Smlouva č. CTU/ 2024_0057
uzavřená ve smyslu ustanovení § 1746 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „OZ“)

Smluvní strany:

1. **Česká republika – Český telekomunikační úřad**
   se sídlem: Sokolovská 219/58, Praha 9
   adresa pro doručování pošt. přihrádka 02, 225 02 Praha 025
   jejímž jménem jedná: Ing. Marek Ebert, předseda Rady ČTÚ
   ID datové schránky: a9qaats
   bankovní spojení: Česká národní banka, pobočka Praha
   Číslo účtu: 725001/0710
   IČO: 701 06 975
   DIČ: CZ70106975 (osoba identifikovaná k dani)

   (dále jen „Objednatel“) na straně jedné

   a

2. **Seyfor, a.s.**
   se sídlem: Drobného 555/49, Ponava, 602 00 Brno
   zastoupena: Petrem Francem, MBA, MSc., členem představenstva
   ID datové schránky: 46mti92
   bankovní spojení: Raiffeisenbank a.s.
   číslo účtu: 6253399002/5500
   IČO: 015 72 377
   DIČ: CZ01572377
   zapsaná v Obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 7072

   (dále jen „Poskytovatel“) na straně druhé,

uzavírají tuto smlouvu o zajištění servisní podpory a rozvoje IS MOSS/SKS (dále jen „smlouva“).

Článek I.
Účel a předmět smlouvy

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě bude prováděna činnost servisní podpory a rozvoje (dále jen „servisní podpora“) informačního systému Modulární správní systém/Společný katalog subjektů (dále jen „IS MOSS/SKS“ nebo „podporovaný systém“), to vše v návaznosti na výsledek zadávacího řízení v rámci nadlimitní veřejné zakázky na služby s názvem „Zajištění servisní podpory a rozvoj IS MOSS/SKS“ (dále jen „zadávací řízení“).
2. Předmětem této smlouvy je na straně jedné závazek poskytovatele poskytovat objednateli služby servisní podpory IS MOSS/SKS (včetně podpory MS SharePoint a BI/DWH) po dobu 60 měsíců ode dne převzetí podporovaných systémů, to vše v rozsahu a za podmínek stanovených touto smlouvou, a na straně druhé závazek objednatele za řádně a včas poskytnuté služby uhradit poskytovateli sjednanou cenu.

3. Poskytovatel se zavazuje převzít zajištění servisní podpory IS MOSS/SKS a provozu MS SharePoint a BI/DWH včetně provádění provozních úprav ode dne nabytí účinnosti této smlouvy.

Článek II.
Specifikace plnění smlouvy

Poskytovatel se zavazuje za podmínek stanovených v této smlouvě poskytovat objednateli servisní podporu v tomto rozsahu a v rozsahu Přílohy č. 1 (Specifikace předmětu plnění) této smlouvy:

1. Zajištění provozu a údržby:
   a) podporovaných systémů dle dohodnutých SLA parametrů, sledování parametrů provozu produkčního prostředí využitím dohledových nástrojů a včasné informování o případných incidentech, monitoring systémových a aplikačních logů, monitoring a údržba databáze a její optimalizace v součinnosti s objednatelem,
   b) operačního systému na aplikačním serveru včetně provádění aktualizace IS MOSS/SKS a dalších servisních úkonů, které jsou nezbytné pro bezproblémový provoz podporovaných systémů,

   Pro aplikaci MS SharePoint se SLA parametry a provádění záručních a pozáručních oprav nevztahují na vady softwaru, jejichž odstranění vyžaduje součinnost se společností Microsoft.
2. Odstraňování záručních a pozáručních vad podporovaných systémů s garancí dohodnutých SLA parametrů. SLA parametry se nevztahují na vady programového vybavení třetích stran, které není součástí dodávky poskytovatele.
3. Provoz a údržba webového portálu zákaznické podpory (HelpDesk) – správa a konfigurace jednotného místa pro evidenci všech vad a požadavků objednatele.
4. Telefonická a e-mailová podpora (Hot-Line).
5. Uživatelská podpora na úrovni L1, L2 a L3.
6. Provádění provozních úprav a případný rozvoj podporovaných systémů, včetně analytických a implementačních prací.
7. Poskytování konzultací a školení uživatelů podporovaných systémů – zaměstnanců objednatele na základě objednávek.
8. Plnění podle odstavců 6 a 7 tohoto článku je garantováno v celkovém rozsahu 1.750 člověkodnů/5 roků (člověkodnem je myšleno poskytnutí služeb jednou osobou v rozsahu 8 hodin).

Základní pojmy stanovené pro účely této smlouvy jsou uvedeny v Příloze č. 2 (Vymezení pojmů) této smlouvy.

Článek III.
Místo plnění

1. Místem plnění je sídlo objednatele.
2. Služby budou poskytovány vzdáleně nebo v sídle objednatele dle povahy poskytovaného plnění.

Článek IV.
Způsob plnění dle čl. II odst. 1 až 5 smlouvy

1. Popis poskytovaných služeb dle čl. II odst. 1 až 5 této smlouvy je uveden v Příloze č. 1 této smlouvy.

2. Hlášení vad zjištěných při provozu podporovaných systémů je objednatel povinen provádět:
   a) pomocí webového portálu zákaznické podpory poskytovatele (HelpDesk), který je umístěn na webové adrese [redacted]. Přístup na webový portál zákaznické podpory (HelpDesk) bude nastaven všem uživatelům podporovaných systémů, případně dalším uživatelům podle požadavků objednatele;
   b) v případě, že nebude možné z technických důvodů nahlásit vady přes webový portál zákaznické podpory (HelpDesk), je jako další komunikační kanál stanovena e-mailová adresa: [redacted].
   c) v případech nedostupnosti komunikačních kanálů uvedených v písmenech a) a b) tohoto odstavce, je hlášení vady prováděno telefonicky na telefonní číslo poskytovatele: [redacted] (Hot-Line).
3. SLA lhůty začínají plynout od okamžiku ohlášení vady prostřednictvím webového portálu zákaznické podpory (HelpDesk), v případě jeho nedostupnosti pak od okamžiku ohlášení vady prostřednictvím stanovené e-mailové adresy, eventuálně prostřednictvím stanoveného telefonního čísla (Hot-Line). V takovém případě objednatel neodpovídá za následné zanesení ohlášené vady do webového portálu zákaznické podpory (HelpDesk).
4. Do SLA lhůty na odstranění vady se nezapočítává čas potřebný na zajištění součinnosti objednatele, případně třetích stran, ani čas na odstranění chyb v datech primárních zdrojů.
5. V případě, že je vada ohlášena mimo pracovní dobu, uvedené lhůty na zahájení prací na odstranění vady začnou běžet od 8:00 hodin následujícího pracovního dne.
6. Zajištění provozu podporovaných systémů se nevztahuje na vady způsobené:
   a) konfigurací zařízení objednatele, která je v rozporu s požadavky uvedenými v dokumentaci k dílu platné k aktuální verzi podporovaných systémů na provozním prostředí objednatele,
   b) zavirováním nezaviněným poskytovatelem,
   c) užíváním díla v rozporu s pokyny uvedenými v dokumentaci k dílu platné k aktuální verzi podporovaných systémů na provozním prostředí objednatele a/nebo v souvislosti s ustanoveními této smlouvy,
   d) komponentami podporovaných systémů, které nejsou v odpovědnosti poskytovatele,
   e) chybou dat primárních zdrojů, pokud se nejedná o chyby, které jsou předmětem vstupní kontroly dat.
7. Poskytovatel garantuje objednateli poskytnutí potřebné součinnosti při odstraňování vad způsobených okolnostmi uvedenými v odstavci 6 tohoto článku, a to na základě zvláštní objednávky.
8. V případě vady identifikuje kategorii závažnosti (A, B, C) zásadně Garant modulu dle svého odhadu. Poskytovatel buď tuto kategorii potvrdí, nebo provede překvalifikaci tak, aby kategorie odpovídala zařazení dle Přílohy č. 1 (Specifikace předmětu plnění) této smlouvy. V případě nesouhlasu uživatele s překvalifikací rozhodne osoba oprávněná jednat za objednatele ve věcech smluvních.
9. V případě, kdy nebude možno opakovatelným postupem nebo doloženou dokumentací docílit navození vady, může poskytovatel tuto vadu odložit a vrátit Garantovi modulu a k jejímu řešení se vrátit znovu až v okamžiku, kdy bude možno vadu spolehlivě navodit. Toto se netýká vad kategorie „A“.
10. Garant modulu je povinen nejpozději do 5 pracovních dnů od převedení vady do stavu „Vyřešeno“ (15 pracovních dnů v případě „Čeká na reakci“) sdělit své stanovisko souhlasu

či nesouhlasu s řešením poskytovateli prostřednictvím webového portálu zákaznické podpory (HelpDesk) nebo v případě jeho nedostupnosti e-mailovou zprávou. V případě, že Garant toto stanovisko v dané lhůtě nesdělí, bude požadavek uzavřen a automaticky považován za vyřešený.

Článek V.
Způsob plnění dle čl. II odst. 6 smlouvy

1. Popis poskytovaných služeb dle čl. II odst. 6 této smlouvy je uveden v Příloze č. 1 (Specifikace předmětu plnění) této smlouvy. Provozní úpravy a rozvoj podporovaných systémů budou probíhat dle dohodnutých SLA parametrů (viz bod 5 přílohy č. 1 této smlouvy).
2. Požadavky na provozní úpravy podporovaných systémů (včetně požadavků na úpravy vyvolané změnami legislativy) zadává objednatel výhradně prostřednictvím webového portálu zákaznické podpory (HelpDesk). Na základě zaevidovaného požadavku poskytovatel provede odhad pracnosti. Změnový/rozvojový požadavek je poskytovatelem zpracován do změnového listu, jehož vzor je přílohou č. 6 (Změnový list) této smlouvy. Smluvní strany mohou o specifikaci změnového požadavku objednatele dále jednat a poskytovatel je povinen obsah výsledku jednání reflektovat ve změnovém listu.
3. O realizaci požadavků na provozní úpravy rozhoduje objednatel v souladu se svými vnitřními předpisy. Požadavky na změnu budou v případě souhlasu objednatele následně realizovány poskytovatelem na základě objednávky vystavené objednatelem. Objednávka bude obsahovat termín nasazení realizace plnění na testovací prostředí IS MOSS/SKS.
4. Akceptace realizovaných požadavků na provozní úpravy bude potvrzena podpisem zástupce objednatele i poskytovatele na Předávacím protokolu.

Článek VI.
Termín a doba plnění

1. Poskytování plnění v podobě servisní podpory a údržby IS MOSS/SKS dle čl. IV této smlouvy po dobu 60 měsíců zahájí poskytovatel (tzn. převezme podporované systémy) nejpozději do 20 pracovních dnů ode dne účinnosti této smlouvy.
2. Poskytovatel se zavazuje poskytovat plnění v podobě rozvoje IS MOSS/SKS dle čl. V této smlouvy po dobu účinnosti této smlouvy řádně nejpozději do termínů stanovených v objednatelem podepsaných změnových listech.

Článek VII.
Předání, převzetí, implementace a testování

1. Plnění dle čl. IV a čl. V této smlouvy bude poskytovatel objednateli poskytovat v termínech ve smyslu čl. VI této smlouvy.
2. Poskytovatel se zavazuje nejméně 2 pracovní dny předem písemně uvědomit kontaktní osoby objednatele uvedené v čl. XV, resp. příloze č. 5 této smlouvy o předpokládaném termínu předání, instalace či implementace plnění nebo jeho části.
3. Poskytovatel se zavazuje předat objednateli k testování plnění dle čl. V této smlouvy včetně testovacích scénářů pro účely testování poté, kdy bylo testování provedeno stranou poskytovatele. Proces testování probíhá stejně i v případě plnění, kdy objednatel nepožaduje vytvoření testovacích scénářů.
4. Výsledkem testování pro plnění dle této smlouvy, zaznamenaném v protokolu o testování, mohou být následující závěry:
   a) „Schváleno“ (tj. při testování nebyly shledány vady či nedostatky bránící převzetí (užití) plnění); a to buď „bez výhrad“ (tj. při testování nebyly shledány žádné vady

či nedostatky), anebo „s výhradou“ (tj. při testování byly shledány vady či nedostatky nebránící převzetí (užití) plnění); objednatel všechny vady a nedostatky specifikuje, projedná s poskytovatelem a stanoví způsob a termín jejich odstranění.

b) „Neschváleno – vráceno“ (tj. při testování byly shledány vady či nedostatky bránící převzetí (užití) plnění); objednatel prostřednictvím HelpDesku všechny vady a nedostatky specifikuje, projedná s poskytovatelem a stanoví způsob a termín jejich odstranění; odstranění zjištěných vad a nedostatků bude ověřeno opětovným testováním a výsledek bude zaznamenán formou dodatku k protokolu o testování.

5. Ukončení testovacího provozu pro plnění dle této smlouvy schválením bez výhrad, anebo schválením s výhradou v objednatelem podepsaném protokolu o testování, je předpokladem implementace plnění na produkční prostředí objednatele.

6. V rámci akceptačního řízení objednatel posuzuje, zda plnění nevykazuje vady v rámci běžného provozu, nebo zda je detailní analýza v souladu s požadavky objednatele, či zda je dokumentace skutečného provedení a provozní dokumentace včetně aktualizace uživatelských příruček v odpovídající kvalitě. Výsledkem akceptačního řízení může být:

a) „Akceptováno“ (tj. při kontrole kvality nebyly shledány vady či nedostatky bránící převzetí (užití) plnění), a to buď „bez výhrad“ (tj. při kontrole kvality nebyly shledány žádné vady či nedostatky), anebo „s výhradou“ (tj. při kontrole kvality byly shledány vady či nedostatky, které samy o sobě nebo ve spojení s jinými nebrání převzetí (užití) plnění); objednatel všechny vady a nedostatky specifikuje, projedná s poskytovatelem a stanoví způsob a termín jejich odstranění; termín k odstranění vad a nedostatků nemá vliv na povinnost poskytovatele dodat řádné plnění nejpozději do termínů ve smyslu čl. VI této smlouvy; odstranění zjištěných vad a nedostatků bude v akceptačním řízení dále ověřeno a výsledek bude zaznamenán formou dodatku k akceptačnímu protokolu.

b) „Neakceptováno“ (tj. při kontrole kvality byly shledány vady či nedostatky bránící převzetí (užití) plnění); objednatel všechny vady a nedostatky specifikuje, projedná s poskytovatelem a stanoví způsob a termín jejich odstranění; termín k odstranění vad a nedostatků nemá vliv na povinnost poskytovatele dodat řádné plnění nejpozději do termínů ve smyslu čl. VI této smlouvy; odstranění zjištěných vad a nedostatků bude v akceptačním řízení dále ověřeno a výsledek bude zaznamenán formou dodatku k akceptačnímu protokolu.

7. Plnění musí být akceptováno nejpozději 15 pracovních dnů ode dne implementace na produkční prostředí, nebude-li dohodnuto jinak. Akceptační řízení je ukončeno podpisem akceptačního protokolu oprávněnými osobami obou smluvních stran, nebyly-li v rámci akceptačního řízení shledány vady, jinak podpisem dodatku k akceptačnímu protokolu, z nějž bude vyplývat, že vady zjištěné v rámci akceptačního řízení byly odstraněny.

8. Vady plnění zjištěné po akceptaci předmětu plnění musí objednatel uplatnit u poskytovatele bez zbytečného odkladu po jejich zjištění a poskytovatel je povinen je odstranit neprodleně.

9. Plnění nebo jeho části budou předány poskytovatelem objednateli v elektronické podobě. Jeho součástí budou výstupy potřebné pro další rozvoj a údržbu IS MOSS/SKS.

Článek VIII.
Práva a povinnosti smluvních stran

1. Smluvní strany jsou povinny se navzájem informovat o veškerých skutečnostech důležitých pro plnění této smlouvy včetně změn kontaktních osob.

2. Objednatel se v rámci zajištění provozu IS MOSS/SKS zavazuje zajistit nezbytnou součinnost poskytovateli a rovněž poskytovateli/provozovateli systémů spolupracujících nebo předávajících si data s IS MOSS/SKS.

3. Objednatel souhlasí, aby hovory v rámci služby Hot-Line mohly být za účelem zkvalitnění služeb zachyceny na záznamové medium. O této skutečnosti je zástupce poskytovatele povinen včas poučit volajícího uživatele objednatele. V případě zájmu objednatele poskytovatel objednateli poskytne nahrávky na základě žádosti objednatele.

4. Poskytovatel se v rámci plnění předmětu této smlouvy zavazuje:

   a) poskytnout objednateli, popřípadě jím určené třetí osobě, nejpozději do 10 pracovních dnů ode dne doručení výzvy, nebude-li stanoveno jinak, nezbytnou technickou součinnost při převádění činností podle této smlouvy či jejich příslušné části na objednatele nebo jím určenou třetí osobu tak, aby objednateli nevznikla škoda; technická součinnost zahrnuje i případnou pomoc týkající se zdrojového kódu a dokumentace; poskytovatel se zavazuje tuto součinnost poskytovat s odbornou péčí, zodpovědně a v přiměřené lhůtě, stanovené objednatelem ve výzvě; maximální rozsah součinnosti je stanoven na 400 člh (cena za 1 člh bude shodná s cenou za 1 člh dle čl. X odst. 3 této smlouvy),

   b) informovat objednatele o plánovaných úpravách a změnách IS MOSS/SKS (např. aktualizace SW pro provoz IS MOSS/SKS či jiných souvisejících informačních systémů), jejichž povaha může mít vliv na bezpečnost a stabilitu systému, či integritu dat, např. provedení významných aktualizací dílčích komponent IS MOSS/SKS, a to elektronicky e-mailem zaslaným minimálně 2 pracovní dny předem; kontaktními osobami pro tato hlášení jsou všechny kontaktní osoby na straně objednatele podle čl. XV, resp. přílohy č. 5 této smlouvy,

   c) informovat objednatele o významné změně ovládání poskytovatele ve smyslu § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (např. případy, kdy dojde k významné změně kontroly nad poskytovatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení či ekvivalentní postavení) nebo změně vlastnictví zásadních aktiv, popř. změně oprávnění nakládat s těmito aktivy, využívanými poskytovatelem k plnění dle této smlouvy,

   d) po celou dobu trvání této smlouvy zajistit:

      - plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak předpisů pracovněprávních, předpisů v oblasti zaměstnanosti, a dále oblasti bezpečnosti a ochrany zdraví při práci, a to vůči všem osobám, které se budou podílet na plnění této smlouvy,

      - dodržování zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů,

      - řádné a včasné plnění finančních závazků vůči svým případným poddodavatelům.

      Plnění uvedených povinností zajistí poskytovatel i u svých případných poddodavatelů,

   e) zajistit, aby se na plnění předmětu smlouvy podíleli pouze členové realizačního týmu, jejichž seznam předložil poskytovatel ve své nabídce v rámci zadávacího řízení, a kteří mají dostatečné odborné předpoklady (odpovídající požadavkům v rámci zadávacího řízení). V případě potřeby změny člena realizačního týmu lze tuto provést toliko s písemným souhlasem objednatele, přičemž objednatel tento souhlas neudělí v případě, že by po takové změně realizační tým kumulativně nesplňoval požadavky objednatele na realizační tým poskytovatele dle požadavků v rámci zadávacího řízení.

5. Poskytovatel negarantuje zajištění plnění podle této smlouvy v případě, že v průběhu trvání této smlouvy bude IS MOSS/SKS bez vědomí a souhlasu poskytovatele upravován či rozvíjen objednatelem nebo jím pověřenou třetí osobou.

6. Poskytovatel se zavazuje informovat objednatele o svém úmyslu, příp. úmyslu případného svého poddodavatele, zahájit (resp. změnit rozsah či povahu) podnikání v elektronických komunikacích ve smyslu § 8 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, potažmo v poštovních službách ve smyslu § 17 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, či poskytovat služby přeshraničního dodávání balíků ve smyslu článku 2 Nařízení Evropského parlamentu a rady (EU) 2018/644 o službách přeshraničního dodávání balíků. Objednatel v takovém případě posoudí (ve smyslu § 79 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů), zda tento úmysl neznamená protichůdné zájmy, které by mohly negativně ovlivnit plnění veřejné zakázky). V případě porušení tohoto závazku uhradí poskytovatel objednateli smluvní pokutu ve výši 500.000 Kč.

Článek IX.
Práva k duševnímu vlastnictví

1. Vytvoří-li poskytovatel pro objednatele v rámci plnění povinností dle této smlouvy autorské dílo, jako konečný výsledek jeho činnosti podle této smlouvy, ve smyslu zákona 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“), (tj. např. grafické komponenty, databáze, počítačové programy), postupuje objednateli okamžikem jeho vytvoření právo výkonu veškerých majetkových autorských práv k tomuto autorskému dílu. Právo objednatele k výkonu majetkových práv k autorským dílům zahrnuje veškeré možné způsoby užívání díla, zejména rozmnožování, distribuci, pronájem, půjčování, vystavování, sdělování veřejnosti a třetím osobám a další způsoby. Poskytovatel prohlašuje, že k postoupení má souhlasy autorů díla. Smluvní strany předpokládají vytvoření autorského díla především v rámci rozvoje IS MOSS/SKS; autorské dílo může být vytvořeno také v rámci poskytování provozní údržby IS MOSS/SKS.

2. V rozsahu, ve kterém nemohou být majetková autorská práva k dílu převedena objednateli v souladu s odstavcem 1 tohoto článku smlouvy, poskytovatel poskytuje okamžikem úhrady ceny plnění objednateli územně a časově neomezenou, výhradní a neodvolatelnou licenci v neomezeném množstevním rozsahu, a to ke všem způsobům užití díla. Objednatel má právo zcela nebo zčásti poskytnout oprávnění tvořící součást licence třetí osobě (podlicence). Objednatel je oprávněn vykonávat všechna práva k dílu, včetně, bez omezení, práva upravit, zpracovat či jinak změnit dílo, či jej spojit s jiným dílem nebo jej zařadit do díla souborného (to vše i prostřednictvím třetí osoby), jakožto i právo uvádět dílo na veřejnost pod svým jménem. Objednatel není povinen licenci využít, přičemž nevyužíváním licence nemohou být nijak dotčeny jeho oprávněné zájmy.

3. Pro případ, že by se na straně poskytovatele jednalo o vytvoření zaměstnaneckého díla ve smyslu § 58 autorského zákona, prohlašuje poskytovatel, že je v plném rozsahu oprávněn individuálními autory vykonávat veškerá majetková autorská práva k dílu včetně oprávnění dílo postoupit na objednatele i třetí strany, resp. že je oprávněn udělit objednateli všechna práva v rozsahu předvídaném v tomto článku smlouvy.

4. Objednatel má vždy také právo autorská díla upravovat, zpracovávat, spojovat s jinými díly, zařazovat do souborného díla, dokončovat, lokalizovat díla nebo překládat díla do jiného jazyka atd.

5. Objednatel je oprávněn vykonávat veškerá majetková autorská práva výlučně svým jménem a na svůj účet.

6. Strany prohlašují, že veškerá zvláštní práva ke všem databázím vytvořeným při plnění smlouvy náležejí objednateli jako pořizovateli databáze. Pokud by objednatel nebyl pořizovatelem jakékoliv databáze vytvořené při plnění této smlouvy, poskytovatel postupuje objednateli veškerá práva pořizovatele databáze k takové databázi okamžikem jejich vzniku.

7. Součástí plnění této smlouvy mohou být také autorská díla jiných osob (výrobců), případně poskytovatele (nebo jeho poddodavatelů) vytvořená před uzavřením této smlouvy nikoliv přímo pro objednatele, která jsou potřebná pro naplnění účelu této smlouvy a u kterých poskytovatel nemůže objednateli poskytnout oprávnění dle odstavců 1 nebo 2 tohoto článku smlouvy, nebo to po něm nelze spravedlivě požadovat (dále jen „proprietární software“). Objednatel nabude k proprietárnímu software nevýhradní oprávnění užít jej způsobem potřebným pro účely a cíle této smlouvy nejméně po dobu trvání této smlouvy a po jejím skončení až do uplynutí 10 kalendářních let po roku, ve kterém skončila účinnost této smlouvy, na území České republiky; další podmínky užití proprietárního software se budou řídit příslušnými licenčními podmínkami.

8. V případě autorského díla jako konečného výsledku činnosti poskytovatele dle této smlouvy, ke kterému nabývá objednatel práva dle odstavců 1 a/nebo 2 tohoto článku smlouvy, se poskytovatel zavazuje předat objednateli 1x za kalendářní pololetí veškerou a úplnou dokumentaci ke zdrojovým kódům (v editovatelném formátu) použité a/nebo vzniklé při plnění povinností dle této smlouvy, nebyly-li již objednateli předány v souladu s čl. VII odst. 8 této smlouvy. Dále se poskytovatel zavazuje předávat objednateli 1x za kalendářní měsíc výkaz práce, obsahující evidenci všech provedených úkonů, které byly na základě této smlouvy za uplynulý kalendářní měsíc provedeny.

9. V případě, že poskytovatel použije při plnění závazků podle této smlouvy jakékoliv open source, free, otevřené, svobodné, veřejné či jiné neproprietární materiály (dále jen „open source“), je povinen zajistit, aby dílo nebylo podřízeno omezujícím open source licenčním podmínkám. Dále se poskytovatel zavazuje zajistit, aby v důsledku použití open source materiálů nebyly porušeny licenční podmínky třetích stran. V případě, že poskytovatel povinnosti podle tohoto odstavce nedodrží, je povinen objednatele chránit a plně odškodnit proti všem nárokům třetích stran.

10. Práva a povinnosti podle tohoto článku zůstávají skončením tohoto smluvního vztahu nedotčena.

11. Objednatel prohlašuje, že disponuje úplnými zdrojovými kódy a instalačními soubory vytvořených systémů včetně struktury databáze systémů. Zdrojové kódy budou poskytnuty poskytovateli po podpisu smlouvy. Veškeré úpravy a rozvoj podporovaných systémů budou implementovány do současného řešení.

Článek X.
Cena a platební podmínky

1. Maximální cena za celkový rozsah plnění podle této smlouvy činí 29.350.000 Kč bez DPH, z toho DPH ve výši 21 % činí 6.163.500 Kč, tj. cena včetně DPH činí 35.513.500 Kč.

2. Z ceny podle odstavce 1 tohoto článku smlouvy činí cena za poskytování služeb v rozsahu uvedeném v čl. II odst. 1 až 5 této smlouvy za 60 měsíců 12.900.000 Kč bez DPH, z toho DPH ve výši 21 % činí 2.709.000 Kč, tj. cena včetně DPH činí 15.609.000 Kč. Cena za 1 měsíc tak činí 215.000 Kč bez DPH.

3. Z ceny podle odstavce 1 tohoto článku smlouvy činí cena za rozvoj IS MOSS/SKS dle požadavků objednatele po dobu účinnosti smlouvy podle čl. II odst. 6 a 7 v rozsahu čl. II odst. 8 této smlouvy (v max. rozsahu 1.750 člověkodnů) 16.450.000 Kč bez DPH, z toho DPH ve výši 21 % činí 3.454.500 Kč, tj. cena včetně DPH činí 19.904.500 Kč. Cena za 1 člh tak činí 1.175 Kč bez DPH.

4. Celková cena za plnění dle odstavce 2 tohoto článku smlouvy je stanovena jako konečná, pevná a nepřekročitelná, přičemž zahrnuje veškeré náklady poskytovatele spojené s předmětem plnění a lze ji měnit pouze při změně sazby DPH. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni uskutečnění zdanitelného plnění, je-li poskytovatel plátcem DPH.

5. Celková cena za plnění dle odstavce 3 tohoto článku smlouvy je stanovena jako maximální a nepřekročitelná, přičemž zahrnuje veškeré náklady poskytovatele spojené s předmětem plnění a lze ji měnit při změně sazby DPH. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni uskutečnění zdanitelného plnění, je-li poskytovatel plátcem DPH. Skutečně uhrazená cena za plnění podle čl. V této smlouvy však může být s ohledem na odstavec 8 tohoto článku smlouvy nižší než celková cena za toto plnění specifikovaná odstavce 3 tohoto článku smlouvy.

6. Podkladem pro úhradu cen za plnění podle odstavců 2 a 3 tohoto článku smlouvy bude daňový doklad – faktura (dále jen „faktura“), která musí obsahovat veškeré náležitosti účetního dokladu předepsané příslušnými právními předpisy (zejména § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 OZ) a číslo této smlouvy. Poskytovatel je oprávněn vystavit fakturu až na základě objednatelem podepsaného výkazu práce servisní podpory (pro cenu za plnění dle odstavce 2 tohoto článku), potažmo na základě podepsaného akceptačního protokolu (pro cenu za plnění dle odstavce 3 tohoto článku). Kopie výkazu práce servisní podpory anebo akceptačního protokolu bude tvořit přílohu faktury. Faktury budou vystavovány zvlášť v případě paušálních plateb (dle odstavce 2 tohoto článku) a zvlášť v případě plateb za plnění rozvojových požadavků (dle odstavce 3 tohoto článku).

7. Cena za poskytování služeb podpory dle odstavce 2 tohoto článku smlouvy bude hrazena měsíčně v částce 215.000 Kč bez DPH, a to na základě daňových dokladů – faktur (dále jen „faktura“) vystavených poskytovatelem k poslednímu dni každého měsíce, ve kterém byly služby podpory poskytnuty. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni zdanitelného plnění.

8. Cena za plnění podle odstavce 3 tohoto článku smlouvy bude hrazena vždy na základě dílčí objednávky po akceptaci plnění v souladu s čl. V této smlouvy.

9. Splatnost faktur je sjednána na 30 dnů od jejího doručení objednateli. V případě faktury doručené objednateli mezi 15. prosincem a 10. lednem je taková faktura splatná nejdříve následujícího 1. února. V případě, že bude faktura objednateli doručena v době rozpočtového provizoria, je splatná do 15 dnů ode dne přidělení finančních prostředků do rozpočtu objednatele.

10. Platební povinnosti objednatele plynoucí z této smlouvy jsou splněny dnem odepsání příslušné částky ve prospěch účtu poskytovatele. Úhrada bude provedena bezhotovostním převodem z účtu objednatele ve prospěch účtu poskytovatele. Platební povinnosti objednatele plynoucí z této smlouvy jsou splněny dnem odepsání částky z účtu objednatele ve prospěch účtu poskytovatele.

11. V případě, že faktura nebude obsahovat některou z předepsaných náležitostí či bude obsahovat chyby v psaní či počtech, je objednatel oprávněn vrátit takovou fakturu poskytovateli k doplnění či opravě. Lhůta splatnosti se v takovém případě přerušuje a počíná znovu běžet od vystavení opravené či doplněné faktury

12. Objednatel je oprávněn fakturu poskytovateli vrátit bez zbytečného odkladu po zjištění, že obsahuje údaje nesprávné, nebo chybí-li některá ze zákonem či touto smlouvou požadovaných náležitostí, a to před uplynutím doby splatnosti, aniž by došlo k prodlení s jeho úhradou. Nová doba splatnosti počíná běžet ode dne vystavení bezvadné faktury.

13. V případě, že průměrný roční index spotřebitelských cen dle údajů Českého statistického úřadu, publikovaných na jeho internetových stránkách, uvedený ke kalendářnímu měsíci odpovídajícímu měsíci, v němž byla smlouva podepsána, vzroste o více než 3 %, zvýší

se neuhrazená část smluvní ceny dle odstavce 1 tohoto článku smlouvy o výši tohoto indexu, a to nejdříve od druhého roku trvání smlouvy. Taková změna smlouvy bude formálně zachycena formou dodatku smlouvy dle čl. XVIII odst. 7 této smlouvy.

Článek XI.
Vyšší moc a okolnosti vylučující odpovědnost

1. Smluvní strany nebudou odpovědné za částečné nebo úplné neplnění smluvních závazků následkem okolností vylučujících odpovědnost v případech tzv. vyšší moci.
2. Výraz vyšší moc znamená a zahrnuje zejména: přírodní katastrofu, požár, záplavy, zemětřesení a dále povstání, stávky, pracovní boje jakéhokoliv druhu nebo terorismus, které mají přímou souvislost a brání plnění povinností ze smlouvy a plnění povinností nelze zajistit jinak nebo je nahradit, nehody, pád letadla včetně nehod, kterým se nedalo vyhnout v souvislosti s plněním této smlouvy včetně přijetí zákona nebo mimořádného rozhodnutí přísl. úřadu v souvislosti se zásahem vyšší moci, pokud příčiny a události mají vliv na plnění povinností stran ze smlouvy a plnění povinností vyplývajících ze smlouvy nelze zajistit jinak.
3. Vyskytne-li se působení překážky, s níž jsou spojeny účinky vylučující odpovědnost, lhůty ke splnění smluvních závazků se prodlouží o dobu trvání takové překážky. Smluvní strana, která je postižena takovou překážkou, je však povinna okamžitě, písemně, uvědomit druhou smluvní stranu o této skutečnosti, o začátku trvání této překážky a předpokládané době jejího trvání.

Článek XII.
Salvátorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

Článek XIII.
Povinnost mlčenlivosti, důvěrnost informací a ochrana osobních údajů

1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:
   a) si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „důvěrné informace“),
   b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé strany nebo i jejím opomenutím přístup k důvěrným informacím druhé strany.
2. Objednatel a poskytovatel se zavazují, že obchodní, technické, jakož i netechnické informace, které mají nebo by mohly mít potenciální hodnotu, a které jim byly svěřeny smluvním partnerem, nezpřístupní třetím osobám bez předchozího písemného souhlasu druhé smluvní strany a nepoužijí tyto informace ani pro jiné účely než pro plnění svých závazků podle podmínek této smlouvy. Za důvěrnou informaci se pokládá vždy taková informace, která je takto kteroukoliv smluvní stranou kdykoliv označena. To však neplatí v případě, že by se stala tato informace, k níž se zavazují k povinnosti mlčenlivosti či k povinnosti zachovat důvěrnost informace, podle tohoto ustanovení smlouvy, obecně známou či dostupnou. To se nevztahuje na výstupy z plnění podle této smlouvy.
3. Poskytovatel se výslovně zavazuje, že informace získané v souvislosti s plněním předmětu smlouvy nezneužije a ani nevyužije k jinému účelu než výlučně k plnění této smlouvy.

4. Poskytovatel se zavazuje, že neposkytne bez souhlasu objednatele žádné informace třetím stranám ohledně plnění této smlouvy, včetně informací o konfiguraci IS MOSS/SKS, které mohl poskytovatel zjistit při implementaci a konfiguraci, nebo jiných prvků, které nejsou součástí plnění této smlouvy. Zároveň se poskytovatel zavazuje, že bude uchovávat citlivé informace ohledně plnění této smlouvy, jako jsou logy, konfigurace a topologie jen po nezbytně nutnou dobu, potřebnou pro řádné a efektivní plnění této smlouvy. Veškeré takové informace je také poskytovatel povinen chránit proti odcizení, či zneužití.

5. Poskytovatel bere na vědomí, že plnění této smlouvy bude spojeno se zpracováním osobních údajů, jak je definováno v zákoně č. 110/2019 Sb., o zpracování osobních údajů a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Ve vztahu ke zpracování osobních údajů se poskytovatel uzavírá s objednatelem smlouvu o zpracování osobních údajů, jež je přílohou č. 8 (Smlouva o zpracování osobních údajů) této smlouvy.

6. Poskytovatel se zavazuje, že všechny povinnosti stanovené mu v tomto článku nebo v souvislosti s ním ve stejné podobě uplatní vůči svým zaměstnancům, resp. tyto povinnosti přenese v rámci svých smluvních vztahů na případné poddodavatele.

Článek XIV.
Kybernetická bezpečnost

1. Ve vztahu k předmětu plnění smluvní strany prohlašují, že plnění smlouvy bude probíhat na aktivech představujících soubor technických a programových prostředků, u nichž je objednatel při jejich ochraně nucen zohlednit příslušné bezpečnostní požadavky v souladu s aktuálně platnými obecně závaznými právními předpisy, zejména zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti – dále jen „VoKB“) a dalšími závaznými akty vydanými ze strany orgánů veřejné moci (Národního úřadu pro kybernetickou a informační bezpečnost či jiného správního orgánu). Smluvní strany dále konstatují, že IS MOSS/SKS je identifikován jako významný informační systém v souladu s VoKB.

2. Poskytovatel se zavazuje poskytnout objednateli veškerou součinnost nezbytnou k tomu, aby objednatel řádně naplňoval právní povinnosti stanovené mu ZoKB a VoKB.

3. Zjistí-li poskytovatel při plnění smlouvy rozpor postupů objednatele s některým z ustanovení ZoKB nebo VoKB, je povinen takový rozpor objednateli neprodleně ohlásit, navrhnout objednateli příslušně správný způsob postupu řešení a poskytnout objednateli potřebnou součinnost k jeho zajištění.

4. Smluvní strany v průběhu plnění smlouvy spolu vzájemně komunikují za účelem dosažení požadované úrovně bezpečnosti. V případě ohrožení anebo porušení kybernetické bezpečnosti, zejména v případě výskytu kybernetické bezpečnostní události anebo incidentu, jsou smluvní strany povinny ihned po zjištění takových skutečností hlásit jejich výskyt druhé smluvní straně a společně podnikat potřebné kroky k zajištění obnovení požadované úrovně bezpečnosti.

5. V případě potřeby poskytne poskytovatel dle požadavků objednatele potřebnou součinnost pro účely testování plánů kontinuity činností a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

6. Po uzavření smlouvy objednatel protokolárně oznámí poskytovateli osoby zastávající bezpečnostní role dle § 6 VoKB a jejich kontaktní údaje – jméno, příjmení, telefonní číslo a adresa elektronické pošty, včetně způsobu komunikace s těmito osobami.

7. Poskytovatel bere na vědomí, že objednatel může průběžně, zpravidla ve spolupráci s třetí stranou, provádět testování IS MOSS/SKS za účelem zjištění jeho bezpečnostních zranitelností. Zjištěná bezpečnostní zranitelnost popsaná pomocí údajů z databáze CVE (Common Vulnerabilities and Exposures; dostupná z [redacted]) se považuje za vadu, kterou je poskytovatel povinen za podmínek této smlouvy odstranit. Závažnost takové vady (dále jen „severita“) bude ohodnocena dle standardu CVSS (Common Vulnerability Scoring System; dostupný z [redacted]). Odstraněním vady dle tohoto odstavce se rozumí zejména provedení aktualizace příslušného programového vybavení nebo implementace bezpečnostního opatření, které zamezí možnosti zneužití zjištěné zranitelnosti, případně, nelze-li zneužití zjištěné zranitelnosti zcela zamezit, sníží pravděpodobnost zneužití zjištěné zranitelnosti na akceptovatelnou úroveň.

8. Na odstraňování vad podle odstavce 7 tohoto článku smlouvy se vztahují ujednání uvedená v příloze č. 1 (Specifikace plnění servisní podpory IS MOSS/SKS) této smlouvy. Lhůty pro odstranění takovýchto vad počínají běžet doložitelným oznámením těchto vad poskytovateli. Pokud je však pro odstranění takové vady nezbytná aktualizace proprietárního softwaru, který je nedílnou součástí IS MOSS/SKS, vydaná výrobcem tohoto proprietárního softwaru, přičemž tento výrobce není totožný s osobou poskytovatele ani není osobou ovládanou poskytovatelem, počínají tyto lhůty pro odstranění vad běžet nejdříve okamžikem vydání takové aktualizace. Poskytovatel je v takovém případě povinen ve lhůtě pro zahájení prací na odstranění vady zaslat tomuto výrobci písemný požadavek na vydání takové aktualizace a tento úkon ve stejné lhůtě písemně doložit objednateli. Prodlení poskytovatele se splněním jeho povinnosti dle věty předchozí se považuje za prodlení se zahájením prací na odstranění dotčené vady.

9. Podrobná specifikace plnění požadavků v oblasti kybernetické bezpečnosti je uvedena v příloze č. 9 (Specifikace plnění požadavků v oblasti kybernetické bezpečnosti) této smlouvy.

Článek XV.
Kontaktní (oprávněné) osoby a komunikace

1. Veškerá komunikace mezi smluvními stranami ve věcech této smlouvy bude probíhat prostřednictvím kontaktních (oprávněných) osob, uvedených v příloze č. 5 (Kontaktní (oprávněné) osoby) této smlouvy.

2. Kontaktní osoby ve věcech technických projednávají a zajišťují záležitosti související s technickým zabezpečením poskytovaného plnění, kontaktní osoby ve věcech smluvních projednávají a dohlížejí na provádění plnění podle této smlouvy, zejména předávají a přijímají informace, podklady, jakož i výsledky plnění, podepisují akceptační protokoly, apod. Kontaktní osoby ve věcech odborných specifikují změnové požadavky objednatele, odpovídají za správnost zapracování změnového požadavku do změnového listu, spolupracují při analýze požadavku a návrhu řešení od poskytovatele, jsou odpovědné za testování plnění a udělení pokynu k vystavení akceptačního protokolu.

3. Kontaktní osoby nejsou oprávněny ke změnám této smlouvy a k jejím doplňkům, ani k jejich zrušení, ledaže se prokáží plnou mocí (pověřením) udělenou jim k tomu statutárním orgánem příslušné smluvní strany.

4. Komunikace mezi objednatelem a poskytovatelem související se zajišťováním provozní údržby MOSS/SKS bude po celou dobu trvání této smlouvy probíhat primárně prostřednictvím poskytovatelem zajišťovaného HelpDesk. Poskytovatel se zavazuje zprovoznit HelpDesk do 20 pracovních dnů od účinnosti této smlouvy.

5. Jako další sekundární komunikační kanál bude poskytovatelem zajištěn Hot-Line.

6. Veškeré dokumenty mající vztah k plnění této smlouvy musí být podepsány alespoň jednou kontaktní osobou k tomu příslušnou za smluvní stranu podle dané oblasti a odbornosti (příp. jeho zástupcem), která úkon činí.

7. Změnu své kontaktní osoby, resp. jejích kontaktních údajů, je daná smluvní strana povinna písemně oznámit nejpozději do 3 dnů ode dne změny. V těchto případech nemusí být změna prováděna postupem podle čl. XVIII odst. 7 této smlouvy.

Článek XVI.
Ukončení smlouvy

1. Tato smlouva může být ukončena splněním, písemnou dohodou obou smluvních stran, odstoupením od smlouvy nebo výpovědí ze strany objednatele.
2. Smluvní strany jsou oprávněny od této smlouvy odstoupit v případech stanovených občanským zákoníkem či touto smlouvou.
3. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným nebo neodstranitelným způsobem své povinnosti vyplývající z této smlouvy.
4. Za podstatné porušení smluvních povinností objednatelem se podle této smlouvy považuje prodlení objednatele s uhrazením ceny plnění o více než 30 dnů.
5. Za podstatné porušení smlouvy poskytovatelem se považuje:
   a) nedodržení povinnosti mlčenlivosti či zachování důvěrných informací,
   b) neplnění povinností spojených s poskytováním provozní údržby IS MOSS/SKS podle čl. IV této smlouvy po dobu delší než 1 kalendářní měsíc,
   c) neodstranění vad ve sjednané lhůtě, a to ani v dodatečně stanovené lhůtě 10 pracovních dnů,
   d) dodatečně zjištěný fakt, že údaje uvedené poskytovatelem v rámci předchozího zadávacího řízení nebyly pravdivé.
6. Stanoví-li oprávněná smluvní strana druhé smluvní straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá smluvní strana v průběhu této lhůty prohlásí, že svůj závazek nesplní.
7. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají dnem doručení odstoupení od smlouvy druhé smluvní straně.
8. Objednatel je dále oprávněn odstoupit od smlouvy, pokud:
   a) bylo vydáno pravomocné rozhodnutí o úpadku poskytovatele nebo bylo zahájeno insolvenční řízení proti poskytovateli na jeho návrh nebo v případě, že soud pravomocně rozhodl o zrušení poskytovatele a nařídil jeho likvidaci nebo poskytovatel přijme rozhodnutí o vstupu do likvidace; nebo
   b) dojde k významné změně kontroly nad poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení ve smyslu čl. VIII odst. 4 písm. c) této smlouvy a tato změna bude objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZoKB.
9. Objednatel je oprávněn tuto smlouvu vypovědět v případě, kdy:
   a) dojde k vyčerpání sjednaného objemu člh pro rozvoj IS MOSS/SKS podle čl. II odst. 8 této smlouvy;
   b) poskytovatel oznámí úmysl svůj, příp. úmysl případného svého poddodavatele, zahájit (resp. změnit rozsah či povahu) podnikání v elektronických komunikacích ve smyslu § 8 zákona o elektronických komunikacích, potažmo v poštovních službách ve smyslu § 17 zákona č. 29/2000 Sb., o poštovních službách, či poskytovat služby přeshraničního dodávání balíků ve smyslu článku 2 Nařízení Evropského

parlamentu a rady (EU) 2018/644 o službách přeshraničního dodávání balíků, přičemž by toto znamenalo protichůdné zájmy objednatele a poskytovatele (příp. jeho poddodavatele), které by mohly negativně ovlivnit plnění veřejné zakázky.

Výpovědní lhůta začíná běžet prvním dnem měsíce následujícího po doručení výpovědi poskytovateli a končí uplynutím posledního dne daného měsíce.

10. V případě ukončení této smlouvy se smluvní strany zavazují vypořádat veškeré své vzájemné závazky do 60 dnů ode dne ukončení smlouvy. Toto ustanovení neplatí v případě, že dojde k odstoupení od smlouvy z důvodů na straně poskytovatele.

11. V případě skončení smlouvy z jakéhokoli důvodu, se poskytovatel na žádost učiněnou objednatelem do uplynutí až 3 měsíců ode dne skončení této smlouvy a dle pokynů objednatele zavazuje poskytnout objednateli veškerou vyžádanou součinnost, dokumentaci a informace, předat objednateli nebo jím určené třetí osobě data z výstupů implementace a rozvoje IS MOSS/SKS a zúčastnit se jednání s objednatelem a případnými třetími osobami za účelem plynulého a řádného převedení všech činností spojených s plněním této smlouvy poskytovatelem na objednatele a/nebo jím určenou třetí osobu, ke kterému dojde po skončení smlouvy (dále jen „exit“). Vyžádá-li si to objednatel, bude součástí exitu i poskytnutí odborného školení osobám určeným objednatelem v rozsahu nejméně 5 hodin, na kterém poskytovatel určeným osobám zejména:

    a) předá přístup do všech administrátorských rozhraní IS MOSS/SKS a vysvětlí, k čemu slouží a jaké mají funkce,

    b) popíše obsah veškeré písemné dokumentace, vzniklé v souvislosti rozvojem IS MOSS/SKS a vysvětlí, k čemu slouží a jak s ní dále pracovat,

    c) popíše architekturu počítačových programů a dalších prvků tvořících IS MOSS/SKS a vysvětlí vazby mezi jejich částmi,

    d) pomůže navázat na jakýkoli nedokončený vývoj tím, že zdokumentuje jeho aktuální stav,

    e) předá objednateli veškeré zálohy software a pomůže objednateli s migrací software na novou infrastrukturu.

Článek XVII.
Sleva z ceny, smluvní pokuty, odpovědnost za škody

1. V případě prodlení objednatele s uhrazením řádně fakturovaných částek podle podmínek stanovených touto smlouvou má poskytovatel nárok na úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení, nejvýše však v součtu do výše 5 % z fakturované částky.

2. V případě prodlení poskytovatele s poskytováním provozní údržby IS MOSS/SKS podle čl. IV této smlouvy oproti reakčním dobám stanoveným v příloze č. 1 (Specifikace plnění servisní podpory IS MOSS/SKS) této smlouvy je objednatel oprávněn požadovat po poskytovateli uhrazení slevy z ceny paušální platby (viz čl. X odst. 7 této smlouvy) v následujícím měsíci po výskytu takového porušení, a to ve výši 10.000 Kč bez DPH za každý započatý den prodlení v případě vady Kategorie A, ve výši 5.000 Kč za každý započatý den prodlení v případě vady Kategorie B a ve výši 2.000 Kč za každý započatý den prodlení v případě vady Kategorie C.

3. V případě prodlení poskytovatele s poskytováním provozních úprav a/nebo rozvoje podporovaných systémů podle čl. V této smlouvy oproti reakčním dobám stanoveným v bodu 5 přílohy č. 1 této smlouvy je objednatel oprávněn požadovat po poskytovateli uhrazení slevy z ceny paušální platby (viz čl. X odst. 7 této smlouvy) v následujícím měsíci po výskytu takového porušení, a to ve výši 1.000 Kč bez DPH za každý započatý den prodlení.

4. V případě porušení své povinnosti mlčenlivosti či důvěrnosti informací stanovené v čl. XIII této smlouvy poskytne poskytovatel v následujícím měsíci po výskytu takového porušení objednateli slevu z ceny paušální platby (za plnění podle čl. IV této smlouvy stanovené v čl. X odst. 7 této smlouvy), a to ve výši 50.000 Kč za každý jednotlivý případ porušení takové povinnosti.
5. Přesáhnou-li slevy z ceny paušální platby dle odstavce 2 a/nebo 4 tohoto článku smlouvy samotnou paušální platbu dle čl. X odst. 7 této smlouvy stanovenou pro následující období, je objednatel oprávněn tyto slevy započíst v následujících měsících. Nebude-li možné slevy dle odstavce 2 a 4 tohoto článku smlouvy započíst v době účinnosti této smlouvy v celé výši, je objednatel oprávněn nezapočtenou část slevy uplatnit vůči poskytovateli jako smluvní pokutu.
6. V případě porušení některého z ustanovení čl. IX této smlouvy má objednatel nárok na smluvní pokutu ve výši 100.000 Kč.
7. Za porušení jiné povinnosti stanovené smlouvou uhradí poskytovatel objednateli částku 5.000 Kč za každý jednotlivý případ porušení této povinnosti.
8. Smluvní pokuta je splatná ve lhůtě 10 dnů ode dne doručení písemné výzvy k její úhradě, není-li objednatelem započtena oproti pohledávce poskytovatele vůči objednateli. Dnem úhrady smluvní pokuty se rozumí den, kdy je částka odpovídající její výši připsána ve prospěch účtu objednatele. Úrok z prodlení je splatný ve lhůtě 21 dnů ode dne doručení písemné výzvy k jeho úhradě.
9. Objednatel nemá právo uplatnit smluvní pokutu či slevu z ceny, jestliže poskytovatel prokáže, že objednatel neposkytl poskytovateli součinnost nezbytnou k tomu, aby poskytovatel mohl splnit svůj závazek.
10. Zaplacením slevy z ceny či smluvní pokuty podle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci.

Článek XVIII.
Závěrečná ustanovení

1. Jestliže bude mít objednatel jakékoli výhrady ať již ve vztahu k poskytovanému plnění předmětu této smlouvy nebo k osobám podílejícím se na straně poskytovatele na plnění předmětu této smlouvy, sdělí je důvěrným způsobem kontaktní osobě poskytovatele podle v čl. XV odst. 1, resp. Příloze č. 5 (Kontaktní (oprávněné) osoby) této smlouvy.
2. Jestliže se bude objednatel domnívat, že výhrady nejsou adekvátně řešeny nebo že jejich charakter či vážnost to vyžadují, bude výslovně kontaktovat odpovědnou osobu poskytovatele uvedenou v záhlaví této smlouvy.
3. Jestliže výhrada dle odstavce 2 tohoto článku smlouvy nebude vyřešena způsobem uspokojivým pro obě smluvní strany, jmenují obě smluvní strany po jednom vedoucím zaměstnanci, který bude oprávněn vyvolat jednání a s vynaložením veškeré dobré vůle vyřešit spornou záležitost. Schůzka se musí uskutečnit v přiměřeně krátké době po písemném vyzvání jedné ze smluvních stran. Pokud nedojde k dohodě, je objednatel oprávněn odstoupit od smlouvy v souladu s čl. XVI odst. 2 této smlouvy.
4. Poskytovatel se zavazuje, že bude respektovat požadavky vyplývající ze ZoKB a VoKB.
5. Smluvní strany bezvýhradně souhlasí s uveřejněním této smlouvy, případných dodatků k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu v souladu se zákonem 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 zajistí objednatel.

6. Objednatel a poskytovatel se zavazují, že bez písemného souhlasu druhé smluvní strany neučiní informace získané při plnění této smlouvy v žádné podobě dostupné třetí straně, ani že je nepoužijí k jiným účelům než k účelům plnění této smlouvy, s výjimkou informací nezbytných pro nastavení systémů spravovaných třetí stranou. Toto ustanovení platí i po dobu 5 let od ukončení účinnosti této smlouvy, nemá však vliv na případné povinnosti objednatele vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
7. Veškeré změny a doplnění této smlouvy (s výjimkou změn kontaktních osob dle čl. XV odst. 7 této smlouvy) lze činit pouze se souhlasem obou smluvních stran písemnou formou, a to prostřednictvím vzestupně číslovaných dodatků, jinak jsou neplatné.
8. Jakékoli oznámení ve smyslu této smlouvy od druhé smluvní strany musí být učiněno písemně.
9. Smlouva vzniká dnem podpisu oprávněnými zástupci smluvních stran a nabývá účinnosti dnem 1. prosince 2024.
10. Tato smlouva se vztahuje na právní nástupce smluvních stran.
11. Tato smlouva je smluvními stranami vyhotovena v elektronické podobě a opatřena elektronickým podpisem oprávněných zástupců obou smluvních stran.
12. Obě smluvní strany prohlašují, že se s textem této smlouvy seznámily, obsahu porozuměly, souhlasí s ním a na důkaz toho připojují své podpisy.
13. Nedílnou součástí této smlouvy jsou přílohy:

    Příloha č. 1 – Specifikace plnění servisní podpory IS MOSS/SKS

    Příloha č. 2 – Vymezení pojmů

    Příloha č. 3 – Popis podporovaných systémů

    Příloha č. 4 – Technická specifikace podporovaných systémů

    Příloha č. 5 – Kontaktní (oprávněné) osoby

    Příloha č. 6 – Změnový list (vzor)

    Příloha č. 7 – Přehled modulů IS MOSS – schéma

    Příloha č. 8 – Smlouva o zpracování osobních údajů

    Příloha č. 9 – Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

    Příloha č. 10 – Metodika vývoje včetně popisu tvorby veškeré dokumentace.

V Praze dne

Objednatel:

Ing. Marek Ebert

Digitálně podepsal Ing. Marek Ebert
Datum: 2024.10.29 11:17:16 +01'00'

……

Ing. Marek Ebert
předseda Rady
Českého telekomunikačního úřadu

V Brně dne

Poskytovatel:

Petr Franc

Digitálně podepsal Petr Franc
Datum: 2024.10.15 10:39:02 +02'00'

……

Petr Franc, MBA, MSc.
člen představenstva
Seyfor, a.s.

Specifikace předmětu plnění

Požadavky na zajištění servisní podpory a SLA parametry

1. Zajištění provozu a údržby podle čl. II odst. 1 a 2 Smlouvy

1.1. Lhůty pro odstraňování vad se řídí dle kategorie jejich závažnosti a stanovených SLA parametrů:

Stupeň závažnosti	Klasifikace vady	Reakční doba	Doba vyřešení
1	Kategorie A	max. 2 hodiny	max. NBD (následující pracovní den)
2	Kategorie B	max. 4 hodiny	max. 3 pracovní dny (pokud nebude oboustranně písemně dohodnuto jinak)
3	Kategorie C	max. 1 pracovní den	max. 7 pracovních dnů (pokud nebude oboustranně písemně dohodnuto jinak)

Vada kategorie A

- Definice – Systém jako celek je mimo provoz nebo je převážná část jeho funkcí anebo celý modul nedostupný. Jde o vadu, která způsobuje tak závažné problémy, že objednatel nemůže systém používat v základních funkcích nebo nijak ovládat. Další užívání systému nebo celého modulu musí být pozastaveno, dokud vada nebude odstraněna. Vady této úrovně by způsobily velkou ztrátu nebo úplné znemožnění samotné podstaty účelu užití systému, nebo by způsobily stav, kdy by bylo další užití aplikace nebezpečné nebo by způsobilo úplné zastavení systému.
- Název kategorie v HelpDesk – Bránící v provozu.

Vada kategorie B

- Definice – Důležitá funkce systému je nedostupná a nelze ji vyvolat jiným způsobem nebo ji nelze jednoduchým způsobem nahradit organizačním opatřením. Jedná se o závažnou vadu, kdy funkčnost dodaného řešení je degradována tak, že tento stav omezuje běžný provoz objednatele. Vada této úrovně by způsobila nemožnost použít podstatné funkce či data systému bez jejich rozumné náhrady. Užití ostatních částí systému ale může pokračovat.
- Název kategorie v HelpDesk – Nebránící v provozu.

Vada kategorie C

- Definice – Funkční vada drobnějšího charakteru, výpadky funkcí, které lze zajistit jiným způsobem či řešit organizačním opatřením. Jedná se o vadu neohrožující další provoz a užití systému, která nemá vliv na ostatní části systému, ani nedochází ke ztrátě žádných závažných dat.
- Název kategorie v HelpDesk – Ostatní funkční vady.

Klasifikaci vady do jednotlivých kategorií určuje objednatel.

SLA lhůty začínají plynout od okamžiku ohlášení vady podle čl. IV odst. 3 smlouvy, tj. prostřednictvím portálu HelpDesk, v případě nedostupnosti portálu HelpDesk pak od okamžiku ohlášení vady prostřednictvím stanovené e-mailové adresy, eventuálně prostřednictvím stanoveného telefonního čísla (Hot-Line). V takovém případě objednatel neodpovídá za následné zanesení ohlášené vady do portálu HelpDesk, které provede poskytovatel.

Do SLA lhůty na odstranění vady se nezapočítává čas potřebný na zajištění součinnosti objednatele, případně třetích stran, ani čas na odstranění chyb v datech primárních zdrojů. Vyplyne-li z objektivních skutečností potřeba lhůty delší, než je stanovena u jednotlivých kategorií, lze písemně dohodnout lhůtu delší. Za objektivní skutečnosti lze považovat zásah vyšší moci, chybnou funkci operačních a databázových platforem, časový rozsah potřebných prací jdoucí nad stanovený rámec.

Poskytovatel garantuje dobu vyřešení jen za předpokladu, že technické vybavení objednatele, na kterém je IS MOSS/SKS provozován, toto umožňuje a splňuje požadavky uvedené v Příloze č. 4 smlouvy.

1.2. Další požadované činnosti v rámci servisní podpory

- Sledování běhu podporovaných systémů a odstraňování překážek, které zabraňují jejich užívání v souladu s odsouhlaseným zadáním.
- Analýza a řešení vad hlášených pomocí HelpDesk. Udržování aplikačního programového vybavení nutného pro běh podporovaných systémů.
- Proaktivní sledování běhu podporovaných systémů pomocí dohledových nástrojů.
- Vyhodnocování a zpracování logů o běhu podporovaných systémů.
- Údržba databáze podporovaných systémů.
- Přijímání, validace, řešení a uzavírání (případně zamítání) vad, nahlášených prostřednictvím HelpDesk.
- Nasazování opravných verzí podporovaných systémů.

2. Provoz a údržba webového portálu zákaznické podpory (HelpDesk) podle čl. II odst. 3 Smlouvy

Zajištění jednotného prostředí k hlášení, evidenci a řízení životního cyklu vad, požadavků a změn u podporovaných systémů objednatele.

Poskytovatel zajistí poskytnutí, konfiguraci a správu HelpDesk jako jednotného kontaktního místa k hlášení, evidenci a řízení životního cyklu vad, požadavků a změn (dále jen „Hlášení“) u podporovaných systémů.

HelpDesk umožní objednateli – uživatelům jednotlivých systémů přehled o evidovaných Hlášeních a způsobech a termínech jejich řešení pro účely zpětné kontroly plnění.

Dostupnost HelpDesk pro uživatele podporovaných systémů prostřednictvím Internetu.

Servisní hodiny: 7 x 24 x 365

Dostupnost min. 95 % (měřeno za kalendářní měsíc)

3. Telefonická a e-mailová podpora (Hot-Line) podle čl. II odst. 4 Smlouvy

Zajištění komunikačního místa pro vznášení a odpovídání dotazů uživatelů objednatele poskytovateli, které nevyžadují přípravu a zásah do systémů ani jejich dat ze strany poskytovatele.

Rychlé řešení běžných dotazů týkajících se podporovaných systémů, poskytování informací a konzultací, které nevyžadují přípravu a zásah do systémů ani jejich dat ze strany poskytovatele, a to na vyhrazené telefonické lince a emailové adrese. Na základě kontaktování vyhrazeného čísla proběhne zodpovězení dotazu, resp. kontaktování e-mailové adresy bude zpracován a odeslán e-mail.

Součástí služby telefonické a e-mailové podpory (Hot-Line) není Metodická podpora uživatelům (zajišťují pověřené osoby objednatele – garanti modulů MOSS/SKS) a školení uživatelů.

Servisní hodiny: 5 x 9, Po – Pá: 8:00 – 17:00

4. Řešení požadavků na uživatelskou podporu na úrovni L1, L2 a L3 podle čl. II odst. 5 Smlouvy

Zajištění provádění zásahů, které není schopen vykonat sám objednatel bez pomoci (technické či metodické) poskytovatele.

Opravy situací vzniklých v důsledku chybného uživatelského postupu.

Opravy chybně zadaných dat či dat přenesených z jiných systémů.

Vytváření výstupů dle požadavků objednatele, které nevyžadují zásah do podporovaných systémů a s ním spojené nasazení nové verze.

Nahlašování požadavků uživateli podporovaných systémů prostřednictvím HelpDesk.

Servisní hodiny: 5 x 9, Po – Pá: 8:00 – 17:00

5. Provádění provozních úprav funkcionality a rozvoj podporovaných systémů podle čl. II odst. 6 Smlouvy

Zajištění procesu úprav a změn podporovaných systémů na základě požadavků objednatele evidovaných prostřednictvím HelpDesk.

Na základě zaevidovaného požadavku poskytovatel připraví specifikaci návrhu řešení, provede odhad pracnost a zpracuje změnový list.

Servisní hodiny: 5 x 9, Po – Pá: 8:00 – 17:00

SLA pro provozní úpravy a rozvoj (čl. V odst. 1 Smlouvy)

Kategorie	Klasifikace	Vytvoření Změnového listu (včetně odhadu pracnosti)	Dodání funkcionality na testovací prostředí
1	Vysoká	max. 5 pracovních dnů	max. 10 pracovních dnů
2	Střední	max. 10 pracovních dnů	max. 15 pracovních dnů
3	Nízká	max. 15 pracovních dnů	max. 20 pracovních dnů

Lhůta pro vytvoření Změnového listu se počítá ode dne zaevidování požadavku v HelpDesk, případně od okamžiku poskytnutí nezbytně nutného doplnění/upřesnění zaevidovaného požadavku ze strany objednatele na základě žádosti poskytovatele.

Lhůta pro dodání funkcionality na testovací prostředí se počítá ode dne potvrzení objednávky poskytovatelem. Poskytovatel je povinen potvrdit objednávku zaslanou objednatelem nejpozději do 2 pracovních dnů ode dne jejího doručení.

6. Školení a konzultace podle čl. II odst. 7 Smlouvy

Zajištění proškolení nebo odborné konzultace pro uživatele objednatele dle jeho individuálních potřeb. Poskytovatel na základě objednávky vystavené objednatelem zajistí pro uživatele objednatele odborné školení týkající se podporovaných systémů, připraví školící materiály v elektronické podobě, přípravu školícího prostředí a zpracuje prezenční listinu.

Servisní hodiny: 5 x 9, Po – Pá: 8:00 – 17:00

Vymezení pojmů

Základní pojmy jsou stanoveny pouze pro účely této smlouvy

Podporované systémy:

„Informační systém Modulární Správní Systém/Společný katalog subjektů“ (IS MOSS/SKS) – Informační systém jako aplikace klasické třívrstvé architektury:

- Databázová vrstva: vlastní databázový server Oracle obsahující potřebnou databázovou strukturu včetně podpůrných databázových funkcí.
- Aplikační vrstva: produkční aplikační server systému MOSS/SKS.
- Klientská vrstva: klient instalovaný na jednotlivých klientských stanicích.
- Rozhraní na externí aplikace
- Reporty: Vlastní tiskové sestavy pro potřeby uživatelů v prostředí MS SQL Reporting services

APV a klientská vrstva obsahují:

- Modul Evidence podnikatelů v elektronických komunikacích (EPEK)
- Modul Evidence podnikatelů v poštovních službách (EPPS)
- Modul Správa čísel (SC)
- Modul Evidence plateb (P1)
- Obecné principy vedení Správního řízení (SŘ)
- Modul Účastnické spory (S1)
- Modul Druhý stupeň (S2)
- Modul Správní trestání (ST)
- Modul Vymáhání pohledávek (VP)
- Modul Elektronické vypravení spisu (EVS)
- Modul Univerzální služba (US)
- Modul Námitky v poštovních službách (NPS)
- Modul Podněty, stížnosti a dotazy (PSD)
- Modul Odborná způsobilost (OZ)
- Modul Bezdrátové místní informační systémy (BMIS)
- Modul Evidence subjektů (ES)
- Modul Společný katalog subjektů (SKS)

Rozhraní MOS/SKS na externí aplikace ČTÚ:

- Rozhraní na spisovou službu GINIS
- Rozhraní na Lokální jednotný identitní prostor (LJIP)
- Rozhraní na Elektronický sběr dat (ESD)
- Rozhraní na Automatizovaný systém monitorování kmitočtového spektra (ASMKS)
- Export dat EPEK, EPPS, SC a BMIS pro web ČTÚ

„MS SharePoint – Intranet ČTÚ v prostředí Microsoft SharePoint“ zahrnující:

- Doplněk pro automatické přidělování evidenčních čísel smluv
- Doplněk pro rezervaci jednacích místností
- Doplněk pro hledání v telefonním seznamu
- Doplněk pro přehled o přítomnosti/nepřítomnosti zaměstnanců
- Synchronizace Active Directory do skupin SharePointu.

„Business Inteligence a datový sklad“ (dále jen BI/DWH) obsahující:

- Report výkonnosti v jednotlivých modulech MOSS/SKS.

Pojmy servisní podpory:

„Doba vyřešení“ – časový interval, který uplyne od nahlášení vady, servisního požadavku nebo provozního incidentu do doby jeho vyřešení. Do času pro vyřešení se nezapočítává čas, kdy je vyžadována nezbytná součinnost objednatele nebo je řešení servisního požadavku s vědomím objednatele nebo z jeho rozhodnutí přerušeno. Součinností může být např. poskytnutí vzdáleného přístupu.

„Garant modulu“ – jmenovaný zaměstnanec objednatele, odpovídající za stanovení pracovního postupu správné obsluhy příslušné části podporovaných systémů nebo modulu.

„Garant smlouvy“ – jmenovaný zaměstnanec objednatele, odpovídající za plnění smlouvy.

„Hot-Line“ – komunikační místo pro vznášení a odpovídání dotazů uživatelů objednatele, které nevyžadují přípravu a zásah do systémů ani jejich dat ze strany poskytovatele.

„Konzultace“ – vysvětlení konkrétních postupů, zodpovězení konkrétních dotazů zpravidla v rámci individuální návštěvy v sídle objednatele na jeho vyžádání. Může být organizováno pro více uživatelů objednatele. Každá konzultace je doložena prezenční listinou dokládající účastníky, konzultovanou problematiku a rozsah (spotřebu času). Prezenční listina je přílohou Výkazů práce.

„Odstranění vady“ – obnovení plného užívání a oprava chybných dat v Systému. Za odstranění vady se považují i prokázaná zjištění vady aplikací/řešení, které poskytovatel nedodává nebo prokázaná nutnost nasazení aktualizované verze aplikací/systémů, které poskytovatel nedodává, pokud k tomuto nedošlo v důsledku odstraňování jiných vad, nebo nasazení nové verze APV a pokud toto nemohl poskytovatel předvídat.

„Webový portál zákaznické podpory“ (HelpDesk) – webové rozhraní poskytovatele, jednotné místo pro evidenci všech vad a požadavků objednatele, které slouží k evidenci a řízení workflow požadavků.

„Reakční doba“ – čas, který uplyne od nahlášení vady, servisního požadavku nebo provozního incidentu do zahájení servisní činnosti pracovníky poskytovatele, včetně zahájení analýzy příčiny hlášení.

„Servisní hodiny“ – pracovní dny od 9 do 17 hodin. Hodinou poskytovatele se rozumí hodina v pracovní dny a v pracovní době, dnem se rozumí pracovní den. Jeden pracovní den je 8 hodin.

„Sídlo Objednatele“ – sídlo ČTÚ v Praze, včetně všech pracovišť oblastních odborů, v Praze, Českých Budějovicích, Plzni, Ústí nad Labem, Hradci Králové, Brně a Ostravě.

„Školení“ – seznámení s funkcionalitou a obsluhou nového systému nebo jeho nové části. Zpravidla je organizováno pro více uživatelů objednatele současně v prostředí vhodném pro realizaci školení. Každé školení je doloženo prezenční listinou dokládající účastníky, školenou problematiku a rozsah (spotřebu času). Prezenční listina je přílohou Výkazů práce.

„Úroveň podpory L1“ – zajišťuje příjem a evidenci požadavků Garantů objednatele odpovědným zaměstnancem poskytovatele, zpětné potvrzení jejich přijetí, kategorizace a řízení procesu do vypořádání požadavku. Zajišťuje Hot-line a řeší běžné provozní problémy, které nevyžadují analytické nebo programátorské zásahy. Nositelem této úrovně je zaměstnanec poskytovatele. Předmětem podpory L1 není metodická podpora uživatelů.

„Úroveň podpory L2“ – řeší požadavky na podporu, které přesahují schopnosti zákaznické podpory L1, zejména provádí rozbor požadavku, hledá příčinu vady a podává profesionální vysvětlení/doporučení postupu. Je-li k vyřešení požadavku potřebná úprava produktu, zadává ji na úroveň podpory L3. U požadavků na změnu provádí analytickou přípravu a odhad pracnosti. Nositelem této úrovně jsou zaměstnanci poskytovatele, kteří disponují znalostí produktu, algoritmů řešení, procesů a toků dat, včetně schopnosti analýzy požadavků.

„Úroveň podpory L3“ – provádí požadované úpravy Systémů podle zadání (realizuje změny v produktu). Zajišťuje zapracování těchto změn do příslušné verze produktu a ověření správnosti zapracování (otestování). Nositelem řešení této úrovně je zaměstnanec poskytovatele.

„Vada“ – stav, který znemožňuje používání Systému nebo jeho části k účelu, pro který byl vytvořen nebo stav, který umožňuje pouze omezené používání řešení nebo jeho části k účelu, pro který byl vytvořen. Tento stav není považován za plnohodnotný provoz. Vady jsou kategorizovány dle stupně závažnosti na vady kategorie A, B, C.

„Výkaz práce“ – výkaz dokládající skutečnou spotřebu kapacit odvedené práce.

„Vyřešením“ – se rozumí připravení opraveného řešení k nasazení do provozního prostředí. V případě vady kategorie A se vyřešením servisního požadavku rozumí i stav, kdy je možno dočasným opatřením požadavek převést na vadu kategorie B.

„Změnový list“ – dokument obsahující náležitosti pro věcné schválení, objednávku, realizaci a akceptaci požadavku na provozní úpravu podporovaných systémů.

Popis podporovaných systémů

Český telekomunikační úřad (dále jen „ČTÚ“) jako ústřední správní orgán pro výkon státní správy ve věcech stanovených zákonem, včetně regulace trhu a stanovování podmínek pro podnikání v oblasti elektronických komunikací a poštovních služeb vykonává činnosti vyplývající ze zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „ZEK“) a ze zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů (dále jen „ZoPS“).

ČTÚ vykonává působnost prostřednictvím jednotlivých útvarů, tj. sekcí, odborů a samostatných oddělení. Jeho sídlem je Praha a dislokovaná pracoviště má i v dalších městech. Jsou jimi odbory pro oblast jihočeskou a západočeskou se sídlem v Plzni, pro oblast severočeskou se sídlem v Ústí nad Labem, pro oblast východočeskou se sídlem v Hradci Králové, pro oblast jihomoravskou se sídlem v Brně a pro oblast severomoravskou se sídlem v Ostravě.

Jedním z informačních systémů (IS), které ČTÚ používá pro zajištění činností výkonu státní správy v elektronických komunikacích a poštovních službách je Modulární správní systém/Společný katalog subjektů (dále jen „MOSS/SKS“). Základním jádrem MOSS/SKS je funkcionalita pro vedení správních řízení ČTÚ. Na tuto funkcionalitu navazují další moduly dle jednotlivých činností. MOSS/SKS podporuje činnosti referentů napříč odbornými útvary ČTÚ. Všichni uživatelé MOSS/SKS v rámci ČTÚ mají k údajům v MOSS/SKS řízený přístup na základě svých oprávnění.

IS MOSS/SKS je identifikován jako významný informační systém v souladu s vyhláškou č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritérií.

MOSS/SKS je zakomponován do prostředí ČTÚ, tzn. je zasazen do infrastruktury ICT v organizaci a integrován s vybranými aplikacemi (specifikace uvedena níže).

MOSS/SKS svými moduly pokrývá následující oblasti (agendy, procesy), které spadají do výkonu státní správy v EK a které jsou zároveň v kompetenci ČTÚ:

Modul evidence podnikatelů v elektronických komunikacích (dále jen „modul EPEK“)

Modul EPEK slouží k evidenci podnikatelů v elektronických komunikacích (EK). Obsahuje přehled jimi nabízených služeb, zajišťovaných sítí, vedených správních řízení, souvisejících spisů, kontaktních a dalších informací.

Modul EPEK umožňuje přijetí oznámení podnikání v této oblasti, automatizované zpracování tohoto podání v navazujícím správním řízení, vedení veškeré související komunikace s provozovatelem, další úkony související s vydáním osvědčení o oznámení podnikání v oblasti EK, zpracování oznámení změn, přerušení nebo ukončení podnikání.

Modul Evidence provozovatelů poskytujících nebo zajišťujících poštovní služby (dále jen „modul EPPS“)

Modul EPPS slouží k evidenci provozovatelů poskytujících nebo zajišťujících poštovní služby (PS). Obsahuje přehled jimi nabízených služeb, vedených správních řízení, souvisejících spisů, kontaktních a dalších informací.

Modul EPPS umožňuje přijetí oznámení podnikání v této oblasti, zpracování tohoto podání v navazujícím správním řízení, vedení veškeré související komunikace s provozovatelem, další úkony související s vydáním osvědčení o oznámení podnikání v oblasti PS, zpracování oznámení změn, přerušení nebo ukončení podnikání.

Modul Evidence Subjektů (dále jen „modul ES“)

Modul ES umožňuje evidenci subjektů, s nimiž ČTÚ přichází do styku v rámci ostatních agend vedených v MOSS/SKS. Evidence subjektů je společnou agendou pro všechny činnosti podporované MOSS/SKS.

Modul Správní řízení (dále jen „modul SŘ“)

Modul SŘ představuje vedení správního řízení v obecné podobě podle zákona č. 500/2004 Sb., správní řád. Modul SŘ je východiskem pro všechna další správní řízení specializovaná pro určitou věc.

Modul Rozhodování sporů 1. stupeň (dále jen „modul S1“)

Modul S1 slouží k vedení účastnických sporů, které ČTÚ řeší na základě § 129 odst. 1 ZEK v oblasti námitek (podání od účastníka služby), dluhů (podání od operátorů) a ostatní obecné spory mezi účastníkem a operátorem.

Modul Správní řízení 2. stupně (dále je „modul S2“)

Modul S2 slouží pro vedení správních řízení, kdy se některý z účastníků využil opravný prostředek proti rozhodnutí/usnesení ve správním řízení prvního stupně (pokud spor rovnou neřeší soud). Mezi správním řízení 2. stupně a správním řízením 1. stupně je vedena souvislost (související spis).

Modul Správa čísel (dále jen „modul SC“)

Modul SC slouží k přidělování a správě čísel a kódů podle číslovacích plánů, která je prováděna ve smyslu ZEK. Přidělení čísel je realizováno ve správním řízení na základě žádosti o přidělení čísel (kódů). Výsledkem jsou přidělená čísla nebo kódy, případně zamítnutí přidělení. Kromě přidělení čísel je řešena i změna přidělení a odejmutí. Je tak udržována vazba mezi záznamem přidělení a všemi změnami přidělení.

Modul správní trestání (dále jen „modul ST“)

Modul ST slouží pro zpracování správních řízení, která se týkají spáchání přestupků spadajících do působnosti ČTÚ. Modul ST má jasně stanovené schéma procesu tak, aby jednotlivé kroky na sebe navazovaly od samotného zahájení řízení až po jeho ukončení, čemuž napomáhají i napojené centrální šablony potřebné pro řízení o přestupcích v jednotlivých krocích.

Kromě propojení jednotlivých modulů v agendě MOSS/SKS (např. s modulem PSD) je modul ST propojen i s APV ASMKS (IS Automatizovaný systém monitorování kmitočtového spektra – informační systém ČTÚ), kdy je při uzavírání případu, ve kterém bylo zjištěno porušení povinnosti, založen nový podnět, který se přímo objeví v MOSS/SKS v modulu ST.

Modul námitky v poštovních službách (dále jen „modul NPS“)

V modulu NPS jsou řešeny námitky proti vyřízení reklamace podle § 6a, resp. § 36a odst. 1 písm. e) ZoPS – Posouzení návrhu o námitce, výběr správního poplatku, vydání rozhodnutí, včetně administrativních úkonů.

Modul evidence plateb (dále jen „modul P1“)

Modul P1 slouží k celkové správě předepsaných a došlých plateb, které byly stanoveny ČTÚ v jednotlivých agendách správního řízení. Modul P1 umožňuje vzájemné proúčtování plateb, správu jednotlivých účtů a následně vytváření výstupních sestav jako např. evidenci o pohledávkách.

Modul vymáhání pohledávek (dále jen „modul VP“)

Modul VP slouží pro vymáhání pohledávek ČTÚ týkajících se agend zpracovávaných v MOSS/SKS a které jsou v MOSS/SKS evidovány. Jednotlivé pohledávky lze pro vybranou činnost vybrat z množiny všech předpisů plateb, které se zobrazují v nabídce „Pohledávky k vymáhání“. Zahájit řízení lze i s více pohledávkami, ovšem stejného subjektu.

Modul Podněty, stížnosti, dotazy (dále jen „modul PSD“)

Modul PSD je modulem, ve kterém jsou vyřizována podání účastníků služeb EK a PS, jejichž obsahem je stížnost, dotaz, žádost o radu a přešetření, popř. podnět k zahájení řízení z moci úřední. Jde o modul, ve kterém jsou vedeny spisy, které nejsou návrhem na správní řízení dle zákona, i když se jimi v některých případech stát mohou.

Modul Univerzální služba (dále jen „modul US“)

Modul US zajišťuje evidenci plátců na účet univerzální služby a slouží k výpočtu a následnému stanovení výše příspěvku na účet univerzální služby. Řeší rovněž evidenci příjemců dotací a jejich ztotožňování vůči základním registrům.

Modul elektronické vypravení spisu (dále jen „modul EVS“)

Modul EVS slouží ke konverzi a elektronickému podepsání dokumentů vytvořených mimo MOSS/SKS. Vytvořený dokument je možné pomocí modulu EVS uložit na disk, odeslat emailem či odeslat do datové schránky. Zdrojový dokument musí být před vstupem do modulu EVS ve finální podobě – uživatel má pouze možnosti vložit do dokumentu razítko s nabytím právní moci a vykonatelnosti.

Modul evidence zkoušek odborné způsobilosti (dále jen „modul OZ“)

Modul OZ slouží k evidenci průkazů odborné způsobilosti, přípravě zkoušek odborné způsobilosti a vydávání průkazů odborné způsobilosti. Modul OZ komplexní správu všech činností vyžadovaných podle vyhlášky č. 157/2005 Sb., o náležitostech přihlášky ke zkoušce k prokázání odborné způsobilosti k obsluze vysílacích rádiových zařízení, o rozsahu znalostí potřebných pro jednotlivé druhy odborné způsobilosti, o způsobu provádění zkoušek, o druzích průkazů odborné způsobilosti a době jejich platnosti.

Modul evidence stanic bezdrátových místních informačních systémů (dále jen modul „BMIS“)

Modul BMIS slouží k evidenci vysílacích stanic BMIS podle všeobecného oprávnění č. VO-R/2/05.2018-5 k využívání rádiových kmitočtů a provozování stanic BMIS v pásmu 70 MHz. V modulu BMIS jsou údaje o provozovatelích BMIS a o jimi provozovaných stanicích. Uvedené údaje jsou zveřejněny na webu ČTÚ.

Modul SKS – Společný katalog subjektů – databáze subjektů, které jsou využívány v jednotlivých IS ČTÚ. SKS na jejich pokyn stahuje data o subjektech z příslušných zdrojových systémů při splnění požadavků, které jsou na komunikaci s těmito systémy kladeny, včetně logování. V případě, že je požadována a je pro příslušný údaj dostupná, zajišťuje SKS následnou synchronizaci změn stažených údajů. Základním zdrojovým systémem je systém základních registrů, odkud jsou stahovány (v některých případech i zapisovány) údaje z registru obyvatel, osob, územní identifikace a práv a povinností, dále pak z dalších registrů dostupných pomocí kompozitních služeb ISZR (AISEO, AISC, AISEOP, AISCD). Údaje o subjektech jsou doplňovány údaji z dalších registrů, například insolvenčního rejstříku ISIR nebo systému datových schránek. Modul SKS uložené údaje verzuje a tím zajišťuje historii subjektů, kterou některé registry standardně nedrží.

Přehled plánovaných úprav a aktivit v rámci plnění servisní smlouvy pro systém MOSS/SKS (2024-2029):

- Úpravy komunikace MOSS/SKS pro předávání metadat pro potřeby Jmenného rejstříku v IS GINIS (eSSL).
- Provedení optimalizace datového modelu a vyčištění nepotřebných a zastaralých dat/tabulek.
- Rozvoj služeb přes ISSS.
- Odhlašování změn z ISZR.
- Úprava procesů v IS MOSS/SKS v oblasti vedení správních řízení (ukončování, archivace, skartace řízení a anonymizace údajů) – v souladu s procesy v IS GINIS.
- Zpracování plnohodnotných procesů pro práci s el. spisem v modulech IS MOSS/SKS.
- Úpravy IS v souvislosti s napojením na IS Samoobslužný portál ČTÚ (realizace projektu SOP 2024-2025).

- Zajištění přepracování/aktualizace dokumentace IS MOSS/SKS v souvislosti s provedenými úpravami.
- Postupná modernizace a úpravy informačního systému MOSS/SKS v návaznosti na změny právních předpisů v oblasti elektronických komunikací a poštovních služeb.
- Úpravy IS MOSS/SKS související s vývojem právní úpravy a požadavků v oblasti digitalizace a elektronizace, zajištění bezpečnosti uvedeného IS a jeho napojení na ostatní IS.

Popis funkcionality MS SharePoint v prostředí ČTÚ

Portál ČTÚ MS SharePoint byl vytvořen z důvodu zajištění jednoho prostoru pro sdílení a ukládání dokumentů pro jednotlivé útvary, pracovní skupiny a projektové týmy. Jedná se v podstatě o soubor webů, seznamů a knihoven dokumentů propojených pomocí webových stránek. Přístupová práva jsou jednotlivým uživatelům přidělována na základě rozhodnutí ředitelů jednotlivých odborů, vedoucích oddělení, eventuálně vedoucího pracovní skupiny podle jejich úlohy nebo pracovní pozice.

Portál ČTÚ MS SharePoint obsahuje informace určeným zaměstnancům ČTÚ a členům Rady ČTÚ (dále jen „zaměstnanci“). Na intranetu zveřejňuje ČTÚ údaje a informace pro zaměstnance, které jsou určeny pro vnitřní potřebu. Obsahuje sekce týkající se základních dokumentů ČTÚ, závazných pokynů, zápisů z porad atd., ale i sekce s informacemi obecnějšími – telefonní seznamy, odkazy na jídelní lístky atd. Nedílnou součástí portálu ČTÚ MS SharePoint je sekce, kde jsou publikovány šablony, formuláře a vzory, které se používají při písemné korespondenci ČTÚ (interní i externí). Na portálu ČTÚ MS SharePoint jsou dále k dispozici informace týkající se spisové služby GINIS nebo MOSS/SKS. Pro všechny zaměstnance jsou v sekci Informace pro uživatele PC umístěny uživatelské příručky pro práci v jednotlivých informačních systémech (IS).

Funkcionalita vyvinutá pro potřeby ČTÚ nad MS SharePoint:

- Doplněk pro automatické přidělování evidenčních čísel smluv
- Doplněk pro rezervaci místností
- Doplněk pro hledání v telefonním seznamu
- Doplněk pro přehled o přítomnosti/nepřítomnosti zaměstnanců
- Synchronizace Active Directory do skupin SharePointu.

Popis BI/DWH

Portál BI byl realizován mezi lety 2009 a 2010. Sdružuje a zpracovává data ze systémů MOSS/SKS a Spectra. BI pracuje nad datovým skladem – DWH – OLAP kostky. Kostky jsou plněny prostřednictvím integračních služeb MS SQL serveru z ORACLE databází MOSS/SKS a Spectra. Jednotlivé sestavy pracují v rámci MS SQL server Reporting Services. Vlastní MS SQL server databáze je využívána také, ale jen pro aplikační účely.

BI zobrazuje údaje a ukazatele z oblastí:

Portál BI – dashboard,

Poplatky a pohledávky,

Předpisy,

Správní řízení,

Správa spektra,

Správa čísel,

Evidence podnikatelů,

Spory a pokuty

Reporty MOSS/SKS:

Souhrn sestav nad daty MOSS/SKS, které ale nepatří do systému BI, nicméně některé z reportů používají technologii datového skladu BI, tj. integrační služby a OLAP kostky v DWH.

Seznam sestav:

OZ - počty průkazů; P1 - jmenovitý přehled neuhrazených pokut; P1 - přehled o celkových úhradách pokut (v3); P1 - přehled o celkových úhradách SP (v3); P1 - přehled výběru pokut; P1 - přehled výběru SP; PSD - elektronické komunikace (MMZ); PSD - poštovní služby (MMZ); S1 – dokumenty; S1 - podklad pro MMZ (2012); S1 - počet rozhodnutí; S1 - přehled nerozhodnutých případů; S2 - jednání komise; S2 – spisy; SC - pohledávky rozhodnutí po lhůtě; SC - pohledávky rozhodnutí před lhůtou; SC - počet rozhodnutí; SC – statistiky; SC - statistiky čísla; SC - uhrazené SP za období; ST - přehled přestupků dle § 110 odst. 2 zákona č. 250/2016 Sb.; VP - vymáhané pohledávky.

Funkcionalita informačních systémů ČTÚ třetích stran spolupracujících s IS MOSS/SKS:

IS GINIS – systém elektronické spisové služby – zajišťuje elektronickou evidenci spisů, dokumentů a komunikace ČTÚ s externímu subjekty.

IS LJIP – Lokální Jednotný Identitní Prostor – centrální úložiště uživatelských identit zaměstnanců ČTÚ včetně aplikačních a agendových činnostních rolí, zajišťuje autentizaci a autorizaci uživatelů přistupujících do připojených IS ČTÚ.

IS APV ASMKS – Automatizovaný systém monitorování kmitočtového spektra – zajišťuje sběr a vyhodnocení dat ze stacionárních a mobilních měřících stanic na území celé České republiky pro zajištění činností vyplývající ze ZEK.

IS ESD – Elektronický sběr dat – zajišťuje sběr dat od podnikatelů v EK dle ZEK a od provozovatelů poskytujících PS nebo zajišťujících PS dle ZoPS.

Ostatní

Z jednotlivých modulů MOSS/SKS jsou pravidelně exportována data pro zobrazení na internetových stránkách ČTÚ v sekci Databáze nebo pro datové sady pro portál Otevřená data.

Technická specifikace podporovaných systémů

IS MOSS/SKS je z pohledu architektury tzv. vícevrstvý, se samostatnou databázovou, aplikační a klientskou vrstvou. Toto vícevrstvé složení systému umožňuje rozšiřování systému o další funkcionalitu případně o jeho integrování s dalšími systémy a rejstříky.

Z pohledu komunikační infrastruktury je systém provozován na virtuální privátní síti spojující jednotlivé lokální oblasti s ústředím Úřadu. Klient je na koncové stanice distribuován pomocí technologie ClickOnce.

Aplikační programové vybavení (dále jen „APV“) IS MOSS/SKS a další programové vybavení potřebné pro jeho provoz:

Aplikační server

- Operační systém MS Windows Server 2019 nebo vyšší + automatické aktualizace
- IIS verze 7.0 nebo vyšší
- .NET Framework verze 4.7
- Klientské utility Oracle na aplikačním serveru pro komunikaci s databázovou vrstvou

Databáze

- Oracle Database 19 nebo vyšší
- MS SQL Server 2016 standard se službou Microsoft SQL Server Reporting Services 11.0.3000.0 nebo vyšší

Klientská stanice

- Operační systém MS Windows 10 Pro nebo vyšší
- .NET Framework verze 4.7 nebo vyšší
- O 365
- Acrobat Reader 10 nebo vyšší
- Knihovna Pdf Signer 1.35 nebo vyšší, od Software 602
- Microsoft Access Database Engine 2016 x64 Redistributable na stanicích, které využívají import dat z MS Excel
- BIT4ID Universal Middleware

MS SharePoint

- Aplikační server s OS MS Windows Server 2016 Datacenter
- MS SharePoint 2013 Standard Edition instalovaný na aplikačním serveru
- Databázový server s OS MS Windows Server 2016 Datacenter
- MS SQL Server 2016 Standard Edition instalovaný na databázovém serveru

BI/DWH

- tytéž systémové komponenty jako MS SharePoint, navíc:
- MS SQL Reporting Services a MSSQL Analysis Services pro SQL Server 2016 nebo vyšší

Kontaktní osoby

Kontaktními osobami jsou:

a) ve věcech smluvních na straně objednatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

ve věcech odborných na straně objednatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

ve věcech technických na straně objednatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

b) ve věcech smluvních na straně poskytovatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

ve věcech odborných na straně poskytovatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

ve věcech technických na straně poskytovatele:

Jméno	E-mail	Telefon	Mobil
[redacted]			

Změnový list
ZL_XX_XX - Název

Smlouva č. CTU/2024_0057	
Datum nahlášení:	Žadatel: Řešitel:
Název změny:	
Popis změny	
Pracnost realizace změny v člh (konzultace, analýza, vývoj, testování, dokumentace)	
Změny v datovém modelu:	Ano/Ne
Vliv změny na bezpečnost:	Ano/Ne
Vliv změny na webové služby:	Ano/Ne
Vliv změny na ochranu osobních údajů	Ano/Ne
Dopady do dokumentace:	Ano/Ne
Termín dodání (datum nasazení na testovací prostředí)	
Termín dodání (datum nasazení na produkci)	
Schválení realizace v uvedeném rozsahu pracnosti	
Datum:	
Objednatel	**Poskytovatel**
Jméno/funkce:	Jméno/funkce:
Podpis:	Podpis:

Správa dokumentu

Historie změn

Verze	Datum	Seznam změn	Změnil

Pojmy a zkratky

Pojem	Vysvětlení

Odkazy na jiné dokumenty

Odkaz	Jméno dokumentu	Verze

1. Zadání

2. Detailní analýza

3. Harmonogram

4. Zhodnocení dopadů

4.1. Změny v datovém modelu

4.2. Dopady do rozhraní

4.3. Dopady na bezpečnost

4.4. Dopady do dokumentace

Obecné moduly pro správní řízení (vyznačeny žlutě)

FW - Framework

Vzhled a ovládání
- jednotné uživatelské rozhraní celého systému

Přístupová práva
- pro definování uživatelů, rolí a přístupových práv

Administrace systému
- funkcionalita pro správce systému

Systém číselníků
- systém pro sdílení shodných údajů napříč úřadem

Definování sestav a filtrů
- univerzální dotazovač nad seznamy
- export do Excelu

Přizpůsobení aplikace
- funkcionalita pro nastavení a změnu parametrů systému pro správce a pro uživatele

Tvorba dokumentů
- funkcionalita pro tvorbu, úpravu a tisk tiskových výstupů pomocí šablon

Logování
- záznam činnosti uživatelů do aplikačního logu
- systémový log

Rozhraní na okolní systémy
- technická část rozhraní

SR – Správní řízení — všichni

Vedení správního řízení (obecně)
- vedení elektronického spisu
- zahájení, vedení, ukončení řízení
- stav správního řízení
- řízení práv ke spisu (oprávněná úřední osoba, nahlížení do spisu)
- předávání spisu v rámci ČTÚ
- návaznost na související spisy

Spis
- nositel čj. („desky spisu“)
- základní informace o spisu
- sdružuje všechny ostatní informace k řízení
- referátník
- sběrný arch

Úkony
- formalizovaný zápis jakékoliv činnosti v řízení
- definován seznam na základě věci spisu a stavu řízení
- umožňují provádět logické kontroly zadávaných dat
- evidence data a referenta, který úkon učinil
- v návaznosti na úkon tvorba tiskové sestavy

Dokumenty
- evidence založení přijatého dokumentu do spisu
- vytváření dokumentů pomocí šablon
- řízení dokumentu (vypravení, evidence doručení)
- komunikace se spisovou službou

Účastníci
- definování účastníků (subjekt, případný zástupce)
- definování doručovací adresy

Platby
- předepsání poplatku
- stanovení pokuty
- podpora stanovení výše platby

Lhůty
- evidence lhůt
- podpora vypočtu lhůt
- sledování plynutí

Vyšší instance
- opravné prostředky (evidence)
- evidence vyjádření k o.p.
- návaznost na spis v další instanci

ES – Evidence subjektů — všichni

Evidování údajů o subjektech
- načítání / reklamace dat z ROB, ROS RUIAN, AISEO, AISC, AISEOP a zápis do ROS a RPP pomocí SKS
- registrace k sledování změn v ISZR a automatické přebírání + notifikace
- podpora kompletní historie provedených změn a promítání do řízení
- načítání údajů z insolvenčního rejstříku a jejich pravidelná aktualizace

Profil subjektu
- přehled se subjektem vedených řízení

Spisová služba
- zapisování informací o subjektech do GINIS

P1 – Evidence plateb — všichni

Vedení účtů
- vytváření a vedení účtů (pro předpisy a platby)

Předpisy
- evidování předpisů plateb
- podpora předpisu před NPM
- účetní stornování chybných předpisů
- podpora hromadných soupisek

Platby
- import výpisu (banka, pošta)
- hromadné platby
- platby kolkem a hotově

Sledování úhrad
- automatické a manuální párování
- informování ostatních modulů o platbách a plynutí doby splatnosti
- vypořádání přeplatků

Rozhraní ASMKS Realizována WS

Rozhraní ESD Realizována WS

Rozhraní web Realizována XML

LTD server Realizována WS

EVS — všichni

- Konverze MOSS i externích dokumentů do pdf formátu a připojení kvalifikovaného podpisu s časovým razítkem.
- Podpora razítek NPM
- Odeslání konvertovaného dokumentu spisové službě

Rozhraní LJIP Realizována WS

Rozhraní SKS Komunikace přes rozhraní

Rozhraní GINIS Realizována WS

Rozhraní ISIR Realizována WS

Jednotlivé aplikace (využívající obecné moduly)

SC – Správa čísel (číslovací plány) — 610

Správní řízení k přidělování čísel
- vedení spisu o přidělení (změně přidělení) čísel
- kontrola duplicity a typu čísla
- evidence poplatků za čísla včetně přeplatků a nedoplatků

Evidence formátů čísel (strom) a přiřazení
- definování formátů čísel
- evidence přiřazení a následných změn v přiřazení čísel (bloků) podnikatelům
- evidence blokací čísel
- publikace na web

EPEK – Evidence podnikatelů v elektronických komunikacích — oblasti, 610

Evidence osob oprávněných k podnikání
- subjekty včetně přidělování IČO
- hlášené sítě a služby, oprávněné osoby, historie
- číselník sítí a služeb
- seznamy podnikatelů, publikace na web

Řízení k oznámení činnosti
- vedení spisu o oznámení / změně / ukončení činnosti
- evidování hlášených služeb (změn)
- vydávání osvědčení

EPPS – Evidence podnikatelů v poštovních službách — 610

Evidence osob oprávněných k podnikání
- subjekty včetně přidělování IČO
- hlášené služby, oprávněné osoby, historie
- číselník služeb
- seznamy podnikatelů, publikace na web

Řízení k oznámení činnosti
- vedení spisu o oznámení / změně / ukončení činnosti
- evidování hlášených služeb (změn)
- vydávání osvědčení

BMIS – Evidence sítí — oblasti, 620

Evidence sítí - není správním řízením
- evidence údajů z podání
- evidence údajů o provozovatelích
- evidence údajů o stanici
- sestavy a publikování na web

US – Univerzální služba — 611

Správní řízení ke stanovení výše čisté ztráty

Řízení ke stanovení tržního podílu plátců (opatření obecné povahy)

Správní řízení ke stanovení příspěvku

Evidence příjemců dotací a kontrola oprávněnosti

S1 – Účastnické spory — oblasti

Správní řízení k účastnickým sporům (dluhy, námitky)
- vedení spisu
- evidence dat řízení relevantních pro danou věc
- hromadné zpracování činností nad více spisy

Automatizované zpracování elektronických podání
- identifikace ve spisové službě a zpracování
- ztotožnění účastníků v ISZR
- rozpad dat dle aktuálního data zpracování

S2 – Správní řízení II. stupeň — 603

Správní řízení ve 2. instanci
- vedení druhoinstančního spisu (odvolání, rozklad, mim. opr. prostředky)
- automatické přebírání dat z prvního stupně
- jednání komise, vyznačování rozhodnutí do prvostupňových spisů
- evidence soudních jednání

ST - Správní trestání — všichni

Správní řízení pro uložení pokut
- zakládání řízení i z podnětů z ASMKS či PSD
- evidence prohřešku včetně příslušného pokutovacího paragrafu
- vytváření předpisu před nabytím právní moci
- sledování úhrady po nabytí právní moci a případná příprava spisu k vymáhání

NPS – Námitky — oblasti

Správní řízení k námitkám v poštovních službách
- vedení spisu
- evidence dat řízení relevantních pro danou věc

VP – Vymáhání pohledávek — všichni

Obecně
- zahajování řízení nad pohledávkami po splatnosti
- možnost spojování pohledávek
- sledování dluhů po splatnosti, 6 a 20 letých lhůt

Výzva k úhradě
- poslední upomínka před vymáhacím procesem

Posečkání
- možnost odložení platby a splátkový kalendář

Zjišťování majetku
- obesílání za účelem zjištění majetku dlužníka

Insolvenční řízení
- přihláška do insolvenčního řízení a sledování jeho průběhu

Exekuce (zaměstnavatel, banka, externí…)
- vedení exekučního spisu včetně nákladů exekuce

Odpis
- odpis části či celého dluhu

PSD – Podněty, stížnosti a dotazy — všichni

Řešení podnětů, stížností a dotazů od občanů na elektronické komunikace a poštovní služby - není správním řízením
- zahájení řízení s neznámým obyvatelem (neověřen v ISZR)
- komunikace emailem
- evidence dat příslušejících zvolené tematické oblasti
- možnost vytvořit podnět pro správní trestání
- předání věci kompetentnímu orgánu
- možnost vyřešit věc odpovědí

OZ - Odborná způsobilost — 613, 631, 638

Plánování termínů zkoušek odborné způsobilosti
- příprava, změna, rušení a vyhodnocování termínů zkoušek

Vydávání a prodlužování průkazů odborné způsobilosti
- evidence přihlášek ke zkouškám, zvaní na termín, výsledky
- tisk a vydávání průkazů OZ, prodlužování, tvorba duplikátů

Smlouva o zpracování osobních údajů

uzavřená podle čl. 28 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“)

mezi těmito smluvními stranami:

1. Česká republika – Český telekomunikační úřad

Se sídlem:	Sokolovská 58/219, Vysočany, 190 00 Praha 9
Adresa pro doručování:	poštovní přihrádka 02, 225 02 Praha 025
ID datové schránky:	a9qaats
Bankovní spojení:	ČNB Praha
Číslo účtu:	725001/0710
IČO:	701 06 975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
Jejímž jménem jedná:	Ing. Marek Ebert, předseda Rady ČTÚ

(dále jen „objednatel“) na straně jedné

a

2. Seyfor, a.s.

Se sídlem:	Drobného 555/49, Ponava, 602 00 Brno
Zastoupená:	Petrem Francem, MBA, MSc., členem představenstva
ID datové schránky:	46mti92
Bankovní spojení:	Raiffeisenbank a.s.
Číslo účtu:	6253399002/5500
IČO:	015 72 377
DIČ:	CZ01572377

Zapsaná v Obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 7072

(dále jen „poskytovatel“) na straně druhé,

společně označované také jako „smluvní strany“ nebo jednotlivě též jako „smluvní strana“.

1.Objednatel
Úvodní ustanovení

1. Poskytovatel se na základě smlouvy č. CTU/2024_0057 o zajištění jeho podpory, údržby a rozvoje IS MOSS/SKS, uzavřené mezi smluvními stranami (dále jen „Smlouva“), zavázal poskytnout plnění tak, jak je uvedeno v článku 1 Smlouvy a v článcích navazujících. Při plnění předmětu Smlouvy může docházet k práci s osobními údaji. Osobními údaji se pro účely této smlouvy o zpracování osobních údajů (dále jen „Zpracovatelská smlouva“) rozumí osobní údaje nebo jakékoli identifikátory subjektů údajů, kterými jsou zejména zaměstnanci a pracovníci objednatele v Informačním systému Modulární správní systém/Společný katalog subjektů (dále jen „IS MOSS/SKS“), subjekty údajů, o kterých IS MOSS/SKS uchovává data a další subjekty údajů, jejichž osobní údaje byly poskytovateli předány či případně zpřístupněny pro účel poskytování plnění dle Smlouvy (dále také „Osobní údaje“).
2. V rámci poskytování plnění může docházet ke zpracování Osobních údajů poskytovatelem. Tato Zpracovatelská smlouva upravuje podmínky zpracování osobních údajů objednatelem jako správcem Osobních údajů a poskytovatelem jako zpracovatelem Osobních údajů ve smyslu čl. 28 GDPR.

3. Není-li v této Zpracovatelské smlouvě stanoveno jinak, mají pojmy použité s velkým počátečním písmenem stejný význam jako ve Smlouvě. Pro vyloučení pochybností se pod IS MOSS/SKS rozumí pojem tak, jak je definován v předmětu plnění Smlouvy.

2.
Úlohy a pokyny pro zpracování údajů

1. Smluvní strany berou na vědomí a souhlasí s tím, že:
   a) Poskytovatel je zpracovatelem Osobních údajů,
   b) Objednatel je správcem, případně zpracovatelem Osobních údajů,
   a) obě smluvní strany se zavazují plnit své povinnosti vyplývající z platných právních předpisů, které se vztahují na zpracování Osobních údajů.
2. Poskytovatel bude zpracovávat Osobní údaje pouze v souladu s platnými právními předpisy a za účelem:
   a) poskytování plnění pro objednatele, a
   b) jak bude dále uvedeno v dalších písemných pokynech udělených objednatelem.
3. Za písemný pokyn dle odstavce 2 písm. b) tohoto článku Zpracovatelské smlouvy se považuje také pokyn učiněný prostřednictvím komunikačních nástrojů uvedených ve Smlouvě.

3.
Doba trvání zpracování osobních údajů

Poskytovatel bude Osobní údaje zpracovávat pouze po dobu trvání Smlouvy nebo do doby výmazu všech Osobních údajů ze strany poskytovatele dle této Zpracovatelské smlouvy, a to vždy na základě jednoznačného požadavku objednatele k provedení této činnosti.

4.
Povaha a účel zpracování osobních údajů

1. Poskytovatel může pro účely poskytování plnění objednateli zpracovávat Osobní údaje, a to výhradně v elektronické formě, přičemž předmětem zpracování může být i migrace dat, analýza, tvorba rozhraní a dokumentace a další činnosti potřebné pro poskytování plnění.
2. Účelem zpracování osobních údajů bude poskytování plnění.

5.
Druhy osobních údajů

Předmětem zpracování podle této Zpracovatelské smlouvy budou všechny Osobní údaje, které jsou uchovávány v IS MOSS/SKS, a k jejichž zpracování byl na základě písemného zmocnění či Zpracovatelské smlouvy poskytovatel pověřen. Objednatel vždy vymezí rozsah a účel pověření, dobu zpřístupnění a případná bezpečnostní opatření a zapojení dalších osob odlišných od autorizovaných osob poskytovatele.

6.
Kategorie subjektů údajů

1. Osobní údaje se budou týkat těchto kategorií subjektů údajů:
   a) zaměstnanci a pracovníci objednatele;
   b) uživatelé IS MOSS/SKS;

c) subjekty údajů, o kterých IS MOSS/SKS uchovává data;

d) další subjekty údajů, jejichž osobní údaje byly poskytovateli předány pro účel poskytnutí plnění dalších povinností dle Smlouvy.

7.
Práva a povinnosti smluvních stran

1. Poskytovatel prohlašuje a zavazuje se, že:

   a) dozví-li se o porušení nebo hrozícím porušení zabezpečení Osobních údajů, náhodném nebo protiprávním zničení, ztrátě, změně nebo neoprávněném poskytnutí či zpřístupnění zpracovávaných Osobních údajů, neprodleně, nejpozději však do 24 hodin, písemně informuje objednatele a co nejlépe popíše vzniklé či hrozící bezpečnostní riziko, přičemž objednateli sdělí vhodná opatření pro zabránění nebo minimalizaci porušení zabezpečení osobních údajů a přijme veškerá potřebná opatření pro minimalizaci škody;

   b) bude Osobní údaje zpracovávat pouze v rámci EU či EHP;

   c) Osobní údaje budou zabezpečeny v souladu s článkem 8 této Zpracovatelské smlouvy;

   d) Osobní údaje bude zpracovávat pouze v souladu s touto Zpracovatelskou smlouvou, nebo na základě jiných písemných pokynů objednatele; pro případné další účely zpracování je nutný vždy předchozí písemný souhlas objednatele;

   e) Přijme vhodná přiměřená organizační a technická opatření, jejichž cílem je, aby osoby, které se budou na straně poskytovatele podílet na plnění této Zpracovatelské smlouvy, při styku nebo nakládání s Osobními údaji nepořizovaly kopie Osobních údajů bez předchozího písemného souhlasu objednatele a aby jejich činností nebo opomenutím nedošlo k náhodnému nebo protiprávnímu zničení, ztrátě či pozměnění Osobních údajů, nebo k jejich neoprávněnému zpřístupnění třetím osobám;

   f) bude objednateli nápomocen při zavádění a udržování vhodných technických a organizačních opatření k zabezpečení Osobních údajů, při ohlašování porušení zabezpečení osobních údajů dozorovému úřadu nebo subjektu údajů, při posuzování vlivu na ochranu osobních údajů a při předchozích konzultacích s dozorovým úřadem;

   g) zajistí objednateli prostřednictvím vhodných technických a organizačních opatření součinnost, nejpozději do 14 dnů od vznesení požadavku objednatele, pro splnění objednatelovy povinnosti reagovat na žádosti o výkon práv subjektu údajů či poskytnutí informace o zpracování osobních údajů;

   h) poskytne objednateli na jeho žádost bez zbytečného odkladu, nejpozději však do 10 pracovních dnů od doručení takovéto žádosti, veškerou součinnost nutnou k prokázání, že jsou Osobní údaje dostatečně organizačně a technicky zabezpečeny a poskytne veškerou součinnost v případech, kdy je u objednatele zahájena kontrola dozorového orgánu a zaváže k této povinnosti i své pracovníky, od kterých bude potřebná součinnost;

2. Pokud poskytovatel při zpracovávání Osobních údajů obdrží od subjektu údajů ve vztahu k Osobním údajům jakoukoliv žádost, sdělí poskytovatel subjektu údajů, aby se s žádostí obrátil přímo na objednatele. Poskytovatel se zavazuje poskytnout objednateli veškerou součinnost potřebnou pro vyřízení práva subjektů údajů.

3. Poskytovatel se zavazuje nevyužívat pro zpracování Osobních údajů jakéhokoliv dalšího zpracovatele bez předchozího písemného povolení objednatele a v případě zapojení těchto dalších zpracovatelů tyto smluvně zaváže, aby dodržovali stejné povinnosti na ochranu údajů, jaké jsou uvedeny v této Zpracovatelské smlouvě. Poskytovatel se rovněž zavazuje nesdělovat a nezpřístupňovat Osobní údaje třetím stranám a poddodavatelům, kteří nejsou uvedeni v žádné z příloh Smlouvy bez předchozího

písemného souhlasu objednatele. Objednatel vždy souhlasí se zapojením dalších zpracovatelů, kteří jsou výslovně uvedeni ve Smlouvě.

4. Poskytovatel je povinen umožnit objednateli či jím pověřené osobě kontrolu (včetně auditu či inspekce, dále jednotně označované také jen „audit“), dodržování této Zpracovatelské smlouvy, zejména povinností pro zpracování Osobních údajů z nich vyplývajících, a k těmto kontrolám přispěje dle důvodných pokynů objednatele či kontrolující osoby. Poskytovatel je povinen zajistit možnost provedení kontroly také u osob, které se společně s poskytovatelem podílejí na plnění povinností dle této Zpracovatelské smlouvy tím, že je písemně zaváže, aby objednateli umožnily provedení kontroly zpracování Osobních údajů, a splnění této povinnosti na nich bude k žádosti objednatele písemně vymáhat.

5. Jakoukoliv žádost o audit je objednatel povinen zaslat písemně poskytovateli. Po obdržení žádosti o audit se poskytovatel a objednatel dopředu dohodnou na:

   a) možném termínu provedení auditu, bezpečnostních opatřeních a způsobu zajištění dodržení závazků mlčenlivosti během auditu, a

   b) předpokládaném začátku, rozsahu a době trvání auditu.

   V případě, že k dohodě nedojde ani do 30 dnů ode dne odeslání žádosti, určí podmínky auditu objednatel. Právo jednostranně určit podmínky kontroly, resp. auditu na základě předchozí věty tohoto odstavce, může objednatel uplatnit jednou za kalendářní rok.

6. Poskytovatel může vznést písemné námitky proti jakémukoliv auditorovi, který byl pověřen objednatelem, pokud není auditor podle názoru poskytovatele dostatečně kvalifikován, není nezávislý, je v soutěžním postavení vůči poskytovateli nebo je jinak zjevně nevhodný. Na základě vznesené námitky má objednatel povinnost pověřit jiného auditora, nebo provést audit sám. Objednatel se zavazuje osoby jím pověřené kontrolou a jím pověřené auditory písemně zavázat, aby zachovávali mlčenlivost o všech skutečnostech, o kterých se v souvislosti se svou činností u poskytovatele dozví, nebo k nimž získají přístup, nepořizovali kopie žádných dokumentů či záznamy z nich bez předchozího písemného souhlasu poskytovatele, a aby po celou dobu provádění kontroly (auditu,) jejich činností nebo opomenutím nedošlo k náhodnému nebo protiprávnímu zničení, ztrátě či pozměnění žádných dokumentů, nebo k jejich neoprávněnému zpřístupnění třetím osobám. Bez předchozího písemného souhlasu poskytovatele jsou objednatelem pověření auditoři a osoby pověřené kontrolou oprávněni pořizovat záznamy dokládající porušení povinností týkajících se zpracování Osobních údajů na základě Zpracovatelské smlouvy, která zjistí v rámci auditu; o rozsahu pořízených záznamů však musí poskytovatele bezodkladně písemně vyrozumět a k jeho žádosti mu předložit pořízené záznamy k nahlédnutí.

7. Poskytovatel může být v souvislosti s kontrolou písemně požádán o předložení svých písemných technických a organizačních bezpečnostních opatření v souvislosti s poskytováním plnění, přičemž má povinnost této výzvě vyhovět.

8. Objednatel je odpovědný za plnění všech povinností ve vztahu ke zpracování Osobních údajů, zejména za řádné informování subjektů údajů o zpracování Osobních údajů, získání souhlasu se zpracováním Osobních údajů, pokud je zapotřebí, vyřizování žádostí subjektů údajů, týkajících se realizace jejich práv (jako je právo na informace, přístup, opravu, výmaz, omezení zpracování, vznést námitku apod.).

8.
Bezpečnost osobních údajů

1. Poskytovatel přijal níže uvedená opatření a zavazuje se je udržovat pro zajištění zabezpečení zpracování Osobních údajů po celou dobu zpracování.

2. Organizační opatření:

a) Poskytovatel a pracovníci poskytovatele jsou pravidelně školeni na zásady a principy ochrany osobních údajů a kybernetickou bezpečnost;

c) Poskytovatel a pracovníci poskytovatele jsou zavázáni k mlčenlivosti v souvislosti s prací s Osobními údaji;

d) povinnost poskytovatele hlásit jakékoliv kybernetické bezpečnostní incidenty související s poskytováním plnění.

3. Technická opatření:

a) smluvní strany konstatují, že na jejich smluvní vztah se vztahují požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

b) kontrola a monitorování a zajištění přístupu do IS MOSS/SKS umožňující přesné zaznamenání, kdo měl možnost s Osobními údaji pracovat;

c) ochrana pracovních zařízení poskytovatele prostřednictvím vhodného antivirového programu a prostředku firewall, příp. dalšími technickými ochrannými prostředky;

d) zajištění dvoufaktorové identifikace a autentizace na pracovních stanicích poskytovatele, které mají přístup do IS MOSS/SKS.

4. Poskytovatel zabezpečí plnění před kybernetickými útoky nejvhodnějším způsobem s přihlédnutím k povaze Osobních údajů a stavu techniky. Poskytovatel se zároveň zavazuje přijmout veškerá vhodná opatření v souladu s čl. 32 GDPR tak, aby s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, zajistil úroveň zabezpečení odpovídající danému riziku. Poskytovatel současně odpovídá za poškození Osobních údajů třetí stranou, pokud se prokáže, že nebyly odpovědně zabezpečeny v souladu s tímto článkem Zpracovatelské smlouvy.

9.
Předání osobních údajů po skončení zpracování

Po skončení smlouvy bez ohledu na způsob a důvod jejího skončení je poskytovatel povinen všechny Osobní údaje včetně dalších kategorií chráněných údajů a souvisejících metadat předat objednateli včetně všech existujících kopií a Osobní údaje včetně všech dalších kategorií chráněných údajů a souvisejících metadat na všech ostatních zařízeních a nosičích mimo zařízení a nosičů ve vlastnictví či užívání objednatele trvale zničí, s výjimkou případů, kdy je uložení Osobních údajů vyžadované právem České republiky nebo Evropské unie. Provedení likvidace Osobních údajů a dalších kategorií chráněných údajů a souvisejících metadat, je poskytovatel povinen doložit objednateli vhodným způsobem, z něhož bude vyplývat přesně definovaný způsob likvidace konkrétních údajů či metadat.

10.
Další ujednání

1. Poskytovatel není oprávněn vyúčtovat objednateli vynaložené náklady spojené s vyřizováním jakékoliv žádosti, uvedené v článku 7 této Zpracovatelské smlouvy a není

oprávněn požadovat dodatečnou odměnu za zpracování osobních údajů při poskytování plnění.

2. V případě prodlení se splněním jakékoli lhůty dle této Zpracovatelské smlouvy se poskytovatel zavazuje objednateli uhradit smluvní pokutu ve výši 5.000 Kč za každý započatý den prodlení.
3. V případě porušení povinností poskytovatele dle článku 7, 8 či 9 této Zpracovatelské smlouvy případně jiných povinností poskytovatele vyplývajících z této Zpracovatelské smlouvy se poskytovatel zavazuje objednateli uhradit smluvní pokutu ve výši 50.000 Kč za každé jednotlivé porušení.
4. Smluvní pokuta je splatná okamžikem porušení příslušné povinnosti. Dnem splatnosti smluvní pokuty se rozumí den, kdy musí být částka odpovídající její výši připsána ve prospěch účtu objednatele. Uhrazení smluvní pokuty nevylučuje nárok na náhradu škody v plné výši.
5. Poruší-li poskytovatel či osoba, která spolupracuje s poskytovatelem při poskytování Služeb (poddodavatel) kteroukoliv povinnost týkající se či související se zpracováním Osobních údajů, ať již vyplývá z GDPR či jiných předpisů či ze Zpracovatelské smlouvy, a objednateli bude v důsledku takového porušení pravomocně uložena pokuta, zejména ze strany Úřadu pro ochranu osobních údajů, ačkoli objednatel o zahájení takovéhoto řízení poskytovatele bezodkladně písemně vyrozuměl a v řízení použil řádně a včas veškeré věcné argumenty, doklady a důkazy získané zákonným způsobem, jejichž uplatnění nezakládá protiprávní jednání, které mu za tímto účelem poskytovatel poskytl tak, aby mohly být včas použity, zavazuje se poskytovatel na výzvu objednatele, k níž bude dále přiloženo rozhodnutí o uložení pokuty, uhradit objednateli peněžitou náhradu ve výši uložené pokuty, a to bez zbytečného odkladu po prokázání zavinění poskytovatele ve vztahu k porušení, za které byla objednateli pravomocně uložena pokuta, a obdržení písemné výzvy k zaplacení, nejpozději však do 5 pracovních dní od tohoto prokázání a obdržení písemné výzvy.
6. Poruší-li poskytovatel či osoba, která spolupracuje s poskytovatelem při poskytování plnění (poddodavatel) kteroukoliv povinnost týkající se či související se zpracováním Osobních údajů, ať již vyplývá z GDPR či jiných předpisů či ze Zpracovatelské smlouvy, a je-li prokázán vznik materiální či nemateriální újmy třetí osobě jako subjektu údajů v příčinné souvislosti s takovým porušením a objednatel uhradí této poškozené třetí osobě pohledávku na náhradu materiální či nemateriální újmy, zavazuje se poskytovatel na výzvu objednatele uhradit objednateli peněžitou náhradu ve výši uplatněné materiální či nemateriální újmy ze strany třetí osoby, a to bez zbytečného odkladu po prokázání zavinění poskytovatele ve vztahu ke vzniklé újmě a takovémuto porušení a obdržení písemné výzvy k zaplacení, nejpozději však do 5 pracovních dní od tohoto prokázání a obdržení písemné výzvy, a to za podmínky, že objednatel poskytovatele o uplatnění takovéhoto nároku bezodkladně písemně vyrozuměl a použil na obranu proti takovémuto nároku řádně a včas veškeré věcné argumenty, doklady a důkazy získané zákonným způsobem, jejichž uplatnění nezakládá protiprávní jednání, které mu za tímto účelem poskytovatel poskytl tak, aby mohly být včas použity.
7. Smluvní strany se dohodly, že porušením kterékoliv povinnosti poskytovatele plynoucí z právních předpisů v oblasti bezpečnosti informací a ochrany osobních údajů, zejména ze zákona a vyhlášky o kybernetické bezpečnosti, GDPR či dalších právních předpisů či ze Zpracovatelské smlouvy, představuje podstatné porušení smlouvy, jestliže v příčinné souvislosti s ním došlo ke vzniku materiální či nemateriální újmy objednateli, nebo třetí osobě, která není nevýznamná. Smluvní strany shodně prohlašují, že za nevýznamnou újmu považují materiální či nemateriální újmu, která nepřevyšuje částku 500.000 Kč.

8. Tato Zpracovatelská smlouva je vyhotovena elektronicky a bude podepsána zaručeným elektronickým podpisem oprávněnými zástupci smluvních stran.
9. Tato Zpracovatelská smlouva vzniká dnem podpisu oprávněnými zástupci obou smluvních stran a nabývá účinnosti uveřejněním této smlouvy 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 zajistí objednatel. Smluvní strany jsou povinny se navzájem informovat o veškerých skutečnostech důležitých pro plnění této smlouvy včetně změn kontaktních osob.

V Brně dne	V Praze dne
Poskytovatel:	Objednatel:
……..……	……..……
Petr Franc, MBA, MSc. člen představenstva Seyfor, a.s.	Ing. Marek Ebert předseda Rady Českého telekomunikačního úřadu

Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Vymezení pojmů

Pro potřeby této přílohy smlouvy jsou použity následující zkratky a pojmy:

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

VoKB – vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) v platném znění

Kybernetické požadavky – kybernetickými požadavky se rozumí všechny bezpečnostní požadavky ve smyslu ZoKB a VoKB,

Produkční prostředí – produkčním prostředím se rozumí prostředí běžně přístupné uživatelům IS ČTÚ v ostrém provozu,

Testovací prostředí – prostředí určené k provádění testů, vzdělávání uživatelů apod, a to v podobě, nastavení a rozsahu umožňujícím účinně zkoumat funkcionality testovacích verzí IS ČTÚ,

Prostředí objednatele – fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku objednatele anebo logický perimetr definovaný hraničními síťovými prvky ve správě nebo majetku objednatele,

Osoba na straně poskytovatele – fyzická osoba podílející se na poskytování předmětu plnění a mající pracovněprávní či obdobný smluvní vztah s poskytovatelem nebo jeho poddodavateli,

Osobní údaje – každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat,

Zpracování osobních údajů – Jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

1. ÚVODNÍ USTANOVENÍ

1.1 Z důvodu nutnosti plnění povinností stanovených objednateli jakožto povinné osobě ve smyslu VoKB je poskytovatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této přílohy smlouvy. Účelem této přílohy smlouvy tak je dodržet povinnost objednatele dle § 4 odst. 4 ZoKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s poskytovatelem.

1.2 Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy v oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je objednatel oprávněn požadovat od poskytovatele přiměřenou součinnost i nad rámec povinností stanovených v této příloze smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

2. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

2.1 Poskytovatel je povinen se v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně poskytovatele při poskytování předmětu plnění dle smlouvy.

b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy objednateli zpřístupnit.

d) Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

2.2 Poskytovatel je dále povinen dodržovat bezpečnostní politiku objednatele, byl-li s ní prokazatelně seznámen.

3. ŘÍZENÍ AKTIV

3.1 Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

a) Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, hardware prvky – infrastruktura hlasové a datové komunikace,

aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení apod.), a tato aktiva strukturovaně popsat a objednateli předložit následně na vyžádání, a to po celou dobu trvání smlouvy.

4. ŘÍZENÍ RIZIK

4.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle smlouvy.

b) V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro objednatele nebo změn spravovaných aktiv) vytvořit a bude-li to objednatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:

i) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;

ii) Identifikaci a hodnocení rizik s vazbou na předmět plnění;

iii) Realizovaná bezpečnostní opatření;

iv) Nepokrytá bezpečnostní rizika a návrh opatření;

v) Vyhodnocení bezpečnostních událostí a incidentů;

vi) Aktuální stav souladu poskytovatele s kybernetickými požadavky včetně přehledu kybernetických požadavků, které:

- nebyly aplikovány, včetně odůvodnění, a
- byly aplikovány, včetně způsobu plnění.

5. ORGANIZAČNÍ BEZPEČNOST

5.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Jmenovat nejpozději do 30 dnů po uzavření smlouvy odpovědnou kontaktní osobu/y pro potřeby zajištění plnění kybernetických požadavků a související komunikace mezi smluvními stranami (dále jen „kontaktní osoba pro kybernetickou bezpečnost“). Kontaktní osobu/y pro kybernetickou bezpečnost sdělí poskytovatel písemně objednateli v téže lhůtě.

b) Využívat pro poskytování předmětu plnění dle smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních předpisů objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle smlouvy a stanovit bezpečnostní role těchto oprávněných osob s jasně definovanými odpovědnostmi a pravomocemi.

6. ŘÍZENÍ DODAVATELŮ

6.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Využívá-li při poskytování předmětu plnění dle smlouvy subdodavatele, zajistit v obdobném rozsahu dodržování kybernetických požadavků rovněž ve smluvních vztazích se svými subdodavateli.

b) Dodržovat podmínky při zpracování osobních údajů pro zapojení každého dalšího poskytovatele.

7. BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 9 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit, aby kontaktní osoba pro kybernetickou bezpečnost nejpozději do 60 dnů od uzavření smlouvy potvrdila písemně objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle smlouvy za poskytovatele byly prokazatelně seznámeny s těmito kybernetickými požadavky a příslušnými ustanoveními interních předpisů objednatele.

b) Dodržovat příslušná ustanovení interních předpisů objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje:

i) školení pracovníků poskytovatele zajištěné objednatelem

ii) protokolární či elektronické předání příslušných předpisů nebo

iii) objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy, jejichž konkrétní jmenovitý seznam bude poskytovateli – současně s poskytnutím přístupu – protokolárně předán.

c) Při provádění dohledu nad předmětem plnění dle smlouvy, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění dle smlouvy.

d) Zajistit, aby osoby podílející se na poskytování plnění objednateli v prostředí/nebo s prostředky objednatele:

i) pro uložení a sdíleni dat a informací objednatele využívaly pouze k tomu schválené prostředky (aktiva);

ii) neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující dobré jméno objednatele;

iii) nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;

iv) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

v) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani ke zdrojům jiných subjektů;

vi) nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků objednatele, a to ani v případě, kdy jim byl prostředek objednatele svěřen do správy;

vii) nepodílely se s prostředky objednatele na šíření spamu ani škodlivého softwaru,

a to i tehdy, pokud jsou prostředky objednatele používány mimo jeho prostředí.

7.2 Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům objednatele je na straně objednatele zpracování osobních údajů pověřených osob poskytovatele, které se podílejí na poskytování plnění dle smlouvy. Pokud nebude objednateli umožněno osobní údaje pověřených osob poskytovatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům objednatele.

7.3 Poskytovatel je dále povinen:

a) Prohlubovat znalostí osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

b) Stanovit práva a povinnosti osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

8. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 10 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění dle smlouvy.

b) Na vyžádání ve lhůtě, která nebude kratší než 10 pracovních dnů, poskytnout objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

c) Zajistit, že pro poskytování předmětu plnění dle smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou legislativou, a to především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů).

8.2 Poskytovatel je dále povinen provést a zabezpečit dodržování následujících opatření:

a) Implementaci procesů pro řízení ICT (tj. řízení incidentů, řízení změn, řízení životního cyklu systémů apod.).

b) Zavedení postupů pro ochranu proti škodlivému kódu včetně řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle smlouvy.

c) Zavedení pravidel a postupů pro ochranu informací a dat.

d) Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv a pracovní postupy pro řešení mimořádných stavů.

e) Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění dle smlouvy.

9. ŘÍZENÍ ZMĚN

9.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 11 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Přiměřeně reagovat na změny v oblasti kybernetické bezpečnosti na straně objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

b) Aktivně spolupracovat při testování významné změny v oblasti kybernetické bezpečnosti na straně objednatele.

10. ŘÍZENÍ PŘÍSTUPU

10.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele.

b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu poskytovatele. V opačném případě musí poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit objednateli kdykoli v průběhu trvání účinnosti této smlouvy a tři měsíce po jejím ukončení, ve lhůtě, která nebude kratší než 6 pracovních dnů.

c) Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou, 1 rok, 1 měsíc apod).

d) Zajistit, aby osoby podílející se na poskytování předmětu plnění dle smlouvy a mající přístup k informačním aktivům objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

e) Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně poskytovatele, které přistupují do prostředí objednatele.

10.2 Poskytovatel bere na vědomí, že oprávnění přístupu k systémům ICT objednatele je možné povolit pouze fyzické identitě zaměstnance poskytovatele/subdodavatele, a to na základě příslušného požadavku poskytovatele.

10.3 Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.

10.4 Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet objednatelem zablokován a řešen jako bezpečnostní incident a dále mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům objednatele).

11. AKVIZICE, VÝVOJ A ÚDRŽBA

11.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, pokud jsou předmětem plnění dle smlouvy či jeho součástí.

b) Není-li Smlouvou stanoveno jinak, předat při ukončení smlouvy objednateli kompletní provozní a bezpečnostní dokumentaci předmětu plnění dle smlouvy. Ta musí být předána minimálně v následujícím rozsahu:

   i) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

   ii) dokumentaci obsahující popis autorizačního konceptu a oprávnění;

   iii) dokumentaci obsahující instalační a konfigurační postupy;

   Výše uvedenou dokumentaci poskytovatel předá objednateli v přiměřené lhůtě, nejpozději pak dle předchozí dohody smluvních stran.

11.2 V případě, že předmět plnění dle smlouvy zahrnuje částečně i vývoj softwaru, je poskytovatel povinen:

a) Dodržovat a implementovat obecně uznávané „nejlepší praktiky“ pro bezpečný vývoj softwaru. Základním pravidlem zde je myslet na bezpečnost softwaru ve všech jeho vývojových fázích.

b) Na vyžádání alespoň 6 pracovních dnů předem umožnit objednateli audit prováděného nebo provedeného plnění a na písemnou žádost objednatele předložit ve stanovené lhůtě vyvíjený zdrojový kód na provedení tzv. codereview, a to především za účelem ověření skutečnosti, zda poskytovatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito bezpečnostními požadavky.

c) Poskytovat objednateli v termínech stanovených objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru (nejdříve však od zahájení testovacího provozu) či kdykoli po jeho předání.

d) Pokud je součástí plnění dle smlouvy i instalace operačního systému, případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v testovacím prostředí či produkčním prostředí objednatele.

e) Zajistit bezpečnost testovacího prostředí u poskytovatele a ochranu poskytnutých testovacích dat objednatelem.

f) Zajistit, že v rámci poskytovaného plnění bude dodávaný software

   i) v souladu s bezpečnostními politikami a standardy objednatele;

   ii) otestován na soulad s bezpečnostními politikami objednatele, pokud byl s takovými bezpečnostními politikami prokazatelně seznámen.

g) Instalovat software pouze na základě předem schválených migračních postupů objednatelem.

h) Předat zdrojový kód objednateli bezpečnou formou zajišťující jeho integritu.

i) Zajistit řízení verzí zdrojového kódu, jeho zálohování a jeho uložení mimo produkční prostředí.

12. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

12.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 14 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy:

a) Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů.

b) Bez zbytečného odkladu hlásit objednateli všechny kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím kontaktní osoby pro kybernetickou bezpečnost.

c) Vyhodnocovat informace o kybernetických bezpečnostních incidentech a uchovávat je pro budoucí použití, a to s ohledem na požadavky použitelné platné a účinné legislativy.

d) V případě vzniku kybernetické bezpečnostní události a následného zvládání a vyhodnocování možného kybernetického bezpečnostního incidentu a/nebo v případě podezření na možný kybernetický bezpečnostní incident poskytnout objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či podezřelém jednání osob na straně poskytovatele.

e) Spolupracovat při analýze příčin kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Zhotovitel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

f) Po dohodě s objednatelem realizovat bez zbytečného odkladu opatření požadovaná objednatelem ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení pokračování kybernetického bezpečnostního incidentu, nejpozději pak v termínech prokazatelně stanovených objednatelem.

12.2 Poskytovatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků, jehož příčina je na straně poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.

13. ŘÍZENÍ KONTINUITY ČINNOSTÍ

13.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění dle smlouvy.

b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu těchto aktiv zajistit dle sjednané SLA.

14. KONTROLA A AUDIT

14.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy poskytnout adekvátní součinnost při výkonu kontroly objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZoKB.

14.2 Poskytovatel umožní objednateli alespoň jednou ročně po dobu účinnosti smlouvy provedení auditu kybernetické bezpečnosti (dále jen audit) u poskytovatele a jeho případných subdodavatelů:

a) jehož rozsah bude ohraničen v rámci ICT prostředků poskytovatele používaných pro potřeby plnění smlouvy a uloženými či zpracovávanými daty a informacemi objednatele v ICT prostředí poskytovatele a

b) jehož předmětem bude naplnění kybernetických požadavků a vyhodnocení rizik dle bodu 4 této přílohy smlouvy.

14.3 Objednatel je oprávněn při provedení auditu využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za případnou způsobenou újmu.

14.4 Poskytovatel umožní objednateli audit provedený prostředky objednatele nebo třetí strany, a to v lokalitě poskytovatele i vzdáleně, pokud to technické prostředky poskytovatele umožňují.

14.5 Poskytovatel je povinen nedostatky zjištěné:

a) na základě provedení hodnocení rizik dle bodu 4 této přílohy smlouvy, nebo

b) v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této přílohy smlouvy

odstranit ve lhůtě určené v písemném oznámení objednatele, která nebude kratší než 20 pracovních dnů. Nestanoví-li objednatel lhůtu v písemném oznámení, zavazují se smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší 60 dnů.

14.6 Poskytovatel je dále povinen:

a) Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění kybernetických požadavků.

b) Na požádání s objednatelem konzultovat kdykoli v průběhu realizace plnění dle smlouvy detailní nastavení bezpečnostních opatření k naplnění kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

c) Neprodleně informovat objednatele o všech významných změnách v naplnění kybernetických požadavků, které nastanou kdykoli v průběhu trvání smlouvy.

d) Bezodkladně a s vyvinutím maximálního úsilí zajistit náhradní způsob naplnění kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.

e) Při výkonu své činnosti včas a prokazatelně upozornit objednatele na případnou zřejmou nevhodnost jeho příkazů či doporučení, vztahujících se ke kybernetickým požadavkům, jejichž následkem může vzniknout případná újma anebo nesoulad s příslušnými zákony nebo jinými obecně závaznými právními předpisy.

15. TECHNICKÁ OPATŘENÍ

15.1 Poskytovatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 VoKB, které musí splnit objednatel. Minimálně se poskytovatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

a) Dodržovat příslušné interní předpisy objednatele, s nimiž byl prokazatelně seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěna aktiva systémů ICT, anebo datové nosiče.

b) V rozsahu předmětu plnění dle smlouvy zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv objednatele, pokud s ní byl poskytovatel seznámen.

c) Realizovat bezpečnostní opatření pro odstranění nebo blokování komunikačních spojení, která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.

d) Realizovat přístupy z mobilních zařízení k aktivům v produkčním i testovacím prostředí objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).

e) Připojovat do produkčního prostředí objednatele pouze ta síťová zařízení (switch, wifi router apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně objednatele.

f) Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pakliže tento je součástí sjednaného rozsahu předmětu plnění dle smlouvy a je současně ve správě poskytovatele.

g) Na aktiva objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí objednatele následující typy nástrojů, pokud vysloveně nejsou součástí předmětu plnění dle smlouvy:

   i) Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

   ii) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

   iii) Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

   iv) Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do počítačového systému.

   v) Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje stávající bezpečnostní opatření v prostředí Objednatele.

h) Připojovat do prostředí objednatele pouze zařízení ICT, která splňují následující požadavky:

   i) jsou příslušným způsobem zabezpečena a chráněna proti malware a jinému škodlivému softwaru – minimálně instalovaný a aktivní antivir s aktuální definiční sadou, pokud možno instalované veškeré doporučené bezpečnostní záplaty pro OS a používaný SW, správně nakonfigurovaný a aktivní firewall;

   ii) způsob jejich připojení je definován v příslušné provozní nebo projektové dokumentaci nebo je v souladu s příslušnými interními předpisy objednatele.

i) Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.

j) Na vyžádání poskytnout objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu

předmětu plnění dle smlouvy, a to po celou dobu trvání Smlouvy a pak po dobu 2 let po jejím ukončení.

k) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

l) Pro veškeré on-line transakce realizované prostřednictvím webových technologií implementovat doporučené a schválené TLS/SSL certifikáty s cílem zajistit důvěrnost a integritu komunikace protistran.

m) Veškeré neveřejné informace poskytnuté objednatelem a ukládané na mobilní zařízení anebo přenosná paměťová média, která jsou ve správě poskytovatele, chránit vhodným šifrováním a proti neautorizovanému přístupu.

15.2 Poskytovatel bere na vědomí, že v případě, kdy technické spojení ze strany poskytovatele narušuje bezpečný chod ostatních služeb objednatele, může být toto spojení ze strany objednatele bez předchozího upozornění ihned ukončeno.

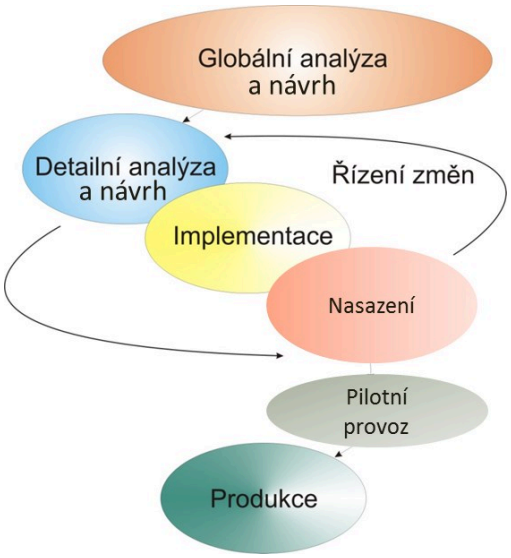
15.3 Poskytovatel bere na vědomí, že veškeré jeho aktivity a jeho plnění realizované v prostředí objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění smlouvy a v souladu s příslušnými interními dokumenty objednatele.

Obsah

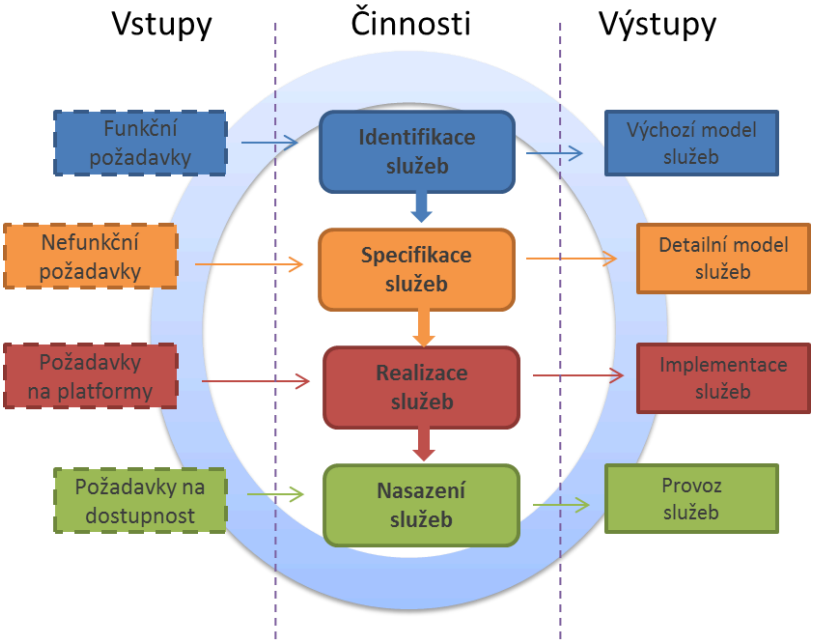
1 METODIKA ŘÍZENÍ IMPLEMENTACE

Životní cyklus vývoje systému vychází z metodiky Uchazeče pro vývoj aplikačního software. Metodika je založena na principech definovaných standardem ISO/IEC 12207. Uvedený standard definuje tři skupiny procesů, které probíhají v rámci životního cyklu informačního systému: základní, pomocné a organizační. Pro dodávku jsou podstatné především základní procesy vývoje. Pro základní procesy vývoje metodika zahrnuje etapy a doporučení dle rámce MMDIS (Multidimesional Management and Design of Information Systems).

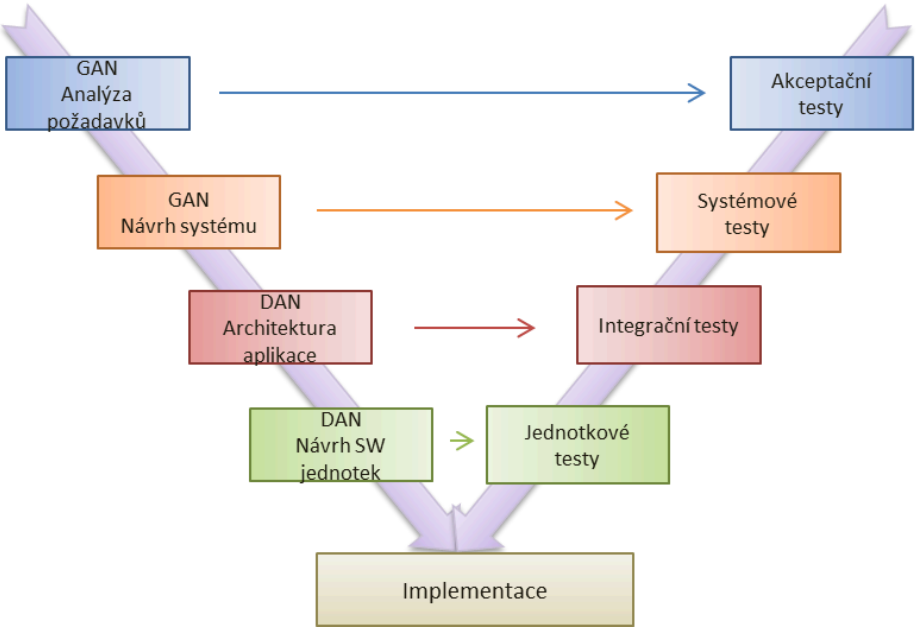
Etapy realizace systému jsou znázorněny na následujícím schématu. Globální analýza a návrh probíhá pro celý systém, další etapy vždy pro jednotlivá plnění Projektu (moduly/přírůstky).



Zároveň budou systémy vyvíjeny tak, aby výsledné produkty byly principiálně založené na architektuře orientované na služby (Service Oriented Architecture). Metodika vývoje je proto rozšířená o SOA principy vycházející z metodiky IBM RUP/SOMA© , jejíž schéma je uvedeno na následujícím obrázku.



Pro zajištění kvality metodika zahrnuje použití tzv. V-modelu – viz následující obrázek. Na levé straně schématu ve směru shora dolů jsou popsány aktivity, jejichž pomocí je upřesňováno zadání. Na pravé straně jsou pak ve směru zdola nahoru uvedeny příslušné úrovně testování, které mají ověřit, zda požadavky pro danou úroveň jsou splněny. Dno písmene pak reprezentuje vývoj dodávky.



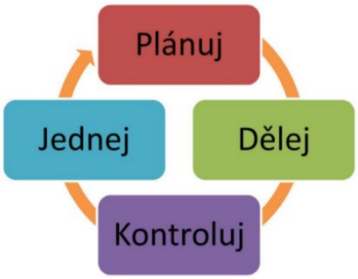
Množiny vstupních a výstupních požadavků spolu se závěrečnou revizí zajišťují, že výsledná dodávka splňuje požadavky zadání a Zadavatele tak, jak byly dohodnuty a zakotveny při analýze systému.

Metodický přístup k řešení projektu bude mít tři úrovně:

- Řídící - splňující požadavky Objednatele.
- Projektovou – metodika projektového řízení, podle níž bude projekt realizován.
- Implementační – metodika řízení postupu implementace.

Všechny úrovně musí být ve vzájemné vyvážené tak, aby bylo možné provádět cyklicky změny vyvolané novými požadavky nebo změnou prostředí.

Řídícím principem v rámci navrhovaného projektu je uplatnění PDCA přístupu (Plan-Do-Check-Act) obsahující čtyři fáze:



- **Plánuj** – vytvoření koncepce a návrh řešení
- **Dělej** – realizace prototypu
- **Kontroluj** – verifikace prototypu a zohlednění nových vlivů a požadavků
- **Jednej** – zapracování změn

V navrhované metodice není postup projetu striktně rozdělován na analytickou fázi a návrhovou fázi. Je postavena na tom, že v každé fázi probíhá jak analýza, tak návrh. Nicméně v souladu se zadávacími podmínkami jsou v metodice obě fáze zcela jasně definovány.

Jednotlivé výstupy implementace budou zpracovány zejména v souladu s následujícími mezinárodně uznávanými standardy a metodikami:

- The Open Group Architecture Framework (TOGAF) - architektonický rámec vyvíjen v rámci Open Group který je zaměřen na proces budování a udržování enterprise architektury;
- BPMN (Business Process Model and Notation) - standard pro modelování podnikových procesů. Jde o soubor principů a pravidel, který slouží pro grafické znázorňování podnikových procesů pomocí procesních diagramů;
- ArchiMate - vizualizační nástroj pro návrh enterprise architecture dle metodiky TOGAF;
- FURPS (Functionality, Usability, Reliability, Performance, Supportability) – metodika pro popis a validaci prioritních požadavků byznys zákazníka po porozumění jeho potřebám. Požadavky uvedené níže jsou strukturovány dle metodiky FURPS.

1.1 STRUČNÝ POPIS FÁZÍ REALIZACE SYSTÉMU

1.1.1 ANALYTICKÁ FÁZE

Popisuje systém na základě podporovaných procesů a katalogu požadavků Zadavatele do takové podrobnosti, aby bylo možné definovat technologickou a aplikační architekturu budoucího systému a celý systém rozdělit na samostatně realizovatelné části (přírůstky), specifikovat jejich rozhraní a rozhraní na okolní systémy.

Hlavní výstupy:

- Specifikace společné vize a koncepce celého systému,
- Specifikace funkčních a nefunkčních požadavků na celý systém a definice základních omezení požadovaného systému,
- Globální analytický (konceptuální) model systému,
- Návrh zajištění bezpečnosti systému,
- Specifikace vlivu systému na organizaci a procesy Zadavatele a dotčených externích subjektů,
- Definice globální architektury systému,
- Rozdělení realizace do samostatně realizovatelných částí systému (přírůstků).

Uvedené kroky a jejich výstupy jsou stručně popsány dále v obecné rovině a následně upřesněny pro klíčové části projektu.

Specifikace a koncepce celého systému

Vize projektu shrnuje vrcholové zadání projektu a slouží k dohodě všech zainteresovaných stran na předmětu řešení v rámci projektu. Rekapituluje hlavní cíle projektu, jaké problémy stávajícího stavu řeší, identifikuje všechny zainteresované strany a jejich zájmy a očekávání. Dále shrnuje předpoklady a omezení pro realizaci projektu, hlavní požadované vlastnosti systému a očekávané přínosy.

Specifikace požadavků na celý systém

Specifikace požadavků obsahuje seznam a popis funkčních a nefunkčních požadavků na celý systém. Jedná se především o:

- Zhodnocení současného stavu a skutečných informačních potřeb Zadavatele,
- Podrobnější popis požadavků ze zadání, tak aby bylo možné specifikovat hlavní skupiny požadovaných funkcí systému:
    - požadavky vrcholového vedení a liniových řídících pracovníků,
    - požadavky na funkce, data a schopnosti systému a základní uživatelské požadavky,
- Bezpečnostní cíle a požadavky na bezpečnost (na přístupová práva, na autorizaci přístupu, utajení, zabezpečení provozu a údržby apod.),
- Požadavky na rozhraní systému a ergonomii, na provoz a údržbu:
    - požadavky na logování (specifikace dat a událostí, které je potřeba ukládat do logů pro hledání chyb);
    - požadavky na použitelnost (předložený grafický manuál a očekávaný vnější vzhled aplikace, konzistence uživatelského rozhraní, dokumentaci a podklady ke školením);
    - požadavky na spolehlivost (tj. možnou frekvenci a možný dopad chyb, možnost zotavení systému po chybě);
    - požadavky na provoz (doba provozu v průběhu dne, rychlost, dostupnost, přesnost, doba reakce, doba obnovy);
    - požadavky na nutnou archivaci dat;
- Nalezení základních omezení pro návrh systému,
- Stanovení priorit požadavků.

Požadavky jsou evidovány v Katalogu požadavků. Katalog požadavků bude vytvářen v nástroji Enterprise Architect. V průběhu zjišťování požadavků je posuzován vliv nově definovaných požadavků na rozsah projektu a případně inicializován proces změny podléhající pravidlům Řízení změn. Katalog požadavků podléhá schválení Zadavatelem.

Globální model systému

Obsahuje rozpracování základní představy o vyvíjeném systému vyplývající z koncepce stanovené v této nabídce a doplněné o závěry z analýzy požadavků. Vymezení hranice budoucího SW systému (co je uvnitř a co vně SW systému). Definice základních funkcí systému, aktérů (rolí), hlavních vstupů a výstupů systému a hlavních objektů, které budou tvořit budoucí systém. Výstupem bude kontextový digram a přehled hlavních Use Case systému.

Globální analytický model bude obsahovat:

- Vymezení hranice aplikačního systému, tvořená kontextovým schématem, z něhož jsou zřejmé hlavní prvky okolí aplikačního systému - aktéři (lidé, organizace, okolní aplikační systémy),
- Vymezení rolí aktérů z pohledu celého systému („katalog aktérů“ – název, popis role),
- Seznam událostí, na které musí systém reagovat (externí včetně časových a interní události),
- Vymezení základních požadovaných funkcionalit systému,
- Přehledový UseCase model s popisem účelu každého případu užití,
- Věcný popis rozhraní systému a okolí (vstupy, výstupy),
- Vymezení hlavních typů věcných („business“) objektů systému resp. datových objektů – seznam a jejich definice (význam) ve formě konceptuálního (analytického) class modelu,

- Hlavní datové entity vycházející z byznys tříd – konceptuální datový model,
- Určení a návrh číselníků (společných pro celý systém),
- Katalog webových služeb – včetně vazeb na logický datový model; katalog služeb s detailním popisem služby bude doplněn v během návrhu.

Globální model podléhá schválení Zadavatelem.

Návrh zajištění bezpečnosti systému

Řešení bude navrženo podle nejnovějších Microsoft bezpečnostních standardů. Řešení striktně využívá Windows autentizaci, delegování uživatelů, Kerberos. To umožnuje zapnout bezpečnostní auditovaní, které je standardní součástí platformy a na všech vrstvách sledovat auditní stopu uživatele. Předpokládá se kompletně šifrovaná komunikace mezi serverovými komponenty, mezi uživateli, přistupující na servery. Data na databázových serverech včetně záloh budou šifrována bez možnosti přístupu administrátory.

Uchazeč garantuje, že dodané řešení MOSS bude ve shodě se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Uchazeč garantuje, že dodané řešení bude v souladu s GDPR. Systém bude implementován podle nejnovějších bezpečnostních principů a podle Microsoft “Best practice”. Systém předpokládá zabezpečení na úrovni uživatelských rolí (row level security), kompletní šifrování dat, šifrování přenosu. Dále maskování dat (pokud je v databázi uloženo rodné číslo a uživatel může vidět například jenom jeho část).

Součástí platformy je kompletní auditování systému a uživatelů.

Specifikace vlivu systému na organizaci a procesy Zadavatele a dotčených externích subjektů

Předmětem popisu je prostředí organizace Zadavatele, resp. té jeho části, pro kterou se systém vyvíjí včetně dotčených spolupracujících organizací vykonávajících zpracovávanou agendu. Předmětem je vyjasnění organizačních hledisek týkajících se požadovaných resp. potřebných změn souvisejících s navrhovanou koncepcí systému, jako jsou nutné změny v organizaci zákazníka, odpovědnosti, vliv na pracovní postupy, potřeba vzniku nových funkčních míst. Tato činnost bude zpracována v těsné součinnosti se zástupci Zadavatele. Projektový tým může doporučit potřebné změny, jejich realizace je v kompetenci Zadavatele.

V rámci specifikace je proveden:

- Stručný popisu odpovídající části organizace ve vztahu k navrhovanému systému,
- Definice lokalit,
- Přiřazení funkčních míst aktérům (rolím) vymezeným v Koncepci systému,
- Vymezení základu odpovědnosti nově navrhovaných funkčních míst ve vztahu k systému a jejich zdůvodnění.

Definice globální architektury systému

Zahrnuje konfigurační analýzu, která je podkladem pro upřesnění technické a technologické architektury a jejímž předmětem je analýza podkladů pro kvantitativní charakteristiky systému. Zaměřuje se zejména na:

- zdroje dat pro naplnění databází, možnosti jejich získání, způsob výběru platných dat, postup čištění,
- odhad min. a max. počtu výskytů entit (typů byznys objektů),
- odhad objemů přenášených dat,
- odhady provozních časových závislostí – rozložení zátěžových parametrů v čase (během dne, týdne apod.),
- odhady časového vývoje – nárůst zátěžových parametrů s rozšiřováním systému,
- návrh přístupu k migraci dat - vymezení přístupu k problémům spojených s migrací stávajících datových struktur do nového systému, rizika, bezpečnost dat, možné způsoby zabezpečení.

Dále zahrnuje definici technické a technologické architektury, jejímž výstupem je rozložení funkcí a dat v organizaci a hrubé kvantitativní údaje z konfigurační analýzy. Výstupem je HW a SW architektura systému, tedy specifikace platforem, komunikačních kanálů a rozdělení systému do vrstev (UI-vrstva, business, data). Součástí výstupu je též:

- ověření navržené SW platformy a vývojového prostředí – tedy operační systém, DB systém (obojí v rámci platforem definovaných v této nabídce), vývojové frameworky, komunikační systémy, grafické zobrazovací systémy,
- ověření, zda globální funkce lze pomocí zvolené SW platformy implementovat,
- ověření a doplnění parametrů HW platforem,
- ověření pokrytí kvantitativních a výkonových požadavků zvolenými platformami,
- ověření realizovatelnosti požadovaných funkcí a práce s definovanými objekty zvolenými vrstvami,
- ověření shody vlastností definované architektury s bezpečnostní politikou,
- shoda technické architektury s platnými normami a standardy vyžadovanými Zadavatelem.

Výstupem je globální Component model a Deployment model.

Rozdělení realizace do samostatně realizovatelných částí systému (přírůstků).

Cílem kroku je rozdělení realizace na přírůstky, které je možné dále samostatně detailně analyzovat, navrhnout a implementovat tak, aby bylo možné postupně dodávat použitelné části systému Zadavateli. Prováděna bude „alokace“ požadavků, funkcí a tříd (typů objektů) do těchto přírůstků a definice rozhraní mezi nimi.

Součástí výstupu této části analýzy je tedy:

- Definice samostatně realizovatelných částí systému (subsystémů/přírůstků) a zdůvodnění kritérií pro toto dělení,
- Rozdělení systémových funkcí a objektů mezi samostatně realizovatelné části (například formou matice),
- Popis rozhraní subsystémů/přírůstků a způsobu zajištění jejich konzistence s cílem dosáhnout co nejmenšího počtu tříd (objektů) a funkcí na rozhraní,

- Vymezení neautomatizovaných činností (dočasných, nahrazujících funkcionalitu plánovanou do dalších přírůstků),
- Stanovení harmonogramu realizace přírůstků.

Realizovatelný návrh přírůstků bude předložen ke schválení Zadavateli.

Schválení výstupů fáze Analýza

Soubor výstupů fáze Analýza se předkládá Zadavateli ke schválení a následně po akceptaci slouží jako závazné podklady pro činnosti prováděné v dalších etapách životního cyklu projektu. Akceptačními kritérii jsou:

- Schválení Katalogu požadavků na systém a zapracování případných připomínek,
- Schválení Globálního analytického modelu systému,
- Schválení samostatně realizovatelných částí (přírůstků) a harmonogramu jejich realizace,
- Realizovatelnost koncepce systému a navrženého analytického modelu v rámci definované technické architektury.

1.1.2 FÁZE DESIGN

Cílem fáze je specifikovat systém (jeho definovanou část/přírůstek) do takové úrovně podrobnosti, kdy je možné kvalifikovaně naplánovat a zahájit jeho implementaci. Provádí se pro každý subsystém/přírůstek definovaný ve fázi Analýza.

Výsledkem fáze Design je (obecně):

- detailní konceptuální model systému,
- podrobný návrh vlivu vyvíjeného systému na organizaci s popisem povinností příslušných funkčních míst vzhledem k navrhovanému systému;
- návrh bezpečnostní politiky;
- návrh cílové architektury řešení;
- návrh postupu testování;
- návrh metodiky migrace dat (dokumenty, uživatelská oprávnění/role);
- návrh akceptačních kritérií;
- limity a omezení řešení.

Jednotlivé části fáze a jejich výstupy jsou popsány v následujících kapitolách. Následně jsou konkretizovány pro klíčové části projektu.

Detailní konceptuální model

Detailní model věcné části systému bude obsahovat detailní popis případů použití systému ve vazbě na požadavky a specifikaci tříd, tak aby byly jasně definovány realizovány definované funkční (věcné) požadavky, které se týkají daného přírůstku.

Detailní model zahrnuje:

- Use-Case model (Podrobný popis uživatelských postupů):
    - přehled rolí (aktérů), kterých se postupy týkají,

    - rozdělení systému do modulů (Package diagram),
    - Pro každý modul Use-Case diagramy, kde pro každou funkci jeden elementární Use-Case a jeho základní scénář, případně alternativní scénáře,
    - návaznost a obsah uživatelského rozhraní formulářů,
    - testovací požadavky;
- Model tříd:
    - definice vztahů mezi třídami – asociace a jejich násobnost,
    - doplnění všech známých atributů (z popisu věcné oblasti, případně pro stavy objektů),
    - doplnění metod („business metod“),
    - stavové diagramy pro složité třídy,
    - doplnění tříd – generalizace/specializace, abstraktní třídy,
    - kontrola reuse,
    - testovací požadavky,
- Logický datový model:
    - popis transformace class modelu do logického datového modelu,
    - popis entit,
    - atributy entit a jejich typy,
    - vztahy mezi entitami (včetně pravidel pro realizaci vztahů m:n a generalizace/specializace),
- Doplněný katalog webových služeb:
    - název služby,
    - popis služby,
    - parametry služby:
        - vstupní parametry,
        - výstupní parametry,
    - typ služby (referenční/nereferenční),
    - způsob iniciace,
    - zpracování pouze jednoho záznamu (ano/ne),
    - povolený počet odpovědí,
- Uživatelský scénář zpracování:
    - základní (hlavní) – popis transformace (zpracování) výstupu služby, zpracování vstupních parametrů a dat systému,
    - alternativní (chybový),
- Prototyp navrhované části:
    - funkční prototyp uživatelského rozhraní realizovaný v používaném vývojovém prostředí
    - ověřuje úplnost požadavků a specifikace případů užití a je podkladem k doplnění Class modelu a datového modelu.

Detailní specifikace vlivu na organizaci, návrh přístupových práv

Obsahem je specifikace navrhovaných organizačních změn a prostředků, jak těchto změn dosáhnout. Dále bude provedeno přiřazení aplikačních rolí k funkčním místům, stanovení rozdělení odpovědností a náplně funkčních míst vztažených k navrhovanému informačnímu systému, rozpracování popisu

rolí, tak aby zahrnoval pracovní postupy vzhledem k používání navrhované aplikace (tj. například musí být jednoznačně určena odpovědnost za správnost a aktuálnost určitých dat, odpovědnost za jejich archivaci apod.) a popis nutných neautomatizovaných činností zajišťovaných uživateli a jejich návaznost.

Bude deklarováno rozdělení odpovědnosti a náplň funkčních míst vztažených k navrhovanému systému a vytvořeno přiřazení rolí funkčním místům z organizační struktury (matice „funkční místo / role“). Dále bude sestavena definice přístupových práv rolí k funkcím i ke skupinám dat.

Součástí výstupu této činnosti tedy jsou:

- Matice přiřazení funkčních míst aktérům (rolím),
- Popis rolí - vymezení odpovědnosti funkčních míst a jejich zdůvodněn,
- Definice přístupových práv k funkcím a datům systému.

Detailní návrh architektury systému

V detailním návrhu bude vytvořen detailní popis řešení systému. Popis řešení obsahuje:

- Upřesnění architektury systému,
- Návrh implementačních částí systémů,
- Návrh persistence datových tříd (databáze) – datový model,
- Specifikaci pomocných datových struktur systému,
- Popis rozhraní mezi jednotlivými částmi systému.

Návrh postupu migrace dat

V rámci návrhu perzistence datových tříd bude vytvořena koncepce migrace dat ze stávajících systémů Zadavatele. Z této koncepce vyjde návrh postupu migrace dat, v němž bude popsána součinnost Zadavatele, součinnost zdrojových systémů a jejich tvůrců, dále budou definovány migrační procesy a navrženy podpůrné nástroje. Součástí návrhu bude rovněž závazný harmonogram a definice dopadů do procesů Zadavatele včetně návrhů na opatření vedoucí k minimalizaci těchto dopadů.

Návrh akceptačních kritérií

Návrh akceptačních kritérií bude důsledně vycházet z požadavků definovaných v Katalogu požadavků. Pro jednotlivá akceptační kritéria budou následně připraveny a popsány testovací a ověřovací scénáře, které budou – po odsouhlasení Zadavatelem - tvořit závazný podklad pro provádění akceptačního testování.

Limity a omezení

Limity a omezení řešení budou shromažďovány ve strukturované formě během fáze Analýza. Rozdělena budou do dvou kategorií:

- Limity a omezení při tvorbě, dodávce a implementaci řešení,
- Limity a omezení technická a provozní.

Schválení návrhu

Jednotlivé návrhové dokumenty budou před zahájením fáze Vývoje samostatně nebo jako součást výstupu širší etapy schvalovány dílčími schvalovacími řízeními Zadavatelem. Ve schválené podobě (po zapracování připomínek) se stanou součástí projektové dokumentace.

1.1.3 FÁZE VÝVOJ

Fáze programování jednotlivých přírůstků je zahájena vždy po schválení podkladů fáze Analýza a Design. Činnost programování může být rozdělena na dílčí činnosti, které mohou být jednotlivě zahájeny po schválení příslušných částí návrhu. V průběhu programování se vytvářejí jednotlivé implementační části. Využívá se již vytvořených prototypů a aplikační komponenty, které zvyšují produktivitu vývoje a optimalizují dopad změn do návrhu a realizace. Implementují se jednotlivé navržené metody tříd, implementuje se fyzický datový model tak, aby bylo umožněno jeho opakovatelné plnění. Současně se implementují testovací data.

V případě potřeby se zároveň vytvářejí pomocné implementační části sloužící k vytvoření testovacího prostředí.

Přezkoušení implementačních částí

Předmětem interních vývojových unit testů je ověřit základní funkce implementovaných částí a jejich integrovatelnosti do systému. Cílem přezkoušení je poskytnout pro integraci implementační části, které jsou funkční a stabilní.

Implementační dokumentace

Ve zdrojových kódech programů, v databázových skriptech a jiných implementačních kódech se formou komentářů a poznámek uvádějí vztahy jednotlivých částí kódu k návrhu databázových a programových struktur.

Dokumentovány jsou minimálně následující objekty:

- Databázové tabulky (název tabulky, seznam a popis atributů včetně domén, primární klíče, seznam a popis cizích klíčů, seznam a popis indexů),
- Programové moduly (název modulu, popis funkcí modulu),
- Třídy (název třídy, vlastnosti tříd, seznam a popis konstruktorů, seznam a popis atributů včetně datových typů, seznam metod, poznámky)
- Metody, interface (název metody, seznam a popis parametrů, návratová hodnota, poznámky).

1.1.4 FÁZE TESTOVÁNÍ

Testy implementovaného řešení budou probíhat v několika úrovních. V průběhu implementace bude Uchazeč průběžně testovat všechny dílčí části systému (přírůstky) i jejich jednotlivé verze. Testy budou prováděny v testovacím prostředí Zadavatele. Pokud testy proběhnou v pořádku a Zadavatel danou verzi akceptuje, bude příslušný přírůstek nasazen do pilotního provozu, resp. připraven k zahájení rutinního provozu.

V závěru kapitoly je opět uvedena konkretizace výstupů fáze pro klíčové části projektu. Uchazeč zajišťuje v rámci testovacích procesů:

- Přípravu testovacích scénářů s postupem a vyhodnocením testů
- Přípravu prostředí pro testování včetně testovacích dat
- Provedení testů v součinnosti s pracovníky Zadavatele
- Zaznamenání výsledků testů to testovacích scénářů, kategorizace zjištěných vad, způsob a termín vypořádání

Typy testů

Cílem testování prováděného Uchazečem je nalézt chyby (resp. ověřit bezchybnost) realizovaného řešení nebo jeho části. Požadavky na testování se shromažďují v průběhu vývoje systému ve fázích analýzy, návrhu a vývoje. Z požadavků vzniklé testovací scénáře jsou podkladem pro provádění jednotlivých testů.

- Unit testy
- Funkční testy
- Regresní testy
- Migrační testy
- Zátěžové testy
- Bezpečnostní testy
- Integrační testy
- Akceptační testy (UAT)

Unit testy

Testy Uchazeče v průběhu vývoje realizované na vývojovém prostředí Uchazeče.

Funkční testy

Cílem funkčních testů je prověřit funkcionalitu přírůstku nebo celého řešení. Testuje se funkcionalita definovaná ve funkční specifikaci, vnitřní funkce a chování systému.

Regresní testy

Provádí interně Uchazeč. Jsou používány pro ověření, zda se při opravě chyb nepoškodila jiná část systému. Principem regresního testování je provést úplnou sadu testů, které byly v minulosti na příslušném modulu nebo funkci prováděny. Do regresního testování lze zapojit nejenom funkční testování, ale i ostatní druhy testů.

Migrační testy

Testy pro ověření správnosti provedených migrací dat. Cílem testů je dosáhnout transparentního a zaručeného přenosu dat a obsahu z původních modulů MOSS do nových modulů. Součástí testů je odladění migračních skriptů.

Zátěžové testy

Provádí Uchazeč zpravidla ve spolupráci se Zadavatelem. Slouží k prověření výkonových parametrů systému. Zátěžový test se navrhuje tak, aby testovaná část systému plnila určené funkce v reálném čase a s reálným zatížením např. počtu uživatelů, datových toků, jejich frekvence a objemu.

Bezpečnostní testy

Provádí Uchazeč ve spolupráci se Zadavatelem. Představují testování zabezpečení databázových a síťových aplikací proti případnému zneužití dat. Testuje se autentifikace, autorizace, penetrace a zneužití.

Integrační testy

Provádí Uchazeč ve spolupráci se Zadavatelem. Slouží k ověření schopnosti systému spolupracovat s ostatními systémy provozovanými Zadavatelem a jeho způsobilosti začlenění do provozního softwarového prostředí Zadavatele. Provedení těchto testů je podmíněno součinností Zadavatele při zajišťování odpovídajícího testovacího prostředí dotčených ostatních systémů a při ověření výsledků testů, pokud nejsou tyto systémy Uchazeči zpřístupněny.

Uživatelské akceptační testy (UAT)

Provádí Zadavatel ve spolupráci s Uchazečem. Cílem akceptačních testů je prokázat shodu funkcionality řešení se zadáním, testy proto představují pokud možno reálné použití systému. Ověřují, zda implementované funkce systému naplňují požadavky uvedené v zadání a zda je tedy systém způsobilý k předání do provozu. Výsledkem akceptačních testů je Protokol o akceptačním testování, který specifikuje vady díla a odchylky od zadání a osvědčuje způsobilost pro zahájení:

- rozšířeného pilotního provozu,
- rutinního provozu

Příprava testů probíhá souběžně s implementační fází vývoje řešení. V té době jsou připravovány vhodné testovací nástroje, postupy a vzorová data. Funkční testy (jejich přípravu lze zahájit již s návrhem systému) jsou zahájeny ihned po vzniku první verze a zároveň se rozbíhá příprava regresních testů pro verze následující. Tento postup je opakován následně pro každou další verzi a následně přírůstek – ihned po vzniku jsou zahájeny funkční testy a úprava regresních testů. Sady testů pro určitou verzi jsou prováděny formou testovací kampaně, během které obvykle není prováděn vývoj a převážná část kapacit Uchazeče je soustředěna na testování. Výsledkem a cílem kampaně je vytvoření plně funkční a Zadavatelem akceptované verze systému schopné nasazení do provozního prostředí.

Testovací data (datová základna) umožňují provádět testy nad jinými než reálnými daty Zadavatele. Tento přístup je nezbytný, pokud Zadavatel k testům nad reálnými daty nedá výslovné svolení. Funkční ani zátěžové testy systému nemohou poskytnout relevantní výstupy, tj. nemohou odhalit závažné chyby v systému, nejsou-li prováděny nad obsahově i objemově kvalitními testovacími daty. Testovací data navíc musí obsahovat i data nabývající limitních, podlimitních a nadlimitních hodnot, data chybná, neúplná apod., tak aby bylo možné ověřit chování aplikací i v těchto nestandardních případech. Testovací data obecně dodává Zadavatel a vždy by měla v co nejširší míře simulovat reálná data a zohlednit konfliktní situace, které by mohly nastat při provozu, jak je uvedeno výše.

Testovací prostředí

Předpokládáno je použití dvou testovacích prostředí:

- u Uchazeče - oddělené od vývojového prostředí a určené pro testy průběžných verzí (jeho pořízení a provoz je v odpovědnosti Uchazeče);
- u Zadavatele - odděleně od provozního prostředí, na něm budou prováděny integrační a akceptační testy a zároveň může sloužit jako prostředí školící, pokud pro účely školení není požadováno vybudování samostatného prostředí

Testovací prostředí by se mělo svými parametry co nejvíce blížit parametrům produkčního prostředí. Obecně musí platit, že parametry produkčního prostředí jsou vždy lepší než parametry testovacího/školícího prostředí.

Poznámka: upřesnění počtu a typů prostředí bude součástí Prováděcího projektu.

Vyhodnocení testů

Pro objektivní vyhodnocení testů budou před každým provedením testu specifikována kritéria pro úspěšné nebo neúspěšné provedení testu. Při provádění testů budou vznikat protokoly o provedených testech umožňující jejich vyhodnocení. Protokoly akceptačních testů jsou součástí každého předávaného přírůstku či jeho verze.

Testovací dokumentace

Během realizace projektu jsou vytvářeny testovací dokumenty:

- Plán testů: tvoří základní dokument implementace testování do projektu vývoje nabízeného řešení. Dokument specifikuje, jaké testy budou prováděny a v jakém rozsahu. Slouží jako podklad pro stanovení požadavků na zdroje pro testování v rámci projektu. Tento plán vznikne v rámci plánu projektu.
- Testovací scénáře: předpisy provedení jednotlivých testů, které slouží zpravidla k ověření jednoho typu výstupu, jedné funkcionality systému. Obsahují postup provádění testu, vstupní data a očekávané výstupy. Jeden testovací případ může obsahovat více variant vstupních dat a jim odpovídajících očekávaných výsledků. Součástí testovacích scénářů je i protokol popisující celkový průběh provádění testovacího scénáře.

Součinnost Zadavatele při testování

Úspěšné provedení testů vyžaduje součinnost ze strany Zadavatele zejména v těchto oblastech:

- Zajištění přístupu testerů Uchazeče k testovacímu prostředí Zadavatele;
- Součinnost při integračních testech:
    - integrační testy testují spolupráci s navazujícími systémy. Bude nutné zajistit přístup na testovací rozhraní okolních aplikací, nebo - pokud toto rozhraní neexistuje – zajištění přístupu k rozhraní a zároveň ošetření testů tak, aby nebyl ovlivněn provoz těchto okolních aplikací,

    - dále je nutná spolupráce při vyhodnocování výsledků integračních testů, v testech je třeba ověřit, že rozhraní bylo použito správně a v cílovém systému mělo požadovaný efekt;
- Součinnost při akceptačních testech:
    - schvalování návrhu akceptačních testů (testovací scénáře),
    - stanovení týmu (vybraní klíčoví uživatelé) provádějícího akceptační testy,
    - spoluúčast s Uchazečem při provedení testů včetně zaznamenání a klasifikace zjištěných vad,
- Schvalování výsledků testů.

Poznámka: Součinnost Zadavatele a Uchazeče při provádění testů bude popsána v rámci Prováděcího projektu.

1.1.5 FÁZE NASAZENÍ

Kapitola popisuje obecné aspekty fáze a v závěru opět uvádí jejich konkretizaci pro klíčové části projektu.

Nasazení aplikace, verzování a integrace

Verze jednotlivých modulů a dalších částí a jejich integrace do výsledného systému se spravují podle samostatné metodiky verzování. V plánu verzí se zohlední jak jednotlivé navržené přírůstky (hrubé dělení) tak postupná implementace jednoho detailního návrhu, tj. přírůstku (jemné dělení).

Každá integrovaná verze systému se přezkouší s cílem zjistit základní funkčnost a provozuschopnost celého systému.

Migrace dat

Provedení migrace dat ze stávajících systémů Zadavatele je významným a kritickým krokem projektu a bude předmětem samostatného etapy/přírůstku projektu. Uchazeč předpokládá těsnou součinnost jak s pracovníky Zadavatele, kteří s původními systémy pracovali (klíčoví uživatelé), tak s tvůrci/dodavateli těchto systémů. Migrace bude provedena podle harmonogramu dohodnutého se Zadavatelem teprve poté, co budou připraveny a řádně otestovány všechny pomocné prostředky (skripty, programové nástroje) a postupy. Uchazeč počítá s využitím testovacího prostředí pro provedení cvičné migrace, během níž bude ověřena správnost všech kroků procesu migrace i výsledné transformace dat do nového provozního prostředí. Proces migrace dat bude předmětem standardního akceptačního řízení.

Pilotní provoz

Pilotní provoz je klíčovou činností pro akceptaci Díla, ať už v jeho částech nebo celku. Bude předcházet rutinnímu (v případě dílčí akceptace rozšířenému pilotnímu) provozu a bude sloužit k podrobnému seznámení klíčových uživatelů Zadavatele s dodaným řešením. Během pilotního provozu bude k dispozici potřebná HW a SW infrastruktura, bude zprovozněno dodané řešení s testovacími daty a budou zaučeni určení uživatelé, kteří budou pilotně testovat provozní vlastnosti řešení v podmínkách co možná nejbližších reálnému provozu. Během pilotního provozu budou mít

testující uživatelé k dispozici plnou podporu projektového týmu Uchazeče pro konzultace postupů a problémů.

V průběhu pilotního provozu bude otestována migrace dat a ověřena její úspěšnost. Uživatelé budou následně schopni vyzkoušet chování dodaného řešení s reálnými daty. Data vzniklá během pilotního provozu nebudou přenášena do ostrého provozu – zde se počítá zavedení dat finální migrací bezprostředně před zahájením ostrého provozu.

1.1.6 PROVOZNÍ A UŽIVATELSKÁ DOKUMENTACE

Součástí předání každé nové verze dodaného informačního systému (nebo její podstatné části) do ostrého provozu bude také předání/aktualizace odpovídající provozní a uživatelské dokumentace.

Přehled dodávané dokumentace

- Systémová – administrátorská příručka
- Instalační příručka
- Uživatelská příručka
- Zdrojové kódy

Systémová - administrátorská příručka

Systémová příručka je základní dokumentací sloužící administrátorům při řízení a správě dodaného informačního systému. Bude vypracována Uchazečem ve spolupráci s administrátory Zadavatele (s ohledem na návaznost dodaného řešení na jeho technologické okolí) a její údržba/aktualizace bude prováděna cyklicky v návaznosti na dodání podstatných dílčích částí plnění či jeho nových verzí.

Příručka obsahuje popis architektury a topologie systému z pohledu zákazníka, tj. rozmístění HW a SW komponent systému v organizačních jednotkách a lokalitách, hrubý popis součinnosti všech komponent (nástin datových toků) a způsobu jejich provozu (trvalý, ovládaný obsluhou apod.), popis řešení nejzávažnějších poruchových stavů (výpadek uzlu, výpadek komunikace apod.) a jejich důsledků na provoz systému.

Příručka rovněž obsahuje popis správy uživatelských přístupů a rolí a správu integračních rozhraní.

Instalační příručka

Instalační příručka bude popisovat veškeré technické a technologické postupy a procesy spojené s instalací dodaného řešení. Výsledkem instalačního procesu je pak plně funkční v iniciálním stavu připravené pro práci uživatelů všech rolí. Součástí instalační příručky mohou být doprovodné programové prostředky předané Objednateli na vhodném datovém nosiči, které automatizují některé kroky instalačního procesu (např. instalační skripty).

Uživatelská příručka

Uživatelská příručka bude sestavena z několika samostatných částí:

- Úvod a ovládání systému – základní popis účelu systému, ovládací prvky a způsob jejich používání

- Návod k obsluze – popis systému a jeho rutinní používání. Definuje, jak zahájit práci se systémem a poskytuje návod k obsluze základních prvků systému, a to včetně příkladů použití a popisu chování uživatele při chybách
- Referenční příručka - popis všech prvků systému a jejich použití. Obsahuje kompletní seznam chybových hlášení a popis, jak se chovat a co dělat pro návrat do normální práce (pokud popis není předmětem on-line helpu)

Zdrojové kódy

Pokud je předmětem Smlouvy předání zdrojových kódů dodávaného systému, budou tyto kódy předány Zadavateli na základě předávacího protokolu k datu/verzi systému zahájení ostrého provozu. A dále pak vždy po publikaci hlavní nové verze systému. Použití zdrojových kódů Zadavatelem se řídí smluvními podmínkami uvedenými ve Smlouvě o dílo.

2 IMPLEMENTACE ROZVOJOVÝCH POŽADAVKŮ

Při vývoji budou respektována nastavená pravidla a architektura systému MOSS. MOSS a jeho moduly jsou vždy skládány z jednotlivých základních komponent, jejichž spojením vzniká požadovaná funkcionalita. Mezi tyto komponenty se řadí Záznamy (entity), Seznamy, Detaily obrazovek, Průvodci, Úkony, Lhůty, Šablony, Makra, Akce, Konfigurace a Číselníky. V rámci vývoje bude ke každé této komponentě vznikat samostatný dokument (list), který detailně popisuje chování a vlastnosti této komponenty tak, aby bylo možné ji posoudit z uživatelského hlediska, tak následně list využít jako jediný zdroj pro vývoj samotné funkcionality. Tento přístup má několik přínosů:

1) K vývoji nevznikají žádné dodatečné interní dokumenty dodavatele v rámci předání práce mezi analytickým a vývojářským týmem. V rámci interní metodiky je nastaveno pravidlo, že předání práce probíhá výhradně předáním zpracovaných a zadavatelem odsouhlasených listů. Pokud se při vývoji funkcionality objeví nejasnosti či problémy, jsou vždy vypořádávány upřesněním / opravou listu po odsouhlasení zadavatelem – zadavatel má díky tomu jistotu, že každá vyvíjená vlastnost systému je zachycena v dokumentaci, ke které má přístup a kterou odsouhlasil. Dokumentace je tak vždy aktuální.

2) Pro každou komponentu je vyhrazen právě jeden list, který postupně upravují jednotlivé dílčí změnové požadavky – díky tomu je zajištěno, že budoucí změny respektují historické úpravy a není nutné procházet jednotlivé změnové požadavky pro získání aktuálního stavu komponenty.

3) Jednotlivé listy jsou verzovány, přičemž každá verze je spojena s příslušnou změnou. Lze tak vždy dohledat, jakým způsobem příslušná změna komponentu upravila, ale zároveň v poslední verzi listu je vždy aktuální stav zahrnující všechny předchozí úpravy.

4) Díky přesnému a kompletnímu popisu dané komponenty je pokaždé možné provést kompletní testování požadovaného chování komponenty nejen v upravované části, ale v celém novém rozsahu, a to jak na vývojářské, tak na testerské úrovni.

5) Součástí každého listu je i uživatelská a administrátorská dokumentace příslušné komponenty, která je díky tomu vždy aktualizována již při tvorbě nové verze listu. Zadavatel díky tomu vidí dokumentaci již na počátku vývoje a zároveň je schopen ji využít již ve fázi

akceptace a s ní spojenému uživatelskému testování. V případě potřeby je možné tyto části listů spojit do samostatných dokumentů komplexní nápovědy s odkazem na původní listy.

Vývoj funkcionalit většinou zahrnuje úpravu většího množství komponent. Z toho důvodu bude vytvářen pomocný materiál v podobě změnového listu, který popisuje seznam všech komponent, které jsou předmětem úprav spolu s dalšími informacemi, které mají obecnější charakter. Změnový list bude zároveň vždy spojen se změnovým požadavkem na portálu zákaznické podpory, kde bude také dostupný. Veškeré zásahy do zdrojového kódu pak budou vždy identifikovány pomocí kódu změnového listu, případně kódů jiného incidentu z portálu zákaznické podpory. Při dokončení vývoje změnového požadavku budou zadavateli předány zdrojové kódy souborů dotčených změnovým požadavkem a informace o provedené změně se objeví v seznamu novinek po nasazení nové verze (přesné znění informace je součástí změnového listu a díky tomu je rovněž dopředu odsouhlasené zadavatelem).

Datové modely bude v souladu s architekturou systému MOSS přímo součástí zdrojových kódů v podobě Entity Data Modelů (EDM), odkud budou pomocí Core frameworku transformovány do jednotlivých objektů. V důsledku toho se nemůže stát, že by byl datový model neaktuální, neboť jeho aktuálnost je nutnou podmínkou pro realizaci změnových požadavků a samotné spuštění systému při nasazování nové verze, v rámci kterého navíc dochází k porovnání modelu s využívanou relační databází a k návrhu případných nutných úprav vedoucích k zachování konzistence.

2.1 ŠABLONY LISTŮ JEDNOTLIVÝCH KOMPONENT

Akce - [Název]

Zařazení	*Modul*
Garant	*Jméno garanta*
Soubor	*ACT_list akce_v1*
# změny	*Identifikace změny, která verzi vytvořila*
Práva pro spuštění	*Požadovaná role*
Vstupní parametry	*Položka – typ položky; povinnost; popis*
Validace před spuštěním	*Podmínky nutné před spuštěním akce*
Akce	*Popis akce*
Ostatní	
Nápověda	*Uživatelská nápověda*
Administrace	*Pokyny pro administrátora aplikace*
Ikona	

3 Akce – [Název]

Zařazení	*Modul*
Garant	*Jméno garanta*
Soubor	*ACT_list akce_v1*
# změny	*Identifikace změny, která verzi vytvořila*
Práva pro spuštění	*Požadovaná role*
Vstupní parametry	*Položka – typ položky; povinnost; popis*
Validace před spuštěním	*Podmínky nutné před spuštěním akce*
Akce	*Popis akce*
Ostatní	
Nápověda	*Uživatelská nápověda*
Administrace	*Pokyny pro administrátora aplikace*
Ikona	

Detail - ***[Název]***

Zařazení (modul, detail)	*modul*	
Garant	*Jméno garanta*	
Soubor	*DET_list detailu_v1*	
# změny	*Identifikace změny, která verzi vytvořila*	
Práva pro zápis	*Požadovaná role*	
Práva pro čtení	*Požadovaná role*	
Zobrazené položky	*Popis zobrazených položek, sekcí, rozložení do sloupců*	
Akce		
Tlačítka v záhlaví		
Ostatní		
Nápověda	*Uživatelská nápověda*	
Administrace	*Pokyny pro administrátora aplikace*	

Ikona	

4 Lhůta – [Název]

Zařazení	*Modul*		
Garant	*Jméno garanta*		
Soubor	*LHT_list lhůty_v1*		
# změny	*Identifikace změny, která verzi vytvořila*		
Typ lhůty	*Lhůta spisu / lhůta dokumentu / lhůta předpisu*		
Způsob počítání konce	*Bez posunu konce / pracovní den*		
Standardní délka (Oblast, věc, délka)	*modul*	*věc*	*Délka ve dnech*
Založení lhůty	*modul*	*věc*	*Způsob založení lhůty*
Stav lhůty při založení	*modul*	*věc*	*Nastavený stav*
Spuštění lhůty	*modul*	*věc*	*Způsob spuštění lhůty*
Akce při spuštění	*modul*	*věc*	*Akce při spuštění lhůty*
Možnost prodloužení	*modul*	*věc*	*ANO / NE*
Pozastavení lhůty	*modul*	*věc*	*Způsob přerušení lhůty*
Akce při pozastavení	*modul*	*věc*	*Akce při pozastavení lhůty*
Opětovné spuštění lhůty	*modul*	*věc*	*Způsob opakovaného spuštění lhůty*
Ukončení lhůty	*modul*	*věc*	*Způsob ukončení lhůty*
Akce při ukončení	*modul*	*věc*	*Akce při ukončení lhůty*
Akce při doběhnutí	*modul*	*věc*	*Akce při doběhnutí lhůty*
Nápověda	*Uživatelská nápověda*		
Administrace	*Pokyny pro administrátora aplikace*		
Ikona			

Kód makra:	*$$[Název]*
Text do šablony	*Čj. hlavního dokumentu zásilky*
Garant	*Jméno garanta*
Soubor	*MAK_lis makra_v1*
# změny	*Identifikace změny, která verzi vytvořila*
Předpoklad pro použití	*Záznam, nad kterým je makro funkční*
Obsah makra	
Ostatní	
Aliasy	*Alternativní makra se stejným obsahem*
Nápověda	*Uživatelská nápověda*
Administrace	*Pokyny pro administrátora aplikace*

Sekce ***detailu - [Název]***

Zařazení (modul, detail)	*modul*	*název detailu*
Garant	*Jméno garanta*	
Soubor	*SDET_01 - sekce detailu_v1*	
# změny	*Identifikace změny, která verzi vytvořila*	
Práva pro zápis	*Požadovaná role*	
Práva pro čtení	*Požadovaná role*	
Zobrazené položky	*Popis zobrazených položek*	
Akce	*Akce spouštěné interaktivními prvky*	
Tlačítka v záhlaví	○	
Ostatní	•	
Nápověda	*Uživatelská nápověda*	
Administrace	*Pokyny pro administrátora aplikace*	

Ikona	

5 Seznam – [Název]

Zařazení (modul)	*Modul*	
Garant	*Jméno garanta*	
Soubor	*SEZ_list seznamu_v1*	
# změny	*Identifikace změny, která verzi vytvořila*	
Práva pro zápis	*Požadovaná role*	
Práva pro čtení	*Požadovaná role*	
Sloupce	*Seznam sloupců ve výchozím nastavení*	
Data (bez aplikace filtrů)	*Úplná množina dat bez aplikace uživatelských filtrů*	
Filtry	*Dostupné filtry*	
Akce při poklepání na řádku	*Akce při rozkliknutí řádku*	
Tlačítka v záhlaví	*Seznam dostupných tlačítek a popis jejich funkcionalit*	
Výchozí řazení	*Způsob výchozího řazení seznamu*	
Ostatní	*Výběr více řádek – ANO /NE* *Možnost přidání záznamu – ANO / NE* *Možnost odebrání záznamu – ANO / NE* *Možnost exportu – ANO / NE* *Barvy:*	
Nápověda	*Uživatelská nápověda*	
Administrace	*Pokyny pro administrátora aplikace*	
Ikony		

Úkon - [Název]

Zařazení	*Modul*		
Garant	*Jméno garanta*		
Soubor	*UKN_list úkonu_v1*		
# změny	*Identifikace změny, která verzi vytvořila*		
Práva pro zápis	*Požadovaná role*		
Práva pro čtení	*Požadovaná role*		
Dostupnost ***(Oblast, věc, stav)***			
Zobrazené položky	*Seznam položek dostupných v datech úkonu*		
Akce	*Akce spouštěné interaktivními prvky*		
Ostatní	•		
Při založení úkonu	*Akce při založení úkonu*		
Při uzavření úkonu	*Akce při uzavření úkonu*		
Akce při zrušení	*Akce při zrušení úkonu*		
Dostupné šablony ***(Oblast, Věc, Šablona)***			
Nápověda	*Uživatelská nápověda*		
Administrace	*Pokyny pro administrátora aplikace*		
Ikona			

Průvodce - [Název]

Zařazení (modul)	*Modul*	
Kód průvodce	*WIZXXXX*	
Garant	*Jméno garanta*	
Soubor	*WIZ_list průvodce (WIZXXXX)_v1*	
Práva pro spuštění	*Požadovaná role*	

Inicializace průvodce		
Krok 01.1	***Název kroku***	*Název kroku*
	Popis kroku	*Popis kroku*
	položky kroku	*Obsah kroku*
	inicializace kroku při první průchodu	*Nastavení hodnot při prvním průchodu*
	akce kroku	*Akce spouštěné interaktivními prvky*
	dokončení kroku	*Akce při dokončení kroku*
	tlačítka	*Dostupná tlačítka kroku*
Dokončení průvodce		*Akce při dokončení průvodce*
Nápověda		*Uživatelská nápověda*
Administrace		*Pokyny pro administrátora aplikace*

Záznam - [Název]

Název záznamu:	*[Název]*	
Zařazení (modul)	*Modul*	
Garant	*Jméno garanta*	
Soubor	*ZAZ_list záznamu_v1*	
# změny	*Identifikace změny, která verzi vytvořila*	
Práva pro zápis	*Požadovaná role*	
Práva pro čtení	*Požadovaná role*	
Atributy ***(typ, povinnost, popis)***	• *Název atributu – typ; povinnost; popis*	
Akce při založení	*Akce při založení záznamu*	

Akce při změně	*Akce při uložení upraveného záznamu*
Akce při smazání	*Akce při smazání záznamu*
Editor	*Zobrazeno (v tomto pořadí)* • *Název atributu*
Výchozí označení	*Definice výchozího označení záznamu*
Ostatní	•
Nápověda	*Uživatelská nápověda*
Administrace	*Pokyny pro administrátora aplikace*
Ikona	