobních údajů kategorie fyzických osob a skupin, kterých se to pravděpodobně týká nebo má týkat;
b) jak může poptávaný nástroj interagovat s hardwarem nebo softwarem, který není součástí samotného poptávaného nástroje, nebo jak může, tam, kde je to relevantní, být za účelem interakce s nimi použit;
c) popis hardwaru, na kterém má poptávaný nástroj pracovat.
4.2. Dodavatel je povinen tuto dokumentaci aktualizovat při každé podstatné změně během doby trvání smlouvy a následně ji zpřístupnit objednateli.
4.3. Bezpečnostní dokumentace musí být vypracována v češtině.
4.4. Objednatel má právo pořizovat kopie bezpečnostní dokumentace a v rozsahu nezbytném pro vnitřní potřebu v rámci organizace objednatele.

4.5. Dodavatel uvede seznam souborů dat použitých pro trénování (je-li to relevantní), validaci a testování nástrojů. Zvlášť uvede soubory dat objednatele a soubory dat dodavatele a třetích stran. V případě souborů dat objednatele bude uveden popis, k jakým účelům může dodavatel soubory dat použít (kromě plnění smlouvy) a zda je Dodavatel povinen soubor dat na konci doby trvání smlouvy zničit. V případě souborů dat Dodavatele a souborů dat třetích stran bude popsáno, které soubory dat může objednatel použít, a zda je dodavatel povinen soubory dat předat.

4.6. Podrobný popis prvků poptávaného nástroje a procesu jeho vývoje zahrnující:

a) specifikace návrhu systému, zejména obecnou logiku poptávaných nástrojů a algoritmů;

b) hlavní možnosti volby návrhu, včetně odůvodnění a učiněných předpokladů, také ve vztahu k osobám nebo skupinám osob, ohledně kterých má být systém používán;

c) popis architektury systému vysvětlující, jak na sebe komponenty softwaru vzájemně navazují nebo jsou do sebe začleněny a integrovány do celkového zpracování;

d) použité postupy ověřování a testování, včetně informací o použitých ověřovacích a testovacích údajích a jejich hlavních charakteristikách; ukazatele použité k měření přesnosti, spolehlivosti, kybernetické bezpečnosti a dodržení jiných příslušných požadavků stanovených v tomto dokumentu, jakož i potenciálně diskriminační dopady; testovací protokoly a všechny zprávy o testování, datované a podepsané odpovědnými osobami;

e) požadované informace uvedené v článku 2-4.

5. Seznam použitých zkratek

Zkratka	Popis
TLS	Protokol Transport Layer Security (TLS) je kryptografický protokol poskytující možnost zabezpečené komunikace přes nedůvěryhodnou síť (datová linka, internet). Je využíván pro služby WWW, elektronickou poštu a další datové přenosy
AES	Advanced Encryption Standard (AES, česky standard pokročilého šifrování) je standardizovaný algoritmus používaný k šifrování dat v informatice. Jedná se o symetrickou blokovou šifru šifrující i dešifrující stejným klíčem data rozdělená do bloků pevně dané délky.
HSM	Hardwarový bezpečnostní modul (HSM) chrání nejdůležitější kryptografické operace organizace. Izoluje a chrání šifrovací klíče, čímž snižuje riziko vnitřních hrozeb a externích kybernetických útoků.

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OWASP	Open Worldwide Application Security Project (nezisková nadace, která se věnuje zlepšování zabezpečení softwaru)
API	zkratkou API(Application Programming Interface) se označuje rozhraní pro aplikace. Jedná se o rozhraní, kterým mohou komunikovat dvě aplikace mezi sebou a vyměňovat si tak data.

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	C8C07E556CB20EE6F9A35C7D89EDDE26F4B79B67D0F960150DF038D7BF45348B
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby

Příloha č. 15 – Vzor Akceptačního Protokolu

Objednatel	Česká republika – Ministerstvo vnitra
Poskytovatel	Národní agentura pro komunikační a informační technologie, s. p.
Smlouva	*Číslo platné Smlouvy*
Datum předání	*Datum*
Akceptační protokol č.	*Číslo*

Název Projektu	*„Digitalizace správy dokumentů a využívání umělé inteligence v Ministerstvu vnitra“*
Registrační číslo Projektu	*CZ.31.3.0/0.0/0.0/25_165/0011697*

Popis	
Popis předmětu akceptace	

Objednatel a Poskytovatel svým podpisem stvrzují předání a akceptaci Plnění dle výše specifikované Smlouvy.

V Praze dne ……

Společnost	Jméno	Podpis
Akceptoval za Objednatele		
Předal za Poskytovatele		

Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.

Změnou datového formátu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.
Nepodařilo se získat informace o podpisu.

Typ vstupního dokumentu:	.PDF
Otisk vstupního souboru:	A4716CE911778AE71913B57E746B0B9130BB0D3F58C1703AA913C6D8FF9E627D
Použitý algoritmus:	SHA256_SBB 2.16.840.1.101.3.4.2.1

Subjekt, který změnu formátu dokumentu provedl:
Ministerstvo vnitra, Nad Štolou 3, 17034 Praha 7

Datum vyhotovení ověřovací doložky:
1.6.2026

Jméno a příjmení osoby, která změnu formátu dokumentu provedla:
Horáčková Jana

Elektronická pečeť - 1.6.2026
Certifikát :
Jméno : MVCR - pečeť spisové služby