

ISVS SSLP

(Opis predmetu obstarávania)

Identifikácia projektu

Povinná osoba	Kancelária Národnej rady Slovenskej republiky
Názov projektu	Informačný systém verejnej správy Systém na sledovanie legislatívneho procesu
Zodpovedná osoba za projekt	Ing. Karol Guniš
Realizátor projektu	Kancelária Národnej rady Slovenskej republiky
Vlastník projektu	JUDr. Peter Vodráška LL.M.

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Schválil	Ing. Karol Guniš	Kancelária Národnej rady Slovenskej republiky	Riaditeľ odboru		

Verzia 1.5

Obsah

1.	POPIS ZMIEN DOKUMENTU	5
1.1.	História zmien	5
2.	ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE	5
2.1.	Použité skratky	5
2.2.	Konvencie pre typy požiadaviek (katalóg požiadaviek, príloha č.2)	6
3.	POŽIADAVKY NA TECHNICKÚ A ODBORNÚ SPÔSOBILOSŤ DODÁVATEĽA	6
3.1.	Zoznam dodávok tovaru alebo poskytnutých služieb za predchádzajúce štyri roky od vyhlásenia verejného obstarávania	7
3.2.	Predloženie údajov o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy alebo riadiacich zamestnancov (kľúčoví experti)	7
4.	SÚLAD S LEGISLATÍVOU	10
5.	LICENCIE, ZDROJOVÉ KÓDY a práva duševného vlastníctva	12
5.1.	Licenčné zabezpečenie	12
5.2.	Ak je predmetom dodávky krabicový SW	12
5.3.	Ak je predmetom dodávky špecializované konfigurovateľné riešenie, platformy alebo nástroje - špecializovaný SW	12
5.4.	Ak je predmetom dodávky unikátne softvérové dielo	12
5.5.	Preexistujúci SW	13
5.6.	Vyhnutie sa vendor lock-in	13
6.	POŽADOVANÉ VÝSTUPY – projektový popis produktu	14
6.1.	Produktové výstupy pre jednotlivé etapy	14
6.2.	Komplexná dokumentácia	17
6.2.1.	Etapa „Analýza a dizajn“	18
6.2.2.	Etapa „Implementácia“	19
6.2.3.	Etapa „Testovanie“	20
6.2.4.	Etapa „Nasadenie“	20
6.2.5.	Akceptácia Dokumentov	20
6.2.6.	Testovanie	21
6.2.7.	Požiadavky na realizáciu školení	21
6.2.8.	Akceptácia diela	21
6.2.9.	Akceptácia školenia	23
6.2.10.	Akceptácia dodávky tovaru, resp. licencie:	23
6.2.11.	Akceptácia vykonaných prác:	23
7.	POPIS NAVRHOVANÉHO RIEŠENIA	24
8.	ARCHITEKTÚRA RIEŠENIA PROJEKTU	25

8.1.	Biznis vrstva	27
8.1.1.	TO BE stav biznis procesov.....	27
8.2.	Aplikačná vrstva	32
8.2.1.	AS IS Aplikačná architektúra.....	32
8.2.2.	TO BE Aplikačná architektúra a popis vzťahov	32
8.2.3.	ISVS MW	35
8.2.4.	Dátová vrstva	38
8.2.5.	Technologická vrstva.....	38
8.2.6.	Bezpečnostná architektúra	39
9.	ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY.....	41
10.	Rozsah dodávky.....	41
11.	Prepojenia, integrácie, migrácie a rozhrania.....	42
11.1.	INTERNÉ rozhrania	42
11.2.	MIGRÁCIE ÚDAJOV.....	42
12.	PREVÁDZKA A ÚDRŽBA.....	43
12.1.	Životný cyklus produktu / Doba udržateľnosti projektu	43
12.2.	Prevádzkové požiadavky	43
12.2.1.	Požadovaná dostupnosť ISVS.....	43
12.3.	Účel a predmet podpory	44
12.3.1.	Paušálne služby a rozvoj diela.....	44
12.3.2.	Vykonanie pravidelnej profylaktiky na týždennej báze	49
12.4.	Systém podpory používateľov.....	50
12.5.	Popis Objednávkových služieb a špecifikácia spôsobu plnenia	51
13.	HARMONOGRAM JEDNOTLIVÝCH ETÁP, FÁZ DIELA	56
14.	PRÍLOHY A REFERENCIE.....	59
14.1.	Príloha č.1 Technické podklady.....	59
14.2.	Príloha č.2 Katalóg požiadaviek.....	59
14.3.	Príloha č.3 Komunikácia modulov	59
14.4.	Príloha č.4 Rozdelenie modulov projektu z pohľadu komunikácie.....	59
14.5.	Príloha č.5. Komunikácia modulov ISVS SSLP s ISVS DKS.....	59
14.6.	Príloha č.6 Závazná štruktúra rozpočtu.....	59
14.7.	Príloha č.7 Databázy – počet tabuliek a stĺpcov	59
14.8.	Referencia 1: Metais ISVS_10611	59
14.9.	Referencia 2: Metais Projekt rozvoja IT projekt_999: Vybudovanie Systému na Sledovanie Legislatívneho Procesu (SSLP).....	59

1. POPIS ZMIEN DOKUMENTU

1.1. História zmien

Verzia	Dátum	Zmeny	Meno
1.0	17.10.2021	Vypracovane	Mgr. Martin Roman
1.1	12.1.2022	Aktualizácia OPISU	Mgr. Martin Roman
1.2	10.2.2022	Aktualizácia OPISU	Mgr. Martin Roman
1.3	25.2.2022	Aktualizácia OPISU	Mgr. Martin Roman
1.4	28.2.2022	Aktualizácia OPISU	Mgr. Martin Roman
1.5	1.3.2022	Aktualizácia OPISU, Bižutéria	Mgr. Martin Roman

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

Účelom dokumentu je v súlade s Vyhláškou 85/2020 Z. z. o riadení projektov stanoviť opis predmetu obstarávania projektu informačný systém verejnej správy SSLP.

2.1. Použité skratky

ID	SKRATKA	POPIS
1.	AOTS	Automatizovaný systém pre správu prepisov
2.	BPM	Business Process Management
3.	BRE	Business rule engines
4.	ISVS	Informačný systém verejnej správy
5.	DMS	Dokument manažment systém
6.	eREG	Elektronická registratúra
7.	SSLP	Informačný systém na sledovanie legislatívneho procesu
8.	MW	Middleware
9.	DKS	Digitálny konferenčný systém
10.	GUI	Graphical user interface
11.	K NR SR	Kancelária Národnej rady Slovenskej republiky
12.	VO	Verejný obstarávateľ

13.	HW	Hardvér
14.	SW	Softvér
15.	FAT	Funkčné testy
16.	UAT	Akceptačné testy
17.	PID	Projektový iniciálny dokument
18.	RTO	Recovery Time Objective
19.	RPO	Recovery Point Objective
20.	DNR/DFŠ	Detailný návrh riešenia/ Definitívna funkčná špecifikácia
21.	AIS	Agendový informačný systém
22.	MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
23.	Parlamentný informačný systém	Súbor všetkých informačných technológií ktoré zabezpečujú poskytovanie IT služieb Kanceláriou Národnej rady SR

2.2. Konvencie pre typy požiadaviek (katalóg požiadaviek, príloha č.2)

Požiadavky v rámci projektu boli rozdelené na:

- Funkčné
- Nefunkčné
- Technické

Číslovanie je vzostupné od čísla 1 až po konečné číslo vyjadrujúce požiadavku. Pre číslo je zaradená skratka ID.

3. POŽIADAVKY NA TECHNICKÚ A ODBORNÚ SPÔSOBILOSŤ DODÁVATEĽA

Verejným obstarávateľom stanovené podmienky účasti vyplývajú z potreby preukázania minimálnych praktických skúseností uchádzača s poskytovaním služieb rovnakého alebo obdobného charakteru ako je predmet tejto zákazky. Celková hodnota požadovaných referencií vychádza z predpokladanej hodnoty zákazky a náročnosti obstarávaných služieb. Podmienka účasti je primeraná a jej potreba vyplynula z dôvodu overenia skutočnosti, či uchádzači disponujú odbornými skúsenosťami z oblasti predmetu zákazky, resp. s obdobnými odbornými skúsenosťami a sú oprávnení a schopní ho dodať. Splnenie týchto podmienok účasti by malo zaručiť, že uchádzač ovláda problematiku nevyhnutnú na poskytnutie tohto predmetu zákazky.

Verejným obstarávateľ požaduje preukázanie nasledovných skutočností pre naplnenie podmienok:

3.1. Zoznam dodávok tovaru alebo poskytnutých služieb za predchádzajúce štyri roky od vyhlásenia verejného obstarávania

Uchádzač predloží zoznam poskytnutých služieb za predchádzajúcich 4 roky od vyhlásenia verejného obstarávania s uvedením cien, lehôt dodania a odberateľov; dokladom je referencia, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ podľa zákona o VO, a to v súlade s § 34 ods. 1 písm. a) a § 34 ods. 2 zákona o VO.

Uchádzač predloženým Zoznamom poskytnutých služieb za predchádzajúce 4 roky od vyhlásenia verejného obstarávania, doplneným referenciou, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ, preukáže realizáciu minimálne jedného projektu (zákazky/zmluvy) v minimálnej hodnote 400 000,00 Eur bez DPH, ktorého súčasťou bolo dodanie, implementácia a/alebo údržba elektronického informačného systému s podporou pre riadenie pracovných procesov, riadeného workflow štrukturovaných a neštrukturovaných údajov, podporou schvaľovania dokumentov.

Verejný obstarávateľ odporúča uchádzačom, aby v zozname poskytnutých služieb v opise k uskutočnenej zákazke/zmluve vymedzili procesy, ktorých uskutočnenie verejný obstarávateľ požaduje, resp. uviedli skutočnosti, z ktorých bude možné požadované procesy overiť.

3.2. Predloženie údajov o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy alebo riadiacich zamestnancov (kľúčoví experti)

Verejný obstarávateľ požaduje predložiť údaje o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy alebo riadiacich zamestnancov (kľúčoví experti).

Z uchádzačom predložených dokladov musia byť minimálne zrejmé:

1. Údaje o vzdelaní a odbornej praxi kľúčových expertov, čo uchádzač u týchto kľúčových expertov preukáže predložením profesijných životopisov, alebo ekvivalentnými dokladmi.
2. Z každého predloženého profesijného životopisu príslušného kľúčového experta alebo ekvivalentného dokladu musia vyplývať nasledovné údaje/skutočnosti:
 - Meno a priezvisko príslušného kľúčového experta,
 - **Najvyššie dosiahnuté vzdelanie príslušného kľúčového experta (inštitúcia, od-do, získaný doklad o vzdelaní/titul/diplom).**
 - História zamestnania/odbornej praxe príslušného experta vo vzťahu k predmetu zákazky (zamestnávateľ/odberateľ, trvanie pracovného pomeru/trvanie odbornej praxe / rok a mesiac od – do, pozícia, ktorú príslušný kľúčový expert zastával).
 - Praktické skúsenosti príslušného kľúčového experta (názov **zmluvy/projektu/predmetu plnenia**, **názov odberateľa zmluvy/projektu/predmetu plnenia zmluvy**, **názov zamestnávateľa**, popis **zmluvy/projektu/predmetu plnenia**, pozícia na **zmluve/projekte/predmete plnenia**, obdobie rok a mesiac od - do **poskytovania služieb**, meno a priezvisko aspoň jednej kontaktnej osoby a číslo telefónu a emailový kontakt odberateľa, kde si bude môcť verejný obstarávateľ overiť informácie).

Uchádzač vyššie uvedeným spôsobom preukáže splnenie nasledovných minimálnych požiadaviek na kľúčových expertov č. 1 až 5:

Kľúčový Expert č.1 - Projektový manažér pre implementáciu:

- 1 zodpovedná osoba;
- Ukončené vysokoškolské vzdelanie minimálne 2. Stupňa - uchádzač preukáže scanom originálu dokladu o najvyššom dosiahnutom vzdelaní alebo scanom úradne osvedčenej kópie originálu dokladu;
- Minimálne 5 rokov odbornej praxe v riadení projektov v oblasti informačných systémov - uchádzač preukáže v profesijnom životopise kľúčového experta;
- Minimálne 3 praktické skúsenosti s riadením projektov v pozícii projektový manažér projektov implementácie softvérových riešení - uchádzač preukáže v profesijnom životopise kľúčového experta v rámci zoznamu minimálnych praktických skúseností;
- Získaný a platný certifikát projektového manažmentu (min. Úrovne prince 2 practitioner, ipma c/b alebo pmi pmp) na odbornú spôsobilosť pre riadenie projektov alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou - uchádzač preukáže scanom originálu platného certifikátu alebo scanom originálu platného ekvivalentného rovnocenného dokladu alebo scanom úradne osvedčenej kópie originálu certifikátu/ekvivalentného rovnocenného dokladu.

Kľúčový expert č. 2: Špecialista pre bezpečnosť a kyberbezpečnosť ISVS

- 1 zodpovedná osoba;
- Ukončené vysokoškolské vzdelanie minimálne 2. Stupňa - uchádzač preukáže scanom originálu dokladu o najvyššom dosiahnutom vzdelaní alebo scanom úradne osvedčenej kópie originálu dokladu;
- Minimálne 5 rokov odbornej praxe v oblasti kyberbezpečnosti informačných systémov - uchádzač preukáže v profesijnom životopise kľúčového experta;
- Minimálne 1 praktická skúsenosť v oblasti bezpečnosti informačných systémov v súlade s bezpečnostnými štandardmi - uchádzač preukáže v profesijnom životopise kľúčového experta v rámci zoznamu minimálnych praktických skúseností;
- Získaný a platný certifikát cisa alebo cism alebo cissp alebo medzinárodne uznávaný ekvivalent daného certifikátu vydaný akreditovanou (certifikovanou) autoritou - uchádzač preukáže scanom originálu platného certifikátu alebo scanom originálu platného ekvivalentného rovnocenného dokladu alebo scanom úradne osvedčenej kópie originálu certifikátu/ekvivalentného rovnocenného dokladu.

Kľúčový expert č. 3: IT programátor/vývojár

- 1 zodpovedná osoba;
- Ukončené minimálne stredoškolské vzdelanie s maturitou - uchádzač preukáže scanom originálu dokladu o najvyššom dosiahnutom vzdelaní alebo scanom úradne osvedčenej kópie originálu dokladu;
- Minimálne 5 rokov odbornej praxe v oblasti návrhu, programovania a vývoja komplexných informačných systémov - uchádzač preukáže v profesijnom životopise kľúčového experta;
- Minimálne 1 praktickú skúsenosť v oblasti návrhu, programovania a vývoja informačných systémov - uchádzač preukáže v profesijnom životopise kľúčového experta v rámci zoznamu minimálnych praktických skúseností;
- Získaný a platný certifikát s minimálnou úrovňou certified soa professional alebo ekvivalent daného certifikátu vydaný akreditovanou (certifikovanou) autoritou - uchádzač preukáže scanom originálu platného certifikátu alebo scanom originálu platného ekvivalentného rovnocenného dokladu alebo scanom úradne osvedčenej kópie originálu certifikátu/ekvivalentného rovnocenného dokladu.

Kľúčový expert č. 4: IT tester

- 1 zodpovedná osoba;
- Ukončené minimálne stredoškolské vzdelanie s maturitou - uchádzač preukáže scanom originálu dokladu o najvyššom dosiahnutom vzdelaní alebo scanom úradne osvedčenej kópie originálu dokladu;
- Minimálne 3 roky odbornej praxe v oblasti testovania softvérových aplikácií, funkčných a nefunkčných požiadaviek na softvérové riešenie - uchádzač preukáže v profesijnom životopise kľúčového experta;
- Získaný a platný certifikát v oblasti testovania softvérových aplikácií istqb ctfl alebo ekvivalent daného certifikátu vydaný akreditovanou (certifikovanou) autoritou - uchádzač preukáže scanom originálu platného certifikátu alebo scanom originálu platného ekvivalentného rovnocenného dokladu alebo scanom úradne osvedčenej kópie originálu certifikátu/ekvivalentného rovnocenného dokladu.

Kľúčový expert č. 5: Databázový špecialista

- 1 zodpovedná osoba;
- Ukončené minimálne stredoškolské vzdelanie s maturitou - uchádzač preukáže scanom originálu dokladu o najvyššom dosiahnutom vzdelaní alebo scanom úradne osvedčenej kópie originálu dokladu;
- Minimálne 5 rokov odbornej praxe v oblasti návrhu a realizácii databáz - uchádzač preukáže v profesijnom životopise kľúčového experta;
- Minimálne 1 praktickú skúsenosť v oblasti návrhu a implementácie databázového riešenia - uchádzač preukáže v profesijnom životopise kľúčového experta v rámci zoznamu minimálnych praktických skúseností.

4. SÚLAD S LEGISLATÍVOU

- Dopytovaný informačný systém bude základnou službou v zmysle zákona č. 69/2018 o kybernetickej bezpečnosti.
- Plnenie musí byť v súlade s platnou legislatívou, najmä:

LEGISLATÍVNE ŠTANDARDY
Ústava Slovenskej republiky č. 460/1992 Zb. v znení neskorších predpisov
Ústavný zákon č. 397/2004 Z. z. o spolupráci Národnej rady Slovenskej republiky a vlády Slovenskej republiky v záležitostiach Európskej únie
Ústavný zákon č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu v znení neskorších predpisov
Zákon NR SR č. 350/1996 Z. z. o rokovacom poriadku NR SR v znení neskorších predpisov
Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon č. 357/2004 Z. z. o ochrane verejného záujmu pri výkone funkcií verejných funkcionárov v znení neskorších predpisov
Legislatívne pravidlá tvorby zákonov č. 19/1997 Z. z. (uznesenie Národnej rady Slovenskej republiky č. 519 z 18. decembra 1996, uznesenie Národnej rady Slovenskej republiky č. 1146 zo 6. novembra 2008 a uznesenie Národnej rady Slovenskej republiky č. 1169/2018 zo 16. mája 2018)
Podrobnejšie pravidlá rokovania Národnej rady Slovenskej republiky (uznesenie Národnej rady Slovenskej republiky zo 4. februára 1997 č. 522 a uznesenie Národnej rady Slovenskej republiky z 22. marca 1999 č. 208)
Pravidlá hlasovania na schôdzach Národnej rady Slovenskej republiky (uznesenie Národnej rady Slovenskej republiky uznesením zo 4. februára 1997 č. 523)
Elektronická forma podávania a doručovania materiálov Národnej rade Slovenskej republiky (uznesenie Národnej rady Slovenskej republiky č. 1146/2008 zo 6. novembra 2008 a uznesenie Národnej rady Slovenskej republiky č. 1169/2018 zo 16. mája 2018)
Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 486/2009 Z. z. o uzavretí Lisabonskej zmluvy, ktorou sa mení a dopĺňa Zmluva o Európskej únii a Zmluva o založení Európskeho spoločenstva v platnom znení
ŠTANDARDY pre eGOVERNMENT
Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Zákon č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov
Zákon proti byrokracii č. 177/2018 Z.z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním ISVS
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
Nariadenie Európskeho parlamentu a rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
ŠTANDARDY pre KYBERNETICKÚ a INFORMAČNÚ BEZPEČNOSŤ
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
Zákon č. 45/2011 Z.z. o Kritickej infraštruktúre Z.z.
Trestný zákon č. 300/2005 Z.z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí)
Zákon elektronických komunikáciách č. 351/2011 Z.z. (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
Zákon o dôveryhodných službách (elektronický podpis) č. 272/2016 Z.z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu (EIDAS)
ŠTANDARDY pre KVALITU ÚDAJOV
Zákon o e-Governmente (§52) - povinnosť referencovania sa a využívať referenčné údaje.
Zákon o e-Governmente (§10) - povinnosť využívať „Modul procesnej integrácie a integrácie údajov (jeho časti ISVS CSRÚ)“ a realizovať integráciu údajov, synchronizáciu údajov pri referencovaní a pri výmene údajov s referenčnými registrami a základnými číselníkmi.
Metodické usmernenie č. 1/ 2019 k zálohovaniu údajov v databázach domén, registrátorov a kontaktov súvisiacich so správou domén najvyššej úrovne alebo jeho náhrada
ŠTANDARDY RIADENIA KVALITY
VYHLÁŠKA 85/2020 Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o riadení projektov
Riadenie kvality podľa Smernice STN EN ISO 9001: 2016
ŠTANDARDY pre LICENCIE
Uznesenie vlády č. 286/2019 o povinnosti prednostne pristupovať k platným a účinným centrálnym IKT zmluvám
Ostatné všeobecne záväzné právne predpisy ktoré sa dotýkajú predmetu obstarávania, uvedených zákonov

5. LICENCIE, ZDROJOVÉ KÓDY A PRÁVA DUŠEVNÉHO VLASTNÍCTVA

5.1. Licenčné zabezpečenie

Dodávateľ zabezpečí licenciu pre ISVS, ktorá pokryje všetky požadované parametre pre produkčné prostredie. Licencia musí zohľadňovať výkonnostné požiadavky a škálovateľnosť výkonu. Licencia musí pokrývať vysoko dostupné riešenie.

Práva získané v rámci plnenia prechádzajú aj na prípadného právneho nástupcu VO.

5.2. Ak je predmetom dodávky krabicový SW

- Pri dodaní krabicového SW sa podmienky riadia pravidlami pre použitie preexistujúceho SW v kapitole 5.5, avšak musia byť zohľadnené podmienky plánovaného životného cyklu ISVS tak, aby počas plánovanej prevádzky nedošlo k prevádzkovým problémom ktoré by vyplynuli z podmienok stanovených výrobcom špecializovaného SW.

5.3. Ak je predmetom dodávky špecializované konfigurovateľné riešenie, platformy alebo nástroje - špecializovaný SW

- Pri dodaní špecializovaného SW sa podmienky riadia pravidlami pre použitie preexistujúceho SW v kapitole 5.5, avšak musí byť zohľadnený plánovaný životný cyklus ISVS tak, aby počas plánovanej prevádzky nedošlo k prevádzkovým problémom ktoré by vyplynuli z podmienok stanovených výrobcom špecializovaného SW a to ani v prípade ak by prevádzku a technickú podporu počas životného cyklu prevzala 3. strana.
- Pokiaľ dodávateľ vytvorí v rámci plnenia pre verejného obstarávateľa zákaznicke úpravy pre špecializovaný SW vo forme programátorských prác, ktorých výsledok možno považovať za unikátne SW dielo, tak sa na všetky takéto úpravy vzťahujú všetky pravidlá obsiahnuté v kapitole 5.4 platné pre unikátne SW dielo.

5.4. Ak je predmetom dodávky unikátne softvérové dielo

- Pokiaľ dodávateľ vytvorí v rámci plnenia pre verejného obstarávateľa počítačový program chránený autorským právom, dodávateľ udelí verejnému obstarávateľovi súhlas používať taký počítačový program ako licenciu nevýhradnú, časovo neobmedzenú, územne obmedzenú na územie Slovenskej republiky, v neobmedzenom rozsahu (najmä na neobmedzený počet zariadení a užívateľov) a na všetky spôsoby použitia.
- SW bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu¹, a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužitá na činnosť smerujúcu k narušeniu alebo k zničeniu informačného systému verejnej správy.
- Dodávateľ odovzdá výlučnú kontrolu nad funkčným vývojovým a produkčným prostredím dodaného informačného systému, vrátane úplného aktuálneho zdrojového kódu, práv na používanie akéhokoľvek podkladového vývojového frameworku, vývojového komponentu použitého pri vývoji, preexistujúceho softvéru bezodkladne po dodaní diela VO.
- Všetky použité podkladové vývojové frameworky, vývojové komponenty použité pri vývoji, preexistujúci softvér musia byť v čase podpisu zmluvy oficiálne podporované výrobcom.
- Dodávateľ je povinný odovzdať verejnému obstarávateľovi funkčné vývojové a produkčné prostredie, vrátane úplného aktuálneho zdrojového kódu pri ukončení zmluvy.

¹ VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2017/863 Z 18. MÁJA 2017, KTORÝM SA AKTUALIZUJE VEREJNÁ OPEN SOURCE SOFTVÉROVÁ LICENCIA EURÓPSKEJ ÚNIE (EUPL) V ZÁUJME ĎALŠEJ PODPORY ZDIELANIA A OPĀTOVNÉHO POUŽÍVANIA SOFTVÉRU VYVINUTÉHO VEREJNÝMI SPRÁVAMI (Ú. v. EÚ L 128, 19. 5. 2017)

- Dodávateľ prevedie na verejného obstarávateľa aj všetky osobitné práva na štruktúru a dátový model použitých databáz s príslušnou dokumentáciou a použitých súvisiacich technických riešení.
- Verejný obstarávateľ je bez potreby akéhokoľvek ďalšieho povolenia dodávateľa oprávnený udeliť inému orgánu verejnej moci Slovenskej republiky sublicenciu na použitie počítačového programu bez ohľadu na účel na aký bude budúci Informačný systém vytvorený, vrátane subjektov ovládaných týmito orgánmi verejnej moci v zmysle § 66a zák. č. 513/1991 Zb., Obchodný zákonník alebo subjektov zriadených orgánom verejnej moci za účelom plnenia úloh vo verejnom záujme (bez ohľadu na právnu formu).

5.5. Preexistenčný SW

Pokiaľ dodávateľ pri plnení alebo ako jeho súčasť použije (spravidla ich spracovaním) počítačový program dodávateľa alebo tretích strán, v takomto prípade udelí verejnému obstarávateľovi oprávnenie používať takýto počítačový program v súlade s osobitnými licenčnými podmienkami tretích strán. Pre kvalifikovanie počítačového programu tretej strany je nevyhnutné splniť jednu z podmienok:

- Ide o „preexistenčný proprietárny softvér“ tzn.: taký softvér (softvérový produkt) výrobcov/ subjektov vykonávajúcich hospodársku/ obchodnú činnosť bez ohľadu na právne postavenie a spôsob ich financovania ktorý je na trhu bežne dostupný.
 - Ide o „preexistenčný open source softvér“ tzn. taký open source softvér, ktorý umožňuje spustenie, analyzovania, modifikáciu a zdieľanie zdrojového kódu, vrátane detailného komentovania zdrojových kódov a úplnej užívateľskej, prevádzkovej a administrátorskej dokumentácie.
- Na SW produkty tretích strán, tzn. preexistenčné obchodne dostupné SW, preexistenčné obchodne nedostupné SW (krabicové SW, systémové SW, operačné SW a iné), ako aj preexistenčné open source SW, a ktoré neboli vytvorené na základe tejto zmluvy pre VO, sa budú aplikovať vždy konkrétne licenčné podmienky subjektu vykonávajúceho majetkové práva k danému SW produktu. Dodávateľ sa v rámci plnenia predmetu tejto zmluvy zaväzuje pre VO zabezpečiť potrebnú licenciu/sublicenciu v rozsahu, ktorý vyžaduje plnenie tejto zmluvy. Za predpokladu, že licencie podľa predchádzajúcej vety tohto článku stratia platnosť a účinnosť, Dodávateľ je povinný zabezpečiť kvalitatívne zodpovedajúci ekvivalent pôvodných licencií na obdobie platnosti a účinnosti tejto zmluvy, a to takým spôsobom, aby bol VO schopný zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku Diela alebo jeho časti (informačného systému) počas celého životného cyklu.
 - Ak sú s použitím preexistenčného SW, služieb podpory k nemu v rozsahu v akom sú nevyhnutné, či iných súvisiacich plnení, spojené akékoľvek poplatky, je Dodávateľ povinný v rámci ceny diela riadne uhradiť všetky tieto poplatky za celú dobu trvania Zmluvy.
 - Všetky využitia preexistenčných proprietárnych a open source softvérov v rámci projektu musia byť samostatne zadokumentované vrátane ich licenčných podmienok.
 - Všetky využitia preexistenčných proprietárnych a open source softvérov v rámci projektu musia byť konzultované s verejným obstarávateľom.

5.6. Vyhnutie sa vendor lock-in

- Dodávateľ je povinný dodržiavať technické štandardy a postupy tak, aby sa pri vývoji SW diela minimalizovali úpravy, ktoré by bránili prevzatiu iným dodávateľom.
- Súčasťou ponuky vo verejnom obstarávaní musí byť aj zoznam plánovaných technológií, frameworkov a produktov dodávateľa, resp. tretích strán - s odkazom na licenčné a obchodné podmienky ich používania.

- VO má právo schvaľovať použitie akéhokoľvek preexistujúceho SW počas dodávky, prevádzky a rozvoja diela (písomne, musí existovať záznam v dokumentácii).
- VO má právo schvaľovať použitie nových produktov a technológií počas dodávky, prevádzky a rozvoja diela (písomne, musí existovať záznam v dokumentácii).
- VO má právo kontrolovať výstupy dodávateľa počas realizácie diela a životného cyklu diela .
- VO je jediným a výhradným disponentom so všetkými informáciami zhromaždenými alebo získanými počas projektu a prevádzky projektom vytvoreného riešenia vrátane jeho zmien a servisu.
- Dodávateľ je povinný odovzdať primeranú dokumentáciu potrebnú pre prevádzku a úpravy diela (logika systému, model fungovania systému atď..) k akceptovanej časti plnenia v rozsahu ktorý umožní prebrať správu systému tretej strane.
- Dodávateľ je povinný výkon majetkových autorských práv, dokumentácie a okomentovaného zdrojového kódu k SW dielu dodať najneskôr k momentu (aj priebežnej) akceptácie.
- Dodávateľ má povinnosť zabezpečiť pri zmene dodávateľa úplnú súčinnosť pri prechode na nového dodávateľa, najmä v oblasti architektúry a integrácie informačných systémov.
- Dodávateľ má povinnosť zabezpečiť akúkoľvek a všetku potrebnú aj kontinuálnu súčinnosť budúcemu poskytovateľovi služieb prevádzky, podpory a rozvoja k dielu.
- Dodávateľ je povinný pri akceptácii Diela alebo jeho časti odovzdať VO úplný aktuálny komentovaný zdrojový kód zapečatený, na neprepisovateľnom technickom nosiči dát s označením časti a verzie Informačného systému, ktorej sa týka. Zdrojový kód musí byť v podobe, ktorá zaručuje možnosť overenia, že je kompletný a v správnej verzii, tzn. umožňujúcej kompiláciu, inštaláciu, spustenie a overenie funkcionality, a to vrátane kompletnej dokumentácie zdrojového kódu. Zároveň musí byť odovzdaný zdrojový kód pokrytý testami (aspoň na 90%), musí dosahovať rating kvality (statická analýza kódu) podľa CodeClimate/CodeQL atď. (minimálne stupňa B).
- Iba v prípade neexistencie centrálnej licenčnej zmluvy pre daný SW produkt/licenciu resp. v prípade, ak je možné nákup zrealizovať za výhodnejších podmienok, ako sú uvedené v centrálnej licenčnej zmluve, je možné dodávať SW individuálne v rámci projektu.

6. POŽADOVANÉ VÝSTUPY – PROJEKTOVÝ POPIS PRODUKTU

Požiadavky na funkčné, nefunkčné a technické produktové výstupy sú definované v štruktúrovanej forme v rámci prílohy č.2 - Katalóg požiadaviek.

Realizácia projektu bude prechádzať štandardnými etapami riadenia IT projektov. Pre tieto etapy sú definované jasné výstupy, ktoré majú byť dodané a budú predmetom akceptačných kritérií.

Z pohľadu výstupov, vzhľadom na predmet projektu a plánovanú časovú realizáciu, bude projekt implementovaný podľa počtu inkrementov evidovaných v rámci v rámci prílohy č.2 - Katalóg požiadaviek.

Výsledným produktom bude dodaný ISVS so všetkými definovanými komponentami akcentujúcimi všetky požiadavky definované v rámci DNR/DFŠ, ktorá bude detailizovať navrhované požiadavky v zmysle prílohy č.2. - Katalóg požiadaviek.

6.1. Produktové výstupy pre jednotlivé etapy

Každý modul prechádza štandardnými etapami riadenia IT projektov a to:

- Analýza a dizajn
- Nákup HW a licencií
- Implementácia a testovanie

- Nasadenie a post-implemenačná podpora

Pre tieto etapy sú definované jasné výstupy, ktoré majú byť dodané a budú predmetom akceptačných kritérií.

Výsledným produktom bude dodaný komplexný systém SSLP so všetkými definovanými modulmi akcentujúcimi všetky požiadavky definované v rámci DNR/DFŠ, ktorá bude detailizovať navrhované požiadavky v zmysle funkčnej špecifikácie jednotlivých modulov.

Rámcová špecifikácia produktových výstupov pre jednotlivé etapy projektu.

Etapy	Požadované výstupy
Analýza a dizajn	<p>DNR/DFŠ</p> <ul style="list-style-type: none"> - Návrh riešenia funkčných / nefunkčných požiadaviek a obmedzení. - Návrh riešenia vizuálnych a nevizuálnych komponentov. - Rámcová špecifikácia riešenia (Popis produktu, Dekompozícia produktu, Vývojový diagram produktu). - Detailná technologická, aplikačná a biznis architektúra - analýza architektúry existujúcich systémov, procesov a požiadaviek na prostredia, t.j. dodanie detailnej špecifikácie cieľovej biznis, IS a technologickej architektúry vzhľadom na existujúce prostredie s maximálnym využitím už realizovaných investícií verejného obstarávateľa. - Detailný popis funkcionality a biznis požiadaviek, blokové a dátové modely finálneho produktu. - Požiadavky na nevizuálne komponenty (integračné služby, OpenAPI,...). - Požiadavky na vizuálne komponenty (GUI): <ul style="list-style-type: none"> a) Vytvorenie informačnej architektúry a mapovanie používateľskej cesty. b) Vytvorenie prototypu používateľského rozhrania viacerými iteráciami . <p>Návrh riešenia technických požiadaviek</p> <ul style="list-style-type: none"> - Technická architektúra – časť fyzická architektúra. - Špecifikácia správy používateľov a používateľských profilov (vrátane rolí a práv). - Špecifikácia technologických riešení a predpokladov na dosiahnutie výkonnostných požiadaviek. - Analýza a plán migrácie. - Požiadavky pre audit. <p>Bezpečnostný projekt (podlieha schvaľovaniu VO)</p> <ul style="list-style-type: none"> - Bezpečnostná architektúra - analýza rizík a hrozieb a návrh ich eliminácie, definovanie požiadaviek na bezpečnosť, bezpečný návrh/architektúra, kontrola návrhu a súladu s legislatívou. <p>Stratégia a plán testovania (podlieha schvaľovaniu VO)</p> <ul style="list-style-type: none"> - Príprava podkladov pre riadenie kvality (definovaním merateľných výkonnostných parametrov na vytváranie, overovanie projektových produktov, definovanie akceptačných kritérií, ktoré sú vhodné na požadovaný účel, register kvality). <p>Navrhnutie metodiky testovania a detailných testovacích scenárov (podlieha schvaľovaniu VO)</p> <ul style="list-style-type: none"> • Opis produktu a jeho komponentov. • Štruktúrovaný opis úrovni testovania celého riešenia a jeho komponentov. • Organizácia testov a personálne zabezpečenie. • Testovanie celého riešenia a jeho komponentov: <ul style="list-style-type: none"> ○ Testovacie prípady ○ Testovacie prostredie ○ Testovacie dáta

	<ul style="list-style-type: none"> ○ Testovacie záznamy a protokoly • Klasifikácia chýb. • Manažment riadenia chýb a opráv. • Monitoring a reporting testovania. • Spôsoby vyhodnotenia výsledkov testovania. • Vytvorenie bezpečnostných testovacích scenárov. <p>Typy testov:</p> <ul style="list-style-type: none"> ○ Funkčné testy FAT. ○ Bezpečnostné testy - minimálne v rozsahu dokumentu „Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti“ (dostupná na https://www.csirt.gov.sk). ○ Systémové integračné testy. ○ Závažové a výkonnostné testovanie. ○ Používateľské testy funkčného používateľského rozhrania (UX testovanie). ○ Používateľské akceptačné testovanie UAT. <p>Navrhnutie štruktúry dokumentácie a registrov (katalógov) (podlieha schvaľovaniu VO).</p> <p>Implementačný plán pre všetky moduly a funkčné oblasti samostatne (podlieha schvaľovaniu VO).</p> <p>Komunikačný plán (podlieha schvaľovaniu VO).</p>
Nákup HW a licencií	Dodanie hardvéru a licencií nevyhnutných pre realizáciu diela.
Implementácia a testovanie	<p>Nasadenie do pred produkčného prostredia:</p> <ul style="list-style-type: none"> – Príprava testovacieho prostredia. – Príprava produkčného prostredia. – Administratívna príprava produkčného prostredia (procesy, SLA, dokumentácia). – Inštalácia riešenia do produkčného prostredia. – Migrácia dát. – Sprístupnenie riešenia v produkčnom prostredí vybraným používateľom – administrátorom K NR SR. – Implementácia zabezpečí dodanie požadovanej funkcionality jednotlivých modulov a ich funkčnosť s nasledovnými aktivitami: <ul style="list-style-type: none"> ○ Prípravu technologických prostredí. ○ Implementáciu funkcionality jednotlivých výstupov, integráciu výstupov/produktu. ○ Vytvorenie bezpečnej základnej konfigurácie, zabezpečenie prostredia. ○ Akceptácia produktu. ○ Implementácia integračných požiadaviek <p>Produktová dokumentácia:</p> <ul style="list-style-type: none"> – Technická dokumentácia. – Dokumentácia popisujúca nastavenie systému, užívateľské role, informačné zdroje a databázy, integračné rozhrania. – Prevádzková dokumentácia: <ul style="list-style-type: none"> ○ Dokumentácia popisujúca odporúčané postupy pre prevádzku systému a pre servis a údržbu systému: <ul style="list-style-type: none"> ▪ Inštalačná príručka a pokyny na inštaláciu - dokumentácia popisujúca presné postupy pri prvotnej inštalácii, ako aj pri preinštalovaní systému (alebo jeho časti).

	<ul style="list-style-type: none"> ▪ Integrovaná príručka - dokumentácia obsahujúca popis integrácie na iné informačné systémy, webservisy alebo vstupné zdroje pre ISVS MW, katalóg integračných služieb. ○ Prevádzkový opis a pokyny pre servis a údržbu: <ul style="list-style-type: none"> ▪ Dokumentácia obsahujúca postupy pri spúšťaní, servisovaní a údržbe ako SW aplikácii, tak aj HW komponentov. ○ Havarijný plán: <ul style="list-style-type: none"> ▪ pokyny pre zálohovanie a obnovu, zoznam systémových poruchových správ a reakcie na ne v prípade výpadku, alebo havárie, RTO, RPO. <p>– Používateľská dokumentácia:</p> <ul style="list-style-type: none"> ○ Používateľská príručka: <ul style="list-style-type: none"> ▪ Všeobecná. ▪ Pre jednotlivé používateľské role so všetkými životnými situáciami a detailnými postupmi pre ne ktoré daná rola v systéme rieši. ○ Administrátorská príručka. <p>– Bezpečnostný projekt.</p> <p>– Súlad spracúvania osobných údajov (GDPR).</p> <p>– Analýza bezpečnosti, ktorý bude súčasťou bezpečnostného projektu podľa prílohy č. 3 vyhlášky č. 179/2020 a 362/2018 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.</p> <p>Realizácia školiacich aktivít.</p> <p>Realizácia testovania:</p> <ul style="list-style-type: none"> – Funkčné testy FAT. – Bezpečnostné testy vrátane penetračného testovania. – Systémové a integračné testy. – Záťažové a výkonnostné testovanie. – Používateľské testy funkčného používateľského rozhrania (UX testovanie). – Používateľské akceptačné testovanie UAT. – Pripravenosti na nasadenie do produkčného prostredia. <p>Podpísané akceptačné protokoly o vykonaní každého požadovaného druhu testu v časti Testovanie ako zo strany dodávateľa, tak aj zo strany odberateľa.</p>
<p>Nasadenie a post- implementačná podpora</p>	<ul style="list-style-type: none"> – Nasadenie do produkcie a vyhodnotenie nasadenia. – Intenzívna podpora po nábehu funkčnosti ISVS produktívnej prevádzky. – Korekcie, úpravy. – Príprava prechodu na SLA režim. – Monitorovanie.

Tu definované požiadavky sú minimálne, pričom dodávateľ je povinný plniť aj legislatívne požiadavky ktoré nie sú uvedené v tejto kapitole.

6.2. Komplexná dokumentácia

Pod pojmom komplexná dokumentácia sa rozumie projektová, produktová, technická, bezpečnostná, prevádzková a používateľská dokumentácia (vrátane dokumentovaného a komentovaného zdrojového kódu, architektonickej a analytickej dokumentácie, a pod.), ktorá predstavuje akýkoľvek a všetok podkladový materiál použitý na vytvorenie diela bez ohľadu, na to v ktorej etape dodávky diela bola vytvorená a prevzatá. Dokumentáciou sa rozumie dokumentácia v zmysle predchádzajúcej vety bez ohľadu na druh hmotného nosiča, na akom je zachytená a prevzatá.

Dokumentáciou nie sú myšlienky ani princípy. Vlastnícke právo k dokumentácii prechádza na VO jej prevzatím, tzn. momentom podpisu akceptačného protokolu/záverečného akceptačného protokolu.

Po vykonaní plnenia/plnení v rámci etapy/fázy diela a po úspešnej realizácii akceptačných testov, dodávateľ odovzdá príslušné plnenia/plnenie v rámci etapy/fázy diela, vrátane dokumentácie, ktorá sa vzťahuje na príslušnú etapu/fázu diela VO na základe písomného akceptačného protokolu podpísaného zástupcami obidvoch zmluvných strán. Podpisom akceptačného protokolu VO potvrdzuje prevzatie plnenia v rámci etapy/fázy diela alebo jeho časti vrátane dokumentácie, tzn. na VO prechádza týmto momentom vlastnícke právo k plneniu v rámci etapy diela alebo jeho časti, ako aj vlastnícke právo k dokumentácii. Súčasťou akceptačného protokolu je zoznam dokumentácie k plneniu alebo jeho časti, ktorú VO podpisom prevezme.“

Pri odovzdávaní sa od dodávateľa očakávajú v jednotlivých etapách projektu nasledovné dokumenty v elektronickej, editovateľnej podobe, ako aj v podobe pdf. Tu definované požiadavky na dodanie dokumentácie sú minimálne, pričom dodávateľ je povinný plniť aj legislatívne požiadavky ktoré nie sú uvedené v tejto kapitole (pre každý modul musí byť dokumentácia samostatne oddelená). Všetky časti dokumentácie ktorých charakter umožňuje aby boli uložené v štruktúrovanej forme musia byť uložené aj v štruktúrovanej forme umožňujúcej ich automatizované spracovanie.

6.2.1. Etapa „Analýza a dizajn“

- **Detailný návrh riešenia / Definitívna funkčná špecifikácia:**
 - Detailná identifikácia všetkých relevantných požiadaviek (funkčných a nefunkčných) a obmedzení.
 - Dodávateľ je povinný uviesť detaily týkajúce sa fázovania dodávky plnenia spolu s informáciami o licencovaní vrátane detailnej špecifikácie počtu a druhu licencií vo väzbe na autora.
- **Detailná technologická a aplikačná architektúra:**
 - Analýza architektúry existujúcich systémov, procesov a požiadaviek na prostredia, t. j. dodanie detailnej špecifikácie cieľovej biznis, IS a technologickej architektúry vzhľadom na existujúce prostredie.
 - Metodika použitá pre implementáciu dátovej výmeny v prostredí K NR SR.
- **Prototyp GUI a navigácie** (v prípade ak je predmetom dodávky alebo jej časti unikátne softvérové dielo s GUI rozhraním):
 - Prototyp UX dizajnu v rozsahu ktorý je nevyhnutný na posúdenie návrhu v zmysle platnej metodiky MIRRI.
- **Testovacie scenáre:**
 - Navrhnutie metodiky testovania a detailných testovacích scenárov.
 - Podklady pre riadenie kvality.
 - Časový plán akceptačných testov.
- **Bezpečnostný projekt:**
 - podľa prílohy č. 3 Vyhlášky č. 179/2020
 - dokument Analýza bezpečnosti
- **Projektový plán/ dokumentácia pre všetky funkčné oblasti samostatne.**
- **Štruktúra a obsah registrov.**

6.2.2. Etapa „Implementácia“

- **Technická dokumentácia (Konfiguračná príručka a pokyny pre diagnostiku):**
 - Dokumentácia popisujúca nastavenie systému, užívateľské role, informačné zdroje a databázy, integračné rozhrania systému.
- **Používateľská dokumentácia:**
 - **Používateľská príručka:**

Dokumentácia popisujúca životné situácie a postupy pre ne pre užívateľa v každej užívateľskej roli, životné situácie a postupy pre ne musia byť súčasťou školení.
 - **Administrátorská príručka:**

Dokumentácia obsahujúca aplikačné funkcie prístupné iba pre administrátora systému.

Popisujúca životné situácie a postupy pre ne.
- **Prevádzková dokumentácia:**
 - Dokumentácia popisujúca odporúčané postupy pre prevádzku systému a pre servis a údržbu systému.
 - **Inštalčná príručka a pokyny na inštaláciu:**
 - Dokumentácia popisujúca presné postupy pri prvotnej inštalácii, ako aj pri preinštalovaní systému (alebo jeho časti).
 - **Integračná príručka:**
 - Dokumentácia obsahujúca popis integrácie na iné informačné systémy, integračné služby alebo vstupné zdroje pre ISVS MW, katalóg integračných služieb.
 - Použitá metodika pre implementáciu dátovej výmeny v prostredí K NR SR.
 - **Prevádzkový opis a pokyny pre servis a údržbu:**
 - Dokumentácia obsahujúca postupy pri profylaktike, spúšťaní, servisovaní a údržbe ako SW aplikácií, tak aj HW komponentov.
 - **Havarijný plán:**
 - Detailné pokyny pre zálohovanie a obnovu, zoznam systémových poruchových správ a reakcie na ne v prípade výpadku, alebo havárie, RTO, RPO.
- **Bezpečnostný projekt:**
 - V súlade s §23 zákona 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
 - V súlade s vyhláškou č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
 - Dodávateľ sa zaväzuje zaistiť bezpečnosť a odolnosť produktu alebo jeho časti voči aktuálne známym typom útokov a pred jeho odovzdaním vykonať testovanie na prítomnosť známych zraniteľností. V prípade zistenia zraniteľností sa Dodávateľ zaväzuje tieto zraniteľnosti odstrániť, vykonať opätovné testovanie a zdokumentovaný výsledok testovania odovzdať VO spolu s dodávaným riešením.

- **Súlady spracúvania osobných údajov (GDPR):**
 - Právna analýza súladu spracúvania osobných údajov v dodávanom informačnom systéme voči požiadavkám platnej legislatívy SR a EÚ na ochranu osobných údajov, posúdený vplyv spracovateľských operácií na ochranu osobných údajov (DPIA (Data Protection Impact Assessment)).
- **Analýza bezpečnosti**, ktorá bude súčasťou bezpečnostného projektu podľa prílohy č. 3 vyhlášky č. 179/2020 a 362/2018 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
- **Zdrojové kódy.**

6.2.3. Etapa „Testovanie“

- Podpísané akceptačné protokoly o vykonaní každého požadovaného druhu testu v časti Testovanie ako zo strany dodávateľa, tak aj zo strany odberateľa.

6.2.4. Etapa „Nasadenie“

- Prezenčné listiny školení.
- Protokol o nasadení systému do testovacej a následne ostrej prevádzky.
- Aktualizovaná komplexná dokumentácia.

6.2.5. Akceptácia Dokumentov

Dokumentom je myslená akákoľvek časť alebo celok dokumentácie ktorá je súčasťou komplexnej dokumentácie projektu a je dodávaná v jednotlivých etapách projektu.

- Dokumenty budú VO odoslané v lehotách definovaných v Zmluve alebo Projektovom pláne na pripomienkovanie v elektronickej forme vo forme e-mailovej správy. V prípade požiadavky VO (definovanej v Zmluve, Projektovom pláne) bude Dokument odovzdaný osobne v papierovej forme a v elektronickej forme na CD. Zároveň môže byť realizovaná aj prezentácia Dokumentu.
- V prípade osobného prevzatia písomnej formy dokumentu podpíše zástupca VO preberací protokol.
- VO je povinný zaslať pripomienky k Dokumentu e-mailom v dohodnutej lehote odo dňa prevzatia (doručenia) Dokumentu vo formáte MS Excel, alebo MS Word.
- Dodávateľ pripomienky zapracuje. V prípade, že niektorú z pripomienok nie je možné akceptovať, zabezpečí Dodávateľ písomné vyjadrenie pripomienkujúceho, že po vysvetlení situácie berie svoju pripomienku naspäť.
- Novú verziu Dokumentu so zapracovanými pripomienkami zašle Dodávateľ VO v rovnakej forme v akej odovzdal prvú verziu Dokumentu s vyznačenými zmenami.
- V prípade osobného prevzatia písomnej formy novej verzie Dokumentu podpíše zástupca VO preberací protokol.
- VO je povinný po dodaní novej verzie Dokumentu preveriť spôsob zapracovania pripomienok.
- V prípade nesúhlasu musí zaslať VO svoje stanovisko bezodkladne.
- Pripomienkovanie sa bude rovnakým spôsobom opakovať, pokiaľ nebude zo strany VO vyjadrený súhlas so zapracovanými pripomienkami.
- Takto pripravený dokument bude predložený na schválenie a akceptáciu Projektovému manažérovi VO. Po jeho akceptácii sa stáva záväzným dokumentom pre Projekt.

- Konečná verzia Dokumentu bude po akceptácii odovzdaná VO v dvoch vyhotoveniach v písomnej forme a jedenkrát v elektronickej forme na CD. O prevzatí Dokumentov bude potvrdený preberací protokol.
- Dodávka Dokumentu sa považuje za ukončenú a riadne splnenú jeho akceptáciou a prevzatím.

6.2.6. Testovanie

V etape projektu „Testovanie“ sa požaduje vykonanie a akceptovanie zo strany VO nasledovných druhov testov:

- Funkčné testovanie (FAT).
- Systémové a integračné testovanie (SIT).
- Záťažové a výkonnostné testovanie.
- Bezpečnostné testovanie (SW/HW a kybernetická bezpečnosť) v súlade s nariadením CSIRTU na linke ([CSIRT.SK \(gov.sk\)](http://CSIRT.SK.gov.sk)).
- Používateľské testy funkčného používateľského rozhrania (UX).
- Používateľské akceptačné testovanie (UAT).
- Úspešné uskutočnenie testovania a potvrdenie akceptačného protokolu nezbavuje Dodávateľa povinnosti odstrániť všetky Vady plnenia v lehote stanovenej v akceptačnom protokole.
- Po odstránení Vady VO písomne potvrdí jej odstránenie.
- Podpísaním akceptačného protokolu sa dodávka programových úprav považuje za riadne splnenú a prevzatú VO.

6.2.7. Požiadavky na realizáciu školení

Požaduje sa realizácia školení v nasledovnom rozsahu:

- školenie administrátorov – do 5 ks:
 - Inštalačný a konfiguračný postup.
 - Havarijný plán.
 - Administráciu systému v plnom rozsahu funkcionality softvéru ISVS SSLP.
- školenie používateľov.

Požaduje sa príprava a realizácia školení pre jednotlivé role používateľov :

- V rámci realizácie školení sa požaduje dodanie školiacich materiálov a podkladov, ktoré budú po ukončení školení odovzdané VO. Dodávateľ je povinný pri akejkoľvek zmene funkcionality školiace materiály aktualizovať a aktualizované ich odovzdať VO.
- Školenie musí pokryť všetky životné situácie pre jednotlivé role používateľov.
- Dodávateľ nahrá video zo školenia a záznam poskytne VO s právami na použitie výlučne pre potreby VO za účelom školenia zamestnancov.

6.2.8. Akceptácia diela

- V registri kvality sú presne definované akceptačné kritériá a testovacie procedúry, ktoré musí produkt spĺňať, aby mohla byť implementácia považovaná za ukončenú.
- Ak je výsledkom vykonania akceptačných testov zistenie, že produkt alebo jeho časť nespĺňa dohodnutú funkčnosť a tým nenapĺňa účel a cieľ produktu, a to z dôvodov, za ktoré zodpovedá Dodávateľ, produkt má vady. Za Vady produktu sa považuje aj nesúlad správania

sa produktu voči odsúhlasenému registru kvality. Na iné skutočnosti namietané VO Dodávateľ nie je povinný prihladať ak nemajú zásadný vplyv na funkčnosť produktu na akceptáciu.

- Počas testovania je VO oprávnený hlásiť Dodávateľovi Vady vo funkcionalite produktu. V prípade, že sa Zmluvné strany v Zmluve alebo Projektovom pláne Projektu dohodli, že testovanie bude prebiehať za osobnej účasti zástupcu Dodávateľa, dohodnú sa aj na harmonograme a dobe testovania dodanej produktu.
- Po úspešnej realizácii testovacích procedúr Projektový manažér Dodávateľa predloží Projektovému manažérovi VO akceptačný protokol za účelom akceptácie implementácie produktu.
- V prípade, že sa počas realizácie testovacích procedúr vyskytnú Vady, VO v súčinnosti s Dodávateľom vyhotoví ich súpis s rozdelením do troch kategórií v zmysle kategorizácie incidentov SLA podmienok.
- Projektový manažér Dodávateľa navrhne lehoty, v ktorých sa Dodávateľ zaväzuje odstrániť jednotlivé Vady.
- Projektový manažér VO schváli akceptačný protokol, obsahujúci stanovisko k akceptácii plnenia. Stanovisko k akceptácii plnenia môže byť vo forme:
 - Bez výhrad.
 - Akceptované s výhradami.
 - Neakceptované.
- Úspešné uskutočnenie testovania a potvrdenie akceptačného protokolu nezbavuje Dodávateľa povinnosti odstrániť všetky Vady plnenia v lehote stanovenej v akceptačnom protokole. Dodávateľ zodpovedá za vady produktu v čase jeho odovzdania VO.
- Po odstránení Vady VO písomne potvrdí jej odstránenie.
- Produkt/modul sa vždy považuje za riadne vykonaný a VO prevzatý až ku dňu kedy bol po akceptácii prvý krát spustený do produkčnej prevádzky.
 - **Limity vád pre akceptáciu a vady diela**

V prípade výskytu vady pri akceptácii alebo prevádzke diela je Dodávateľ povinný rozlíšiť či sa jedná o incident alebo problém alebo o inú vadu diela. V prípade ak sa jedná o incident alebo problém je povinný kategorizovať vadu na základe kapitoly 12.

- Incident/problém kategórie A alebo B je kritickou vadou.
- Incident/problém kategórie C je normálnou vadou.

Kategória vady	Popis	Povolený počet defektov na modul
Kritická	<p>Vady s dopadom na základné funkcionality ISVS, ktorý by v prípade výskytu v produkčnom prostredí znemožnil prevádzku ISVS alebo jeho časti, alebo spôsobil chybnú funkčnosť ISVS alebo jeho časti.</p> <p>Vady schopné spôsobiť zastavenie alebo poškodenie Diela alebo iných systémov VO.</p> <p>Vady bezpečnosti produktu.</p> <p>Neschopnosť spracovať bežnú prevádzkovú záťaž.</p>	0

	<p>V prípade výskytu sa zastavuje akceptačné testovanie.</p> <p>Iné záručné vady s dopadom na základné funkcionality ISVS, ktorý by v prípade výskytu v produkčnom prostredí znemožnil prevádzku ISVS alebo jeho časti, alebo spôsobil chybnú funkčnosť ISVS alebo jeho časti.</p>	
Normálna	<p>Vady s nepodstatným dopadom na prevádzku ISVS, ktorý by v prípade výskytu v produkčnom prostredí nespôsobil chybnú funkčnosť ISVS alebo jeho časti. Nemá dopad na testovanie.</p> <p>Iné záručné vady</p>	3

6.2.9. Akceptácia školenia

- Účastníci školenia vyslaní na školenie VO sú povinní svoju účasť na školení potvrdiť v prezenčnej listine.
- Podpísanie prezenčnej listiny účastníkmi školenia je akceptáciou školenia VO.

6.2.10. Akceptácia dodávky tovaru, resp. licencie:

- Dodávka tovaru (HW) a licencií (SW) prebieha na mieste určenom v Zmluve alebo Projektovom pláne Projektu.
- Projektový manažér Dodávateľa v prípade dodávky tovaru upozorní VO vopred na termín dodávky. Licencie (SW) sa dodávajú v termínoch definovaných v Zmluve alebo Projektovom pláne Projektu.
- Pri preberaní dodávky podpíše VO preberací protokol. Podpísaním preberacieho protokolu sa dodávka považuje za riadne splnenú a prevzatú VO.

6.2.11. Akceptácia vykonaných prác:

- Po vykonaní prác podľa Zmluvy Dodávateľ predloží VO na akceptáciu výkaz prác. V prípade ak VO nemá k vykonaným prácam výhrady, do 5 pracovných dní po doručení výkazu prác Projektový manažér schváli akceptačný protokol k vykonaným prácam.
- V prípade ak má VO k vykonaným prácam oprávnené výhrady (práce neboli preukázateľne poskytnuté v súlade so Zmluvou), je povinný doručiť Dodávateľ výhrady k vykonaným prácam do 10 pracovných dní odo dňa doručenia výkazu prác VO.

7. POPIS NAVRHOVANÉHO RIEŠENIA

Základným cieľom projektu nie je zefektívňovať procesy v rámci NR SR, ale predovšetkým eliminovať riziká vyplývajúce zo zastaranosti existujúceho informačného systému. Z pohľadu biznis architektúry sa jedná o rovnaký prístup v AS IS ako aj TO BE stave. Z pohľadu aplikačnej architektúry je podstatné zachovanie modularity navrhovaného systému formou akoby plug in jednotlivých modulov. Preto je ako existujúca, tak aj navrhovaná aplikačná architektúra postavená práve na modularite a z pohľadu AS IS a TO BE stavu je totožná.

Rozdielne bude technické riešenie jednotlivých komponentov tak, aby napĺňalo požiadavky na jednotlivé moduly definované v prílohe tohto dokumentu.

Z hľadiska zapojenia OVM do projektu, projekt sa týka výlučne Kancelárie Národnej rady Slovenskej republiky.

Projekt Kancelárie NR SR je z pohľadu opakovateľnosti a využitia výstupov a výsledkov projektu jedinečný. Vyplýva to z úsekov a agend, ktoré NR SR zabezpečuje v zmysle platnej legislatívy. NR SR je v tomto ohľade jedinou a špecifickou inštitúciou v právnom systéme SR. Z pohľadu využitia výstupov a výsledkov sa dá uvažovať o využití skúseností z tvorby elektronických služieb založených na informovaní verejnosti o dianí v inštitúciách verejnej správy kde sa rozhoduje formou hlasovania. Podobný princíp sa uplatňuje pri regionálnej a miestnej samospráve ale v neporovnateľne menšom rozsahu. Súčasný stav poskytovaných služieb umožňuje občanovi cez webové sídlo sledovať aktuálny stav jednotlivých výstupov. Teda ak čaká na novú informáciu musí denne sledovať webovú lokalitu, ktorá požadované informácie zverejňuje. V cieľovom stave bude zrealizovaná časť webovej lokality, na ktorej bude možné záujemcovi po identifikácii si objednať mailové notifikácie o požadovaných udalostiach. Súčasne budú všetky relevantné dáta cez projekt „opendata“ sprístupňované v štruktúrovanej podobe cez integračné služby ľubovoľnému záujemcovi.

Súčasťou projektu je najmä:

- Obmeniť existujúci agendový informačný systém „Systém na sledovanie legislatívneho procesu“, ktorý bol vyvinutý rámci projektov PHARE SR 9305 04 01 a SR 9813 0201. Súčasťou uvedeného SW bolo elektronické využívanie modulov, ktoré sú aj súčasťou tohto projektu.
- Vytvoriť jednotné prostredie, do ktorého bude možné presne popísaným spôsobom vkladať ďalšie moduly bez toho, aby to musel vykonať pôvodný dodávateľ.
- Vytvoriť ISVS, ktorý bude základom pre riadenie legislatívneho procesu či už pre poslancov, alebo pre zamestnancov a neskôr aj pre širokú odbornú, resp. laickú verejnosť.
- Vytvoriť prostredie, ktoré bude pripravené poskytovať údaje novému digitálnemu konferenčnému systému (ISVS_10610) v rokovacej sále a súčasne bude pripravené využívať informácie vzniknuté v uvedenom komponente.
- Vytvoriť prostredie, ktoré bude pripravené poskytovať údaje novému systému na prepisovanie rozpravy zo zvukovej, resp. video podoby do textovej podoby a zároveň bude schopné využívať informačné zdroje vzniknuté v systéme prepisov.
- Vytvoriť prostredie, ktoré bude pripravené poskytovať štruktúrované údaje o vystúpeniach poslancov do archívneho systému videí, pomocou ktorého si bude možné jednoduchým spôsobom pozrieť vo video podobe, či už zvolený časový interval, alebo zvolené vystúpenie poslanca. V cieľovom stave sa očakáva, že spolupráca videoarchívu a systému SSLP umožní jednoduchým spôsobom spustiť vysielanie videa o jednom rokovačom bode / parlamentnej tlači v spojenej podobe (napriek skutočnosti, že sa o danej téme rokovalo niekoľko nesúvislých intervaloch počas niekoľkých nie za sebou idúcich dní) bez toho, že by užívateľ musel hľadať kedy sa o danej téme jednalo. Veľmi obdobná funkcionálna sa očakáva aj nad prepismi vystúpení.

Systém na sledovanie legislatívneho procesu bude slúžiť primárne podľa požiadaviek zákona č. 350/1996 Z. z. o rokovačom poriadku NR SR na zabezpečenie odborných, organizačných a technických úloh spojených so zabezpečovaním činnosti Národnej rady, jej výborov, osobitných kontrolných výborov a

komisíí vrátane parlamentnej dokumentácie a tlačovej služby, čím sleduje elektronickú podporu pôsobnosti Národnej rady Slovenskej republiky v oblasti zákonodarstva, kontroly a vnútornej i zahraničnej politiky.

System je navrhnutý tak, že každá agenda je riadená samostatným modulom informačného systému a bude obsahovať nasledujúce moduly.

1. Zákonodarne zbory
2. Volebné obdobia
3. Organizačná štruktúra
4. Poslanci
5. Poslanecké kluby
6. Výbory NR SR
7. Komisie
8. Delegácie
9. Skupiny priateľstva
10. Asistenti poslancov
11. Kancelárie poslancov
12. Zahraničné pracovné cesty
13. Účasť poslancov na schôdzach NR SR
14. Ospravedlnenia poslancov
15. Rozhodnutia predsedu NR SR
16. Hodina otázok
17. Interpelácie
18. Pozmeňujúce a doplňujúce návrhy
19. Doručovanie materiálov
20. Parlamentné tlačé
21. Harmonogram schôdzí NR SR
22. Program schôdze NR SR
23. Hlasovania na schôdzach NR SR
24. Uznesenia NR SR

25. Informácia podľa §70 RP
26. Stanoviská legislatívneho odboru
27. Schválené zákony
28. Zákony napadnuté na Ústavnom súde
29. Legislatívny proces
30. Agenda výborov
31. Podujatia NR SR
32. Video dokumentácia
33. Denná informácia
34. Fotodokumentácia
35. E-schôdza
36. Aplikácia
37. Notifikácie
38. Evidencia akreditácií
39. Oprávnenia
40. Žiadosť o sprístupnenie informácií
41. Rezervačný systém podujatí
42. Materiály parlamentného inštitútu
43. Kreačná činnosť NR SR
44. Kontrolná činnosť NR SR
45. Eurovoc
46. SSEZ
47. Majetkové priznania

8. ARCHITEKTÚRA RIEŠENIA PROJEKTU

V tabuľke eGov komponentov sú uvedené všetky komponenty, ktoré súvisia s projektom a sú uvedené META IS:

Názov	Typ (ISVS, AS, KS)	Budovaný / Rozvíjaný
Agenda výborov	agendový	plánujem vybudovať

Asistenti poslancov	agendový	plánujem vybudovať
Delegácie	agendový	plánujem vybudovať
Denná informácia	agendový	plánujem vybudovať
Doručovanie materiálov	agendový	plánujem vybudovať
E-schôdza	agendový	plánujem vybudovať
EUROVOC	agendový	plánujem vybudovať
Fotodokumentácia	agendový	plánujem vybudovať
Aplikácia	prezentačný	plánujem vybudovať
Harmonogram schôdze	agendový	plánujem vybudovať
Hlasovania na schôdzach	agendový	plánujem vybudovať
Hodina otázok	agendový	plánujem vybudovať
Informácia podľa §70 RP	agendový	plánujem vybudovať
Interpelácie	agendový	plánujem vybudovať
Kancelárie poslancov	agendový	plánujem vybudovať
Komisie	agendový	plánujem vybudovať
Kontrolná činnosť NR SR	agendový	plánujem vybudovať
Kreačná činnosť NR SR	agendový	plánujem vybudovať
Legislatívny proces	agendový	plánujem vybudovať
Majetkové priznania	agendový	plánujem vybudovať
Materiály parlamentného inštitútu	agendový	plánujem vybudovať
Modul administrácie DKS	agendový	plánujem vybudovať
Modul prihlasovania sa do rozpravy	agendový	plánujem vybudovať
Notifikácie	agendový	plánujem vybudovať
Oprávnenia	agendový	plánujem vybudovať
Organizačná štruktúra	agendový	plánujem vybudovať
Ospravedlnenia poslancov	agendový	plánujem vybudovať
Parlamentné tlačie	agendový	plánujem vybudovať
Podujatia NR SR	agendový	plánujem vybudovať
Poslanci	agendový	plánujem vybudovať
Poslanecké kluby	agendový	plánujem vybudovať
Pozmeňovacie návrhy	agendový	plánujem vybudovať
Program schôdze	agendový	plánujem vybudovať
Rezervačný systém podujatí	agendový	plánujem vybudovať
Rozhodnutia predsedu NR SR	agendový	plánujem vybudovať
Schválené zákony	agendový	plánujem vybudovať
Skupiny priateľstva	agendový	plánujem vybudovať

SSEZ	agendový	plánujem vybudovať
Stanoviská LO	agendový	plánujem vybudovať
Účasť poslancov na schôdzach NR SR	agendový	plánujem vybudovať
Uznesenia NR SR	agendový	plánujem vybudovať
Video dokumentácia	agendový	plánujem vybudovať
Volebné obdobia	agendový	plánujem vybudovať
Výbory	agendový	plánujem vybudovať
Zahraničné pracovné cesty	agendový	plánujem vybudovať
Zákonodarné zbory	agendový	plánujem vybudovať
Zákony napadnuté na Ústavnom súde	agendový	plánujem vybudovať
EUROVOC	agendový	plánujem vybudovať
SSEZ	agendový	plánujem vybudovať

Tabuľka 1 Tabuľka eGov komponenty

8.1. Biznis vrstva

8.1.1. TO BE stav biznis procesov

8.1.1.1. Používatelia riešenia

Používateľov ISVS SSLP môžeme rozdeliť do 2 skupín:

1. Interní používatelia – predseda NR SR, podpredsedovia NR SR, poslanci NRSR

ID	AKTÉR / STAKEHOLDER	Bližší popis vo vzťahu k PIS
1.	Predseda Národnej rady SR	Používateľ systému. Predseda Národnej rady SR riadi schôdze NR SR, najmä zastupuje Národnú radu SR navonok, podpisuje uznesenia Národnej rady SR, vyhlasuje úplné znenie zákona, na ktoré ho splnomocnil zákon, vymenúva a odvoláva vedúceho kancelárie, môže prerušiť schôdzu Národnej rady SR a ďalšie úlohy podľa zákona.
2.	Podpredseda NR SR	Používateľ systému. Riadi a organizuje úseky činnosti NR SR podľa poverenia predsedom Národnej rady SR. Zastupuje predsedu NR SR v plnení jeho úloh, ktorými ich poverí. Vykonáva ďalšiu činnosť podľa zákona.
3.	Poslanec NRSR	Používateľ systému. Poslanec je povinný zúčastňovať sa na schôdzach Národnej rady SR a jej výborov, do ktorých bol zvolený. Je povinný zúčastňovať sa aj na činnostiach, ktoré patria do ich pôsobnosti, ktoré mu Národná rada SR alebo výbor určil alebo ktorými ho poveril. Vykonáva ďalšiu činnosť podľa zákona.

2. Interní používatelia – odborní zamestnanci Kancelárie NR SR, technickí zamestnanci OI K NR SR

ID	AKTÉR / STAKEHOLDER	Bližší popis vo vzťahu k PIS
1.	Vedúci Kancelárie NR SR	Používateľ systému. Je štatutárnym orgánom kancelárie, ktorú riadi a organizuje jej činnosť. Vydáva organizačný poriadok, registratúrny poriadok a ďalšie vnútorné predpisy kancelárie. Koná v mene Kancelárie NR SR.
2.	Riaditeľ odboru informačných a komunikačných technológií K NR SR	Správa systému PIS. Riadi správu a prevádzku informačných systémov Národnej rady SR
3.	Zamestnanec odboru informačných a komunikačných technológií K NR SR	Obsluha systému PIS. Zabezpečuje správu a prevádzku informačných systémov Národnej rady SR.
4.	Zamestnanec vecných odborov K NR SR	Používateľ systému. Vykonáva agendu v jeho pôsobnosti, pričom využíva podporu informačne – komunikačných technológií.
5.	Obsahový správca modulov	Správca systému. Realizuje obsahovú správu a údržbu modulu, pričom komunikuje s vecnými odbormi pri ich aktualizácii.

8.1.1.2. Základné biznis požiadavky

Umožnenie realizácie biznis procesov:

- Evidencia zákonodárnych zborov a volebných období.
- Evidencia poslancov a ich zoskupení.
- Zvolávanie schôdzí NR SR.
- Účasť poslancov na schôdzi NR SR.
- Priebeh schôdze NR SR.
- Legislatívny proces.
- Majetkové priznania.
- Eurovoc.
- SSEZ, IPEX.

Hlavnou biznis požiadavkou je pokryť všetky požadované procesy či už Národnej rady SR, alebo Kancelárie NR SR v súlade so všetkými právnymi požiadavkami tak, aby sa stali maximálne elektronizované, riadené procesmi v súlade s platnou legislatívou, no v maximálnej miere konfigurovateľné tak, aby ich bolo možné upravovať internými zdrojmi organizácie. Všetky procesy musia spĺňať štandardy kladené na elektronizáciu procesov v štátnej správe pri zachovaní vysokej bezpečnosti, autenticity (teda aby každý krok bolo možné dosledovať - kto, kedy a v akom procese ho vykonal), so zachovaním požiadavky, že každý údaj musí byť v informačnom systéme iba a práve raz v mieste (proces, informačnom systéme, ..) kde vznikol. Druhou významnou požiadavkou na uvedený projekt je zabezpečenie jednotného rozhrania ISVS na ovládanie jednotlivých agend/ modulov informačného systému, kde bude v budúcnosti podľa presne popísaných pravidiel možné dopracúvať nové moduly, resp. ovládať a obmieňať existujúce (v prípade možných zmien) jednotnými postupmi, čo výrazne zjednoduší ovládanie procesov zamestnancami kancelárie NR SR.

Vo všeobecnosti sa jednou agendou zaoberá jeden zamestnanec organizačnej štruktúry, no z hľadiska zastupiteľnosti je vždy potrebné mať v oprávneniach možnosť nastavenia na viacerých. V požadovanom stave sa očakáva, že oprávnenia jednotlivých modulov, či informačných zdrojov sa bude dať nastavovať najmä na pozície z organizačnej štruktúry, rovnako ako aj priamo na zamestnancov z organizačnej štruktúry. V prípade nastavenia na pozície sa neočakáva potreba prestavenia oprávnení, ak sa vymení osoba na danom poste.

8.1.1.2.1. Práca s údajmi

Pre správnu funkčnosť ISVS SSLP musia byť k dispozícii vždy aktuálne dáta z definovaných informačných zdrojov. Pre každý informačný zdroj sa požaduje:

- Každý údaj (dáta informačného zdroja) sa môžu nachádzať v celom parlamentnom informačnom systéme maximálne na jednom mieste.
- V každom informačnom zdroji sa požaduje vytvoriť log informačný zdroj, ktorý bude obsahovať všetky dáta informačného systému a navyše bude obsahovať polia:
 - o Dátum vytvorenia záznamu informačného zdroja log.
 - o Jednoznačný identifikátor osoby z organizačnej štruktúry, ktorá záznam vytvorila.
 - o Jednoznačný identifikátor aplikačnej funkcie, ktorá vykonala záznam.
- Do log informačného zdroja sa budú zaznamenávať všetky zmeny v informačnom zdroji (teda prvé založenie záznamu so všetkými údajmi v čase vytvorenia, kto, kedy a ako ho vytvoril) a následne všetky zmeny (UPDATE) postupne ako boli vykonávané. Na základe týchto údajov sa očakáva jednoznačné identifikovanie kto, kedy a ako menil jednotlivé položky informačného zdroja).
- Zmazať záznam v informačnom zdroji „editorom“ (presunutie do stavu „vymazaný záznam“) je možné iba vtedy, ak v informačnom zdroji „prepojenia modulov“ na neho nie je viazaný žiadny iný záznam iného modulu.
- Požaduje sa, aby každý záznam vo všetkých informačných systémoch mal pole „stav záznamu“, ktorý zabezpečí najmä selekciu údajov, ktoré budú z informačného systému poskytované interným zdrojom, ktoré budú poskytované / zverejňované všetkým externým zdrojom (napr. Webový portál, opendata), resp. Záznamov, ktoré uvidí iba daný „modul ISVS“.
- Požaduje sa, aby nikto okrem „globálneho administrátora“ a integračných služieb súvisiacich so správou GDPR nemal možnosť vymazať žiadny záznam z informačného zdroja; aplikačné funkcie „vymazať“ zabezpečia iba označenie záznamu stavom „vymazaný“, čo zapríčiní, že takýto údaj nebude prístupný žiadnemu externému zdroju, ani žiadnemu užívateľovi s výnimkou „globálneho administrátora“ aj to iba v danom module ISVS, ktorý poskytuje modifikáciu údajov v informačnom zdroji.

8.1.1.2.2. Vplyv na existujúci proces a okolité prostredie

Nahradenie existujúceho systému nesmie negatívne ovplyvniť plynulé rokovanie NR SR a prevádzku ostatných IS v správe Kancelárie NR SR, ktoré sú využívané na činnosť Kancelárie NR SR a rokovanie NR SR v súčasnosti.

8.1.1.2.3. Integrácie

ISVS SSLP uvažuje s využitím viacerých komponentov ÚPVS ako aj s integráciou na referenčné registre a MetaIS. Rovnako sa počíta s integráciou ISVS SSLP na okolité ISVS (napr. Slov-lex, IS Úradu vlády SR a pod.). Integrácie na referenčné registre budú realizované prostredníctvom ISVS MW.

8.1.1.2.4. Biznis služby riešenia

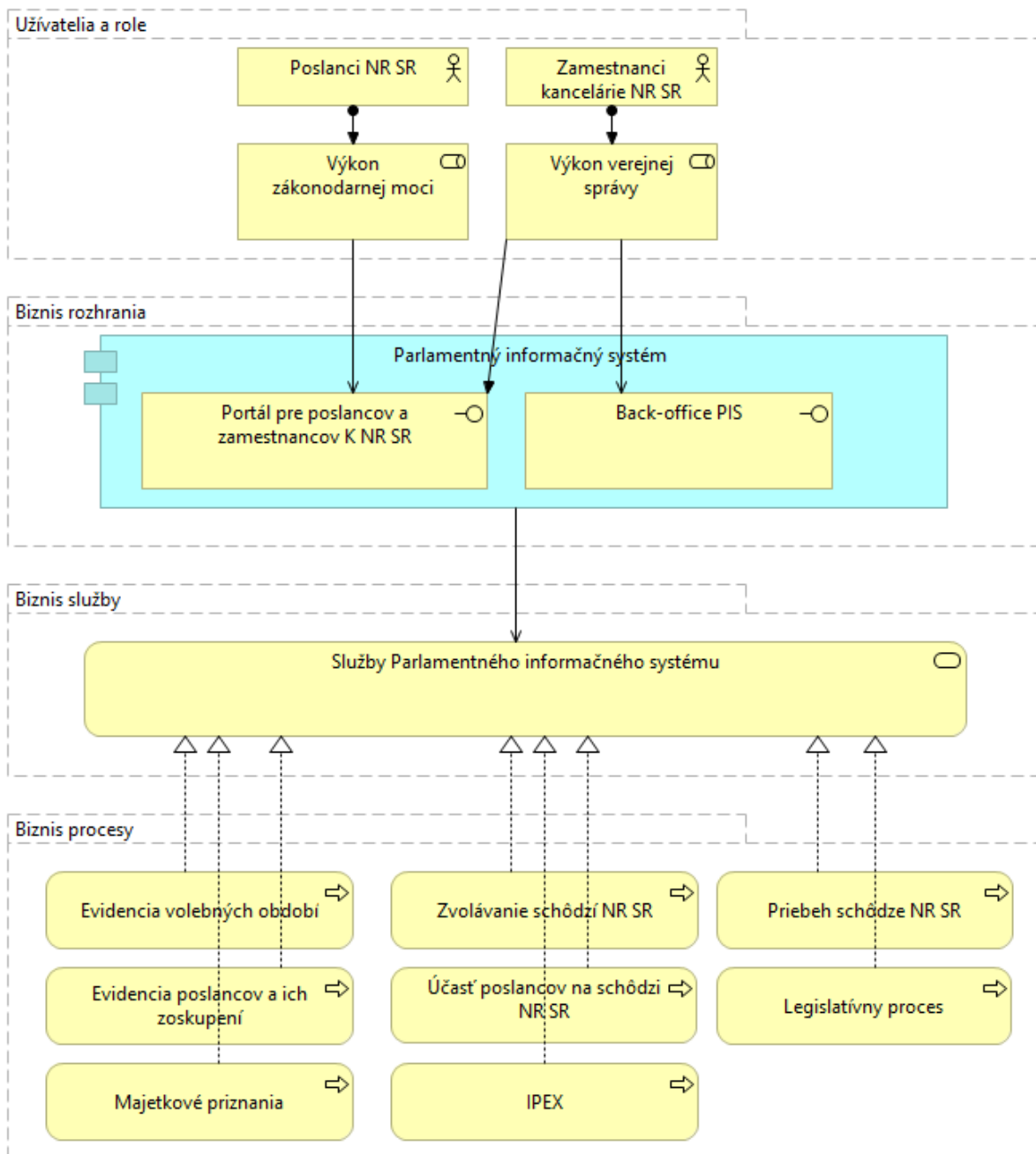
Kľúčovou legislatívnou úpravou z pohľadu zabezpečenia prevádzky a dostupnosti navrhovaných elektronických služieb Národnej rady SR je zákon NR SR č. 350/1996 Z.z. o rokovacom poriadku NR

SR v znení neskorších predpisov, ktorý sa vzťahuje k väčšine nasledovných súčasných a navrhovaných služieb:

- Informovanie o harmonograme schôdzí Národnej rady Slovenskej republiky.
- Informovanie o zvolaní schôdze Národnej rady Slovenskej republiky..
- Informovanie o výsledku denného rokovania Národnej rady Slovenskej republiky.
- Informovanie o schôdzi Národnej rady Slovenskej republiky .
- Informovanie o zápisnici zo schôdze výboru Národnej rady Slovenskej republiky.
- Informovanie o uznesení o spoločnej správe výborov.
- Podanie ospravedlnenia neúčasti poslanca na schôdzi a/alebo na výbore Národnej rady Slovenskej republiky.
- Informovanie o ospravedlnení neúčasti poslancov na schôdzi a/alebo výbore Národnej rady Slovenskej republiky.
- Podanie materiálu na rokovanie Národnej rady Slovenskej republiky.
- Podanie pozmeňujúceho a doplňujúceho návrhu.
- Podanie otázky do hodiny otázok.
- Podanie interpelácie.

8.1.1.3. Navrhovaná biznis architektúra riešenia

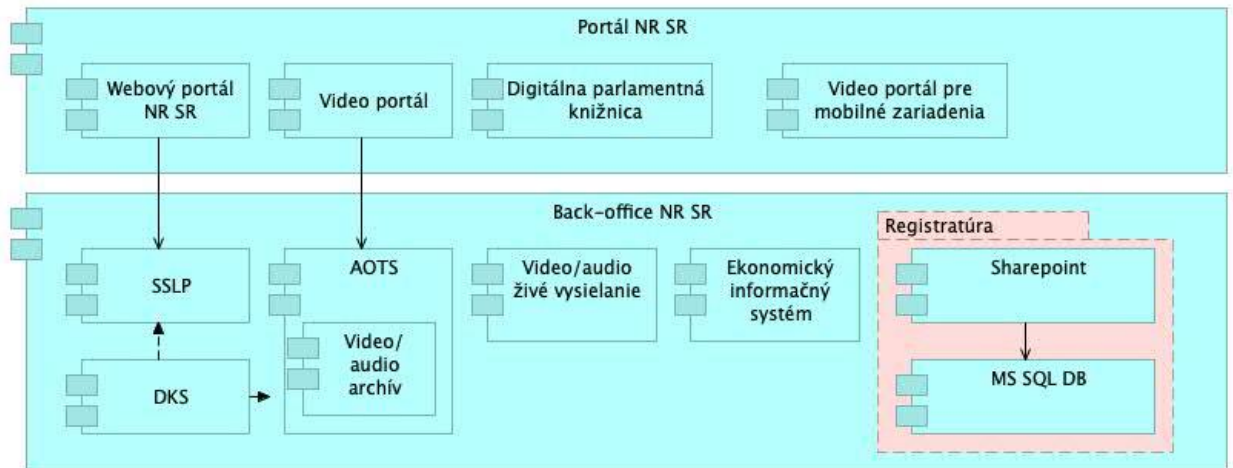
Na nasledujúcej schéme je definovaná biznis architektúra navrhovaného riešenia:



8.2. Aplikačná vrstva

8.2.1. AS IS Aplikačná architektúra

Schéma nižšie zobrazuje high level pohľad na súčasnú aplikačnú architektúru K NR SR so špecifickým zobrazením ISVS SSLP. Ako je vidieť zo schémy, súčasnú aplikačnú architektúru NR SR charakterizuje izolovanosť jednotlivých komponentov a ich vnútorná integrácia a integrácia na potrebné externé ISVS. Uvedené špecificky platí pokiaľ ide o SSLP a v denno-dennej práci zamestnancov NR SR sa prejavuje neefektívnosťou a duplicitným nahrávaním informácií a dokumentov do informačných systémov K NR SR.



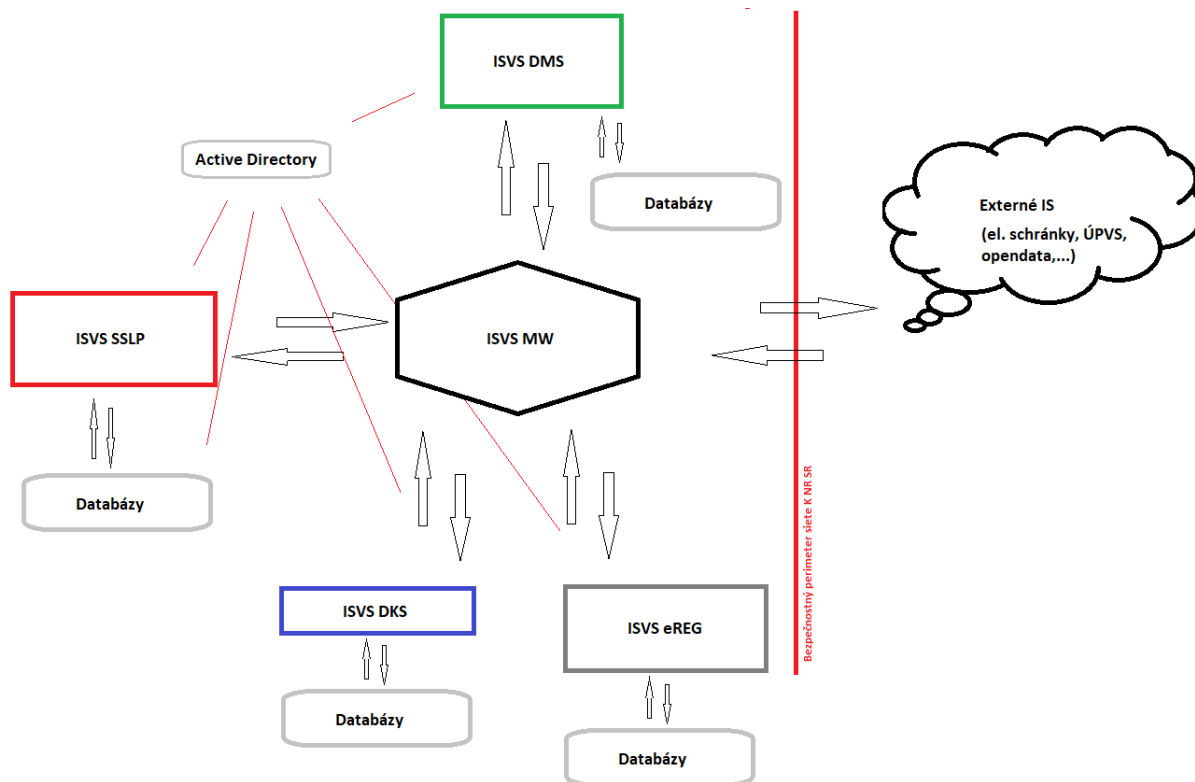
8.2.2. TO BE Aplikačná architektúra a popis vzťahov

ISVS SSLP musí byť integrovaný na Active directory VO vrátane single sign-on a zároveň musí pri implementácii podporovať integráciu na budúce úložisko dát v ISVS DMS prostredníctvom ISVS MW a umožniť integráciu služieb ISVS SSLP tak, aby bola v súlade s platnými štandardmi pre informačné systémy verejnej správy. Ponúknuté riešenie ich musí využívať na integráciu, resp. ukladanie všetkých neštruktúrovaných dát ISVS DMS prostredníctvom integračných služieb vypublikovaných v ISVS MW.

Architektúra cieľového riešenia počíta s implementáciou ISVS SSLP v prostredí s vysokou integráciou s internými IS K NR SR aj externými IS. K NR SR predpokladá vybudovanie integrovanej architektúry IS K NR SR s vysokou mierou výmeny údajov, pričom všetky IS by mali byť schopné v maximálnej možnej miere využívať funkcionality ostatných IS. Cieľom je dosiahnuť aby K NR SR opakovane nenakupovala rovnakú funkcionality ako vie poskytnúť už existujúci informačný systém pričom samotný návrh jednotlivých riešení musí počítať s jednoduchou výmenou jednotlivých IS na konci ich životného cyklu.

K NR SR plánuje nasadenie ISVS MW ktorý zabezpečí optimálnu výmenu údajov medzi IS. Integrované práce na ISVS MW nie sú predmetom projektu, bude ich realizovať systémový integrátor ktorý bude spravovať ISVS MW.

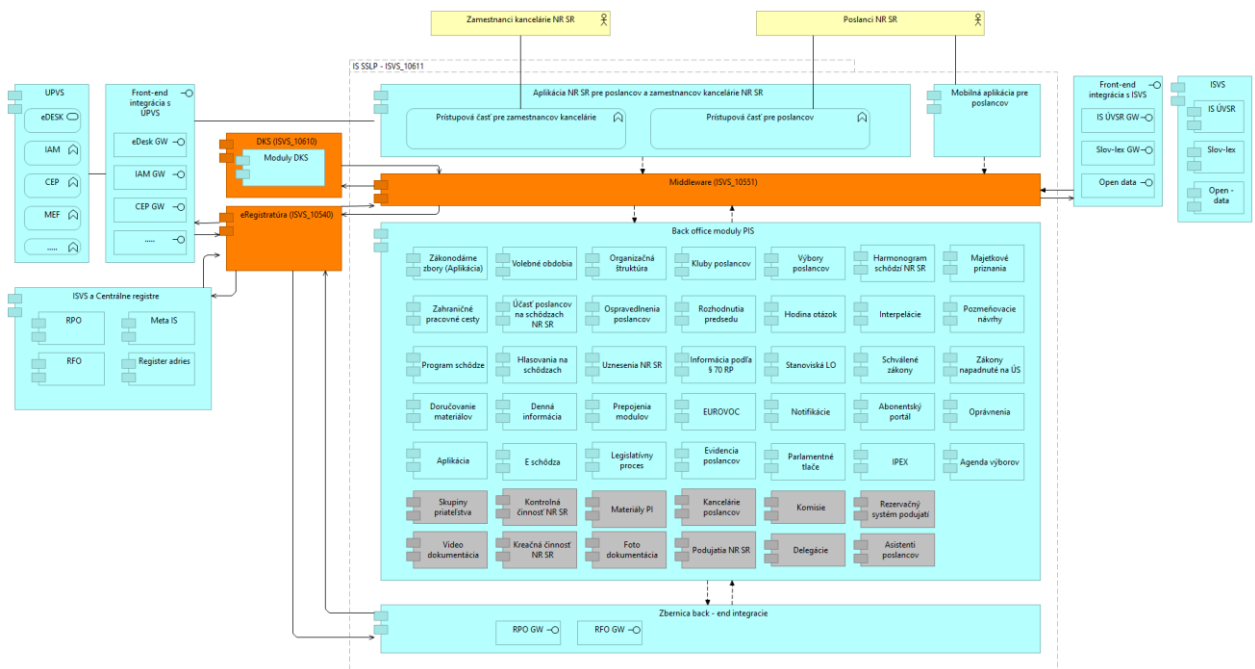
Zároveň plánuje nasadenie ISVS DMS ktorý bude slúžiť ako infraštruktúrna služba na ukladanie neštruktúrovaných súborov s metadátami zo všetkých IS K NR SR. Cieľom je v maximálnej možnej miere zamedziť duplicitám v jednotlivých IS KNRSR.



Obr.: Schéma to be architektúry

ISVS DMS	Document management system je predmetom iného obstarávania. Bude zabezpečovať ukladanie neštruktúrovaných dát pre všetky IS K NR SR. Implementovaný bude ako infraštruktúrna služba s integračným rozhraním.
ISVS DKS	Digitálny konferenčný systém je predmetom iného obstarávania. Bude technicky zabezpečovať chod schôdzí NR SR a zber štruktúrovaných údajov z jej priebehu. Údaje bude následne poskytovať ostatným IS prostredníctvom integračných služieb.
ISVS eREG	Elektronická registratúra je predmetom iného obstarávania.
ISVS MW	ISVS MW je predmetom iného obstarávania. Zabezpečí štandardy, koordináciu a implementácie dátovej výmeny medzi IS K NR SR. Dodávateľ bude zároveň systémovým integrátorom ISVS MW.
Active Directory	Autentizačná a autorizačná služba K NR SR. Autorizácia pre jednotlivé funkcionality ISVS SSLP je v správe ISVS SSLP.
Externé IS (moduly ÚPVS, Slovlex, Centrálny register, Metais, Prepisovací systém)	Externé informačné systémy. Komunikácia výhradne prostredníctvom ISVS MW.

Na nasledujúcej schéme je návrh aplikačnej architektúry riešenia:



Z pohľadu architektúry informačných systémov projekt je navrhnutý tak, aby boli naplnené dva ciele:

- Predseda NR SR, podpredsedovia NR SR a poslanci NR SR budú mať k dispozícii moderný ISVS vďaka, ktorému budú realizované rokovania NR SR a súvisiace procesy.
- Úradník Kancelárie NR SR bude prostredníctvom ISVS schopný plniť úlohy súvisiace so zabezpečením rokovania NR SR.

8.2.2.1. Portál pre poslancov

ISVS (Portál) pre používateľov bude základným komponentom vrstvy front-office a predstavuje centrálné používateľské rozhranie pre poskytovanie elektronických služieb. ISVS bude mať vlastnú architektúru na úrovni Národnej rady SR a bude integrovaný s Ústredným portálom verejnej správy kvôli previazaniu na eGovernment služby centrálnych komponentov a ďalšie základné komponenty ÚPVŠ.

Aby bolo možné integráciu používateľského rozhrania a interoperabilitu komponentov dosiahnuť efektívne, bude zadefinované jednotné aplikačné komunikačné rozhranie (API) pre všetky komponenty webového portálu Národnej rady SR. Veľký dôraz pri ISVS bude daný na celkovú ergonómiu ovládania a navigáciu. Ovládacie prvky Portálu a jeho jednotlivých sekcií budú vhodne navrhnuté, umiestnené a zoskupené do tematických skupín, s dôrazom na ergonómiu, prehľadnosť a jednoduchosť používania.

Komponent front-office bude integrovaný so všetkými ostatnými komponentmi ISVS SSLP a bude slúžiť ako grafické užívateľské prostredie, čiže pomocou neho bude používateľ komunikovať s ostatnými komponentmi. Dodanie portálu nie je predmetom tohto projektu.

8.2.2.2. Portál pre úradníkov (zamestnancov kancelárie NR SR)

Na portáli bude pre úradníkov vytvorený samostatný „site“, kde budú k dispozícii používateľské rozhrania dostupných back-office modulov.

8.2.2.3. Back-office

V rámci back-office každá agenda je riešená prostredníctvom samostatného modulu, každý modul bude riešený samostatnými oddeliteľnými formulármi, aplikačnými funkciami, informačnými zdrojmi ako aj samostatnými zdrojovými kódmi tak, aby umožňovali v budúcnosti ich jednoduchšiu výmenu, resp. rozširovanie tak, aby nebolo do verejnej súťaže potrebné poskytovať celé zdrojové kódy, ale vždy iba

„príslušnú časť kódov“. Tento spôsob v budúcnosti umožní „rozširovanie“ jednotlivých modulov bez viazanosti na pôvodného dodávateľa, ako aj „rozširovanie“ jednotlivých modulov bez straty „záruky na ostatné časti ISVS“. Za týmto účelom sa však požaduje pomerne dôsledné zdokumentovanie jednotlivých častí „zdrojových kódov“, ktorá časť je pre ktorý modul.

Back-office moduly pre jednotlivé agendy sú uvedené v časti 4.1.4 Rozsah projektu.

8.2.3. ISVS MW

Moduly ISVS SSLP sú v rámci komunikácie rozdelené v prílohe č. 4 Rozdelenie modulov projektu z pohľadu komunikácie do farebne odlišených „fiktívnych“ ISVS skupín. Moduly v rámci skupiny môžu komunikovať (poskytovať, resp. využívať dáta iného modulu) priamo (napr. prostredníctvom funkcionality SQL servera).

Moduly medzi skupinami musia na vzájomnú komunikáciu vždy využívať integračné služby implementované prostredníctvom ISVS MW.

Každý modul musí poskytovať všetky svoje dáta do ISVS MW, ktorého účelom bude tieto dáta ďalej poskytovať pre rôzne potreby (OPENDATA, webové sídlo, iné informačné systémy). V priebehu vytvorenia DNR/DFŠ budú definované skupiny dát, ktoré musí informačný systém poskytovať (naprieč všetkými jeho modulmi) vo forme integračných služieb a z hľadiska optimalizácie výkonu bude definované, či daná skupina dát bude vytváraná v rámci informačného systému, alebo až v rámci ISVS MW (teda, či štruktúra a obsah integračnej služby bude vytvorený na základe surových dát poskytovaných každým modulom až v ISVS MW, alebo sa daný dataset pre integračnú službu vytvorí už napr. formou SQL View v databáze ISVS SSLP a prostredníctvom integračnej služby ISVS MW bude iba poskytovaná ďalej). Všetky moduly ISVS SSLP, ktoré potrebujú využívať dáta z iného informačného systému musia tieto dáta získavať prostredníctvom integračných služieb ISVS MW. Dodávateľ projektu ISVS SSLP bude musieť spolupracovať pri návrhu a implementácii uvedených integračných služieb a tieto práce musia byť súčasťou cenovej ponuky celého diela.

8.2.3.1. Integrácie

V priebehu vytvorenia DNR/DFŠ budú definované skupiny rozhraní, ktoré musí informačný systém poskytovať vo forme integračných služieb. Všetky ISVS ktoré potrebujú využívať dáta iného informačného systému musia tieto dáta získavať prostredníctvom integračných služieb ISVS MW. Teda rovnako aj ISVS, ktorých dáta sa očakávajú pri spracúvaní v iných informačných systémov musia poskytovať „svoje“ dáta formou integračných služieb ISVS MW.

Integračné práce na ISVS MW zabezpečí systémový integrátor zodpovedný za prevádzku, riadenie zmien a implementačné práce na ISVS MW. Samotná architektúra integrácií musí byť vypracovaná v spolupráci so systémovým integrátorom ISVS MW. Dodávateľ ISVS SSLP bude musieť spolupracovať pri nasadzovaní uvedených integračných služieb a tieto práce musia byť súčasťou cenovej ponuky celého diela.

V prípade ak počas implementácie etapy/ fázy projektu niektorého modulu nebudú k dispozícii integračné služby ISVS MW a/alebo ISVS eREG a/alebo ISVS DMS alebo ISVS DKS, VO preberie Etapu/Fázu projektu resp. modul bez realizovaných integračných služieb a dodávateľ bude povinný dodatočne realizovať implementáciu integračných služieb na dané ISVS po ich nasadení bez dodatočných nákladov pre VO v čo najkratšom možnom termíne. Všetky vytvorené súbory do integrácie s ISVS eReg, alebo ISVS DMS si musí uchovávať interne v rámci daného modulu, resp. ISVS SSLP a po spustení integrácie s ISVS eReg / ISVS DMS musí preniesť všetky súbory do ISVS eReg/ISVS DMS.

Pre integračné rozhrania platia princípy:

- všetko čo je verejné musí byť publikované pre ISVS MW.

- Všetky integračné datasety musia pri poskytovaní údajov poskytnúť aj informáciu:
 - Ak údaje obsahujú osobné údaje, musia obsahovať informáciu o klasifikácii týchto údajov z hľadiska GDPR. Ak neobsahujú osobné údaje musia poskytnúť informáciu o tom že neobsahujú.
 - Ak údaje obsahujú osobné údaje, musí existovať aj integračná služba s rovnakým datasetom ale anonymizovanými osobnými údajmi.
 - Ak údaje obsahujú údaje klasifikované v zmysle zákona o kybernetickej bezpečnosti, musia obsahovať informáciu o ich klasifikácii.
- Pre každý ISVS musia existovať integračné služby:
 - Služba umožňujúca prehľadať všetky uložené osobné údaje minimálne na základe základe uložených osobných údajov, ich klasifikácie, účelu spracovania, doby spracovania.
 - Služba umožňujúca vykonať trvalú anonymizáciu osobných údajov na základe uložených osobných údajov, ich klasifikácie, účelu spracovania, doby spracovania atď..
- Dokumentácia musí obsahovať katalóg integračných služieb.
- Počet špecializovaných integračných rozhraní musí byť minimalizovaný, väčšina služieb bude poskytovaných prostredníctvom univerzálnych synchronných a asynchronných rozhraní.
- Väčšina služieb musí byť realizovaných ako asynchrónne kvôli minimalizácii závislosti integrovaných systémov z hľadiska dostupnosti.
- Pre všetky nastavenia autentizácie a autorizácie v ktorejkoľvek časti isvs musí vždy existovať integračné rozhranie ktoré umožní v plnom rozsahu čítať existujúce role, oprávnenia a používateľov. Zároveň musí existovať integračné rozhranie ktoré umožní nastavovanie rolí, oprávnení a používateľov v plnom rozsahu z externého systému (identity management system).
- Pre všetky logované informácie musia existovať read only integračné rozhrania schopné poskytovať logy v reálnom čase. Teda v čase volania musí druhá strana dostať aktuálne zapísané informácie..

8.2.3.2. Spoločná integračná zbernica ISVS MW

Všetky integrácie na externé systémy budú včlenené do spoločnej integračnej zbernice ISVS MW. Požiadavkou je vhodne nadimenzovať priepustnosť všetkých integračných rozhraní.

Spoločná integračná zbernica bude umožňovať integráciu s nasledovnými externými systémami:

- Centrálné systémy eGovernmentu:
 - Spoločné moduly ÚPVS.
 - MetaIS.
 - IS CSRÚ - Informačný systém centrálnej správy referenčných údajov.
- Centrálné registre – RFO, RPO, RA.
- Agendové ISVS – IS ÚV SR, Slov-lex.

Rovnako bude zabezpečená aj integrácia medzi DKS a SSLP, tak aby DKS mohlo využívať príslušné moduly SSLP, ktoré sú:

- Volebné obdobia.
- Organizačná štruktúra.
- Poslanci.
- Kluby poslancov.
- Hodina otázok.
- Interpelácie.
- Parlamentné tlačé.
- Program schôdze.
- Hlasovania na schôdzach NRSR.

- Uznesenia NRSR.
- Agenda výborov.
- Denná informácia.
- E – schôdza.
- Aplikácia.

8.2.3.3. Integrácia na CSRÚ

Informačný systém centrálnej správy referenčných údajov (CSRÚ) je centrálnou integračnou a orchestračnou platformou, ako taký nie je zdrojom žiadnych údajov. Služby IS CSRÚ nebudú priamo dostupné pre volanie z ISVS SSLP, dostupné budú len konkrétne integračné služby ISVS MW.

8.2.3.4. Centrálné registre

Z pohľadu centrálnych registrov je potrebné zabezpečiť nasledované integrácie:

- Register fyzických osôb - Bude vytvorené integračné rozhranie RFO GW. Prvotné hromadné stotožnenie záznamov o fyzických osobách v RFO so záznamami fyzických osôb evidovaných v IS SSLP (resp. v existujúcich IS NR SR) bude realizované offline dávkou, s využitím služby Hromadné porovnanie údajov. IS RFO poskytuje informácie o zmenách údajov fyzických osôb v registri na základe konceptu záujmových osôb. Pre každú fyzickú osobu je definovaný tzv. odberateľ resp. skupina odberateľov. V prípade zmeny údajov fyzickej osoby v registri je vygenerovaná tzv. zmenová dávka s väzbou na všetkých odberateľov, pre ktorých je FO záujmovou osobou.

IS SSLP bude v dohodnutých časových intervaloch volať elektronickú službu IS RFO Poskytnutie zoznamu JIFO so zmenenými referenčnými údajmi, pomocou ktorej získava údaje záujmových osôb, u ktorých došlo k zmene, resp. oprave údajov. Po spracovaní týchto údajov sa potvrdzuje ich prijatie volaním elektronickej služby IS RFO Potvrdzovanie prijatia zmien.

- Register právnických osôb - Bude vytvorené integračné rozhranie RPO GW. Bude realizovaná Žiadosť o vytvorenie a následný import iniciálnej dávky z RPO. IS SSLP bude preberať pravidelne zmenové dávky z RPO.
- Register adries - Bude vytvorené integračné rozhranie RA GW. Bude realizovaná Žiadosť o vytvorenie a následný import iniciálnej dávky z RA. IS SSLP bude preberať pravidelne zmenové dávky z RA.

8.2.3.5. Agendové ISVS

VO plánuje po vytvorení integračných podmienok na strane agendových systémov Úradu vlády SR vytvoriť Front-end integráciu na agendové systémy Slov-lex a IS ÚV SR. Keďže v súčasnosti nie je vytvorené integračné rozhranie, ktoré by umožňovalo elektronické podanie dokumentu z Slov-lex (napr. podávanie vládnych návrhov zákonov do NR SR) alebo do IS Úradu vlády SR (napr. zasielanie vylosovaných otázok do hodiny otázok ministrom vlády SR), nie je možné definovať spôsob výmeny dokumentov spomenutých ISVS.

Cieľom projektu je však zabezpečiť proces vytvorenia a podania materiálu do Národnej rady SR a odoslania schváleného materiálu do Slov-lex prostredníctvom integračných služieb ISVS Middleware a nie výmena dokumentov medzi ISVS mailovými správami (ako je to doposiaľ). Pokiaľ ide o integráciu na ÚV SR cieľom je zabezpečiť proces spracovania otázky podanej v rámci hodiny otázok, odoslania otázky z Národnej rady SR a prijatia odpovede z IS Úradu vlády SR, ako aj proces spracovania interpelácie, odoslania interpelácie z Národnej rady SR a prijatia odpovede na interpeláciu z IS Úradu vlády SR.

8.2.4. Dátová vrstva

Dátová architektúra IS SSLP bude vychádzať z princípov a požiadaviek na samotný informačný systém z funkčného hľadiska a predpokladá maximalizáciu zdieľania údajových základní dotknutých informačných systémov tak, aby sa zabránilo redundancii dát a rozdielne štruktúrovaným dátam.

Cieľom dátovej centralizácie a konsolidácie je podpora:

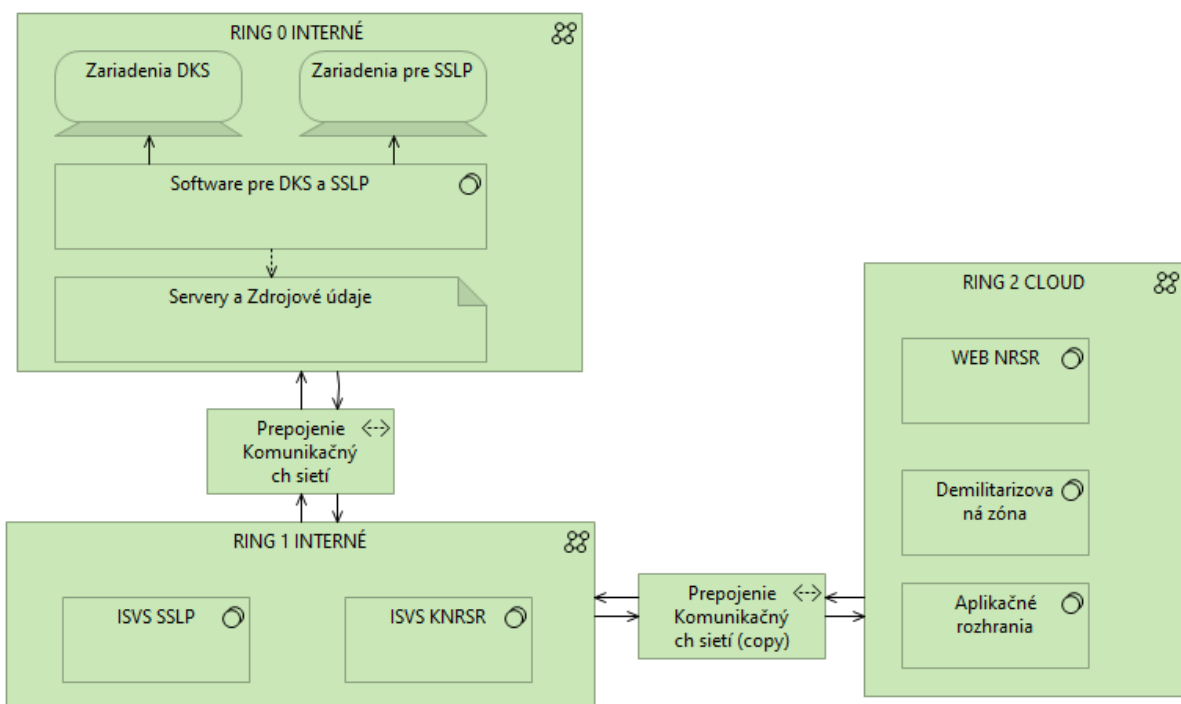
- Vnútornej integrácie IS SSLP a ISVS MW prepájajúcej aplikačné moduly na konsolidovanú integračnú zbernicu.
- Vonkajšej integrácie - prepojenie na referenčné registre verejnej správy (v prípade Národnej rady predovšetkým štandardné číselníky) prostredníctvom ISVS MW.
- Zjednotenia využívania údajovej základne.
- Integrity a komplexnosti údajov; jednoznačnosti a účelnosti využitia dát.
- Ochrany a zabezpečenia dát pred neoprávneným prístupom alebo zneužitím.

8.2.5. Technologická vrstva

Pri návrhu infraštruktúry potrebnej pre prevádzku riešenia sa vychádzalo z analýzy súčasného stavu, rizík spojených s aktuálnym stavom kľúčových komponentov infraštruktúry, definovaných požiadaviek ale aj požiadaviek jednotlivých softvérových (SW) komponentov celého riešenia.

K NRSR disponuje dostatočnými technologickými kapacitami, ktoré budú využité aj v rámci systému SSLP. Zároveň treba podotknúť, že celá technologická infraštruktúra Kancelárie Národnej rady je postavená na troch základných okruhoch, ktoré majú svoje základné špecifiká.

Na nasledujúcej schéme je definovaná technologická architektúra navrhovaného komplexného riešenia, ktoré nezahŕňa len SSLP ale aj DKS, ktoré je naviazané na niektoré moduly SSLP.



Obr.: Schéma to be technologickéj architektúry

V rámci navrhovanej technologickéj architektúry sú nasledovné špecifiká:

- RING 0 – táto sieť musí byť odpojiteľná od ostatných systémov a to z titulu možností realizácie tajných rokovaní NRSR v zmysle rokovacieho poriadku. V tomto prípade sa potrebné údaje

„natiehnuť“ z informačných systémov SSLP a KNRSR na servery do databáz v rámci RING 0 a sieť sa odpojí. Následne po rokovaní sa sieť opätovne prepojí a doplnia sa výsledky rokovania do príslušných systémov a modulov.

- RING 1 – predstavuje sieť pre interné informačné systémy, ktoré aj z pohľadu dôležitosti nie je možné hostovať v cloude, lebo sa jedná o primárnu infraštruktúru na zabezpečenie nevyhnutných úloh štátu.
- RING 2 – predstavuje sieť, kde budú hostované systémy, ktoré môžu byť nasadené v cloude. Jedná sa o prezentačné nástroje ako WEB NRSR a aplikačné rozhrania, ktoré poskytujú služby tretím stranám.

V rámci NRSR prebehla v minulosti obmena HW komponentov, ktoré v súčasnosti vyhovujú moderným riešeniam. Riešenie bude teda postavené ako on premise.

Nasadenie ISVS bude teda v rámci existujúcej infraštruktúry.

- **Platforma** – VO očakáva nasadenie ISVS v rámci svojej existujúcej infraštruktúry. Z tohoto dôvodu musí dodané riešenie podporovať architektúru procesora x86-64 AMD EPYC 7351P a nasadenie v prostredí MS Windows 2019 datacenter Hyper-V cluster a MS Virtual Machine Manager 2019. VO disponuje voľnými licenciami Windows 2019 server. V prípade využívania databázy musí podporovať MS SQL server 2019 cluster (poskytne VO) alebo vlastnú databázu ktorá ale musí byť súčasťou inštalácie produktu a musí byť vysoko dostupná. V prípade využitia vlastnej databázy musí byť súčasťou riešenia aj licencie a kompletná technická podpora na databázu a zálohovanie počas celého životného cyklu ISVS.
- VO požaduje nasadenie do interného prostredia (on premises) a teda nie je prípustné cloudové riešenie. VO preferuje v maximálnej možnej miere využitie investícií v existujúcich informačných technológiách.
- **Škálovateľnosť** – dodané riešenie a jeho licenčný model musí umožňovať škálovateľnosť výkonu v súlade s rastúcimi požiadavkami na systémové zdroje.
- **Vysoká dostupnosť** – komponent ISVS pre produkčné prostredie musí byť nasadený v konfigurácii pre vysokú dostupnosť (hardvér aj softvér). Vysokú dostupnosť na úrovni HW poskytne K NR SR prostredníctvom MS Hyper-V cluster 2019 a MS SQL 2019 cluster. Vysokú dostupnosť SW na aplikačnej úrovni zabezpečí dodávateľ ISVS.
- Dodávateľ poskytne súčinnosť pri návrhu a implementácii výpočtovej a sieťovej infraštruktúry potrebnej k správne chodu ISVS v konfigurácii s vysokou dostupnosťou.
- Dodávateľ realizuje inštaláciu a konfiguráciu ISVS a súvisiacich softvérových súčastí potrebných k správne chodu ISVS na definovanej infraštruktúre.
- Dodávané riešenie musí obsahovať procedúry na zálohovanie a obnovu. VO predpokladá využitie existujúceho riešenia zálohovania MS DPM2019, Disk to Disk to Tape.
- **Autentizácia** – ISVS musí byť integrovaný na Active directory vrátane plného využívania single sign-on a zároveň musí pri implementácii podporovať integráciu na budúce úložisko dát v dokument manažment systéme (ISVS DMS) prostredníctvom ISVS MW a umožniť integráciu služieb ISVS tak, aby bola v súlade s platnými štandardami pre informačné systémy verejnej správy.
- Vzhľadom na existenciu technicky dostatočného technologického riešenia a požadované prevádzkové vlastnosti je nasadenie do cloudového riešenia neprípustné. Preferuje sa v maximálnej možnej miere využitie investícií v existujúcich informačných technológiách.

8.2.6. Bezpečnostná architektúra

Prevádzka riešenia bude realizovaná v rámci vlastnej infraštruktúry, ktorá je kontinuálne aktualizovaná proti najnovším bezpečnostným hrozbám. Súčasťou riešenia je aj viacero bezpečnostných nástrojov zabezpečujúcich zvýšenú ochranu prevádzkovaných systémov. Je využívaná niekoľkoúrovňová

bezpečnostná ochrana a analýza zloženú z produktov (napr. Firewall, IPS, IDS, DDoS, SIEM, NBAD a ďalšie.).

Všetky rozhrania si budú vyžadovať pripojenie pomocou SSL. Zabezpečený bude monitoring sieťových prístupov, bezpečnosti údajov na diskových poliach, logovanie prístupov a zmien, ako aj služba poskytovania bezpečnej prístupovej siete. V rámci samotného IS budú využívané analytické nástroje pre monitorovanie a vyhodnocovanie bezpečnosti. V rámci IKT vybavenia bude zabezpečené nástroje pre ochranu proti škodlivému softvéru. IKT vybavenie v rámci miest podpory bude využívať VPN prepojenie. Pred spustením IS do prevádzky budú v spolupráci s CSIRT.SK realizované penetračné testy.

Povinnosťou bude preukázať súlad so zákonom č. 95/2019 zákona o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Pre úspešnú realizáciu projektu je potrebné zabezpečiť dodržanie pravidiel stanovených Vyhláškou č. 78/2020 (resp. jej novelizácii) Z. z. o štandardoch pre informačné technológie verejnej správy. Z hľadiska ochrany osobných údajov bude dátový manažment realizovaný v súlade so zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Implementácia a prevádzka systému musí v oblasti bezpečnosti brať do úvahy aj zákon 69/2018 Z. z. o kybernetickej bezpečnosti, v znení neskorších predpisov. Bude vypracovaný bezpečnostný projekt rešpektujúci tieto pravidlá.

Dodávateľ sa zaväzuje, že pri dodávke informačného systému zabezpečí vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.

8.2.6.1. Auditné záznamy a logovanie

- Všetky aktivity administrátorov a používateľov musia byť zaznamenávané.
- ISVS musí podporovať parametrizovateľnú tvorbu logov.

Musí byť implementované logovanie a logy sa musia zaznamenávať minimálne v rozsahu (vždy úspešné aj neúspešné):

- a) Prihlásenie a odhlásenie (vrátane zdrojovej IP, mena PC, loginu AD).
- b) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny.
- c) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie).
- d) Pokusy o kritické operácie.

Logy musia byť ukladané v ISVS minimálne 6 mesiacov po skončení záručnej doby ISVS.

8.2.6.2. Bezpečnosť údajov (technické a organizačné zabezpečenie – pre prístup k údajom)

V rámci projektu bude vypracovaný bezpečnostný projekt podľa prílohy č. 3 Vyhlášky č. 179/2020, obsahujúci bezpečnostné opatrenia, minimálne v rozsahu:

- Technické opatrenie realizované prostriedkami fyzickej povahy, zabezpečenie objektu pomocou mechanických zábranných prostriedkov.
- Riadenie prístupu poverených osôb, riadenie prístupov a opatrenia na zaručenie platných politik riadenia prístupov.
- Ochrana pred neoprávneným prístupom, šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia.
- Autentizácia a autorizácia osôb v informačnom systéme.
- Riadenie zraniteľností, opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu; ochrana pred nevyžiadanou elektronickou poštou.
- Sieťová bezpečnosť, kontrola obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.
- Zálohovanie, test funkčnosti záložných dátových nosičov.

- Likvidácia osobných údajov a dátových nosičov, technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov...
- súlad s bezpečnostnými štandardmi, právnymi predpismi.
- Keďže v projekte dôjde k spracovaniu osobných údajov, bude súčasťou aj posudok vplyvu spracovateľských operácií na ochranu osobných údajov (DPIA (Data Protection Impact Assessment) ešte pred začatím spracúvania osobných údajov.

8.2.6.3. Posúdenie vplyvu a dopadu na ochranu osobných údajov (DPIA – data protection impact assesment)

Keďže v projekte dôjde k spracovaniu osobných údajov, bude posúdený vplyv spracovateľských operácií na ochranu osobných údajov (DPIA (Data Protection Impact Assessment) ešte pred začatím spracúvania osobných údajov.

Pričom bude posúdený kontext v zmysle nasledovných právnych predpisov:

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

9. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Vzhľadom k tomu, že K NRSR v súčasnosti plánuje implementáciu alebo rozvoj viacerých ISVS, súvisí nasadenie tohto projektu z nasledovnými projektami:

Stakeholder	Názov projektu	MetaIS kód projektu	Termín spustenia do prevádzky	Popis závislosti
K NRSR	Obstaranie DMS a paušálne služby	Projekt_981	2022/23	System bude využívať nástroje ISVS_10540 prostredníctvom ISVS MW
K NRSR	Vybudovanie informačného systému ISVS MW	Projekt_985	08/2022	Informačný systém predstavuje integračnú platformu, ktorá bude spájať všetky systémy a poskytovať integráciu na externé systémy.
K NRSR	Vybudovanie informačného systému ISVS eREG	Projekt_979	9/2022	Elektronická registratúra

10. ROZSAH DODÁVKY

Komplexný rozsah dodávky je popísaný v katalógu požiadaviek v prílohe č.2.

11. PREPOJENIA, INTEGRÁCIE, MIGRÁCIE A ROZHRAVIA

V tabuľke nižšie sú uvedené oblasti z pohľadu dát, ktoré sú projektom dotknuté:

MetaIS kód ISVS z projektu	Poskyt. Open data	Poskyt. ref. údajov	Konz. ref. údajov	Modul eSchránky	Platobný modul	Modul MED	Modul CEP	Modul MEF	Modul IAM
isvs_10611	X	X	X	X	X	X	X	X	X

V rámci dodávky riešenia v dátovej oblasti bude zohľadnená Vyhláška úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z.z. štandardoch pre informačné technológie verejnej správy: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/78/> a to v nasledujúcich oblastiach:

- Požiadavky na časť "Otvorených údajov":
 - o Poskytovanie údajov.
 - o Konzumovanie údajov – ak sa identifikuje počas fázy Analýza a dizajn.
- Požiadavka na časť "Referenčné údaje":
 - o Poskytovanie údajov – ak sa identifikuje počas fázy Analýza a dizajn.
 - o Konzumovanie údajov – minimálne v rozsahu údajov požadovaných platnou legislatívou.
- Požiadavky pre časť „Spoločné moduly UPVSEXTERNÉ rozhrania.

Externé rozhrania sú definované v prílohách.

11.1. INTERNÉ rozhrania

Všetky dátové zdroje a rozhrania sú súčasťou príloh.

11.2. MIGRÁCIE ÚDAJOV

V rámci implementácie ISVS SSLP je Dodávateľ povinný zabezpečiť migráciu databázových údajov existujúceho riešenia v plnom rozsahu. Detailný popis migračných scenárov a údajov musí byť súčasťou DNR/DFŠ. VO nedisponuje technickou dokumentáciou k existujúcim databázam.

12. PREVÁDZKA A ÚDRŽBA

12.1. Životný cyklus produktu / Doba udržateľnosti projektu

Ukončenie realizácie projektu – projekt sa považuje za ukončený, ak došlo k fyzickému ukončeniu projektu (skutočne sa zrealizovali všetky aktivity projektu) a finančnému ukončeniu projektu (VO uhradil všetky náklady spojené s realizáciou projektu).

Udržateľnosť projektu znamená udržanie (zachovanie) výsledkov realizovaného projektu vrátane dopracovaní v plne funkčnom stave počas životného cyklu ISVS SSLP. Minimálna doba udržateľnosti projektu je 60 mesiacov (5 rokov). Momentom odovzdania diela v zmysle zmluvy o dielo sa začína obdobie udržateľnosti projektu.

Očakávaný životný cyklus ISVS SSLP (čas prevádzky ISVS od spustenia do produkčného prostredia po ukončenie produkčnej prevádzky) produktu je 8 rokov. Z toho 5 rokov bude riadne plnenie a ďalšie 3 roky bude predstavovať opcia na uplatnenie dvojročnej podpory v 6. a 7., a jednoročnej podpory v 8. roku. Po spustení produkčnej prevádzky bude zabezpečené poskytovanie rozšírenej servisnej podpory pre dodávané riešenie na obdobie 8 rokov (ráta sa od začiatku obdobia udržateľnosti v zmysle predchádzajúceho článku).

12.2. Prevádzkové požiadavky

- požadovaná dostupnosť ISVS, RTO, RPO

12.2.1. Požadovaná dostupnosť ISVS

Popis	Parameter	Poznámka
Prevádzkové hodiny	24 hodín	od 00:00 hod. - do 24:00 hod. počas celého roka
Servisné okno	11 hodín	od 16:00 hod. - do 7:00 hod. počas pracovných dní ak neprebíha rokovanie NR SR, alebo nie je posledný deň na podávanie návrhov zákonov. (resp. na doručenie a zverejnenie iných materiálov podľa príslušných právnych predpisov)
	24 hodín	od 00:00 hod. - 24:00 hod. počas dní pracovného pokoja a štátnych sviatkov ak neprebíha rokovanie NR SR Servis a údržba sa musí realizovať výhradne mimo pracovného času a mimo rokovania NR SR (vo výnimočných prípadoch môže VO odsúhlasiť výnimku) .
Dostupnosť produkčného prostredia ISVS	99%	<ul style="list-style-type: none">• 99% z 24/7/365• Maximálny ročný výpadok je 87,6 hodiny.• Vždy sa za takúto dobu považuje čas od 0.00 hod. do 24.00• Nedostupnosť IS sa počíta od nahlásenia incidentu VO v čase dostupnosti podpory Dodávateľa (t.j. nahlásenie incidentu v čase od 0:00 hod. - do 24:00 hod.). Do dostupnosti IS nie sú započítavané schválené servisné zásahy a údržba a plánované odstávky IS.• V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.

Počas rokovania NR SR nie je možné vykonávať bežnú údržbu a servisné zásahy. V prípade mimoriadnej situácie je možné vykonať servisný zásah alebo údržbu aj počas rokovania NR SR avšak iba po predchádzajúcom súhlase VO pre každý jednotlivý prípad. V prípade ak je možné riešiť nahlásený incident iba prostredníctvom servisného zásahu počas rokovania NR SR, VO poskytne súčinnosť.

RTO (Recovery Time Objective) – nastaví Dodávateľ počas implementácie ISVS. Musí zodpovedať požadovanej dostupnosti.

RPO (Recovery Point Objective) – VO požaduje v prípade havárie ISVS nulovú stratu dát

12.3. Účel a predmet podpory

Účelom podpory je zabezpečenie služieb technickej podpory prevádzky, údržby a rozvoja ISVS z dôvodu zabezpečenia jeho riadnej prevádzkyschopnosti a úprav funkcionalít tak, aby mohla byť zabezpečená interoperabilita so všetkými informačnými systémami, s ktorými bude ISVS integrovaný.

Podpora bude Dodávateľom poskytovaná v nasledovnom rozsahu:

- Správa, posudzovanie, riešenie a odstraňovanie Incidentov a problémov v stanovených lehotách, ktoré zahŕňa:
 - o Pravidelnú profylaktiku prostredia a kontrolu funkčnosti ISVS v stanovených lehotách.
 - o Priebežnú identifikáciu abnormálneho správania, t. J. Monitoruje plánované / schedulované procesy pre spracovanie a publikovanie dát, sleduje výkonové parametre, vykonáva pravidelnú kontrolu nastavenia ISVS podľa posledného odsúhlaseného (schváleného) stavu konfigurácie systému.
 - o Priebežné sledovanie, kontrolu a vyhodnocovanie záznamov z logov.
 - o Priebežné sledovanie, vyhodnocovanie upozorňovanie a poskytovanie nových verzií v súvislosti s informačnou bezpečnosťou (bezpečnostné aktualizácie).
 - o Aktívne upozorňovanie VO Dodávateľom na možné zlepšenia a úpravy alebo zmeny IS.
 - o Aktívne upozorňovanie VO Dodávateľom na vzniknuté incidenty, ako aj stavy systému, pri ktorých môže dôjsť, resp. ktoré môžu viesť k vzniku akýchkoľvek Incidentov.
 - o Realizáciu školení v priestoroch VO alebo prostredníctvom videokonferencie v súvislosti so zmenami v systéme súvisiacimi s vyššie uvedeným (v tomto prípade nesmú vzniknúť pre VO žiadne ďalšie náklady).
 - o Aktualizácie komplexnej dokumentácie k ISVS.
 - o Technická a organizačná podpora pri realizácii prevádzkových zásahov (podpora prevádzky ISVS).
- Ďalšie dodávky, činnosti a práce nevyhnutné pre zachovanie funkčnosti a prevádzky schopnosti ISVS, ktoré nie sú výslovne stanovené ako povinnosť Dodávateľa.

(ďalej len „Paušálne služby“).

12.3.1. Paušálne služby a rozvoj diela

Paušálne služby zahŕňajú zabezpečovanie bežnej servisnej podpory prevádzky ISVS, ako aj poskytovanie podpory pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky v súlade s aktuálnymi platnými požiadavkami. Dodávateľ je povinný zabezpečiť:

- Poskytnutie nových verzií so zapracovanými legislatívnymi zmenami.
- Poskytnutie nových verzií s optimalizovanými funkciami.
- Poskytnutie nových verzií s rozšírenou funkcionalitou všeobecného charakteru.

- Poskytnutie nových verzií isvs v dôsledku zmien v informačných technológiách, alebo dôsledku riešenia problémov/incidentov.
- Distribúciu a nasadenie nových verzií isvs sslp v zmysle predchádzajúcich bodov zabezpečuje dodávateľ pričom ich nasadenie do produkčnej prevádzky vrátane termínu nasadenia musí vždy najskôr schváliť vo.
- Upozorňuje na potrebu inštalácie nových verzií a zabezpečí aktualizáciu komponentov softvéru isvs tak, aby nedošlo k výpadkom poskytovaných služieb v čase prevádzky (zabezpečuje dodávateľ, vo zabezpečí súčinnosť).
- Poskytnutie odpovede cez telefónnu linku dostupnú počas prevádzkových hodín na otázky týkajúce sa problémových situácií vzniknutých pri používaní isvs tzn. K obsluhu, k problémovým stavom isvs a k správaniu sa isvs v rozpore s opisom v dokumentácii.
- Správu, posudzovanie, riešenie a odstraňovanie incidentov, problémov a kybernetických bezpečnostných incidentov podľa vyhlášky č. 165/2018 v stanovených lehotách.

Pre tieto potreby bude zabezpečený riadený a kontrolovaný prístup cez VPN pre dodávateľa. Dodávateľ musí plniť interné pravidlá VO pre používanie VPN a požiadavky Zákona o Kybernetickej bezpečnosti v opačnom prípade mu môže byť prístup cez VPN odobraný aj počas trvania zmluvy bez nároku na úpravu finančného plnenia.

Všetky zmeny v ISVS SSLP musia byť zdokumentované a dokumentácia a zdrojové kódy musia byť poskytnuté VO bezpečným spôsobom najneskôr v čase nasadenia zmeny do produkčného prostredia, zároveň sa VO zaväzuje použiť zdrojové kódy, výlučne v prípade, keď nie je za účelom odstránenia Incidentu možné zabezpečiť prítomnosť dodávateľa a na základe preukázateľných inštrukcií dodávateľa. Dodávateľ nenesie zodpovednosť za prípadné vady ISVS SSLP spôsobené zásahom VO alebo akejkoľvek tretej strany, ktoré neboli zo strany Dodávateľa odsúhlasené.

Na vyžiadanie VO je dodávateľ povinný sprístupniť dokumentáciu aktivít zamestnancov dodávateľa a tretích strán najneskôr do 24 hodín od požiadavky.

12.3.1.1. Správa, kategorizácia, riešenie a odstraňovanie incidentov a problémov v stanovených lehotách

Prostredníctvom paušálnych služieb v súlade s účelom a predmetom plnenia zabezpečuje Dodávateľ proces riadenia a riešenia nahlásených Incidentov a Problémov, ktoré majú, resp. môžu mať, vplyv na dostupnosť a kvalitu prevádzky ISVS.

Za incident je považovaná chyba ISVS, t.j. správanie sa v rozpore s dokumentáciou ISVS (ak sa nejedná o chybu v dokumentácii). Za incident nie je považovaná chyba, ktorá nastala mimo prostredia ISVS napr. výpadok poskytovania konkrétnej služby technickej alebo komunikačnej infraštruktúry.

Spôsoby a procesy pre efektívne monitorovanie prevádzky ISVS s cieľom čo najrýchlejšej identifikácie Incidentov a Problémov navrhne Dodávateľ počas realizácie plnenia, pričom musia byť v čo najväčšej miere využité nástroje ktorými disponuje VO.

Pre zefektívnenie procesu odstránenia Incidentov a Problémov musí Dodávateľ využívať nástroje, princípy a praktiky DevOps.

12.3.1.2. Spôsob elektronickej komunikácie pre riešenie Incidentov/Problémov

Nahlasovanie incidentov bude prebiehať:

- Prostredníctvom nástroja, ktorý Dodávateľ zabezpečí pre VO na riadenie incidentov, ktorý bude integrovaný na centrálny tiketovací nástroj VO.

- Dodávateľ zabezpečí možnosť online nahlasovania servisných udalostí s možnosťou sledovania ich stavu riešenia.
- Zabezpečí analýzu požiadavky, identifikáciu a kategorizáciu incidentu/problému.
- Zabezpečí riadenie incidentov a problémov, požadovanú dobu odozvy od nahlásenia , návrh náhradného riešenia a riešenie v požadovanom hraničnom čase.
- Zabezpečí prístup k evidencii nahlásených incidentov, problémov, požiadaviek a reportov.

12.3.1.3. Kategorizácia incidentov a problémov

Naliehavosť incidentu	Popis incidentu
Incident / Problém úrovne A – kritický	Kritická vada / havária, ktorá spôsobuje nedostupnosť, alebo chybnú funkčnosť ISVS alebo jeho časti alebo Incident/Problém môže mať negatívny vplyv na bezpečnosť alebo integritu dát a výsledky ich spracovania v prostredí IS K NR SR. Odstránenie Incidentu/Problému nie je možné dočasne zabezpečiť náhradným riešením Dodávateľa ani organizačným opatrením navrhnutým Dodávateľom.
Incident / Problém úrovne B - vysoký	Vážna vada/ porucha, ktorá spôsobuje nedostupnosť, alebo chybnú funkčnosť ISVS alebo jeho časti alebo Incident/Problém môže mať negatívny vplyv na bezpečnosť alebo integritu dát a výsledky ich spracovania v prostredí IS K NR SR. Odstránenie Incidentu/Problému je možné dočasne zabezpečiť náhradným riešením Dodávateľa alebo organizačným opatrením navrhnutého Dodávateľom, a to v lehote stanovenej pre náhradné riešenie. Odstránenie nesmie mať negatívny vplyv na konzistenciu a integritu dát a výsledky ich spracovania v prostredí IS K NR SR.
Incident / Problém úrovne C – nízky	Bežná vada, bežná porucha, ktorá neobmedzuje prevádzku ISVS alebo jeho časti, nemá dôsledky na využívanie a prevádzku IS a nemá vplyv na bezpečnosť a integritu dát.. Odstránenie Incidentu/Problému nesmie mať negatívny vplyv na bezpečnosť alebo integritu dát a výsledky ich spracovania v prostredí IS K NR SR.
Kybernetický bezpečnostný incident / KB	Ide o incident podľa požiadaviek Vyhlášky č. 165/2018, s klasifikáciou incidentov v súlade s Prílohou č. 1. tejto vyhlášky. Zároveň môže byť kategorizovaný aj ako A, B alebo C.

12.3.1.4. Lehoty na odstraňovanie incidentov a problémov

V nasledujúcej tabuľke sú definované lehoty pre procesy odstraňovania incidentov:

Typ lehoty	Popis lehoty
Okamžité potvrdenie nahlásenia Incidentu/Problému	Znamená že VO môže kedykoľvek prostredníctvom vopred dohodnutých elektronických prostriedkov nahlásiť Dodávateľovi incident/problém a obratom dostane potvrdenie o doručení hlásenia od Dodávateľa.

Lehota reagovania na nahlásený Incident/Problém	Je čas stanovený pre Dodávateľa, do ktorého vykoná prevzatie, potvrdenie prevzatia a preverenie nahláseného Incidentu/Problému, jeho kategorizáciu a zaháji jeho riešenie konkrétnym riešiteľom a ktorý začína plynúť nahlásením Incidentu/Problému postupom podľa nižšie uvedenej Tabuľky.
Lehota náhradného riešenia Incidentu/Problému	Ide sa o čas, do ktorého je Dodávateľ povinný zabezpečiť, resp. uplatniť náhradné riešenie do IS alebo prostredníctvom VO vykonať procesné opatrenia navrhnuté Dodávateľom. Náhradným riešením sa rozumie vykonanie súboru opatrení Dodávateľom, ktoré do doby pre trvalé vyriešenie Incidentu/Problému sfunkčnia IS alebo jeho častí. Pokiaľ sa jedná o procesné opatrenia, Dodávateľ je povinný včas dodať zdokumentovaný proces opatrení tak, aby mohli byť s prihliadnutím na charakter opatrení vykonané Dodávateľom.
Lehota trvalého vyriešenia Incidentu/Problému.	Ide sa o čas, do ktorého je Dodávateľ povinný zabezpečiť, resp. uplatniť trvalé odstránenie Incidentu/Problému ISVS alebo jeho časti tak, aby systém resp. funkčnosť jeho jednotlivých častí, bol plne obnovený.

V nasledujúcich tabuľkách sú uvedené lehoty na odstraňovanie incidentov / porúch:

Odstraňovanie incidentov			Spôľahlivosť	
Úroveň incidentu	Lehota reagovania	Lehota náhradného riešenia	Lehota trvalého vyriešenia	(počet incidentov za mesiac)
Incident úrovne A	Do 30 minút	Neuplatňuje sa	Do 24 hodín	1
Incident úrovne B	Do 30 minút	Do 24 hodín	Do 48 hodín	5
Incident úrovne C	Do 24 hodín pracovného času	Neuplatňuje sa	Do 5 dní pracovného času	Nie je obmedzené

Odstraňovanie problémov			Spôľahlivosť	
Úroveň problému	Lehota reagovania	Lehota náhradného riešenia	Lehota trvalého vyriešenia	(počet problémov za mesiac)
Problém úrovne A	Do 30 minút	Neuplatňuje sa	Do 24 hodín	1
Problém úrovne B	Do 30 minút	Do 24 hodín	Do 48 hodín	5
Problém úrovne C	Do 24 hodín pracovného času	Neuplatňuje sa	Do 21 dní pracovného času	Nie je obmedzené

Počítanie lehôt na odstraňovanie Incidentov/Problémov v rámci pracovného času sa uplatňuje výlučne pri Incidentoch/Problémoch úrovne C. Lehoty na odstraňovanie Incidentov/Problémov úrovne A a Incidentov/Problémov úrovne B plynú bez ohľadu na pracovný čas bez prerušenia (nonstop v režime 24/7).

Spôľahlivosť udáva maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné

alebo technicky súvisiace incidenty sú považované za jeden problém (ak vznikli v rovnakom časovom úseku).

12.3.1.5. Zmluvné pokuty k paušálnym službám

Verejný obstarávateľ má právo požadovať zaplatenie nasledovných zmluvných pokút pri omeškaní s plnením paušálnych služieb nasledovne:

- a) Pri nedodržaní časového limitu na odstránenie incidentu/problému úrovne A: 2000 eur.
- b) Pri nedodržaní časového limitu na odstránenie incidentu/problému úrovne B: 1000 eur.
- c) Pri nedodržaní časového limitu na odstránenie incidentu/problému úrovne C: 500 eur.

a to za každé jednotlivé porušenie a za každý, aj začatý deň omeškania, až do splnenia záväzku, pričom zmluvná pokuta môže byť uložená aj opakovane za každé jednotlivé porušenie.

12.3.1.6. Základné činnosti poskytované v rámci služieb

V nasledujúcej tabuľke sú popísané základné činnosti poskytované v rámci paušálnych služieb / rozvoj diela:

Činnosť	Výstup
Klasifikácia	<ul style="list-style-type: none"> - odsúhlasenie klasifikácie služby (Incident/Problém), resp. návrh na preklasifikovanie služby - odsúhlasenie kategórie úrovne Incidentu/Problému, resp. návrh na preklasifikovanie kategórie
Analýza – preskúmanie, diagnostika a návrh riešenia	<ul style="list-style-type: none"> - návrh náhradného riešenia (úroveň B) a/alebo trvalého vyriešenia (úrovne A, B, C, KBI) s analýzou dopadov (kvalifikovaný odhad termínov) - dodanie úspešných výsledkov testov k navrhovaným riešeniam, security review v zmysle metodiky SDL a potrebnej dokumentácie - požiadavka na potrebu zásahu prostredníctvom vzdialeného prístupu Dodávateľa do IS - rozsah požadovanej súčinnosti
Vyriešenie Incidentu/Problému, resp. dočasná obnova prevádzky ISVS (jeho časti)	<ul style="list-style-type: none"> - dodanie a kontrola releasu (Fix, HotFix..) - nasadenie releasu - funkčný test a security review - obnova, resp. dočasná obnova prevádzky - trvalé vyriešenie Incidentu/Problému (úrovne A, B, C) alebo náhradné riešenie Incidentu/Problému (úroveň B)

V prípade, ak sa zistí, že Incident/Problém stále trvá, tak táto požiadavka na službu zo strany VO bude klasifikovaná ako nevyriešená. Čas nahlásenia požiadavky na službu ostáva pôvodný a všetky časové termíny sa pripočítajú k času od doručenia oznámenia o trvaní Incidentu/Problému.

Realizácia školení, úprava dokumentácie a vytváranie zmenových príručiek:

- V prípade mimoriadnej opodstatnenej potreby priamo súvisiacej s riešením konkrétneho Incidentu/Problému Dodávateľ zabezpečí vyškolenie oprávnených zamestnancov na nové funkcionality v rámci vyriešenia Incidentu/Problému v adekvátnom časovom termíne. V tomto prípade sa osobitná odmena za školenie neposkytuje, je súčasťou ceny za Paušálne služby.
- Ak pri odstraňovaní Incidentu alebo Problému dôjde ku modifikácii postupov správy, inštalácie alebo používania akejkoľvek časti funkcionality ISVS, Dodávateľ spolu s dodaním riešenia je povinný zabezpečiť pri odovzdávaní riešenia aj dodanie aktualizovanej administrátorskej a

prevádzkovej dokumentácie so zaznamenaním vykonaných zmien. Rovnako je povinný Dodávateľ udržiavať aktuálnu a poskytnúť VO komplexnú aktualizovanú dokumentáciu.

- Dokumentácia k jednotlivým plneniam sa odovzdáva priebežne do centrálneho repozitára dokumentácie určeného VO.
- V prípade ak dôjde k pri riešení požiadavky alebo incidentu k životnej situácii alebo postupov k nej pre jednotlivé role ktorá nie je uvedená v používateľskej príručke, vždy musí byť doplnená.
- Dodávateľ nahrá video zo školenia a záznam poskytne VO s právami na použitie výlučne pre potreby VO za účelom školenia zamestnancov.

12.3.2. Vykonanie pravidelnej profylaktiky na týždennej báze

Prostredníctvom tejto podpornej činnosti zabezpečuje Dodávateľ pravidelnú profylaktiku prostredím ISVS na týždennej báze. Ďalej vykonáva sledovanie logov jednotlivých komponentov, identifikuje abnormálne správanie, monitoruje plánované / schedulované procesy pre spracovanie a publikovanie dát, sleduje výkonové parametre, identifikuje Incidenty a Problémy. Spôsoby a procesy pre efektívne monitorovanie prevádzky s cieľom čo najrýchlejšej identifikácie Incidentov a Problémov navrhne Dodávateľ počas poskytovania služby, pričom musia byť v čo najväčšej miere využité interné nástroje VO.

Rozsah profylaktických činností a postupov pre jej vykonanie je určený v prevádzkovej dokumentácii k ISVS.

12.3.2.1. Report k poskytovaným službám

Dodávateľ je povinný pravidelne dodať k poslednému dňu kalendárneho mesiaca prostredníctvom nástroja na riadenie incidentov štrukturovaný report k poskytovaným službám:

Minimálne obsahové náležitosti reportu pre službu riešenia Incidentov/Problémov:

- Zoznam všetkých Incidentov/Problémov za uplynulé obdobie s minimálnym rozsahom:
 - o Na prvej strane musí byť súhrn s výrazne vyznačeným počtom prekročení lehôt plnení.
 - o Jednoznačný identifikátor Incidentu/Problému.
 - o Názov Incidentu/ Problému.
 - o Dátum a čas nahlásenia.
 - o Zoznam riešiteľov.
 - o Skutočné lehoty jednotlivých plnení pre všetky typy lehôt s výrazným vyznačením prekročenia lehôt.
 - o Zoznam nových nasadených verzií modulov s referenciou na incident alebo problém.

Minimálne obsahové náležitosti reportu pre službu riešenia Kybernetických bezpečnostných incidentov (v zmysle požiadaviek Vyhlášky č. 165/2018, par. 2):

- Jednoznačný identifikátor Incidentu.
- Názov Incidentu.
- Kontaktné údaje osoby ktorá incident nahlásila.
- Skutočné lehoty jednotlivých plnení.
- Časové údaje priebehu kybernetického bezpečnostného incidentu.
- Detailný opis priebehu kybernetického bezpečnostného incidentu.
- Prijaté opatrenia s termínmi.

Minimálne obsahové náležitosti reportu pre službu profylaktiky:

- Zoznam dokumentov z profylaktických činností s označením jedinečnej verzie.
- Obdobie, na ktoré sa vzťahuje výkon z profylaktickej činností.
- Autor dokumentu za Dodávateľa.

- Dátum akceptácie jednotlivých dokumentov.
- Vlastník dokumentu za vo, ktorý akceptoval príslušný dokument.
- Výstup: ako podklad pre zostavenie reportu z profylaktickej činnosti môže byť jeden alebo viac dokumentov. Výstup obsahuje minimálne tieto náležitosti:
 1. Osoby, ktoré vykonali profylaktiku.
 2. Kedy bola vykonaná profylaktika.
 3. Časové obdobie, na ktoré sa vzťahuje výkon profylaktiky.
 4. Zoznam kontrolovaných častí isv vo forme checklistu, ktorý obsahuje minimálne:
 - a) Názov kontrolovanej časti isvs s identifikáciou prostredia VO.
 - b) Identifikátor prevádzkového postupu z prevádzkovej dokumentácie (profylaktikou sa môže doplniť/upresniť prevádzkový postup, pokiaľ je zistený nesúlad) .
 - c) Forma vykonania činnosti (napr. Test/overenie prevádzkového postupu/vizuálna kontrola/...) .
 - d) Zistený stav – je skutočný stav zameraný/zistený a dostatočne popísaný kontrolovanej časti isvs počas vykonania profylaktiky.
 - e) Limitná hodnota – je maximálna prípustná hodnota/opísaný stav kontrolovanej časti správania sa isvs, ktorá/ý umožňuje správnu prevádzku systému. Limitné hodnoty sú súčasťou prevádzkovej dokumentácie (profylaktikou sa môžu doplniť/upresniť) .
 - f) Prekročené alebo kritické limitné stavy/správanie sa isvs budú farebne odlišené.
 - g) Označenie, či je alebo nie je vyhodnotený stav správanie sa časti isvs za kritické .
 - h) Odkaz na zdroj (podklad pre vykonanie profylaktiky, napr. Logy, výpis chybových hlásení z databázy, schedulované procesy, zdroj pre zmerané výkonnostné parametre).
 - i) Sumarizáciu kontrolovanej časti isvs, ktorý obsahuje najmä:
 - Upozornenia na možné zlepšenia a úpravy alebo zmeny is, zoznam zaevidovaných incidentov do nástroja na riadenie incidentov dodávateľa vzniknutých počas výkonu profylaktiky.
 - Identifikované abnormálne stavy alebo správanie sa častí isvs, pri ktorých môže dôjsť, resp. ktoré môžu viesť k vzniku akýchkoľvek incidentov alebo bezpečnostných incidentov..
 - Zoznam identifikátorov tých prevádzkových postupov z prevádzkovej dokumentácie, ktorých sa dotkla zmena počas výkonu profylaktiky zoznam doplnených nových prevádzkových postupov s identifikátorom ktoré boli doplnené počas výkonu profylaktiky

12.4. Systém podpory používateľov

Help Desk pre používateľov bude realizovaný cez 3 úrovne podpory, s nasledujúcim označením:

- L1 podpory ISVS (Level 1, priamy kontakt používateľa) - jednotný kontaktný bod VO – IS Service desk K NR SR, ktorý je v správe VO a v prípade jeho nedostupnosti Centrum podpory používateľov (zabezpečuje dodávateľ ISVS).
- L2 podpory ISVS (Level 2, postúpenie požiadaviek od L1) - vybraná skupina garantov, so znalosťou ISVS (zabezpečuje prevádzkovateľ ISVS – VO).
- L3 podpory ISVS (Level 3, postúpenie požiadaviek od L2) – poskytuje dodávateľ.

Podpora L1 (podpora 1. stupňa)	začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek
--------------------------------	---

	koncových užívateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou funkciou podpory 1. stupňa je zhromaždiť informácie, previesť základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v úrovni L1 riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné atď.) a základné užívateľské problémy (typicky zabudnutie hesla), overovanie nastavení SW a HW atď.
Podpora L2 (podpora 2. stupňa)	riešiteľské tímy s hlbšou technologickou alebo funkčnou znalosťou ISVS. Riešitelia na úrovni Podpory L2 sú zodpovední za poskytovanie súčinnosti riešiteľom 1. úrovne podpory pri riešení eskalovaného hlásenia, čo mimo iného obsahuje aj spätnú kontrolu a podrobnejšiu analýzu zistených dát predaných riešiteľom 1. úrovne podpory. Výstupom takejto kontroly môže byť potvrdenie, upresnenie, alebo prehodnotenie hlásenia v závislosti na potrebách VO. Primárnym cieľom riešiteľov na úrovni Podpory L2 je dostať incident alebo požiadavku čo najskôr pod kontrolu a následne ho vyriešiť alebo eskalovať na vyššiu úroveň podpory.
Podpora L3 (podpora 3. stupňa)	predstavuje najvyššiu úroveň podpory pre riešenie tých incidentov a požiadaviek ktoré nie je schopná vyriešiť podpora na úrovni L1 a L2, vrátane prevádzania hĺbkových analýz a riešenia extrémnych prípadov.

- Všetky požiadavky a incidenty musia byť evidované v ISVS service desk VO.
- Centrum podpory používateľov je dostupný pre vybrané skupiny používateľov cez telefón a email pričom nahlásené incidenty aj požiadavky vrátane ich aktualizácii musia byť vždy evidované aj v service desku VO.
- Dostupnosť L3 podpory pre ISVS je 12x5 (12 hodín x 5 dní od 7:00h do 19:00h počas pracovných dní).
- Service desk dodávateľa je dostupný pre nahlasovanie incidentov 24/7/365.

12.5. Popis Objednávkových služieb a špecifikácia spôsobu plnenia

Prostredníctvom Objednávkových služieb zabezpečuje Dodávateľ na základe požiadaviek VO na rozvoj ISVS prostredníctvom zmien (ďalej aj len „**Požiadavka na zmenu**“). Predmetom objednávkových služieb môžu byť práce na úprave alebo rozvoji dodaného produktu, vrátane úpravy existujúcich integračných služieb a dopracovania integračných služieb ktoré neboli predmetom prvotnej dodávky.

Spôsob elektronickej komunikácie

Prostredníctvom nástroja, ktorý VO používa na riadenie Požiadaviek na zmenu.

Nižšie uvedený zoznam činností si vyhradzuje VO upraviť podľa nastavených procesov prostredníctvom nástroja na riadenie Požiadaviek na zmenu, ktoré sú prispôsobované k efektívnemu riadeniu procesov podľa potrieb VO.

Zoznam činností:

1) Posúdenie špecifikácie a kategorizácie Požiadaviek na zmenu

- a) Na špecifikáciu a kategorizáciu Požiadaviek na zmenu je používaný jednotný formulár, prostredníctvom ktorého VO špecifikuje rozsah zmien v ISVS.
- b) Na základe VO vyplneného a doručeného formulára pre Objednávkové služby Dodávateľ potvrdí VO oboznámenie sa s požiadavkami a navrhne časový harmonogram pre vypracovanie činnosti č. 2) Vypracovanie Analýzy dopadov (vrátane posúdenia vplyvu na bezpečnosť) a cenovej ponuky. Dodávateľ má právo požiadať VO o doplnenie informácií slúžiacich k úplnému porozumeniu Požiadaviek na zmenu počas lehoty stanovenej pre činnosť č. 1. Lehota pre činnosť č. 1 Posúdenie špecifikácie a kategorizácie Požiadaviek na zmenu je 5 pracovných dní.
- c) Predpokladom pre zahájenie činnosti č. 2) je odsúhlasenie činnosti č. 1) VO.

2) Vypracovanie a schválenie Analýzy dopadov a cenovej ponuky

- a) Na základe VO vyplneného a doručeného formulára pre Objednávkové služby Dodávateľ doplní formulár pre Objednávkové služby, ktorý Dodávateľ doručí podľa dohodnutého harmonogramu VO a ktorý bude obsahovať podrobný návrh riešenia, vrátane analýzy dopadov, registra kvality, cenovej ponuky a predpokladaného harmonogramu prác s uvedením navrhovanej doby poskytnutia Objednávkových služieb a plán ich realizácie. Súčasťou plánu realizácie Objednávkových služieb bude špecifikácia akceptačných testov a ostatných požadovaných vyplnení pre Dodávateľa.
- b) Po doručení formulára VO je tento povinný zapísať pripomienky do formulára a doručiť ich v lehote **do 10 pracovných dní** odo dňa doručenia formulára VO alebo v rovnakej lehote schváliť Analýzu dopadov a cenovú ponuku vyplývajúce z doručeného formulára bez výhrad. V prípade márneho uplynutia uvedenej lehoty sa považuje Analýza dopadov a cenová ponuka za schválenú zo strany VO v plnom rozsahu a bez výhrad a slúži ako podklad pre rozhodnutie k objednaniu Objednávkových služieb.
- c) Dodávateľ je povinný **do 10 pracovných dní** pripomienky odborne posúdiť a upraviť Analýzu dopadov a cenovú ponuku v súlade so vnesenými pripomienkami. V prípade, ak nie je možné niektorú z pripomienok VO akceptovať, Dodávateľ túto skutočnosť bezodkladne písomne oznámi VO aj s príslušným odôvodnením, v ktorom náležite preukáže rozpor pripomienky s konkrétnou Požiadavkou na zmenu alebo inú relevantnú skutočnosť, ktorá odôvodňuje nezpracovanie pripomienky VO.
- d) VO je povinný **do 7 pracovných dní** od dodania Analýzy dopadov a cenovej ponuky po zapracovaní pripomienok preveriť spôsob zapracovania pripomienok a schváliť Analýzu dopadov a cenovú ponuku alebo v prípade nesúhlasu v uvedenej lehote zaslať svoje stanovisko Dodávateľovi; v prípade márneho uplynutia uvedenej lehoty sa považuje Analýza dopadov a cenová ponuka za schválenú zo strany VO a slúži ako podklad pre rozhodnutie k objednaniu Objednávkových služieb.
- e) Po schválení Analýzy dopadov a cenovej ponuky predloží Dodávateľ Analýzu dopadov a cenovú ponuku na schválenie VO.
- f) Ak nedôjde k schváleniu Analýzy dopadov a cenovej ponuky postupom podľa tohto bodu činnosti č. 2, o ďalšom postupe záväzne rozhodne VO.

3) Objednanie realizácie Objednávkových služieb

- a) Objednávka realizácie Objednávkových služieb je možná len na základe predchádzajúceho rozhodnutia VO o schválení Analýzy dopadov a cenovej ponuky.
- b) VO je oprávnený doručiť Dodávateľovi písomnú záväznú objednávku najneskôr do 3 mesiacov odo dňa schválenia Analýzy dopadov a cenovej ponuky ak nebude dohodnuté inak.

4) Realizácia Objednávkových služieb

- a) K začatiu realizácie Požiadavky na zmenu dôjde až po zaslaní písomnej objednávky VO.
- b) VO a Dodávateľ určia kontaktné osoby zodpovedné za realizáciu Požiadavky na zmenu.
- c) Dodávateľ navrhne detailný plán realizácie Požiadavky na zmenu s definovaním vlastníkov jednotlivých plnení, vrátane definovania požiadaviek na súčinnosť VO a s návrhom termínov plnení jednotlivých úloh vrátane plánu akceptačných testov. VO schvaľuje detailný plán realizácie.
- d) Dodávateľ pravidelne raz týždenne poskytuje odpočet plnenia realizácie zmeny podľa odsúhlaseného detailného plánu realizácie zmeny VO.

5) Otestovanie zmeny Dodávateľom

- a) Dodávateľ sa zaväzuje otestovať implementovanú zmenu na vlastných vývojových prostriedkoch a vykonať bezpečnostné posúdenie zmeny, vrátane dodania security review podľa SDL metodiky rozsahu v odsúhlasenom VO pred vykonaním záverečných akceptačných testov
- b) Dodávateľ sa zaväzuje dodať výsledky testov a výsledky security review VO.
- c) Dodávateľ sa zaväzuje overiť dodržanie štandardov pre ISVS/ITVS.

6) Akceptácia

- Ak je výsledkom vykonania akceptačných testov zistenie, že produkt alebo jeho časť nespĺňa dohodnutú funkčnosť a tým nenapĺňa účel a cieľ produktu, a to z dôvodov, za ktoré zodpovedá Dodávateľ, produkt má vady. Za vady produktu sa považuje aj nesúlad správania sa produktu voči zadaniu. Na iné skutočnosti namietané VO Dodávateľ nie je povinný prihliadať ak nemajú zásadný vplyv na funkčnosť produktu na akceptáciu.
- Počas testovania je VO oprávnený hlásiť Dodávateľovi Vady vo funkcionalite produktu.
- Po úspešnej realizácii testovacích procedúr Dodávateľ predloží VO akceptačný protokol za účelom akceptácie implementácie produktu.
- V prípade, že sa počas realizácie testovacích procedúr vyskytnú Vady, VO v súčinnosti s Dodávateľom vyhotoví ich súpis s rozdelením v zmysle bodu 7 kapitoly 12.5.
- Dodávateľ navrhne lehoty, v ktorých sa Dodávateľ zaväzuje odstrániť jednotlivé Vady.
- VO schváli akceptačný protokol, obsahujúci stanovisko k akceptácii plnenia. Stanovisko k akceptácii plnenia môže byť vo forme:
 - bez výhrad,
 - akceptované s výhradami
 - neakceptované.
- Úspešné uskutočnenie testovania a potvrdenie akceptačného protokolu nezbavuje Dodávateľa povinnosti odstrániť všetky Vady plnenia v lehote stanovenej v akceptačnom protokole. Dodávateľ zodpovedá za vady produktu v čase jeho odovzdania VO.
- Po odstránení Vady VO písomne potvrdí jej odstránenie.
- Produkt/modul sa vždy považuje za riadne vykonaný a VO prevzatý až ku dňu kedy bol po akceptácii prvý krát spustený do produkčnej prevádzky.

- **Limity vád pre akceptáciu objednávkových služieb:**

V prípade výskytu vady pri akceptácii je Dodávateľ povinný rozlíšiť či sa jedná o incident alebo problém alebo o inú vadu produktu. V prípade ak sa jedná o incident alebo problém je povinný kategorizovať vadu na základe kapitoly 12.

- Incident/problém kategórie A alebo B je kritickou vadou.
- Incident/problém kategórie C je normálnou vadou.

Kategória vady	Popis	Povolený počet defektov na modul
Kritická	<p>Vady s dopadom na základné funkcionality ISVS, ktorý by v prípade výskytu v produkčnom prostredí znemožnil prevádzku ISVS alebo jeho časti, alebo spôsobil chybnú funkčnosť ISVS alebo jeho časti.</p> <p>Vady schopné spôsobiť zastavenie alebo poškodenie Diela alebo iných systémov VO.</p> <p>Vady bezpečnosti produktu.</p> <p>Neschopnosť spracovať bežnú prevádzkovú záťaž.</p> <p>V prípade výskytu sa zastavuje akceptačné testovanie.</p> <p>Iné záručné vady s dopadom na základné funkcionality ISVS, ktorý by v prípade výskytu v produkčnom prostredí znemožnil prevádzku ISVS alebo jeho časti, alebo spôsobil chybnú funkčnosť ISVS alebo jeho časti.</p>	0
Normálna	<p>Vady s nepodstatným dopadom na prevádzku ISVS, ktorý by v prípade výskytu v produkčnom prostredí nespôsobil chybnú funkčnosť ISVS alebo jeho časti. Nemá dopad na testovanie.</p> <p>Iné záručné vady</p>	3

7) Zmenové príručky a dokumentácia

- ak pri realizácii Požiadavky na zmenu dôjde ku modifikácii postupov správy, inštalácie alebo používania akejkoľvek časti funkcionality ISVS, Dodávateľ spolu s dodaním riešenia je povinný zabezpečiť pri odovzdávaní riešenia aj dodanie aktualizovanej dokumentácie so zaznamenaním vykonaných zmien. Rovnako je povinný Dodávateľ udržiavať aktuálnu a poskytnúť VO aktualizovanú komplexnú dokumentáciu (vrátane zdrojových kódov (ak je relevantné), detailných dizajnov, dátového modelu a inej dokumentácie, ktoré sú neodmysliteľnou súčasťou ISVS).
- Dokumentácia k jednotlivým plneniam sa odovzdáva priebežne do centrálného repozitára dokumentácie.

8) Školenie

V prípade mimoriadnej opodstatnenej potreby priamo súvisiacej s riešením konkrétneho Incidentu/Problému Dodávateľ zabezpečí vyškolenie oprávnených zamestnancov VO na nové funkcionality v rámci vyriešenia Incidentu/Problému v adekvátnom časovom termíne. V tomto prípade sa osobitná odmena za školenie neposkytuje, je súčasťou ceny za Paušálne služby.

13. HARMONOGRAM JEDNOTLIVÝCH ETÁP, FÁZ DIEĽA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu v mesiacoch)	KONIEC (odhad termínu v mesiacoch)	POZNÁMKA
1.	Účinnosť zmluvy	T	T	
2.	Analýza a dizajn Etapa I. / Fáza 1	T	T+5	DNR/DFŠ <ul style="list-style-type: none"> • popis súčasného stavu • návrh cieľového stavu • definitívne zloženie informačných zdrojov Musí byť ukončená do konca 5. mesiacov od účinnosti zmluvy
3.	Dodanie HW a licencií Etapa I. / Fáza 2	T	T+5	Musí byť ukončená do konca 5. mesiacov od účinnosti zmluvy
4.	Nasadenie do produktívneho prostredia Etapa II. / Fáza 1 Základné moduly SSLP	T+5	T+8	01. Zákonodarne zbory 02. Volebné obdobia 03. Organizačná štruktúra 04. Poslanci 05. Poslanecké kluby 06. Výbory NR SR 07. Komisie 08. Delegácie 09. Skupiny priateľstva 10. Asistenti poslancov 11. Kancelárie poslancov 39. Oprávnenia Musí byť ukončená do konca 8. mesiacov od účinnosti zmluvy
5.	Nasadenie do produktívneho prostredia Etapa II. / Fáza 2	T+8	T+10	16. Hodina otázok 17. Interpelácie 18. Pozmeňovacie a doplňujúce návrhy

	<p>Moduly potrebné pre Digitálny kongresový systém + SSLP</p>			<p>20. Parlamentné tlačë 22. Program schôdze NR SR 23. Hlasovania na schôdzach NR SR 24. Uznesenia NR SR 35. E-schôdza 12. Zahraničné pracovné cesty 13. Účasť poslancov na schôdzach NR SR 14. Ospravedlnenia poslancov 15. Rozhodnutia predsedu NR SR 26. Stanoviská legislatívneho odboru 27. Schválené zákony 28. Zákony napadnuté na ústavnom súde 29. Legislatívny proces 30. Agenda výborov 19. Doručovanie materiálov 21. Harmonogram schôdzí NR SR</p> <p>Musí byť ukončená do konca 10. mesiacov od účinnosti zmluvy</p>
6.	<p>Nasadenie do produktívneho prostredia Etapa II. / Fáza 3 Prepojenie s ISVS DKS</p>	T+10	T+11	<p>33. Denná informácia - integračné služby pre výmenu dát s ISVS DKS (obojsstranné testovanie)</p> <p>Musí byť ukončená do konca 11. mesiacov od účinnosti zmluvy</p>
7.	<p>Nasadenie do produktívneho prostredia Etapa III. / Fáza 1 Ostatné moduly 1</p>	T+11	T+15	<p>31. Podujatia NR SR 32. Video dokumentácia 34. Fotodokumentácia 37. Notifikácie 38. Evidencia akreditácií 40. Žiadosti o sprístupnenie informácií 41. Rezervačný systém podujatí</p> <p>Musí byť ukončená do konca 15. mesiacov od účinnosti zmluvy</p>

8.	Nasadenie do produktívneho prostredia Etapa III. / Fáza 2 Integračné služby	T+10	T+22	<p>V prípade ak počas implementácie etapy/ fázy projektu niektorého modulu nebudú k dispozícii integračné služby ISVS MW a/alebo ISVS eREG a/alebo ISVS DMS alebo ISVS DKS, VO preberie Etapu/Fázu projektu resp. modul bez realizovaných integračných služieb a dodávateľ bude povinný dodatočne realizovať implementáciu integračných služieb na dané ISVS po ich nasadení bez dodatočných nákladov pre VO v čo najkratšom možnom termíne. Všetky vytvorené súbory do integrácie s ISVS eReg, alebo ISVS DMS si musí uchovávať interne v rámci daného modulu, resp. ISVS SSLP a po spustení integrácie s ISVS eReg / ISVS DMS musí preniesť všetky súbory do ISVS ereg/ISVS DMS.</p> <p>Musí byť ukončená do konca 22. mesiacov od účinnosti zmluvy</p>
9.	Nasadenie do produktívneho prostredia Etapa III. / Fáza 3 Ostatné moduly 2	T+18	T+24	<p>42. Materiály Parlamentného inštitútu 43. Kreačná činnosť NR SR 44. Kontrolná činnosť NR SR 36. Aplikácia 45. Eurovoc 46. SSEZ</p> <p>Musí byť ukončená do konca 24. mesiacov od účinnosti zmluvy</p>
10.	Nasadenie do produktívneho prostredia Fáza opcia Majetkové priznania	Dátum uplatnenia opcie	Dátum uplatnenia opcie + 6	<p>47. Majetkové priznania</p> <p>Musí byť ukončená do konca 6. mesiacov od uplatnenia opcie</p>
11.	Podpora prevádzky (SLA) a objednávky (drobný rozvoj)	T+24	T+84	<p>Jedná sa o 60 mesiacov zabezpečenia prevádzky, údržby a objednávkových služieb s následnou opciou na ďalších 3 rokov (2+1)</p>

14. PRÍLOHY A REFERENCIE

14.1. Príloha č.1 Technické podklady

- Technický popis ISVS SSLP, modulov a workflow

14.2. Príloha č.2 Katalóg požiadaviek

14.3. Príloha č.3 Komunikácia modulov

- Štrukturovaná schéma integračných služieb

14.4. Príloha č.4 Rozdelenie modulov projektu z pohľadu komunikácie

- Grafická schéma komunikácie medzi jednotlivými modulmi ISVS SSLP s príkladmi

14.5. Príloha č.5. Komunikacia modulov ISVS SSLP s ISVS DKS

- Grafická schéma komunikácie medzi ISVS SSLP a ISVS DKS

14.6. Príloha č.6 Záväzná štruktúra rozpočtu

- S ohľadom na plnenie uznesenia vlády Slovenskej republiky a napĺňania cieľov stanovených v materiáli „Informatizácia 2.0 revízia výdavkov“ sú organizácie, na ktoré sa vzťahuje toto metodické usmernenie povinné požadovať od dodávateľa stanovenie rozpočtu zmluvy v minimálnom rozsahu, ktorý je definovaný v prílohe.

14.7. Príloha č.7 Databázy – počet tabuliek a stĺpcov

14.8. Referencia 1: Metais ISVS_10611

<https://metais.vicepremier.gov.sk/detail/ISVS/5b90db39-aa98-4425-af6e-2207be74db9b/cimaster?tab=basicForm>

14.9. Referencia 2: Metais Projekt rozvoja IT projekt_999: Vybudovanie Systému na Sledovanie Legislatívneho Procesu (SSLP)

<https://metais.vicepremier.gov.sk/detail/Projekt/024a2b9a-ff5f-49d1-b679-4be191b086cf/cimaster?tab=basicForm>