

Dohoda o integračnom zámere medzi Národným bezpečnostným úradom a Národným centrom zdravotníckych informácií

Subjekt	Národné centrum zdravotníckych informácií	Subjekt	Národný bezpečnostný úrad
Meno	Mgr. Peter Lukáč, PhD.	Meno	pplk. Ing. Bibiána Magáthová, PhD.
Funkcia	generálny riaditeľ	Funkcia	riaditeľka Technickej sekcie
Dátum	26. 09. 2022	Dátum	22. 09. 2022
Podpis		Podpis	

Projekt:	Integrácia za účelom elektronizácie procesu dočasných pracovných neschopností
Dokument:	DIZ_NCZI_NBU.docx
Verzia:	1.3
Dátum:	19.7.2022
Autor:	Marek Ternény
Vlastník:	Národné centrum zdravotníckych informácií

História dokumentu

Verzia	Dátum verzie	Popis zmien	Vypracoval
0.0	26.8.2021		Marian Bielik
0.1	22.2.2022	Doplnenie a upresnenie (zvýraznené v texte)	Marian Bielik, Jan Čejka
1.0	14.4.2022	Popis rozhrania a príloha	Jan Čejka
1.1	9.5.2022	Popis šifrovania	Jan Čejka
1.2	29.6.2022	Doplnenie definície adresárových štruktúr	Jan Čejka, Roman Rodák
1.3	19.7.2022	Zmena definície adresárových štruktúr, doplnenie spôsobu šifrovania, doplnenie nahlasovania chýb, výpadkov a incidentov	Roman Rodák

Obsah

SKRATKY	5		
1 ÚVODNÉ	6		
1.1 IDENTIFIKÁCIA SUBJEKTOV INTEGRAČNÉHO ZÁMERU	6		
1.2 ZDÔVODNENIE A CIELE INTEGRAČNÉHO ZÁMERU	6		
1.3	ROZPOČET	6	
2 ROZSAH	INTEGRÁCIE	6	
2.1 POPIS PROCESOV SÚVISIACICH S POSKYTNUTÍM ÚDAJOV NZIS PRE IS NBÚ		7	
2.2 ARCHITEKTÚRA RIEŠENIA INTEGRÁCIE NZIS A IS NBÚ		7	
2.3 KOMUNIKÁCIA NCZI VOČI IS NBÚ		8	
2.3.1 Zoznam		rozhraní	8
2.3.2 Popis		rozhrania	8
2.3.3 Riešenie chýb, výpadkov a incidentov			8
2.4		LOGOVANIE	9
2.5		TESTOVANIE	10
2.5.1 Zoznam testovacích prípadov (scenárov)			10
3 KOMUNIKAČNÝ	PLÁN	10	
3.1 POPIS ROLÍ A ZODPOVEDNOSTI		11	
3.2 KOMUNIKAČNÉ PROCESY		12	
4	HARMONOGRAM	12	
4.1 NEVYHNUTNÉ		PODMIENKY	13
4.2 EXTERNÉ		ZÁVISLOSTI	13

5 MLČANLIVOSŤ A OCHRANA DÔVERNÝCH INFORMÁCIÍ	13
6 ZÁVEREČNÉ USTANOVENIA	13
7 PRÍLOHY	14

Skratky

NCZI	Národné centrum zdravotníckych informácií
NZIS	Národný zdravotnícky informačný systém
ePN	Elektronická práca neschopnosť
PZS	Poskytovateľ zdravotnej starostlivosti
IS PZS	Informačný systém poskytovateľa zdravotnej starostlivosti
DIZ	Dohoda o integračnom zámere (ďalej len „Dohoda“)
DPN	Dočasná práca neschopnosť
SP	Sociálna poisťovňa
NBÚ	Národný bezpečnostný úrad
IS-NBÚ	Informačný systém Národného bezpečnostného úradu
XSD	XML Schema Definition
ETL	extract, transform, load
SFTP	Secure File Transfer Protocol
SZ	Silová zložka
SD	Service desk – nástroj na evidenciu a riešenie problémov s informačnými systémami
VS platiteľa	Identifikátor osoby zaslaný príslušným úradom
VS príjemcu	Určený identifikátor organizácie (kódový identifikátor silovej zložky)
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
ZoITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
ZoOOU	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

1 Úvodné ustanovenia

1.1 Identifikácia subjektov integračného zámeru

Subjektmi Dohody o integračnom zámere sú Národné centrum zdravotníckych informácií a Národný bezpečnostný úrad. Konzumentom riešenia v rámci integrácie bude IS NBÚ, poskytovateľom riešenia bude IS NZIS.

Subjekty Dohody	Rola	Správca (Gestor)	ISVS spadajúce pod Dohodu
	Konzument	Národný bezpečnostný úrad, so sídlom: Budatínska 30, 851 06 Bratislava IČO: 36061701	IS-NBÚ
	Poskytovateľ	Národné centrum zdravotníckych informácií, so sídlom: Lazaretská 26, 811 09 Bratislava IČO: 00165387,	Národný zdravotnícky informačný systém (NZIS)

1.2 Zdôvodnenie a ciele integračného zámeru

Od 1. januára 2018 je v ostrej prevádzke Systém elektronického zdravotníctva, označovaný ako systém NZIS. Potvrdzovanie dočasnej pracovnej neschopnosti (DPN) je často využívaná služba, do ktorej je zapojený PZS, pacient, SP a aj zamestnávateľ. Potvrdzovanie DPN je stále papierová a procesne zložitá služba nielen pre PZS a pacienta, ale aj pre zamestnancov SP (evidencia DPN a spracovanie dávok) a v konečnom dôsledku aj pre zamestnávateľov (otázka preukazovania prekážok v práci a poskytovania náhrady príjmu pri DPN zamestnanca (náhrady príjmu)).

Na základe schváleného vecného návrhu riešenia pristúpila Sociálna poisťovňa k realizácii projektu Elektronická práceneschopnosť (ePN). ePN nahradí v súčasnosti uplatňované listinné potvrdzovanie DPN a následnú komunikáciu medzi PZS, Sociálnou poisťovňou, pacientom (poistencom) a zamestnávateľom, prenesie do online prostredia. Celá komunikácia, resp. výmena údajov bude prebiehať elektronicky. ePN ako ďalšia funkcionálna NZIS umožní centralizáciu a ľahkú dostupnosť údajov o DPN pre všetkých PZS, resp. príslušných zdravotníckych pracovníkov, ktorí ku svojej práci potrebujú údaje o pacientovi.

Cieľom integračného zámeru je vytvorená ePN lekárom v jeho IS PZS a jej premiestnenie do cieľového IS NBÚ.

1.3 Rozpočet

Náklady na integráciu systémov NZIS časť eZdravie a IS NBU sú hradené na každej strane zvlášť zo samostatných rozpočtových položiek projektov oboch subjektov Dohody.

2 Rozsah integrácie

Rozsah kompletnej integrácie NZIS a IS NBÚ je definovaný §6a a §12 ods. 3 písm. x) bod 1. zákona č. 153/2013 Z. z. v znení neskorších predpisov.

V prípade zmeny rozsahu integrácie sa táto Dohoda bude dopĺňať dodatkami.

2.1 Popis procesov súvisiacich s poskytnutím údajov NZIS pre IS NBÚ

Proces posudzovania a potvrdzovania práce(ne)schopnosti bude prebiehať v nasledovných krokoch:

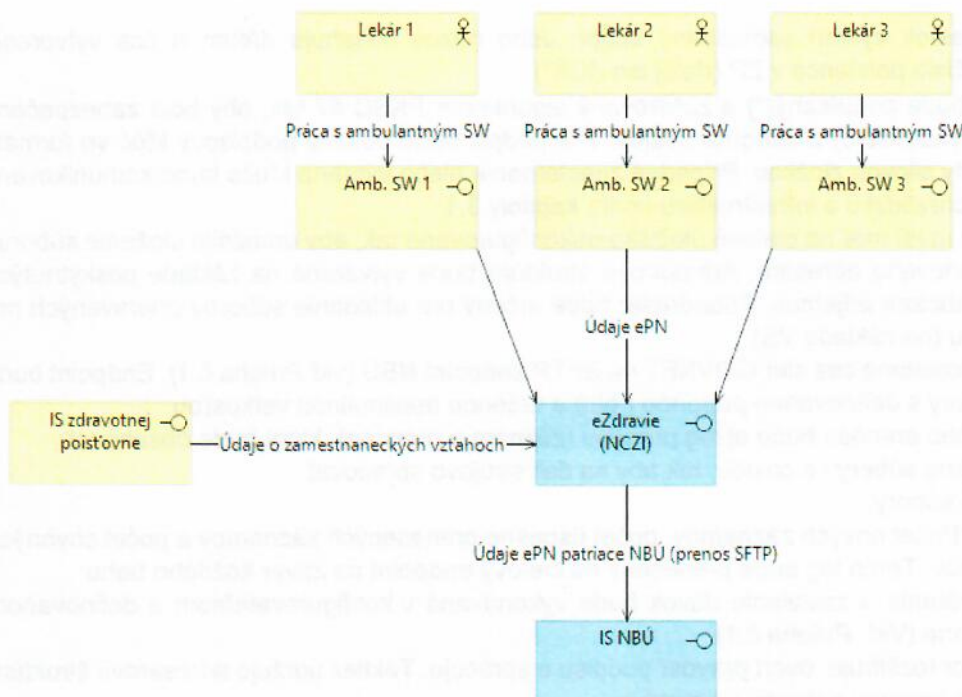
1. Lekári primárne pracujú vo svojich ambulantných/nemocničných systémoch, kde zadávajú novú ePN alebo zadávajú zmeny, doplňujúce alebo upravované údaje na už vystavenej ePN.
Pozn.: Lekár má okrem údajov o fyzickej osobe v prípade poistencov silových rezortov aj informáciu o tom, že sú poistencami silových rezortov, bez bližšej špecifikácie.
2. Tieto údaje o ePN zadané lekárom sú z ambulantných/nemocničných systémov automatizovane zasielané do IS NZIS, kde prechádzajú kontrolami a sú uložené do Registra dočasnej pracovnej neschopnosti.
3. Po vykonaní kontrol, sú dáta odosielané dávkovo, podľa bodu 2.3.2, do NBÚ na definované rozhranie IS NBÚ, šifrovane. Popis šifrovania v prílohe č. 1.

Oprávnený ošetrojúci lekár posudzuje práce(ne)schopnosť pacienta. Zodpovednosť má PZS.

NCZI zabezpečí, aby tento proces umožnil realizovať IS PZS voči eZdraviu.

2.2 Architektúra riešenia integrácie NZIS a IS NBÚ

Na nasledujúcom obrázku je zobrazená architektúra, jednotlivé skupiny používateľov a vzťahy jednotlivých zapojených informačných systémov a aplikácií v riešení funkcionality ePN.



Z pohľadu NBÚ a NCZI ide o nasledujúce hlavné informačné systémy:

1. NZIS – informačný systém na strane NCZI zabezpečujúci zber údajov od lekárov, ich kontrolu a odosielanie do NBÚ, vrátane poskytnutia údajov z registra zamestnávateľských vzťahov lekárom.
2. IS NBÚ – informačný systém na strane NBÚ zabezpečujúci spracovanie neutajovaných informácií z rôznych interných a externých evidencií.

2.3 Komunikácia NCZI voči IS NBÚ

2.3.1 Zoznam rozhraní

V rámci projektu ePN bude pre výmenu údajov medzi informačnými systémami realizované rozhranie na báze prenosu súborov (SFTP), s využitím zabezpečenej siete GOVNET.

Rozhranie pre prenos údajov o ePN z NZIS do IS-NBÚ

- Údaje v rozhraní obsahujú identifikáciu fyzickej osoby, adresy a ďalšie údaje ktorých kombináciou je danú osobu možné jednoznačne identifikovať. Z tohto dôvodu budú tieto údaje v prenose kryptované/šifrované tak, aby ich mohol od kryptovať a spojiť iba cieľový informačný systém.
- Na základe uvedeného je preto aj rozhranie navrhnuté a riešené tak, že časť údajov ktoré prenáša sú šifrované.
- Na strane NZIS bude rozhranie realizované modulom SP_Facade.
- Na strane NBÚ bude rozhranie realizované úložiskom a protokolom SFTP.

2.3.2 Popis rozhrania

Pre SFTP bude v module SP_Facade implementovaný nasledovný ETL mechanizmus:

1. SP_Facade vyhledá všetky prírastky a zmeny ePN, ktoré nemajú poznačený príznak, že boli prenesené do SZ – t. j. za obdobie od posledného generovania súborov pre NBÚ. Pre jednotlivé ePN vygeneruje XML štruktúru, ktorá obsahuje aj všetky dodatočné údaje z ďalších evidencií (JRÚZ).
2. Pre každý prírastok vytvorí samostatný súbor. Jeho názov obsahuje dátum a čas vytvorenia a identifikačné číslo poistenca v ZP (ďalej len „ICK“).
3. Obsah súboru bude podpísaný(*) a zašifrovaný algoritmom PKSC #7 tak, aby bola zabezpečená dôveryhodnosť (autorstvo) a integrita údajov. Pre podpis bude použitý podpisový kľúč vo formáte X.509 poskytnutý silovou zložkou. Prípadné zneplatnenie alebo výmena kľúča bude komunikovaná zástupcami za prevádzku a infraštruktúru podľa kapitoly 3.1
4. Prijemca (NBÚ) musí mať na cieľové úložisko nakonfigurované tak, aby umožnilo uloženie súboru I s cestou z kmeňového adresára. Adresárová štruktúra bude vytváraná na základe poskytnutých variabilným symbolom príjemcu. Podadresár bude určený pre ukladanie súborov pripravených pre daného príjemcu (na základe VS).
5. Súbory budú odosielané cez sieť GOVNET na SFTP endpoint NBÚ (viď Príloha č. 1). Endpoint bude prijímať len súbory s definovanou príponou (.bin) a určenou maximálnou veľkosťou.
6. Súčasťou každého prenosu bude aj log prenosu (záznam o prenose), ktorý bude obsahovať:
 - a. Prenesené súbory i s cestou, tak aby sa dali strojovo spracovať.
 - b. Chybné súbory.
 - c. Sumár: Počet nových záznamov, počet úspešne prenesených záznamov a počet chybných záznamov. Tento log bude prenesený na cieľový endpoint na záver každého behu.
7. Frekvencia vytvárania a zasielanie dávok bude vykonávaná v konfigurovateľnom a definovanom intervale raz denne (Vid'. Príloha č.1).
8. NBÚ prijatý súbor rozšifruje, overí pravosť podpisu a spracuje. Taktiež udržiava adresárovú štruktúru vrátane zálohy a presunu súborov do archívu.

Štruktúra prenášaných dát, názvy súborov a ich zabezpečenie je definované v Prílohe č.1, príloha je neverejnou časťou tohto dokumentu.

2.3.3 Riešenie chýb, výpadkov a incidentov

Pre riešenie chýb a výpadkov je stanovený nasledujúci postup:

Možné chybové stavy v spracovaní:

1. Ak endpoint NBÚ nemá vytvorený alebo dostupný podadresár pre daného adresáta („VS“), a zároveň nie je možné ho vytvoriť, súbor bude uložený do hlavného adresára s doplneným prefixom VS. Informácia bude zalogovaná do výsledného záznamu o prenose
2. Ak vznikne chyba pri podpise alebo šifrovaní záznamu (napr. expirovaná platnosť kľúča), záznam nebude prenesený a chyba bude zapísaná do záznamu o prenose. Systém sa pokúsi o prenos v ďalšom behu.

Príklady chýb/problémov:

1. Nepodarilo sa správu rozšifrovať
2. Chyba pri čítaní dát
3. Chybná štruktúra dát po rozšifrovaní
4. Chyba v číselníkových hodnotách
5. Iné

Postup pri nahlasovaní cez kontaktný formulár:

1. NCZI umožní pracovníkom SZ pre nahlasovanie chýb tohto cez kontaktný formulár na <https://www.ezdravotnictvo.sk/sk/kontaktny-formular>
2. Po odoslaní chyby bude táto zaznamenaná do SD NCZI.
3. Na základe vyhodnotenia hlásenej chyby poverenými pracovníkmi organizácií zvolený postup jej opravy:
 - a. Znovu odoslanie záznamu, v prípade komunikačnej chyby.
 - b. Znovu odoslanie záznamu, po oprave aplikačnej chyby.
 - c. Poskytnutie auditných informácií v požadovanom rozsahu.
 - d. Zápis vyriešenia bezpečnostného incidentu a návrh opatrení k zamedzeniu jeho opakovania.
4. V SD bude vytvorený záznam riešenia hlásenia chyby, o ktorom bude zároveň upovedomený nahlasovateľ prostredníctvom zaslaného e-mailu.

V prípade, že nahlasovateľom chyby/problému je NCZI, alebo je potrebný väčší detail o priebehu riešenia problému pre SZ, alebo prístup k histórii priebehu riešenia pre SZ, je k dispozícii nahlasovanie prostredníctvom nástroja JIRA Service management. NCZI vytvorí kontá v systéme JIRA service management (JIRA SM) pre dohodnutý zoznam pracovníkov SZ. JIRA SM umožní prístup cez webový prehliadač MS Edge, Mozilla Firefox, Google Chrome a Safari. JIRA SM umožní pracovníkom SZ vytváranie nových záznamov (ticketov), zmenu existujúcich ticketov, prehľadávanie existujúcich ticketov. K dispozícii je niekoľko typov ticketov – chyba/incident, návrh na zmenu alebo vylepšenie systému, žiadosť o servisný zásah. Každá zmena ticketu spôsobí vygenerovanie notifikačného e-mailu s popisom zmeny. Tento e-mail obdržia všetci používatelia, ktorí na riešení ticketu participujú (zadávateľ, riešiteľ, sledujúci)

Postup pri nahlasovaní cez JIRA Service management:

1. Používateľ sa prihlási do JIRA SM pomocou mena a hesla.
2. Používateľ zadá nový ticket, ktorý bude následne prenesený do SD NCZI.
3. Na základe vyhodnotenia hlásenej chyby poverenými pracovníkmi organizácií zvolený postup jej opravy rovnako ako v prípade nahlasovania cez kontaktný formulár.
5. Po vyriešení chyby, alebo v prípade potreby doplňujúcich informácií bude v JIRA SM vytvorený záznam o ktorom budú zároveň upovedomení všetci používatelia, ktorí na riešení ticketu participujú.

Chyby logického vyhodnotenia správnosti dát bude NBÚ (ako prijímateľ) riešiť primárne s príslušným lekárom, ako tvorcom záznamu.

V súvislosti s bezpečnostnými incidentami je NBÚ povinný oznámiť všetky skutočnosti, ktoré by mohli zapríčiniť narušenie bezpečnosti rozhrania alebo informačného systému NCZI pre poskytovanie služby NBÚ. V prípade identifikácie incidentu alebo narušenia bezpečnosti súvisiacej s informačnými technológiami používanými pre získavanie údajov z prostredia NCZI, je NBÚ povinný túto skutočnosť neodkladne nahlásiť na kontaktnú adresu (csirt@nczisk.sk) a zabezpečiť súčinnosť pre NCZI v rámci možného riešenia incidentu.

2.4 Logovanie

Na strane NBÚ aj NCZI musí byť implementované logovanie v zmysle zákona č. 95/2019 Z. z.

o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov, pričom logy musia zaznamenávať minimálne nasledovné údaje:

1. čas a dátum udalosti,
2. identifikácia používateľa,
3. identifikácia zariadenia,
4. informácia týkajúca sa udalosti,
5. indikácia úspešnosti, alebo zlyhania operácie,
6. pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port

Logovanie je implementované v rozsahu požiadaviek ZoITVS a ZoKB a ZoOOU.

V prípade vyžiadania NCZI, NBÚ dodá požadované informácie z log súborov z ich časti systému v danom rozsahu najneskôr do 15 dní od výzvy NCZI. NBÚ musí zabezpečiť bezpečné uloženie, riadený prístup k logom a preukázateľnosť ochrany pred neoprávnenou zmenou týchto logov. NBÚ musí zabezpečiť ukladanie log súborov po dobu minimálne 6 mesiacov pre prípad auditu alebo riešenia bezpečnostných incidentov.

V prípade vyžiadania NBÚ, NCZI dodá požadované informácie z log súborov z ich časti systému v danom rozsahu najneskôr do 15 dní od výzvy NBÚ. NCZI musí zabezpečiť bezpečné uloženie, riadený prístup k logom a preukázateľnosť ochrany pred neoprávnenou zmenou týchto logov. NCZI musí zabezpečiť ukladanie log súborov po dobu minimálne 6 mesiacov pre prípad auditu alebo riešenia bezpečnostných incidentov.

2.5 Testovanie

Testovanie riešenia bude realizované v minimálnom rozsahu typov testov:

- **Systémovo-integračné**
 - **Funkcionálne**
 - Integračné - komunikácia medzi systémami cez rozhrania. Integračné testy sieťových prepojení a prístupových bodov. Overenie funkcionality na úrovni vzájomnej komunikácie komponentov.
 - Systémové testy - overenie funkcionality riešenia ako celku. Overenie interakcie viacerých modulov, interakcie systému s operačným systémom, interakciu systému s OS, aplikáciami.
 - **Nefunkcionálne**
 - Výkonnostný test – systém odoláva maximálnemu počtu požiadaviek
 - Test vysokej dostupnosti – systém odoláva hardvérovým výpadkom
 - Bezpečnostný test – ochrana pred neautorizovaným prístupom
- **Používateľské akceptačné testovanie - UAT**
 - Testovanie kompletného biznis procesu za účelom overenia splnenia požiadaviek softvéru

Testy budú realizované v pred finálnej fáze, pred nasadením riešenia do produkcie a následne po odstránení zistených nedostatkov bude vykonaný retest na všetkých uvedených úrovniach. Z dlhodobého hľadiska odporúčame testy zraniteľnosti realizovať 1 x ročne alebo pri každej závažnejšej úprave riešenia, napr. zmena funkcionality alebo zmena na úrovni použitých technológií.

2.5.1 Zoznam testovacích prípadov (scenárov)

Zoznam testovacích scenárov bude vypracovaný po vzájomnom dohovore zúčastnených strán počas prípravy testovacej stratégie.

3 Komunikačný plán

3.1 Popis rolí a zodpovednosti

Cieľom definovania komunikačného plánu je rozdelenie základných zodpovedností, komunikačných línií, eskalácií a údržby dokumentu. Role dodávateľa /konzument/ zahrnuté do rolí Konzumenta.

Rola	Konzument NBÚ	Poskytovateľ NCZI
Projektový manažér	plk. Mgr. Mário Italy mario.italy@nbu.gov.sk	Ing. Jaroslava Demčáková PhD. Jaroslava.Demcakova@nczisk.sk
Hlavný biznis analytik	plk. Mgr. Mário Italy mario.italy@nbu.gov.sk	Ing. Roman Rodák Roman.Rodak@nczisk.sk
Hlavný architekt	plk. Ing. Branislav Šusta branislav.susta@nbu.gov.sk	Ing. Juraj Drusc Juraj.Drusc@nczisk.sk
IT analytik	plk. Ing. Branislav Šusta branislav.susta@nbu.gov.sk	Ing. Marian Bielik Marian.Bielik@nczisk.sk
Test manažér	pplk. Ing. Ivan Urbaník ivan.urbanik@nbu.gov.sk	Adriana Jakľiová Adriana.Jakliova@nczisk.sk
Integračný manažér	plk. Mgr. Mário Italy mario.italy@nbu.gov.sk	Marek Ternény Marek.Terneny@nczisk.sk
Prevádzka a infraštruktúra	pplk. Ing. Ivan Urbaník ivan.urbanik@nbu.gov.sk	Ing. Marian Vilim Marian.Vilim@nczisk.sk

3.2 Komunikačné procesy

Komunikačné procesy prebiehajú na úrovni projektového riadenia a zodpovedných garantov (rolí) na oboch stranách formou pravidelných stretnutí s intervalom 2 týždňov, resp. v závislosti od okolností a stavu úloh. Jednotlivé komunikačné procesy sú zhrnuté v nasledujúcej tabuľke.

Úroveň stretnutí	Komunikačný proces	Výstup
Projektoví manažéri	Návrh integračného zámeru a jeho úprav	Dohoda o integračnom zámere a jeho dodatok
Projektoví manažéri	Eskalácia problémov	Elektronický alebo papierový výstup k eskalácii problému
Projektoví manažéri	Integračné testovanie	Integračný protokol podpísaný projektovými manažermi
Projektoví manažéri	Monitorovanie stavu integračných prác (odporúčaná periodicita raz mesačne)	Zápis zo stretnutia, elektronická alebo papierová statusová informácia
Prevádzka a infraštruktúra	Prepojenie infraštruktúry	Elektronická, alebo papierová statusová informácia o zriadení funkčného prepojenia infraštruktúry
Expertná komunikácia ohľadom biznis modelov	Zorchestrovanie služieb na úrovni biznis modelu	Integračný postup pri testovaní (prípadne úprava dokumentácie zúčastnených strán)
Test manažér	Integračné testovanie	Integračný protokol
Eskalácia na PM	1. stupeň	Zápis

4 Harmonogram

Aktivita	Výstup	Dátum začiatku	Dátum Ukončenia	Zodpovedná osoba
Vypracovanie integračnej a testovacej dokumentácie	Integračný technický návrh (DIZ), Testovací plán	25.7.2022		Projektový manažér,
Nasadenie na testovacie prostredie NCZI		31.8.2022		Projektový manažér, Prevádzka a infraštruktúra
Nasadenie na testovacie prostredie NBÚ		31.8.2022		Projektový manažér, Test manažér
Príprava a vykonanie používateľských akceptačných testov (UAT)	Protokol o ukončení používateľských akceptačných testov (UAT)	2.9..2022	8.9.2022	Projektový manažér, Test manažér
Nasadenie na PROD prostredí NCZI/NBÚ	Akceptačný protokol o zavedení komponentov a integrácie do produkčného prostredia	16.9.2022		Projektový manažér

4.1 Nevyhnutné podmienky

Nevyhnutnými podmienkami integrácie subjektov pre naplnenie Dohody sú:

- dostupné služby prepojenia (SFTP) smerom na NBÚ zo strany NCZI,
- dostupná JIRA SM pre NBÚ na strane NCZI,
- dostupná integračná platforma a back-office systémy na strane NCZI,
- vytvorenie technických prihlasovacích údajov pre údajovú základňu NZIS poskytnutých NBÚ,
- PKI infraštruktúra pre autorizáciu na strane NBÚ,
- dostupná technická špecifikácia poskytovaných služieb NCZI (SFTP, XSD schémy),
- účinná legislatívna úprava.

4.2 Externé závislosti

Rozsah a účinnosť legislatívnej úpravy.

5 Mlčanlivosť a ochrana dôverných informácií

1. Subjekty tejto Dohody sa zaväzujú zachovávať mlčanlivosť o akýchkoľvek informáciách, materiáloch, dokumentácie poskytnutých resp. získaných v súvislosti s touto Dohodou, ako aj s informáciami majúcimi charakter obchodného tajomstva (ďalej len súhrnne „dôverné informácie“) a sú povinné zabezpečiť ich ochranu pred ich vyzradením, únikom, poskytnutím a/alebo sprístupnením tretím osobám.
2. Subjekty tejto Dohody sú oprávnené poskytnúť tretej osobe dôverné informácie len s predchádzajúcim písomným súhlasom druhej strany - subjektu tejto Dohody, okrem prípadov, ak by povinnosť poskytnutia dôverných informácií tretej osobe vyplývala zo zákona alebo z právoplatného rozhodnutia príslušného štátneho orgánu, alebo je informácia poskytnutá odborným poradcom subjektov tejto Dohody, ktorí sú viazaní zákonnou povinnosťou mlčanlivosti (napr. advokáti, daňoví poradcovia, audítori, zmluvná IT spoločnosť), a to v súvislosti s poskytovaním ich služieb dotknutému subjektu tejto Dohody. Ostatné zákonné povinnosti mlčanlivosti ostávajú nedotknuté.
3. V prípade poskytnutia dôvernej informácie tretej osobe v súlade s ich zmluvným vzťahom, je subjekt tejto Dohody, ktorý poskytuje takúto informáciu, povinný zaviazat' tretiu osobu povinnosťou zabezpečiť ochranu dôvernej informácie minimálne v rozsahu a s podmienkami uvedenými v tejto Dohode.
4. Subjekty tejto Dohody sú povinné prijať také technické, personálne a organizačné opatrenia, ktoré zabezpečia primeranú ochranu poskytovaných údajov a zabránia, hoci aj náhodnému zneužitiu, poškodeniu, zničeniu, strate, zmene, alebo nedovolenému prístupu, či sprístupneniu údajov, ako aj akýmkoľvek iným neprípustným formám ich spracúvania v súlade so zákonom o ochrane osobných údajov a nariadenia GDPR.
5. Ochrana osobných údajov podľa tejto Dohody trvá aj po ukončení zmluvného vzťahu založeného touto Dohodou a zaväzuje aj právnych nástupcov účastníkov Dohody. Ukončenie zmluvného vzťahu nemá vplyv na prípadný nárok na náhradu škody, ktorá účastníkovi Dohody vznikla porušením povinností zo strany druhého účastníka Dohody.
6. Subjekty tejto Dohody sú povinné oboznámiť druhú stranu – subjekt tejto Dohody o porušení povinnosti mlčanlivosti bez zbytočného odkladu potom, čo sa o takomto porušení dozvie. Porušujúca strana – subjekt tejto Dohody je povinná bezodkladne vykonať opatrenia na zamedzenie porušovania povinnosti mlčanlivosti.

6 Záverečné ustanovenia

1. Táto Dohoda je vyhotovená v 4 vyhotoveniach, z ktorých dve (2) kópie dostane NBÚ a dve (2) kópie NCZI. Táto Dohoda nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch strán - subjektov Dohody a účinnosť nasledujúci deň po jej zverejnení v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky (ďalej len „register“). Zverejnenie tejto Dohody v registri sa nepovažuje za porušenie mlčanlivosti.

2. Táto Dohoda sa uzatvára na dobu neurčitú.
3. Túto Dohodu je možné meniť a dopĺňať len písomnou dohodou oboch subjektov Dohody vo forme očíslovaných dodatkov.
4. Subjekty tejto Dohody sú povinné si písomne a bezodkladne navzájom oznamovať každú zmenu kontaktných údajov a/alebo kontaktnej osoby uvedených v tejto Dohode, najneskôr do 15 dní odo dňa kedy zmena nastala. Za týmto účelom nie je potrebné vyhotoviť dodatok k tejto Dohode.
5. Oprávnení zástupcovia oboch strán - subjektov tejto Dohody vyhlasujú, že túto dohodu uzavreli slobodne, vážne, určite a zrozumiteľne, nie v tiesni a za nápadne nevýhodných podmienok, rozumejú jej obsahu a na znak súhlasu s jej obsahom ju vlastnoručne podpísali.

7 Prílohy

Príloha č.1 Technická špecifikácia